ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΠΟΛΙΤΙΣΜΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΣ

ΔΙΑΤΡΙΒΗ
για την απόκτηση Διδακτορικού Διπλώματος

Καλλονιάτη Χρήστου

Η ΜΕΘΟΔΟΛΟΓΙΑ PRIS: ΚΑΘΟΡΙΣΜΟΣ ΤΩΝ ΑΠΑΙΤΗΣΕΩΝ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΗ ΦΑΣΗ ΤΗΣ ΣΧΕΔΙΑΣΗΣ ΣΥΣΤΗΜΑΤΩΝ

Συμβουλευτική Επιτροπή:

Επιβλέπουσα:

Ευαγγελία Καβακλή
Επίκουρη Καθηγήτρια
Πανεπιστημίου Αιγαίου

Μέλη:

Γεώργιος Τσεκούρας
Επίκουρος Καθηγητής
Πανεπιστημίου Αιγαίου

Στέφανος Γκρίτζαλης
Αναπληρωτής Καθηγητής
Πανεπιστημίου Αιγαίου

Εξεταστική Επιτροπή:

Πρόεδρος:

Ευαγγελία Καβακλή
Επίκουρη Καθηγήτρια
Πανεπιστημίου Αιγαίου

Μέλη:

Σοφία Δασκαλοπούλου
Καθηγήτρια
Πανεπιστημίου Αιγαίου

Βασίλειος Χρυσικόπουλος
Καθηγητής
Ιονίου Πανεπιστημίου

Νικήτας Νικητάκος
Καθηγητής
Πανεπιστημίου Αιγαίου

Στέφανος Γκρίτζαλης
Αναπληρωτής Καθηγητής
Πανεπιστημίου Αιγαίου

Γεώργιος Τσεκούρας
Επίκουρος Καθηγητής
Πανεπιστημίου Αιγαίου

Κωνσταντίνος Λαμπρινουδάκης
Επίκουρος Καθηγητής
Πανεπιστημίου Αιγαίου

Ευχαριστίες

Η ενότητα αυτή γράφτηκε τελευταία. Πρέπει όμως να διαβαστεί πρώτα από όλα τα κεφάλαια γιατί ανταποκρίνεται σε όλες τις προσπάθειες που χρειάστηκαν για την ολοκλήρωση της διατριβής αυτής.

Νιώθω μεγάλη ευγνωμοσύνη στην επιβλέπουσα καθηγήτριά μου κ. Καβακλή Ευαγγελία για την αμέριστη βοήθεια και εμπιστοσύνη που μου επέδειξε παράλληλα με την επιστημονική επίβλεψη και καθοδήγηση που μου παρείχε. Το συνεχές ενδιαφέρον της και η εύστοχη καθοδήγησή της υπήρξαν ουσιαστικά στοιχεία για την ολοκλήρωση της παρούσας διατριβής. Την ευχαριστώ που μου έδωσε την ευκαιρία να εργαστώ στο εργαστήριο «Πολιτισμικών Πληροφορικών Συστημάτων» μέσα στο οποίο πέρασα τέσσερα δημιουργικά χρόνια. Μέσα από την καρδιά μου ένα μεγάλο ευχαριστώ.

Τον θαυμασμό μου και την ευγνωμοσύνη μου θα ήθελα να εκφράσω επίσης για τον καθηγητή μου κ. Στέφανο Γκρίτζαλη. Η δημιουργική του καθοδήγηση και υποστήριξη όλα αυτά τα χρόνια συνέβαλαν στην υλοποίηση της παρούσας έρευνας. Τον ευχαριστώ για την ερευνητική εμπειρία που μου μετέδωσε. Τον ευχαριστώ που ήταν παρών και με συμβούλευε δίνοντας λύσεις στα ομολογουμένως πολλά προβλήματά που προέκυψαν όλα αυτά τα χρόνια και ερευνητικά αλλά και προσωπικά. Τον ευχαριστώ γιατί στάθηκε δίπλα μου όχι μόνο σαν καθηγητής αλλά και σαν συγγενής.

Την εκτίμηση και το θαυμασμό μου επιθυμώ να εκφράσω για την Πρόεδρο του Τμήματος Πολιτισμικής Τεχνολογίας και Επικοινωνίας Καθηγήτρια κ. Σοφία Δασκαλοπούλου η οποία με συμβούλευε και με καθοδηγούσε πάντα με χαμόγελο και καλή διάθεση. Επίσης την

ευχαριστώ για την τιμή που μου προσέφερε με τη συμμετοχή της στην επταμελή επιτροπή κρίσης της διατριβής μου.

Το μεγάλο μου ευχαριστώ θέλω να εκφράσω στον καθηγητή κ. Τσεκούρα Γεώργιο για τη πολύτιμη βοήθειά του και καθοδήγησή του όλα αυτά τα χρόνια. Δεν θα ξεχάσω ποτέ το ζήλο που επέδειξε στο να μου μεταφέρει τις πολύτιμες γνώσεις του και εμπειρίες του. Πάντα δίπλα μου, σαν αδερφός, δεν σταμάτησε ποτέ να μου δίνει κουράγιο και να με καθοδηγεί με το δικό του μοναδικό τρόπο.

Αξέχαστες θα μου μείνουν οι στιγμές που μοιράστηκα με τους καθηγητές κ. Μαντιμαρούδη Φιλήμονα και κ. Αναγνωστόπουλο Χρήστο. Η προθυμία τους στο να με συμβουλεύουν και να μου μεταδίδουν τις γνώσεις τους όποτε τους το ζητούσα θα τη χαρακτήριζα κάτι παραπάνω από φιλική. Τους ευχαριστώ γιατί παρά το φόρτο εργασίας τους πάντα μου άνοιγαν την πόρτα του γραφείου τους έτοιμοι να με ακούσουν και να με καθοδηγήσουν.

Ένα μεγάλο ευχαριστώ στα μέλη του εργαστηρίου «Πολιτισμικών Πληροφορικών Συστημάτων», και ιδιαίτερα στο Δημήτρη, στη Μαρούσα στη Χαρά και στη Laia που όλο αυτό το διάστημα με την φιλική τους παρουσία συνέβαλαν στην ολοκλήρωση αυτής της διατριβής.

Ευχαριστώ όλους τους φίλους και τις φίλες μου, που με βοήθησαν με τις συμβουλές τους και τη συμπαράστασή τους να ολοκληρώσω την παρούσα διατριβή. Υπήρξαν πολλές στιγμές που η ψυχολογική τους υποστήριξη με βοήθησε να συνεχίσω φτάνοντας σήμερα στο σημείο να γράφω αυτές τις γραμμές. Σε όλους εσάς, ένα μεγάλο ευχαριστώ.

Ευχαριστώ θερμά τον επίκουρο καθηγητή κ. Λαμπρινουδάκη Κωνσταντίνο, τον καθηγητή κ. Νικητάκο Νικήτα και τον καθηγητή κ. Χρυσικόπουλο Βασίλειο για τις εποικοδομητικές τους διορθώσεις και βελτιώσεις στην παρούσα διατριβή καθώς και για την τιμή που μου

προσέφεραν να συμμετάσχουν στην επταμελή επιτροπή κρίσης της διατριβής μου.

Κλείνοντας, θέλω να εκφράσω την αγάπη μου και την ευγνωμοσύνη μου στον πατέρα μου Σπύρο, στη μητέρα μου Ελπινίκη και στον αδερφό μου Θοδωρή. Χωρίς την αγάπη τους, την υποστήριξη τους και τη συμπαράστασή τους δεν θα είχε ολοκληρωθεί ποτέ αυτή η διατριβή. Τους ευχαριστώ που όλα αυτά τα χρόνια των σπουδών μου στάθηκαν στο πλευρό μου στηρίζοντας με ηθικά και υλικά. Τους ευχαριστώ και τους ευγνωμονώ που συμμερίστηκαν την αγωνία αλλά και τις χαρές σε αυτή τη μακρόχρονη και δύσκολη πορεία.

Χ. Σ. Καλλονιάτης

Στους γονείς μου

Περιεχόμενα

Περίληψη

Μία από τις σημαντικότερες προκλήσεις στο χώρο της τεχνολογίας λογισμικού (software engineering) είναι να μπορούν οι χρήστες να εμπιστεύονται το λογισμικό που χρησιμοποιούν καθημερινά, σε επαγγελματικό και προσωπικό επίπεδο. Βασικός παράγοντας που επηρεάζει την εμπιστοσύνη των χρηστών στο λογισμικό είναι η εξασφάλιση της προστασίας της ιδιωτικότητάς τους (privacy).

Οι ερευνητικές περιοχές που ασχολούνται με την προστασία της ιδιωτικότητας κατά την ανάπτυξη πληροφοριακών συστημάτων είναι η τεχνολογία απαιτήσεων (requirements engineering) και η ασφάλεια πληροφοριακών συστημάτων (information systems security). Η μελέτη των δύο αυτών περιοχών υποδεικνύει τα ακόλουθα προβλήματα/ελλείψεις: α) Την έλλειψη μεθοδολογιών που απευθύνονται στην ολοκληρωμένη και αποτελεσματική αντιμετώπιση/ενσωμάτωση των απαιτήσεων της ιδιωτικότητας στη φάση της σχεδίασης συστημάτων, β) Την έλλειψη του τρόπου μετάφρασης των απαιτήσεων ιδιωτικότητας σε τεχνολογικές λύσεις στη φάση της υλοποίησης, γ) Την αδυναμία προσαρμογής του τρόπου υλοποίησης των απαιτήσεων ιδιωτικότητας, από τις αντίστοιχες τεχνολογικές λύσεις, στο περιεχόμενο του υπό ανάπτυξη συστήματος.

Στα πλαίσια της παρούσας διατριβής:

- Διερευνήθηκε η ανάγκη ανάπτυξης μίας μεθοδολογίας που θα απαντά στα προαναφερόμενα ερωτήματα.
- Αποτυπώθηκαν οι βασικές απαιτήσεις που χαρακτηρίζουν την ιδιωτικότητα και που πρέπει να μελετώνται για την πλήρη κάλυψη και υλοποίησή της και αποτυπώθηκαν οι

τεχνολογίες ενίσχυσης της ιδιωτικότητας που υλοποιούν κάθε μία από τις απαιτήσεις αυτές.

- Προτάθηκε μία νέα μεθοδολογία, η μεθοδολογία PriS, για την εύρεση των απαιτήσεων ιδιωτικότητας στη φάση της σχεδίασης συστημάτων και αποτυπώθηκε το εννοιολογικό της πλαίσιο.
- Παρουσιάστηκε ο τρόπος λειτουργίας της προτεινόμενης μεθοδολογίας σε μελέτη περίπτωσης που αφορά σε ένα σύστημα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου.
- Προτάθηκε επίσης μια σειρά από πρότυπα ιδιωτικότητας για την κάθε απαίτηση ιδιωτικότητας, με σκοπό τη σύνδεση των απαιτήσεων με τις διεργασίες που τις υλοποιούν.
- Αναπτύχθηκε ένα φορμαλιστικό μοντέλο της μεθοδολογίας PriS και εφαρμόστηκε στη μελέτη περίπτωσης του συστήματος ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου.

Executive Summary

A major challenge in the field of software engineering today, is to make users trust the software that they use in their every day activities for professional or recreational reasons. Trusting software depends on various elements, one of which is the protection of user privacy.

Two research areas focus on the protection of privacy during system development: software engineering and information systems security. Analysis of current approaches in these areas reveals a number of drawbacks, namely: a) the absence of methodologies that address efficient realisation of privacy requirements during the system design phase b) there is no link between technological solutions and the organisation context of the system into consideration, c) during the implementation phase, privacy enhancing technologies are chosen without paying attention to the context of the system under consideration nor the identified privacy requirements.

In the context of this dissertation:

- Research has been conducted regarding the need for developing a methodology that can answer the above mentioned issues.
- The basic privacy requirements that should be examined for realising privacy as well as the privacy enhancing technologies that implement each of these requirements were defined.
- A new methodology, called PriS, has been proposed for the incorporation of the privacy requirements during the system design phase.
- A case study has been presented for demonstrating the use of the proposed methodology on an e-voting system.

- A number of privacy process patterns have been proposed for the purpose of better relating privacy affected processes with the respective implementation techniques.
- The formal model of PriS has been developed and applied on the e-voting case.

Λίστα Σχημάτων

Λίστα Πινάκων

1. Εισαγωγή

1.1. Οριοθέτηση του Προβλήματος

Η αυξανόμενη διάδοση των σύγχρονων πληροφοριακών συστημάτων αυξάνει την εξάρτηση των χρηστών από αυτά εξαιτίας των ποικίλων σημαντικών παρεχόμενων υπηρεσιών. Παράλληλα, αυξάνει την ανάγκη για ταχεία ανάπτυξη οδηγώντας συχνά στη δημιουργία επισφαλών συστημάτων. Πολλά από τα συστήματα αυτά φιλοξενούνται ή χρησιμοποιούν, κατά ένα σημαντικό βαθμό για την αποτελεσματική λειτουργία τους, το Διαδίκτυο το οποίο, ως ένας σύγχρονος δίαυλος μεταφοράς δεδομένων στον οποίο βασίζεται η σημερινή Κοινωνία της Πληροφορίας, κρύβει πολλούς και σημαντικούς κινδύνους όσον αφορά στην προστασία της ασφάλειας και της ιδιωτικότητας των χρηστών του.

Ολοένα και περισσότερα προσωπικά δεδομένα διανέμονται καθημερινά μέσα από επισφαλή δίκτυα και αποθηκεύονται σε διάφορες βάσεις δεδομένων χωρίς ούτε να λαμβάνονται τα απαραίτητα μέτρα προστασίας των δεδομένων αυτών, αλλά ούτε και να υλοποιούνται οι απαιτούμενες τεχνολογίες ενίσχυσης της προστασίας τους. Στο πλαίσιο αυτό, η ιδιωτικότητα των χρηστών βρίσκεται συχνά σε κίνδυνο.

Πολλές χώρες έχουν αναπτύξει ένα νομοθετικό πλαίσιο με βάση το οποίο καλούνται να συμμορφωθούν όσοι οργανισμοί και επιχειρήσεις που αποθηκεύουν και επεξεργάζονται προσωπικά δεδομένα των χρηστών των συστημάτων τους. Η δημιουργία νομοθετικού πλαισίου και μόνο δεν επιλύει το πρόβλημα της προστασίας της ιδιωτικότητας. Επιπλέον, δεν υπάρχει συνολική εναρμόνιση των νομοθετικών πλαισίων διαφόρων χωρών, εκτός των περιπτώσεων ενιαίων σχηματισμών χωρών.

Παράλληλα, υπάρχει η ανάγκη δημιουργίας μηχανισμών ενσωμάτωσης των νομοθετικών ρυθμίσεων κάθε χώρας στα πληροφοριακά συστήματα που σχεδιάζονται και αναπτύσσονται. Για το λόγο αυτό οι υπεύθυνοι για την προστασία της ιδιωτικότητας έχουν στραφεί στην προστασία της κατά τη φάση της ανάπτυξης των πληροφοριακών συστημάτων, αφού αφενός μεν οι κανόνες που θεσπίζονται στην περιοχή αυτή μπορούν να εφαρμοστούν ανεξάρτητα από πολιτισμικές και κοινωνικές διαφορές μεταξύ χωρών, αφετέρου γιατί η προστασία της ιδιωτικότητας στη διάρκεια της κατασκευής ενός πληροφοριακού συστήματος είναι πιο άμεση και πιο αποτελεσματική. Το γεγονός αυτό εντείνει την ανάγκη μελέτης της ιδιωτικότητας ως βασικό κριτήριο ήδη κατά τη φάση της σχεδίασης, παρά κατά τη φάση της υλοποίησης των πληροφοριακών συστημάτων, όπως υποστηρίζεται και σε πρόσφατες έρευνες (Cannon, J.C. 2004; Kalloniatis, C., Kavakli, E. and Gritzalis, S. 2004).

1.2. Κίνητρα της Παρούσας Έρευνας

Στα σύγχρονα ψηφιακά περιβάλλοντα, κάθε χρήστης πρέπει να παρέχει κάποια δεδομένα με βάση τα οποία αποκτά πρόσβαση στις διάφορες ηλεκτρονικές υπηρεσίες που του προσφέρονται και οι οποίες διευκολύνουν κατά πολύ την προσωπική και επαγγελματική του ζωή. Τα δεδομένα, όμως, αυτά συχνά περιέχουν προσωπικές πληροφορίες για το χρήστη, όπως αριθμό φορολογικού μητρώου, αριθμό πιστωτικής κάρτας, αριθμό ταυτότητας κλπ.

Σχετικές έρευνες (Business, Week 1998; PricewaterhouseCoopers 2001) υποδεικνύουν ότι οι χρήστες των ηλεκτρονικών υπηρεσιών θεωρούν ότι τα δεδομένα τους δεν προστατεύονται επαρκώς και ότι ο κίνδυνος

παραβίασης της ιδιωτικότητάς τους είναι σημαντικός. Συμπεραίνεται λοιπόν ότι η παραβίαση της ιδιωτικότητας αποτελεί ζήτημα άκρως σημαντικό για τους σημερινούς χρήστες υπηρεσιών στον ψηφιακό κόσμο. Επιπλέον, εξίσου σημαντικό ζήτημα που απορρέει από τα παραπάνω είναι το κατά πόσο οι σημερινοί χρήστες εμπιστεύονται τα ίδια τα πληροφοριακά συστήματα που χρησιμοποιούν.

Ένα από τα βασικά κριτήρια που καθορίζουν την εμπιστοσύνη των χρηστών όσον αφορά στη χρήση ενός πληροφοριακού συστήματος είναι ο τρόπος προστασίας της ιδιωτικότητας τους.

Τα προαναφερθέντα ζητήματα, όπως επίσης και το ζήτημα της αντιμετώπισης της ιδιωτικότητας ως ξεχωριστού κριτηρίου ήδη από τη φάση της σχεδίασης και όχι κατά τη φάση της υλοποίησης των πληροφοριακών συστημάτων, αποτελούν τα βασικά κίνητρα της παρούσας διατριβής. Στόχος της παρούσας διατριβής είναι η ανάπτυξη μιας μεθοδολογίας η οποία θα αναγνωρίζει ποιες είναι οι βασικές απαιτήσεις ιδιωτικότητας (privacy requirements) που πρέπει να υλοποιηθούν σε ένα πληροφοριακό σύστημα και με ποια μέθοδο αυτές θα αντιμετωπίζονται στη σχεδίαση του συστήματος, με σκοπό την προστασία της ιδιωτικότητας των χρηστών που θα το χρησιμοποιήσουν.

1.3. Συνεισφορά της παρούσας έρευνας

Η παρούσα διατριβή εισάγει μία νέα μεθοδολογία με σκοπό την ανάλυση της ιδιωτικότητας κατά τη φάση της σχεδίασης πληροφοριακών συστημάτων. Οι ερευνητικές περιοχές στις οποίες αναφέρεται η προτεινόμενη μεθοδολογία είναι: α) η τεχνολογία απαιτήσεων και β) η ασφάλεια πληροφοριακών συστημάτων και συγκεκριμένα η προστασία της ιδιωτικότητας των εμπλεκομένων οντοτήτων.

Δύο είναι τα βασικά ερωτήματα, τα οποία, σε συνδυασμό με τα προαναφερθέντα κίνητρα, οδήγησαν στην εκπόνηση της συγκεκριμένης έρευνας και στην ανάπτυξη της προτεινόμενης μεθοδολογίας:

α) Αν οι υπάρχουσες μεθοδολογίες ανάλυσης απαιτήσεων που προτείνονται συμπεριλαμβάνουν ως κριτήριο την ιδιωτικότητα και κατά πόσο μεθοδεύουν την προστασία της στο υπό-ανάπτυξη σύστημα.

β) Αν οι τεχνολογίες ασφάλειας και προστασίας της ιδιωτικότητας ικανοποιούν τις βασικές της απαιτήσεις, λαμβάνοντας υπόψη το περιεχόμενο του υπό ανάπτυξη συστήματος.

Στο πλαίσιο του πρώτου ερωτήματος, μελετήθηκαν οι μεθοδολογίες ανάλυσης απαιτήσεων και διαπιστώθηκε ότι οι περισσότερες από αυτές δεν αντιμετωπίζουν την ιδιωτικότητα ως ξεχωριστό κριτήριο. Κάποιες από αυτές αντιμετωπίζουν μεν την ιδιωτικότητα ως ξεχωριστό κριτήριο, χωρίς όμως να καθορίζουν τον τρόπο με τον οποίο θα υλοποιηθούν οι απαιτήσεις αυτές κατά τη φάση της σχεδίασης, πάντοτε σε σχέση με το περιεχόμενο και τους στόχους του υπό-ανάπτυξη συστήματος.

Όσον αφορά στο δεύτερο ερώτημα, εντοπίσθηκαν οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (privacy enhancing technologies) που έχουν αναπτυχθεί και η ανάλυση των οποίων οδήγησε στη διαπίστωση ότι οι τεχνολογίες αυτές καλύπτουν η κάθε μια μέρος των απαιτήσεων ιδιωτικότητας χωρίς όμως να λαμβάνουν υπόψη το περιεχόμενο του υπό-ανάπτυξη συστήματος. Καταγράφεται, δηλαδή, αδυναμία σύνδεσης των υπηρεσιών τις οποίες καλείται να παρέχει το σύστημα, όπως αυτές ορίζονται από τη φάση της σχεδίασης και της ανάλυσης των απαιτήσεών του και των τεχνολογιών ενίσχυσης της ιδιωτικότητας.

Με βάση τα παραπάνω ακολουθήθηκαν τα παρακάτω στάδια για την ολοκλήρωση της παρούσας διατριβής.

Πρώτα διερευνήθηκε η ανάγκη ανάπτυξης μίας μεθοδολογίας που θα απαντά στα ερωτήματα που τέθηκαν. Αυτό περιελάμβανε τη μελέτη μεθοδολογιών ανάλυσης απαιτήσεων σχετικών με ζητήματα ασφάλειας και ιδιωτικότητας, καθώς και τον ορισμό ενός συγκριτικού πλαισίου μέσω του οποίου αναδείχθηκαν τα όποια προβλήματα και οι όποιες αδυναμίες των μεθοδολογιών αυτών (Kalloniatis, C., Kavakli, E. and Gritzalis, S. 2004).

Στη συνέχεια αποτυπώθηκαν οι βασικές απαιτήσεις που χαρακτηρίζουν την ιδιωτικότητα και που πρέπει να μελετώνται για την πλήρη κάλυψη και υλοποίησή της και αποτυπώθηκαν οι τεχνολογίες ενίσχυσης της ιδιωτικότητας που υλοποιούν κάθε μία από τις απαιτήσεις αυτές (Kavakli, E., Kalloniatis, C. and Gritzalis, S. 2005).

Το επόμενο βήμα ήταν ο ορισμός μιας νέας μεθοδολογίας, της μεθοδολογίας PriS (Privacy Safeguard) και η αποτύπωση του εννοιολογικού της πλαισίου. Σκοπός της μεθοδολογίας είναι η εύρεση των απαιτήσεων ιδιωτικότητας στη φάση της σχεδίασης συστημάτων (Kalloniatis, C., Kavakli, E. and Gritzalis, S. 2005b).

Έπειτα παρουσιάστηκε ο τρόπος λειτουργίας της προτεινόμενης μεθοδολογίας σε μελέτη περίπτωσης που αφορά στο Γραφείο Διασύνδεσης του Πανεπιστημίου Αιγαίου (Kalloniatis, C., Kavakli, E. and Gritzalis, S. 2005a) καθώς και σε ένα σύστημα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου (Kavakli, E., Kalloniatis, C., Loucopoulos, P. and Gritzalis, S. 2006).

Στη συνέχεια προτάθηκαν μια σειρά από πρότυπα ιδιωτικότητας για κάθε μία απαίτηση ιδιωτικότητας. Σκοπός των προτύπων είναι η ομαλότερη και αποτελεσματικότερη σύνδεση μεταξύ των απαιτήσεων ιδιωτικότητας και των διεργασιών που τις υλοποιούν στο εκάστοτε υπό ανάπτυξη σύστημα (Kalloniatis, C., Kavakli, E. and Gritzalis, S. 2007).

Τέλος, αναπτύχθηκε ένα φορμαλιστικό μοντέλο της μεθοδολογίας PriS και εφαρμόστηκε στη μελέτη περίπτωσης του συστήματος

ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου. Σκοπός του φορμαλιστικού μοντέλου είναι αφενός μεν να αποδειχθεί φορμαλιστικά η λειτουργία της μεθοδολογίας, αφετέρου να καταγραφεί η δυνατότητα περαιτέρω υλοποίησής της σε πρακτικό επίπεδο με τη μορφή εργαλείου λογισμικού (Kavakli, E., Gritzalis, S. and Kalloniatis, C. 2007).

1.4. Δομή της Διατριβής

Η παρούσα διατριβή αποτελείται από οκτώ κεφάλαια.

Στο κεφάλαιο 1 οριοθετείται το πρόβλημα, παρουσιάζονται τα κίνητρα και τα ζητήματα που οδήγησαν στην έναρξη της παρούσας διατριβής, παρουσιάζεται η συνεισφορά της παρούσας διατριβής και περιγράφεται η δομή της.

Στο κεφάλαιο 2 ορίζονται οι έννοιες της ιδιωτικότητας καθώς και οι βασικές απαιτήσεις της.

Στα κεφάλαια 3 και 4 γίνεται μια επισκόπηση των μεθοδολογιών από την περιοχή της τεχνολογίας απαιτήσεων και των τεχνολογιών ενίσχυσης της ιδιωτικότητας αντίστοιχα και συνοψίζονται οι αδυναμίες τους όσον αφορά στα ερωτήματα που προαναφέρθηκαν.

Στο κεφάλαιο 5 παρουσιάζεται η προτεινόμενη μεθοδολογία PriS και εξηγείται ο τρόπος λειτουργίας της.

Στο κεφάλαιο 6 παρουσιάζεται το φορμαλιστικό μοντέλο της προτεινόμενης μεθοδολογίας.

Στο κεφάλαιο 7 περιγράφεται η εφαρμογή της προτεινόμενης μεθοδολογίας και του φορμαλιστικού μοντέλου σε μία μελέτη περίπτωσης ηλεκτρονικού συστήματος ψηφοφορίας μέσω του Διαδικτύου.

Τέλος, στο κεφάλαιο 8 αναφέρονται συμπεράσματα και προτείνονται κατευθύνσεις μελλοντικής ερευνητικής δραστηριότητας.

2. Ιδιωτικότητα και Απαιτήσεις Ιδιωτικότητας

Στο κεφάλαιο αυτό περιγράφονται έννοιες από την επιστημονική περιοχή της ιδιωτικότητας, τονίζεται η ανάγκη της προστασίας της ιδιωτικότητας στη φάση της σχεδίασης συστημάτων, ενώ εισάγονται οι απαιτήσεις της ιδιωτικότητας όσον αφορά στην ανάλυση και σχεδίαση πληροφοριακών συστημάτων.

2.1. Ιδιωτικότητα

Όταν κάποιος χρησιμοποιεί μια τυπική εφαρμογή ηλεκτρονικής επεξεργασίας κειμένου, συνήθως δεν σκέπτεται αν κάποιος βρίσκεται κοντά του και παρακολουθεί το κείμενο που παράγεται. Όταν ο ίδιος χρήστης περιηγείται στο Διαδίκτυο, «είναι ως να βρίσκεται στο κέντρο μιας συναυλίας όπου εκατοντάδες άνθρωποι μπορούν να δουν τι κάνει ή και να ακούσουν τι ακριβώς αναφέρει» (Cannon, J.C. 2004).

Οι περισσότεροι χρήστες Η/Υ χρησιμοποιούν το Διαδίκτυο και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου για επαγγελματικούς και προσωπικούς σκοπούς. Οι υπηρεσίες του ηλεκτρονικού ταχυδρομείου και του Διαδικτύου προσφέρονται από Παρόχους Υπηρεσιών Διαδικτύου (Internet Service Providers). Οι εξυπηρετητές (servers) διατηρούν δεδομένα των χρηστών που τους επισκέπτονται για διάφορους λόγους, όπως καλύτερη και γρηγορότερη παροχή υπηρεσίας την επόμενη φορά που θα ζητηθούν οι ίδιες υπηρεσίες, διευκόλυνση των χρηστών στον τρόπο πρόσβασης στις υπηρεσίες αυτές (διατηρώντας τα στοιχεία αναγνώρισής τους) κ.α. Επίσης, οι Η/Υ αυτοί διατηρούν αποθηκευμένα τα στοιχεία αυτά για σημαντικό χρονικό διάστημα σε ειδικά αρχεία (log files), τα οποία

είναι στη διάθεση του διαχειριστή των συστημάτων αυτών, τόσο για ανάγνωση όσο και για επεξεργασία.

Η χρήση του Διαδικτύου και του ηλεκτρονικού ταχυδρομείου είναι δύο από τις πολλές υπηρεσίες που προσφέρονται σήμερα στους διάφορους χρήστες, και μέσω των οποίων, αφήνουν εν αγνοία τους σημαντικό αριθμό των προσωπικών τους δεδομένων, με αποτέλεσμα να παραβιάζεται η ιδιωτικότητά τους. Κατά πόσο όμως γνωρίζουν οι σημερινοί χρήστες τον κίνδυνο της αποκάλυψης όλων αυτών των δεδομένων, των προσωπικών τους δεδομένων, σε τρίτους μη έμπιστους για αυτούς χρήστες;

Η ιδιωτικότητα, ως ένα ζήτημα κοινωνικό και νομικό, έχει απασχολήσει εδώ και καιρό κοινωνικούς επιστήμονες, φιλόσοφους και νομικούς. Με την αξιοποίηση των Η/Υ και τις ολοένα αυξανόμενες δυνατότητες που προσέφεραν τα σύγχρονα πληροφοριακά συστήματα και τα δίκτυα επικοινωνιών, η ιδιωτικότητα των χρηστών άρχισε να κινδυνεύει.

Στην πορεία για τη δημιουργία μίας παγκόσμιας κοινωνίας της πληροφορίας και με την ύπαρξη ολοένα και περισσότερων προγραμμάτων ανάπτυξης των δικτύων τηλεπικοινωνιών μεταξύ των κρατών, δημιουργούνται ποικίλοι κίνδυνοι όσον αφορά στη διαφύλαξη της ιδιωτικότητας των χρηστών που χρησιμοποιούν ή θα χρησιμοποιήσουν τα δίκτυα αυτά.

Η ιδιωτικότητα, ως βασικό ανθρώπινο δικαίωμα αναγνωρισμένο από τη δήλωση του Οργανισμού Ηνωμένων Εθνών για την προστασία των ανθρωπίνων δικαιωμάτων, αλλά και από πολλές διεθνείς και τοπικές συνθήκες, πρέπει να προστατεύεται σε μια δημοκρατική κοινωνία (Privacy International, Electronic Privacy Information Center 1999).

Η προστασία της ιδιωτικότητας μπορεί να επιτευχθεί με έναν από τους παρακάτω τρόπους:

- Νόμοι για την ιδιωτικότητα και την προστασία δεδομένων
- Τεχνολογίες ενίσχυσης της ιδιωτικότητας που επιλέγονται και εφαρμόζονται από τους χρήστες
- Εκπαίδευση των χρηστών και των επαγγελματιών πληροφορικής σε θέματα ιδιωτικότητας
- Κανονισμοί επιχειρήσεων που αφορούν σε πρακτικές εφαρμογής και υλοποίησης της ιδιωτικότητας

Ο πρώτος ορισμός της ιδιωτικότητας δόθηκε από τους Warren και Brandeis στο άρθρο τους «Το δικαίωμα στην ιδιωτικότητα» (The Right to Privacy) (Warren, S. and Brandeis, L. 1890). Οι δύο αυτοί αμερικανοί δικηγόροι όρισαν την ιδιωτικότητα ως *«το δικαίωμα του να είναι κανείς μόνος του»*.

Πιο πρόσφατα ο Alen Westin απέδωσε τον όρο ιδιωτικότητα ως *«το δικαίωμα του κάθε ανθρώπου ή ομάδας ατόμων ή οργανισμών, να καθορίζουν από μόνοι τους, πότε, πώς και σε ποιο βαθμό οι προσωπικές τους πληροφορίες θα γίνονται γνωστές σε τρίτους»* (Westin, A. 1967). Ως «ομάδες ατόμων ή οργανισμούς» αναφερόμαστε σε νομικά πρόσωπα.

Η ιδιωτικότητα, ως έννοια, προσεγγίζεται από τρεις πλευρές (R.Rosenberg 1992; J.Holvast 1993):

- *Χωρική Ιδιωτικότητα* (territorial privacy): Αναφέρεται στην προστασία της ιδιωτικότητας του ατόμου στο φυσικό χώρο που τον περιβάλει π.χ. να μην μπορούν τρίτοι να παρατηρήσουν τις εργασίες που κάνει ένα άτομο στο γραφείο του.
- *Ιδιωτικότητα του ατόμου* (privacy of the person): Αναφέρεται στην προστασία του ατόμου από αναίτιες παρεμβάσεις τρίτων σε αυτό, π.χ. φυσική έρευνα χωρίς δικαιολογία,

έλεγχο για κατοχή φαρμάκων, ανήθικη και παράνομη έρευνα για την απόκτηση προσωπικών πληροφοριών κλπ.

- *Ιδιωτικότητα της πληροφορίας* (informational privacy): Αναφέρεται στο δικαίωμα του κάθε ατόμου να ελέγχει αν και με ποιο τρόπο τα προσωπικά του δεδομένα συλλέγονται, αποθηκεύονται, επεξεργάζονται και διαμοιράζονται σε τρίτους.

Ο όρος *προσωπικά δεδομένα (personal data)* (Fischer-Hubner, S. 2001) αφορά σε κάθε πληροφορία που προσδιορίζει την προσωπικότητα ενός ατόμου. Ο όρος *προστασία δεδομένων (data protection)* αναφέρεται στην προστασία των προσωπικών δεδομένων με σκοπό τη διαφύλαξη της ιδιωτικότητας και αποτελεί μέρος της γενικής έννοιας της ιδιωτικότητας. Ωστόσο, η ιδιωτικότητα δεν μπορεί να αποτελεί δικαίωμα απόλυτο, για όλες τις περιπτώσεις, μιας και πολλές φορές η προστασία της έρχεται σε αντίθεση με άλλα δικαιώματα ή νόμους και επίσης είναι γενικά αποδεκτό ότι κανένας δεν μπορεί να είναι αναγνωρίσιμο μέλος σε μια κοινωνία χωρίς να αποκαλύπτει μέρος των προσωπικών του δεδομένων.

Σε μια κοινωνία πλήρως δικτυακή όπως η σημερινή, η ιδιωτικότητα βρίσκεται σε κίνδυνο και δεν μπορεί να προστατευθεί μόνον από νόμους και κανονισμούς. Οι υπεύθυνοι για την προστασία δεδομένων απαιτούν πλέον από τους αναλυτές και προγραμματιστές πληροφοριακών συστημάτων να συμπεριλαμβάνουν την ιδιωτικότητα ως τεχνική απαίτηση που πρέπει να λαμβάνεται υπόψη στο υπό-ανάπτυξη σύστημα και πιο συγκεκριμένα θα πρέπει να λαμβάνεται υπόψη από τη φάση της σχεδίασης του συστήματος αποτελώντας ξεχωριστό κριτήριο που πρέπει να υλοποιηθεί.

Για να επιτευχθεί ο παραπάνω στόχος και να μπορέσει η ιδιωτικότητα από μία γενική έννοια να μετατραπεί σε τεχνική απαίτηση,

ορίστηκε μια σειρά από επιμέρους απαιτήσεις, οι *απαιτήσεις ιδιωτικότητας (privacy requirements)* οι οποίες είναι οι ακόλουθες (Fischer-Hubner, S. 2001; Koorn, R., van Gils, H., Hart, J., Overbeek, P. and Tellegen, R. 2004; Pfitzmann, A. and Hansen, M 2007):

- *αυθεντικοποίηση (authentication)*
- *εξουσιοδότηση (authorization)*
- *αναγνώριση (identification)*
- *προστασία δεδομένων (data protection)*
- *ανωνυμία (anonymity)*
- *ψευδωνυμία (pseudonymity)*
- *μη-συνδεσιμότητα (unlinkability)*
- *μη-παρατηρησιμότητα (unobservability)*

Οι απαιτήσεις αυτές καλύπτουν διάφορες πλευρές της ιδιωτικότητας κατά τη χρήση πληροφοριακού συστήματος. Ανάλογα με τον τρόπο προστασίας της ιδιωτικότητας σε ένα πληροφοριακό σύστημα, υλοποιείται μία ή περισσότερες από αυτές.

Στη συνέχεια περιγράφονται αναλυτικά οι απαιτήσεις ιδιωτικότητας, με σκοπό την καλύτερη κατανόηση τους και του τρόπου που αυτές υλοποιούν τμήμα της ευρύτερης έννοιας-στόχου, της ιδιωτικότητας.

2.2. Αυθεντικοποίηση

Η αυθεντικοποίηση είναι η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα μιας οντότητας. Σε ιδιωτικά και δημόσια δίκτυα, η αυθεντικοποίηση υλοποιείται συνήθως με τη χρήση κωδικών πρόσβασης (passwords).

Η αυθεντικοποίηση αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας ενός συστήματος. Ωστόσο, έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας.

Έτσι, όταν μια οντότητα αιτείται τη χρήση μιας υπηρεσίας από ένα πληροφοριακό σύστημα, θα πρέπει να εξετάζεται η υπηρεσία αυτή και ανάλογα να ζητείται η αυθεντικοποίηση ή μη της συγκεκριμένης οντότητας. Με αυτόν τον τρόπο προστατεύεται και η ιδιωτικότητα της οντότητας, αλλά και τα ευαίσθητα δεδομένα του συστήματος.

2.3. Εξουσιοδότηση

Η εξουσιοδότηση είναι η διαδικασία μέσω της οποίας μία οντότητα αποκτά δικαιώματα (π.χ. χρήση, τροποποίηση, προσπέλαση κτλ.) σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος. Σε ένα σύστημα που υπάρχουν πολλοί χρήστες ο διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα από αυτούς με τα αντίστοιχα δικαιώματα, ανάλογα με το ρόλο τους και τις υποχρεώσεις τους στο σύστημα.

Η εξουσιοδότηση, όπως και η αυθεντικοποίηση, αποτελεί κυρίως απαίτηση ασφάλειας. Η εξουσιοδότηση, όμως, συντελεί στην ικανοποίηση της ιδιωτικότητας μιας και τα ευαίσθητα προσωπικά δεδομένα των χρηστών που βρίσκονται αποθηκευμένα σε ένα σύστημα πρέπει να μπορούν να τα προσπελάσουν μόνον εξουσιοδοτημένοι χρήστες. Προστατεύοντας τα προσωπικά δεδομένα των χρηστών ενός συστήματος, προστατεύεται μέρος της ιδιωτικότητάς τους.

Η εξουσιοδότηση συχνά έπεται της αυθεντικοποίησης μιας και πρώτα πρέπει να αναγνωρισθεί θετικά μία οντότητα και μετά να της

ανατεθούν τα αντίστοιχα δικαιώματα ανάλογα με το ρόλο της στο σύστημα.

2.4. Αναγνώριση

Η αναγνώριση έχει ορισθεί ως απαίτηση που ικανοποιεί την ιδιωτικότητα, αφενός μεν της εξωτερικής οντότητας που ζητά να αποκτήσει πρόσβαση σε μία υπηρεσία ή να προσπελάσει ένα σύνολο δεδομένων αυτής, αφετέρου των οντοτήτων των οποίων τα προσωπικά δεδομένα είναι αποθηκευμένα στο σύστημα.

Συγκεκριμένα, από την πλευρά της εξωτερικής οντότητας, η διαδικασία της αναγνώρισης ελέγχει αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και, στη συνέχεια, εξουσιοδότησή της ή όχι. Σε περίπτωση που δεν απαιτείται, προστατεύουν την ιδιωτικότητα της αφού επιστρέφουν τα αντίστοιχα δεδομένα ή την υπηρεσία που ζητήθηκε δίχως την παροχή προσωπικών δεδομένων από αυτή.

Από την πλευρά της προστασίας των δεδομένων που είναι αποθηκευμένα σε ένα σύστημα, η διαδικασία της αναγνώρισης φροντίζει να μην επιτραπεί σε κανέναν μη εξουσιοδοτημένο χρήστη η πρόσβαση σε αυτά, προφυλάσσοντας έτσι την ιδιωτικότητα των κατόχων τους.

2.5. Προστασία Δεδομένων

Η Ευρωπαϊκή Ένωση το 1995 εξέδωσε την οδηγία 95/46/EC (EU, Directive. 1995) που αφορά στην επεξεργασία των προσωπικών δεδομένων και την ελεύθερη διακίνησή τους. Οι βασικοί στόχοι αυτής της οδηγίας είναι η προστασία της ιδιωτικότητας ως θεμελιώδες ανθρώπινο δικαίωμα,

αλλά και η καθιέρωση ελέγχων όσον αφορά στην προστασία της ιδιωτικότητας των δεδομένων που μεταφέρονται μεταξύ των κρατών-μελών της Ευρωπαϊκής Ένωσης.

Σκοπός της συγκεκριμένης απαίτησης είναι η προστασία των προσωπικών δεδομένων από επεξεργασία η οποία έρχεται σε αντίθεση με τη ισχύουσα νομοθεσία, καθώς και με την οδηγία 95/46 της Ευρωπαϊκής Ένωσης

Οι βασικές αρχές της ιδιωτικότητας που εκφράζονται από αντίστοιχους νόμους και από την προαναφερθείσα οδηγία είναι οι ακόλουθες:

- *Αρχή της νομιμότητας και της δικαιοσύνης (principle of lawfulness and fairness)*: Τα προσωπικά δεδομένα πρέπει να συλλέγονται με νόμιμο και δίκαιο τρόπο.
- *Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν (Principle of the purpose specification and purpose binding)*: Ο σκοπός που συλλέγονται τα προσωπικά δεδομένα πρέπει να είναι σαφώς καθορισμένος και να συνάδει με τη νομοθεσία. Η επεξεργασία των δεδομένων πρέπει να διεξάγεται μόνο για το σκοπό για τον οποίο συγκεντρώθηκαν.
- *Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων (Principle of necessity of data collection and processing)*: Η συλλογή και η επεξεργασία των προσωπικών δεδομένων πρέπει να επιτρέπονται μόνο στις περιπτώσεις όπου ο συλλέγων πράττει ενέργειες αντίστοιχες με το σκοπό συλλογής των δεδομένων, αποδεικνύοντας έτσι την αναγκαιότητα, αφού για την εκτέλεση των ενεργειών χρειάζεται τα δεδομένα αυτά.

- *Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των ευαίσθητων δεδομένων (Information, notification and access rights of the data subjects)*: Οι κάτοχοι των δεδομένων πρέπει να έχουν το δικαίωμα της πληροφόρησης και της ενημέρωσης για τα προσωπικά τους δεδομένα, καθώς και το δικαίωμα της πρόσβασης, διόρθωσης, διαγραφής ή και αποκλεισμού των δεδομένων τους σε περιπτώσεις που εκείνοι κρίνουν αναγκαίο.
- *Αρχή της ασφάλειας και της ακεραιότητας (Principle of security and accuracy)*: Κατάλληλοι μηχανισμοί και τεχνολογίες πρέπει να υπάρχουν για να διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των προσωπικών δεδομένων. Τα προσωπικά δεδομένα πρέπει να παραμένουν ασφαλή, ενημερωμένα και ακέραια.
- *Εποπτεία και Επικύρωση (Supervision and sanctions)*: Προβλέπει τη σύσταση Ανεξάρτητης Αρχής Προστασίας Δεδομένων, με σκοπό την επίβλεψη και παρατήρηση της εφαρμογής των κανόνων ιδιωτικότητας. Η ίδια Αρχή θα είναι υπεύθυνη και για την επιβολή κυρώσεων στις περιπτώσεις που σημειώνονται αποκλίσεις από τη νομιμότητα.

2.6. Ανωνυμία

Μια από τις βασικές απαιτήσεις προστασίας της ιδιωτικότητας ενός χρήστη είναι η δυνατότητά του να μπορεί να παραμένει ανώνυμος. Η ανωνυμία διασφαλίζει ότι ένας χρήστης μπορεί να χρησιμοποιήσει μια

υπηρεσία ή να επικοινωνήσει με μια άλλη οντότητα χωρίς να αποκαλύψει την ταυτότητά του (Fischer-Hubner, S. 2001).

Το 1990 ο Pfitzmann (Pfitzmann, A. 1990) ανέπτυξε ένα φορμαλιστικό ορισμό για τον όρο ανωνυμία. Συγκεκριμένα, ορίζεται ως R_U το γεγονός ότι μία οντότητα U (π.χ. ένας χρήστης) κατέχει ένα ρόλο R (π.χ. αποστολέας ή παραλήπτης ενός μηνύματος) στο πλαίσιο μιας επικοινωνίας E. Ορίζεται, επίσης, ως A μία πιθανή κακόβουλη οντότητα (επιτιθέμενος) και ως NC_A το σύνολο των οντοτήτων που δεν ανήκουν στο σύνολο των πιθανών επιτιθέμενων οντοτήτων στο οποίο ανήκει και η οντότητα A.

Με βάση τα παραπάνω, μία οντότητα καλείται ανώνυμη όσον αφορά το ρόλο R, σε μια επικοινωνία E, απέναντι σε έναν επιτιθέμενο A, αν για κάθε παρατήρηση B που μπορεί να κάνει ο A ισχύει η ακόλουθη σχέση:

$$\forall U' \in NC_A: 0 < P(R_{U'} | B) < 1$$

Ωστόσο, η ανωνυμία της οντότητας U στο ρόλο R μπορεί να είναι πλήρως εγγυημένη μόνον όταν η τιμή του $P(R_U|B)$ δεν είναι κοντά στο 0 ή στο 1.

Ανάλογα με το ρόλο που έχει ο χρήστης σε κάθε επικοινωνία έχουν καθοριστεί δύο μορφές υλοποίησης της ανωνυμίας. Η *ανωνυμία του αποστολέα (sender anonymity)* και η *ανωνυμία του παραλήπτη (receiver anonymity)*. Η ανωνυμία του αποστολέα σημαίνει ότι σε μια επικοινωνία, ο χρήστης που έχει το ρόλο του αποστολέα παραμένει ανώνυμος ενώ ο παραλήπτης όχι. Αντίστοιχα, η ανωνυμία του παραλήπτη σημαίνει τη διαφύλαξη της ανωνυμίας του παραλήπτη παρά του αποστολέα.

Μία οντότητα U, που έχει ένα ρόλο R και μετέχει σε μια επικοινωνία E, ορίζεται ως *τελείως ανώνυμη (perfectly anonymous)* αν για κάθε παρατήρηση B του επιτιθέμενου A ισχύει:

$$\forall U' \in NC_A: P(R_{U'}) = P(R_{U'} | B)$$

που σημαίνει ότι ο επιτιθέμενος δε λαμβάνει καμία πληροφορία από τις παρατηρήσεις του στην οντότητα U.

Για το χρήστη που στέλνει/λαμβάνει σε μία επικοινωνία υπάρχει ο όρος της *τέλειας ανωνυμίας αποστολέα/παραλήπτη (perfect sender/receiver anonymity*), που σημαίνει ότι ο επιτιθέμενος δεν έχει τη δυνατότητα να ξεχωρίσει πότε ο αποστολέας/παραλήπτης συμμετέχει σε μια επικοινωνία και πότε όχι.

Το 2007 ο Pfitzmann όρισε λεπτομερέστερα την ανωνυμία ως ακολούθως: *Ανωνυμία μίας οντότητας σημαίνει ότι αυτή δεν είναι αναγνωρίσιμη μέσα σε ένα σύνολο οντοτήτων, το σύνολο ανώνυμων οντοτήτων (Pfitzmann, A. and Hansen, M 2007).* Το σύνολο αυτό περιλαμβάνει όλες τις οντότητες που μετέχουν σε μια επικοινωνία και που πιθανόν θα μπορούσαν να αναγνωρισθούν από διάφορους επιτιθέμενους.

2.7. Ψευδωνυμία

Η απαίτηση της ψευδωνυμίας έχει παρόμοια χαρακτηριστικά με αυτά της ανωνυμίας. Με τη ψευδωνυμία προστατεύεται η αναγνώριση των χρηστών από τρίτες οντότητες. Στην ψευδωνυμία οι χρήστες χρησιμοποιούν ψευδώνυμα για να προστατέψουν την αποκάλυψη της ταυτότητάς τους (Cannon, J.C. 2004). Το ψευδώνυμο είναι ένα αναγνωριστικό μιας οντότητας, διαφορετικό από το πραγματικό της όνομα (Pfitzmann, A. and Hansen, M 2007).

Στο (Fischer-Hubner, S. 2001) ορίζεται η ψευδωνυμία ως η απαίτηση που διασφαλίζει την απόκρυψη της ταυτότητας του χρήστη όταν αυτός

ενεργεί στα πλαίσια μίας επικοινωνίας χρησιμοποιώντας ένα ή περισσότερα ψευδώνυμα. Η ψευδωνυμία υλοποιείται όταν δεν μπορεί να υλοποιηθεί η ανωνυμία, όπως σε περιπτώσεις όπου ο χρήστης πρέπει να είναι υπόλογος των πράξεών του.

Οι Pfitzmann, Waidner και Pfitzmann (Pfitzmann, B., Waidner, M. and Pfitzmann, A. 1990) κατηγοριοποίησαν τα ψευδώνυμα σε δύο κατηγορίες: α) Στα *προσωπικά ψευδώνυμα (personal pseudonyms)* και β) στα *ψευδώνυμα ρόλων (role-pseudonyms).*

Ένα ψευδώνυμο αποκαλείται προσωπικό όταν ανήκει σε κάποιο χρήστη, ο οποίος το χρησιμοποιεί για προσωπική του χρήση σε διάφορες συναλλαγές για μία κάποια χρονική περίοδο. Άρα στη ουσία ένα προσωπικό ψευδώνυμο αντικαθιστά το όνομα του χρήστη.

Ένα ψευδώνυμο αποκαλείται ψευδώνυμο ρόλου όταν, σε αντίθεση με το προσωπικό ψευδώνυμο, δεν συνδέεται με το όνομα του χρήστη, αλλά με το ρόλο που αυτός έχει στα πλαίσια μιας συναλλαγής ή επικοινωνίας. Τα ψευδώνυμα αυτά προσφέρουν μεγαλύτερη προστασία από ό,τι τα προσωπικά, μιας και ισχύουν για ένα συγκεκριμένο ρόλο του χρήστη που μετέχει σε μια συγκεκριμένη επικοινωνία.

2.8. Μη-συνδεσιμότητα

Η απαίτηση της μη-συνδεσιμότητας προστατεύει την ιδιωτικότητα των χρηστών από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, κάτι που θα μπορούσε να οδηγήσει στην αποκάλυψη της ταυτότητας των πρώτων (Cannon, J.C. 2004).

Το 1990 ο Pfitzmann (Pfitzmann, A. 1990) έδωσε ένα φορμαλιστικό ορισμό για τον όρο μη-συνδεσιμότητα.

Συγκεκριμένα, ορίζεται ως $X_{E,F}$ το κοινό χαρακτηριστικό που μπορεί να έχουν δύο συναλλαγές μεταξύ τους ονόματι E και F. Δύο συναλλαγές E και F είναι μη-συνδέσιμες ως προς ένα χαρακτηριστικό X για έναν επιτιθέμενο A αν για κάθε παρατήρηση B που μπορεί να κάνει ο A, η πιθανότητα οι E και F σε σχέση με το X, δεδομένου του B, είναι μεγαλύτερη του 0 και μικρότερη του 1:

$$0 < P(X_{E,F} | B) < 1$$

Ένας πιο αυστηρός ορισμός της μη-συνδεσιμότητας είναι ο ακόλουθος:

$$0 << P(X_{E,F} | B) << 1$$

Οι E και F ορίζονται ως *τελείως μη-συνδέσιμες (perfectly unlinkable)* αν για κάθε παρατήρηση B του επιτιθέμενου A ισχύει:

$$P(X_{E,F} | B) = P(X_{E,F})$$

που σημαίνει ότι ο επιτιθέμενος δεν λαμβάνει καμία πληροφορία από τις παρατηρήσεις των συναλλαγών E και F.

Το 2007 ο Pfitzmann όρισε τη μη-συνδεσιμότητα ως ακολούθως: Δύο ή περισσότερες οντότητες (π.χ. χρήστες, μηνύματα, ενέργειες) είναι μη-συνδέσιμες, από τη πλευρά του επιτιθέμενου, αν μέσα στο ίδιο σύνολο οντοτήτων (ή στο ίδιο περιβάλλον που διεξάγεται η επικοινωνία) ο επιτιθέμενος δεν μπορεί να ξεχωρίσει αν αυτές οι οντότητες σχετίζονται μεταξύ τους ή όχι (Pfitzmann, A. and Hansen, M 2007).

2.9. Μη-παρατηρησιμότητα

Η απαίτηση της μη-παρατηρησιμότητας προστατεύει την ιδιωτικότητα των χρηστών από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν τα ίχνη των πρώτων τη στιγμή που περιηγούνται στο Διαδίκτυο ή χρησιμοποιούν μια υπηρεσία (Cannon, J.C. 2004).

Ο φορμαλιστικός ορισμός της μη-παρατηρησιμότητας δόθηκε το 1990 από τον Pfitzmann (Pfitzmann, A. 1990) ως εξής:

Μια συναλλαγή (ή μέρος αυτής) E είναι μη-παρατηρήσιμη για έναν επιτιθέμενο A, αν για κάθε παρατήρηση B που μπορεί να κάνει ο A, η πιθανότητα της E δεδομένου του B είναι μεγαλύτερη του 0 και μικρότερη του 1:

$$0 < P(E|B) < 1$$

Ένας πιο αυστηρός ορισμός της μη-παρατηρησιμότητας είναι ο ακόλουθος:

$$0 << P(E|B) << 1$$

Αν για κάθε πιθανή παρατήρηση B που μπορεί να κάνει ο A η πιθανότητα να συμβεί η E είναι ίδια με αυτή του να συμβεί η E συναρτήσει του B δηλαδή: $P(E)= P(E|B)$, τότε η επικοινωνία E είναι *τελείως μη-παρατηρήσιμη (perfectly unobservable)*.

Το 2007 ο Pfitzmann επαναπροσδιόρισε τη μη-παρατηρησιμότητα ως ακολούθως: Μία οντότητα (π.χ. χρήστης, μήνυμα, ενέργεια) είναι μη-παρατηρήσιμη σε ένα σύνολο οντοτήτων όταν: α) ο επιτιθέμενος δεν μπορεί να εντοπίσει την οντότητα αυτή και β) ο κάτοχος της οντότητας αυτής παραμένει ανώνυμος σε σχέση με τους άλλους κατόχους των υπόλοιπων οντοτήτων (Pfitzmann, A. and Hansen, M 2007).

2.10. Συμπεράσματα

Στο κεφάλαιο αυτό περιγράφηκαν οι βασικές έννοιες από την επιστημονική περιοχή της ιδιωτικότητας. Στη παράγραφο 2.1 ορίστηκε η ιδιωτικότητα καθώς και συναφείς έννοιές της. Παρουσιάστηκε η ανάγκη προστασίας της ειδικά στα σύγχρονα πληροφοριακά περιβάλλοντα. Στις παραγράφους 2.2-2.9 περιγράφηκαν οι βασικές απαιτήσεις της ιδιωτικότητας οι οποίες καλύπτουν διάφορες πλευρές της κατά τη χρήση ενός πληροφοριακού συστήματος. Μέσω των απαιτήσεων αυτών υλοποιείται η ιδιωτικότητα σε ένα σύστημα.

Στο κεφάλαιο 3 ακολουθεί η περιγραφή των βασικών μεθοδολογιών και πλαισίων που χρησιμοποιούνται στην επιστημονική περιοχή της σχεδίασης συστημάτων για το προσδιορισμό και την ανάλυση των απαιτήσεων ασφαλείας και ιδιωτικότητας.

3. Μεθοδολογίες Ανάλυσης Απαιτήσεων Ασφαλείας

Οι επόμενες ενότητες περιγράφουν γνωστές μεθοδολογίες που έχουν ως στόχο τον προσδιορισμό και τη διαχείριση απαιτήσεων ασφαλείας στη φάση της σχεδίασης συστημάτων. Οι περισσότερες από τις μεθοδολογίες αυτές μπορούν να θεωρηθούν ως γενικά πλαίσια ανάλυσης απαιτήσεων, τα οποία υποστηρίζουν τον προσδιορισμό και τη διαχείριση τόσο των λειτουργικών όσο και των μη-λειτουργικών απαιτήσεων στα πρώτα στάδια της διαδικασίας σχεδίασης ενός συστήματος.

Ο λόγος που εστιάζουμε στις συγκεκριμένες μεθοδολογίες είναι ότι εμπεριέχουν κατάλληλες έννοιες για τη σαφή αναπαράσταση διαφόρων απαιτήσεων ασφαλείας (μεταξύ των οποίων και απαιτήσεις ιδιωτικότητας), καθώς και για το τρόπο που οι απαιτήσεις αυτές μεταφράζονται σε συγκεκριμένες πολιτικές για το υπό-ανάπτυξη σύστημα.

Οι μεθοδολογίες που θα εξεταστούν στο παρόν κεφάλαιο είναι οι ακόλουθες:

- Η μεθοδολογία NFR (Non-Functional Requirement Framework) (Chung, L. 1993)
- Η μεθοδολογία *i** (Yu., E. 1993)
- Η μεθοδολογία Tropos (Mouratidis., H., Giorgini, P. and Manson, G. 2003a)
- Η μεθοδολογία KAOS (Letier, E. and van Lamsweerde, A. 2002b)
- Η μεθοδολογία GBRAM (Goal-Based Requirements Analysis Method) (Antón, A. and Earp, J. 2000)

- Η μεθοδολογία RBAC (Role-Based Access Control) (He, Q. and Antón, A. 2003)
- Η μεθοδολογία M-N (Mofett-Nuseibeh Framework) (Moffett, D. and Nuseibeh, B. 2003)
- Η μεθοδολογία B-S (Bellotti-Sellen Framework) (Bellotti, V. and Sellen, A. 1993)
- Η μεθοδολογία STRAP (STRuctured Analysis for Privacy) (Jensen, C., Tullio, J., Potts, C. and Mynatt, E. 2005)

3.1. Η Μεθοδολογία NFR

Ο στόχος της NFR είναι η εύρεση και η καταγραφή των μη-λειτουργικών απαιτήσεων (non-functional requirements) ενός συστήματος στα πρώτα στάδια της ανάπτυξής του (Chung, L. 1993; Chung, L., Nixon, B., Yu., E. and Mylopoulos, J. 2000). Η NFR επικεντρώνεται στη καταγραφή των αναγκών ενός οργανισμού και όχι στα χαρακτηριστικά του υπό-ανάπτυξη συστήματος. Εστιάζει περισσότερο στους στόχους που θα πρέπει να ικανοποιηθούν και λιγότερο σε τεχνικές απαιτήσεις.

Οι απαιτήσεις ασφαλείας, στη μεθοδολογία NFR, αναπαρίστανται ως μη-λειτουργικές απαιτήσεις που θα πρέπει το υπό-ανάπτυξη σύστημα να ικανοποιεί ώστε να θεωρηθεί ασφαλές. Συγκεκριμένα, η μεθοδολογία αντιμετωπίζει την ασφάλεια με βάση τις τρεις βασικές απαιτήσεις: εμπιστευτικότητα, διαθεσιμότητα και ακεραιότητα.

Ο τρόπος που η NFR διαχειρίζεται τις απαιτήσεις ασφαλείας βασίζεται στην έννοια του στόχου. Συγκεκριμένα, η NFR αναπαριστά τις μη-λειτουργικές απαιτήσεις ως ένα σύνολο από *ανεκτικούς στόχους* (softgoals). Η διαχείριση των στόχων αυτών γίνεται με τον ακόλουθο τρόπο. Πρώτα η μεθοδολογία χρησιμοποιεί ανάλογους μηχανισμούς για

να αποκτήσει τη γνώση του οργανισμού και να καθορίσει τις μη-λειτουργικές του απαιτήσεις. Έπειτα, οι απαιτήσεις αυτές αναλύονται σε συγκεκριμένους ανεκτικούς στόχους. Οι ανεκτικοί αυτοί στόχοι συνδέονται με τους λειτουργικούς στόχους του οργανισμού και εξετάζεται το κατά πόσο μπορούν να υλοποιηθούν. Κατά τη διάρκεια της σύνδεσης των δύο κατηγοριών στόχων, μελετώνται τα εμπόδια που προκύπτουν στην ικανοποίηση των ανεκτικών στόχων από τους λειτουργικούς. Ο στόχος είναι να ξεπεραστούν τα συγκεκριμένα εμπόδια, ώστε οι ανεκτικοί στόχοι (στόχοι ασφαλείας) να μπορούν να εφαρμοστούν και να λειτουργήσουν ομαλά στο υπό-ανάπτυξη σύστημα.

Η μεθοδολογία NFR υποστηρίζεται από φορμαλιστικό μοντέλο. Παράλληλα, έχει δημιουργηθεί ένα εργαλείο λογισμικού (OME) το οποίο παρέχει ένα γραφικό περιβάλλον στο οποίο οι χρήστες μπορούν να σχεδιάσουν τα μοντέλα του οργανισμού που υποστηρίζονται από τη μεθοδολογία. Επίσης, το εργαλείο διαχωρίζει τις φάσεις του καθορισμού των απαιτήσεων, του σχεδιασμού και της υλοποίησης δίνοντας ανάλογες οδηγίες στους χρήστες του.

3.2. Η Μεθοδολογία *i**

Η μεθοδολογία *i** εφαρμόζεται στα αρχικά στάδια της σχεδίασης συστημάτων με σκοπό την αποτύπωση της λογικής και του περιεχομένου ενός οργανισμού (Yu., E. 1993; Yu., E. 1997; Chung, L., Nixon, B., Yu., E. and Mylopoulos, J. 2000). Η μεθοδολογία *i** αναπτύχθηκε αρχικά για να υποστηρίξει επιχειρήσεις και οργανισμούς όσον αφορά στη μοντελοποίηση, στην ανάλυση και στον επανασχεδιασμό των διαδικασιών τους. Πρόσφατα χρησιμοποιήθηκε και για τη μοντελοποίηση απαιτήσεων ασφαλείας και ιδιωτικότητας (Liu, L., Yu., E. and Mylopoulos,

J. 2002; Yu., E. and L., Cysneiros 2002; Liu, L., Yu., E. and Mylopoulos, J. 2003; Yu., E. and L., Cysneiros 2003). Επίσης, η *i** μπορεί να χρησιμοποιηθεί για την ικανοποίηση των απαιτήσεων ασφαλείας και ιδιωτικότητας σε σχέση με τις άλλες μη-λειτουργικές απαιτήσεις ενός συστήματος.

Οι απαιτήσεις ασφαλείας στη μεθοδολογία *i** αναπαρίστανται ως ανεκτικοί στόχοι, έννοια η οποία αναφέρθηκε και στη μεθοδολογία NFR. Η ανάλυση που χρησιμοποιεί η *i** δεν βασίζεται στην ανάλυση των στόχων αλλά στο διαμοιρασμό προθέσεων μεταξύ οντοτήτων (agents). Οι ανεκτικοί στόχοι αποτελούν στόχους που πρέπει να υλοποιηθούν από τις οντότητες του οργανισμού με σκοπό την επίτευξη της καλής λειτουργίας του. Οι οντότητες είναι αλληλοσχετιζόμενες υπό την έννοια ότι για να πετύχουν τους στόχους τους εξαρτώνται από εργασίες που εκτέλεσαν άλλες οντότητες ή μοιράζονται πόρους με άλλες οντότητες.

Βασισμένη στην ιδέα του διαμοιρασμού προθέσεων η *i** διαχειρίζεται τις απαιτήσεις ασφαλείας με τον ακόλουθο τρόπο. Πρώτα αναγνωρίζονται οι οντότητες και οι βασικοί ρόλοι που αυτοί επιτελούν. Έπειτα αναγνωρίζονται οι τρόποι εξάρτησης (dependency) μεταξύ των οντοτήτων σε σχέση με το σκοπό που αυτές επιτελούν. Μετά και το καθορισμό των εξαρτήσεων προσδιορίζονται οι απαιτήσεις ασφαλείας βάσει των προθέσεων που έχει η κάθε οντότητα απέναντι σε αυτές με τις οποίες συσχετίζεται. Μια οντότητα μπορεί να απαιτεί εμπιστοσύνη (trust), ασφάλεια (security) ή ιδιωτικότητα (privacy) από μια άλλη οντότητα. Οι απαιτήσεις αυτές προσδιορίζονται ως ανεκτικοί στόχοι. Στο τέλος, εξετάζονται οι συσχετίσεις μεταξύ των ανεκτικών στόχων όλων των οντοτήτων και πώς αυτές επιδρούν στην υλοποίηση της ασφαλείας του οργανισμού. Υπάρχουν διάφοροι τρόποι συσχέτισης. Για παράδειγμα υπάρχει ο διαχωρισμός θετικών και αρνητικών συσχετίσεων. Κατά την ανάλυση των συσχετίσεων αποφασίζεται ποιες από αυτές εμποδίζουν την υλοποίηση των στόχων των οντοτήτων και αντίστοιχα προσαρμόζονται

ώστε να υλοποιούνται όλοι οι ανεκτικοί στόχοι σε σχέση με τη λειτουργία των οντοτήτων του οργανισμού.

Η μεθοδολογία *i** χρησιμοποιεί το εργαλείο OME (Organization Modelling Environment) που περιγράφηκε προηγουμένως. Επίσης έχει αναπτυχθεί αντίστοιχο φορμαλιστικό μοντέλο που να υποστηρίζει το τρόπο λειτουργίας της μεθοδολογίας.

3.3. Η Μεθοδολογία Tropos

Η μεθοδολογία Tropos αναπτύχθηκε με σκοπό την περιγραφή, τόσο του περιβάλλοντος του συστήματος ενός οργανισμού, όσο και του ίδιου του συστήματος. (Perini, P., Bresciani, P., Giorgini, P., Giunchiglia, F. and Mylopoulos, J. 2001; Mouratidis., H., Giorgini, P. and Manson, G. 2003a). Εφαρμόζεται σε όλες τις φάσεις ανάπτυξης του συστήματος, υιοθετώντας έναν ομοειδή τρόπο ανάλυσης τόσο στη φάση της ανάλυσης απαιτήσεων, όσο και στη φάση του σχεδιασμού και της υλοποίησης του συστήματος. Παράλληλα με την ανάλυση του συστήματος η Tropos εξετάζει και εντοπίζει τις απαιτήσεις ασφαλείας μαζί με τις υπόλοιπες απαιτήσεις του οργανισμού. Αρκετά επηρεασμένη από την *i** η μεθοδολογία Tropos υιοθετεί το μοντέλο της *i** καθώς και τις βασικές της έννοιες όπως οντότητες, εξαρτήσεις, πόρους κτλ.

Για την αναπαράσταση των απαιτήσεων ασφαλείας η Tropos χρησιμοποιεί τρεις έννοιες. Τον *ασφαλή περιορισμό (security constraint)*, την *ασφαλή οντότητα (security entity)* και την *ασφαλή εξάρτηση (security dependency)*. Ένας ασφαλής περιορισμός αφορά σε μια παράμετρο ασφαλείας όλου του συστήματος ενώ μια ασφαλή οντότητα αναπαριστά ένα στόχο ασφαλείας μιας οντότητας ή έναν πόρο ασφαλείας. Τέλος, μια ασφαλής εξάρτηση μεταξύ δύο οντοτήτων που αλληλοσχετίζονται, ορίζει

έναν περιορισμό ασφαλείας που, όταν υλοποιηθεί, υλοποιείται επιτυχώς και η συσχέτιση των οντοτήτων.

Η Tropos διαχειρίζεται τις απαιτήσεις ασφαλείας σε όλες τις φάσεις ανάπτυξης λογισμικού με τον ακόλουθο τρόπο (Mouratidis., H., Giorgini, P. and Manson, G. 2003a; Mouratidis., H., Giorgini, P. and Manson, G. 2003b). Στα αρχικά στάδια της ανάλυσης των απαιτήσεων και μετά την κατανόηση και αποτύπωση του τρόπου λειτουργίας του οργανισμού παράγεται το μοντέλο του οργανισμού με τις ενεργές οντότητες, τις συσχετίσεις τους και τους περιορισμούς ασφαλείας που εφαρμόζονται σε αυτούς. Έπειτα, στα τελικά στάδια της ανάλυσης απαιτήσεων, προκύπτουν από τις συσχετίσεις των οντοτήτων οι λειτουργικές απαιτήσεις του οργανισμού, ενώ οι περιορισμοί ασφαλείας αποτελούν πλέον τις απαιτήσεις ασφαλείας του οργανισμού. Στη συνέχεια, στη φάση του σχεδιασμού της αρχιτεκτονικής, περιγράφεται το σύστημα αποτελούμενο από υπό-συστήματα συνδεδεμένα με δεδομένα και ροές ελέγχου. Τα υπό-συστήματα αυτά σχεδιάζονται ώστε να υλοποιούν τις απαιτήσεις ασφαλείας καθώς και των άλλων μη-λειτουργικών απαιτήσεων. Τέλος, στη φάση της λεπτομερούς σχεδίασης, κάθε μέρος της αρχιτεκτονικής ορίζεται και αναλύεται σε βάθος, μαζί με τις εισόδους, εξόδους, ελέγχους και παραμέτρους ασφαλείας.

Η Tropos υποστηρίζεται από φορμαλιστικά μοντέλα. Παράλληλα, έχει αναπτυχθεί το εργαλείο ST-Tool το οποίο μπορεί να χρησιμοποιηθεί για τη σχεδίαση των μοντέλων της μεθοδολογίας καθώς για την φορμαλιστική ανάλυση των μοντέλων αυτών.

3.4. Η Μεθοδολογία KAOS

Η μεθοδολογία KAOS είναι μια μέθοδος εύρεσης και επεξεργασίας απαιτήσεων βασισμένη σε στόχους (Dardenne, A., van Lamsweerde, A. and Fickas, S. 1993; van Lamsweerde, A., R., Darimont and P., Massonet 1995; Dardenne, A. and van Lamsweerde, A. 1996; van Lamsweerde, A., R., Darimont and Letier, E. 1998; van Lamsweerde, A. and Letier, E. 2000; Letier, E. and van Lamsweerde, A. 2002a; Letier, E. and van Lamsweerde, A. 2002b). Σκοπός της μεθοδολογίας είναι η εύρεση των απαιτήσεων του οργανισμού χρησιμοποιώντας μοντέλα στόχων. Συγκεκριμένα, η KAOS ξεκινά από τους αφαιρετικούς – υψηλού επιπέδου στόχους και καταλήγει αναγνωρίζοντας τις απαιτήσεις, τα αντικείμενα και τις οντότητες του οργανισμού, καθώς και τις ενέργειες που μπορεί να κάνει κάθε οντότητα μέσα στο υπό-ανάπτυξη σύστημα. Οι απαιτήσεις ασφαλείας εντοπίζονται παράλληλα με την εύρεση των στόχων ασφαλείας του οργανισμού.

Η αναπαράσταση των απαιτήσεων ασφαλείας στη KAOS γίνεται με τη μορφή εμποδίων (obstacles) τα οποία εμποδίζουν την υλοποίηση ενός ή περισσότερων στόχων του οργανισμού. Συγκεκριμένα, για να εντοπιστούν οι απαιτήσεις ασφαλείας του οργανισμού εντοπίζονται τα εμπόδια που εμποδίζουν την πραγματοποίηση των στόχων. Ένα εμπόδιο ορίζεται ως μια σειρά από ενέργειες, η εκτέλεση των οποίων δεν είναι επιθυμητή για τη λειτουργία του οργανισμού.

Ο τρόπος με τον οποίο η μεθοδολογία KAOS αντιμετωπίζει τα εμπόδια, καταλήγοντας στον ορισμό των απαιτήσεων ασφαλείας, είναι ο ακόλουθος. Πρώτα, ταυτόχρονα με τον ορισμό των στόχων, εντοπίζονται και τα εμποδία των στόχων αυτών. Όπως και με τους στόχους, έτσι και τα εμπόδια αναλύονται με τη λογική του δέντρου δημιουργώντας έτσι ένα δέντρο εμποδίων. Με το τρόπο αυτό μπορεί να εξαλειφθεί ένα εμπόδιο

ευκολότερα μιας και είναι γνωστό από ποια υπό-εμπόδια αποτελείται. Έπειτα τα εμπόδια που εντοπίστηκαν κατηγοριοποιούνται όπως επίσης και οι στόχοι του οργανισμού. Μέσω της κατηγοριοποίησης διευκολύνεται ο τρόπος εύρεσης των συσχετίσεων μεταξύ των εμποδίων και των στόχων που επηρεάζουν. Τέλος αποφασίζεται ο τρόπος αντιμετώπισης των εμποδίων σε σχέση με τους στόχους που επηρεάζονται. Η μεθοδολογία KAOS εξετάζει τα εμπόδια του κάθε στόχου και αντίστοιχα τους προσαρμόζει ώστε να μπορέσουν να υλοποιηθούν χωρίς να «απειλούνται» από τα συγκεκριμένα εμπόδια. Η προσαρμογή μπορεί να σημαίνει τον επαναπροσδιορισμό των στόχων, τον επαναπροσδιορισμό των οντοτήτων, την εισαγωγή νέων στόχων, ή ακόμα και τον επανασχεδιασμό όλου του συστήματος. Σκοπός πάντα είναι η εξάλειψη όλων των εμποδίων που εντοπίστηκαν.

Η KAOS προσφέρει στους σχεδιαστές συστημάτων μία φορμαλιστική και εκφραστική γλώσσα μοντελοποίησης, στρατηγικές επεξεργασίας απαιτήσεων, καθώς και υποστήριξη με τη μορφή εργαλείου λογισμικού για να τους υποβοηθήσει στον καθορισμό των απαιτήσεων που προέρχονται από τους υψηλού επιπέδου αφαιρετικούς-γενικούς στόχους του συστήματος.

3.5. Η Μεθοδολογία GBRAM

Η GBRAM (Antón, A. 1996; Antón, A. and Earp, J. 2000) είναι μια μεθοδολογία που παρέχει έναν αρκετά σαφή και ευθύ τρόπο στον καθορισμό των στόχων και των απαιτήσεων ενός οργανισμού. Χρησιμοποιείται για τον εντοπισμό και τον επαναπροσδιορισμό των στόχων ενός συστήματος, των σχέσεων μεταξύ τους καθώς και τη

μετατροπή τους σε λειτουργικές απαιτήσεις. Η GBRAM χρησιμοποιείται και για την εντοπισμό απαιτήσεων ασφαλείας και ιδιωτικότητας.

Οι απαιτήσεις ασφαλείας και ιδιωτικότητας στη συγκεκριμένη μεθοδολογία αναπαριστώνται από την έννοια του *στόχου ασφαλείας (security goal)*. Στη μεθοδολογία GBRAM χρησιμοποιείται η τεχνική της ανάλυσης στόχων για τον προσδιορισμό των λειτουργικών και μη απαιτήσεων του οργανισμού. Συγκεκριμένα, η μεθοδολογία χωρίζει τους στόχους του οργανισμού σε πέντε κατηγορίες. Μια από αυτές είναι και οι στόχοι ασφαλείας. Από τους στόχους αυτούς προκύπτουν οι *πολιτικές ασφαλείας και ιδιωτικότητας (security and privacy policies)*. Με τον όρο πολιτική εννοούμε μια σειρά από ενέργειες που πρέπει να υλοποιηθούν με σκοπό την πραγματοποίηση ενός στόχου.

Η διαδικασία εντοπισμού και διαχείρισης των απαιτήσεων ασφαλείας στη GBRAM γίνεται με τον ακόλουθο τρόπο. Πρώτα γίνεται ο εντοπισμός των στόχων του οργανισμού και η δημιουργία του μοντέλου των στόχων. Στη φάση αυτή γίνεται η πρώτη ανάλυση για τον εντοπισμό τυχόν απαιτήσεων ασφαλείας και ιδιωτικότητας που περιέχονται μέσα στους στόχους που εντοπίστηκαν. Έπειτα, ακολουθεί η ανάλυση του κάθε στόχου η οποία οδηγεί στον εντοπισμό τυχόν εμποδίων στην υλοποίησή του, περιορισμών κτλ. Μετά την ανάλυση ακολουθεί ο επαναπροσδιορισμός των στόχων. Στο στάδιο αυτό διαγράφονται στόχοι που μπορεί να εντοπίστηκαν δύο ή και περισσότερες φορές ενώ για τους στόχους που απομένουν γίνεται μια ανάλυση κινδύνων γα τον εντοπισμό τυχόν απειλών και της επίδρασης αυτών στους υπόλοιπους στόχους του οργανισμού. Η ανάλυση αυτή οδηγεί ξανά στο πρώτο βήμα όπου αναγνωρίζονται νέοι στόχοι ή μορφοποιούνται οι υπάρχοντες, ώστε να αντιμετωπισθούν οι απειλές και οι κίνδυνοι που εντοπίστηκαν. Μόλις τελειώσει κι αυτή η φάση, η μεθοδολογία ορίζει μια σειρά από πολιτικές ασφαλείας και ιδιωτικότητας που πρέπει να εφαρμοστούν στο υπό-

ανάπτυξη σύστημα για την αποφυγή των κινδύνων που εντοπίστηκαν προηγουμένως. Στο τέλος, καθορίζονται οι απαιτήσεις ασφαλείας του συστήματος βάση των πολιτικών αυτών.

Η μεθοδολογία GBRAM δεν υποστηρίζεται από φορμαλιστικά μοντέλα ούτε και από εργαλείο/α λογισμικού.

3.6. Η Μεθοδολογία RBAC

Η RBAC (He, Q. and Antón, A. 2003) είναι μια μεθοδολογία που έχει σαν στόχο τον εντοπισμό των απαιτήσεων ιδιωτικότητας ενός οργανισμού. Συγκεκριμένα η RBAC στοχεύει στη μετατροπή των απαιτήσεων ιδιωτικότητας ενός οργανισμού σε πολιτικές ελέγχου πρόσβασης (access control policies) γεφυρώνοντας έτσι το κενό μεταξύ των «γενικών» απαιτήσεων και των «συγκεκριμένων» πολιτικών υλοποίησής τους.

Η μεθοδολογία RBAC συνδυάζει τεχνικές ανάλυσης στόχων και καθορισμού ρόλων για τον εντοπισμό των απαιτήσεων ιδιωτικότητας. Η RBAC αναπαριστά τις απαιτήσεις ιδιωτικότητας ως εργασίες που πρέπει να υλοποιήσουν οι οντότητες του οργανισμού. Συγκεκριμένα, η RBAC εντοπίζει πολιτικές ιδιωτικότητας που αφορούν σε δικαιώματα πρόσβασης. Για να οριστεί μια πολιτική ιδιωτικότητας, η RBAC περιγράφει τρία ξεχωριστά πεδία για κάθε οντότητα: α) τους σκοπούς (purposes), β) τις συνθήκες (conditions) και γ) τις υποχρεώσεις (obligations). Οι σκοποί ανατίθενται σε έναν ή περισσότερους ρόλους της οντότητας, οι οποίοι προέρχονται από τις διαδικασίες του οργανισμού. Για παράδειγμα, ένας ρόλος μπορεί να είναι ο διαχειριστής του συστήματος και ένας σκοπός που μπορεί να του ανατεθεί, είναι η διαχείριση. Οι συνθήκες αφορούν στις λειτουργίες που εκτελεί ένας ρόλος, σε σχέση

πάντοτε με τους σκοπούς του και υλοποιούνται με τη μορφή περιορισμών και αδειών του ρόλου στις λειτουργίες αυτές. Οι υποχρεώσεις περιγράφουν ενέργειες που έπονται κάποιων λειτουργιών των στόχων και βασίζονται στις πολιτικές που έχουν θεσπιστεί και ρυθμίζουν τη λειτουργία του συστήματος και του οργανισμού, γενικά.

Ο τρόπος με τον οποίο η RBAC εντοπίζει και διαχειρίζεται τις πολιτικές ιδιωτικότητας είναι ο ακόλουθος. Πρώτα δημιουργείται ένα μοντέλο δεδομένων βασισμένο στο περιεχόμενο του οργανισμού στο οποίο μοντελοποιούνται τα τρία βασικά πεδία καθορισμού των πολιτικών ιδιωτικότητας. Έπειτα, αναγνωρίζονται οι ρόλοι που επιτελούν οι οντότητες του οργανισμού. Για το κάθε ρόλο εντοπίζονται οι σκοποί που αυτός επιτελεί. Για την επίτευξη ενός σκοπού ορίζονται οι συνθήκες που πρέπει να ισχύουν. Οι πολιτικές ιδιωτικότητας ορίζονται βάση των συνθηκών που πρέπει να ισχύουν ώστε μια οντότητα να μπορέσει να επιτελέσει ένα συγκεκριμένο σκοπό μέσα από ένα ρόλο της σε σχέση με μια άλλη οντότητα ή αγαθό του οργανισμού. Συγκεκριμένα, κάθε πολιτική αποτελεί ένα περιορισμό πρόσβασης ενός ρόλου μιας οντότητας σε μια άλλη οντότητα ή αγαθό. Για τον εντοπισμό και τον καθορισμό των πολιτικών ιδιωτικότητας, η RBAC, χρησιμοποιεί μια διαδικασία μοντελοποίησης ρόλων βασισμένη στη λογική της σχεδίασης στόχων.

Η RBAC δεν υποστηρίζεται από φορμαλιστικά μοντέλα. Έχει οριστεί ένα κανονιστικό πλαίσιο για την έκφραση των συσχετίσεων μεταξύ των ρόλων και των περιορισμών που αυτοί έχουν στα αγαθά του οργανισμού. Επίσης, έχει αναπτυχθεί ένα εργαλείο λογισμικού, το οποίο όμως δεν καλύπτει πλήρως τις δυνατότητες της μεθοδολογίας μιας και δεν υποστηρίζει ανάλυση ρόλων.

3.7. Η Μεθοδολογία M-N

Η μεθοδολογία M-N (Moffett, D. and Nuseibeh, B. 2003) στηρίζεται στη μεθοδολογία KAOS που περιγράφηκε προηγουμένως. Στόχος της είναι η εύρεση και ανάλυση των απαιτήσεων ασφαλείας στα πρώτα βήματα της σχεδίασης συστημάτων. Για το σκοπό αυτό χρησιμοποιεί έννοιες, τόσο από το χώρο της ανάλυσης απαιτήσεων, όσο και από το χώρο της ασφάλειας συστημάτων.

Οι απαιτήσεις ασφαλείας αναπαρίστανται ως στόχοι ασφαλείας του οργανισμού. Συγκεκριμένα, η μεθοδολογία χρησιμοποιεί έννοιες από δύο γνωστικές περιοχές για τον καθορισμό των απαιτήσεων ασφαλείας. Από το χώρο της ανάλυσης απαιτήσεων χρησιμοποιείται η έννοια του στόχου (goal), ενώ από το χώρο της ασφάλειας χρησιμοποιούνται οι έννοιες του αγαθού (asset), καθώς και της απειλής (threat) που στοχεύει στην ολική ή μερική καταστροφή του αγαθού.

Η μεθοδολογία M-N προσδιορίζει τις απαιτήσεις ασφαλείας ξεκινώντας από τον καθορισμό των βασικών στόχων του οργανισμού. Στη φάση αυτή χρησιμοποιείται και η μεθοδολογία KAOS για τον επαναπροσδιορισμό των στόχων και την συγκεκριμενοποίησή τους που βοηθά στην υλοποίησή τους από τις διεργασίες του οργανισμού. Έπειτα εφαρμόζεται μια μεθοδολογία ανάλυσης και διαχείρισης της επικινδυνότητας με σκοπό τον εντοπισμό των αγαθών και των πιθανών απειλών που υπάρχουν σε αυτά. Μέσω της ανάλυσης και διαχείρισης επικινδυνότητας ορίζονται οι στόχοι ασφαλείας του συστήματος. Κάθε στόχος βασίζεται στις αντίστοιχες απειλές που αναγνωρίστηκαν προηγουμένως. Οι στόχοι μετατρέπονται σε απαιτήσεις ασφαλείας, οι οποίες με τη σειρά τους εφαρμόζονται στις λειτουργικές απαιτήσεις του οργανισμού με τη μορφή περιορισμών.

Η συγκεκριμένη μεθοδολογία δεν υποστηρίζεται από φορμαλιστικά μοντέλα ούτε και από εργαλεία λογισμικού.

3.8. Η Μεθοδολογία B-S

Οι Bellotti και Sellen (Bellotti, V. and Sellen, A. 1993) ανέπτυξαν τη μεθοδολογία B-S, σκοπός της οποίας είναι η εύρεση των απαιτήσεων ιδιωτικότητας στη φάση της σχεδίασης συστημάτων και συγκεκριμένα στα αρχικά στάδια της φάσης του καθορισμού των απαιτήσεων ενός οργανισμού.

Οι απαιτήσεις ιδιωτικότητας περιγράφονται στη μεθοδολογια B-S με τη μορφή κριτηρίων ιδιωτικότητας που θα πρέπει να ακολουθεί ο σχεδιαστής για να καθορίσει τις αδυναμίες του εκάστοτε οργανισμού προτείνοντας στη συνέχεια πιθανές λύσεις για την αντιμετώπιση των αδυναμιών.

Ο τρόπος εντοπισμού των απαιτήσεων ιδιωτικότητας στη B-S είναι ο ακόλουθος. Οι σχεδιαστές αξιολογούν τον εκάστοτε οργανισμό βάσει της λίστας κριτήριων ιδιωτικότητας που ορίζει η μεθοδολογία. Η μεθοδολογία ορίζει επίσης μια σειρά ερωτήσεων που μπορεί να κάνει ο σχεδιαστής στο προσωπικό του οργανισμού, ώστε να μπορέσει ευκολότερα να αποτυπώσει και να αξιολογήσει την κατάσταση του οργανισμού. Αφού ληφθούν οι απαντήσεις, καταγράφονται οι αδυναμίες του οργανισμού και αποφασίζει ο σχεδιαστής τον τρόπο αναπαράστασής τους. Οι Hong, Lederer και Landay (Hong, J., Ng, J., Lederer, S. and Landey, J. 2004) πρότειναν μια μεθοδολογία με την ίδια λογική με αυτή των Bellotti και Sellen, αυξάνοντας και βελτιώνοντας τις ερωτήσεις που τίθενται, καθώς και τη λίστα κριτηρίων με βάση τα οποία προτείνονται οι πιθανές λύσεις.

Η μεθοδολογία B-S αναφέρεται στα αρχικά στάδια του καθορισμού απαιτήσεων ιδιωτικότητας. Δεν υποστηρίζεται φορμαλιστικά αλλά ούτε και προσφέρεται κάποια μορφή καθοδήγησης με τη βοήθεια εργαλείων λογισμικού.

3.9. Η Μεθοδολογία STRAP

Η μεθοδολογία STRAP (STRuctured Analysis of Privacy) (Jensen, C., Tullio, J., Potts, C. and Mynatt, E. 2005) αναπτύχθηκε με σκοπό την εύρεση και ανάλυση των απαιτήσεων ιδιωτικότητας στη φάση της σχεδίασης ενός συστήματος. Χαρακτηριστικό της συγκεκριμένης μεθοδολογίας είναι η χρήση διαφόρων τεχνικών, από το χώρο της σχεδίασης και της ασφάλειας συστημάτων.

Οι απαιτήσεις ιδιωτικότητας στη STRAP αναπαρίστανται με τη μορφή αδυναμιών. Η STRAP χρησιμοποιεί την έννοια του στόχου για την αποτύπωση των λειτουργικών απαιτήσεων του οργανισμού. Στο μοντέλο των στόχων που δημιουργείται αποτυπώνονται οι αδυναμίες με τη μορφή εμποδίων ανάμεσα στους στόχους και στους υπό-στόχους.

Ο τρόπος λειτουργίας της μεθοδολογίας αναλύεται στα ακόλουθα βήματα: α) Ανάλυση (Analysis) β) Επαναπροσδιορισμός (Refinement) γ) Αξιολόγηση (Evaluation) και δ) Επανάληψη (Iteration).Ο τρόπος που ακολουθεί η μεθοδολογία για τον εντοπισμό και την αποτύπωση των απαιτήσεων ιδιωτικότητας είναι ο ακόλουθος. Κατά τη φάση της ανάλυσης, αρχικά πραγματοποιείται ανάλυση στόχων του συστήματος. Αποτέλεσμα αυτής της ανάλυσης είναι η αναγνώριση των στόχων, ενεργών οντοτήτων, καθώς και των βασικών συστατικών του συστήματος. Επίσης, συγκεντρώνονται πληροφορίες σχετικές με το περιεχόμενο του υπό-ανάπτυξη συστήματος και καταγράφονται οι

πρώτες απαιτήσεις σχετικά με την διαφύλαξη της ιδιωτικότητας. Όπως και στη B-S, έτσι και εδώ λαμβάνουν χώρα ερωτήσεις για κάθε στόχο και υπό-στόχο που δημιουργήθηκαν από την ανάλυση στόχων. Ως αποτέλεσμα των ερωτήσεων αναγνωρίζονται τυχόν αδυναμίες του συστήματος σε σχέση με την προστασία της ιδιωτικότητας σε αυτό. Οι αδυναμίες καταγράφονται στο διάγραμμα των στόχων με τη μορφή εμποδίων ανάμεσα στους στόχους και στους υπό-στόχους. Επιπλέον, κατηγοριοποιούνται οι αδυναμίες με βάση τις βέλτιστες πρακτικές χρήσης υπηρεσιών πληροφορικής (Fair Information Practices) (Welfare, US Department of Health Education and 1973), αφού διεξαχθεί ανάλυση για εξάλειψη επαναλαμβανόμενων καταγραφών ιδίων αδυναμιών, ώστε να προταθεί πιο εύκολα αντίστοιχη λύση.

Στη φάση του επαναπροσδιορισμού λαμβάνεται η απόφαση εξάλειψης και μείωσης αδυναμιών, οι οποίες, αν και αναγνωρίστηκαν, έχουν λύσεις τόσο απλές που δεν απαιτείται να συνεχίσουν να απασχολούν τους σχεδιαστές. Για τις αδυναμίες αυτές, καταγράφονται οι λύσεις υλοποίησής τους και διαγράφονται από τη λίστα αδυναμιών του συστήματος. Ένας άλλος λόγος εξάλειψης αδυναμιών είναι η αλλαγή της δομής των στόχων.

Στην επόμενη φάση της αξιολόγησης, αξιολογούνται τα διάφορα προτεινόμενα σενάρια σχεδίασης του συστήματος. Κατά τη φάση της σχεδίασης διάφοροι σχεδιαστές/αναλυτές δημιουργούν και προτείνουν ποικίλους τρόπους σχεδίασης για το υπό-ανάπτυξη σύστημα. Στη φάση αυτή πραγματοποιείται η αξιολόγηση των προτάσεων αυτών με βάση κάποια κριτήρια. Πρώτα αξιολογείται ο τρόπος που κάθε πρόταση αναφέρει για την αντιμετώπιση των αδυναμιών του συστήματος. Το σενάριο που μειώνει περισσότερο το βαθμό επικινδυνότητας, διασφαλίζοντας όσο γίνεται καλύτερα την ιδιωτικότητα, θεωρείται ως

αποδοτικότερο σε σχέση με τα άλλα σενάρια. Η STRAP προτείνει μια σειρά από κριτήρια που καθοδηγούν την όλη φάση της αξιολόγησης.

Ακολούθως, στη φάση της επανάληψης, επαναλαμβάνονται τα προηγούμενα βήματα για να μελετηθεί εκ νέου η σχεδίαση του συστήματος συμπεριλαμβανομένων και των όποιων αλλαγών έλαβαν χώρα προηγουμένως. Μελετάται εκ νέου η δομή των στόχων, γίνονται οι απαραίτητες αλλαγές, επαναπροσδιορίζονται οι αδυναμίες, αξιολογούνται τα νέα σενάρια μείωσης της επικινδυνότητας κ.λπ. Η φάση της επανάληψης ολοκληρώνεται όταν δεν υπάρχουν πλέον αλλαγές/βελτιώσεις στις προηγούμενες τρεις φάσεις.

Η STRAP δεν υποστηρίζει φορμαλιστικά μοντέλα. Επίσης, δεν έχει αναπτυχθεί κάποιο εργαλείο λογισμικού για την καθοδήγηση των σχεδιαστών και για την γραφική αναπαράσταση των μοντέλων της μεθοδολογίας.

3.10. Ανάλυση Μεθοδολογιών

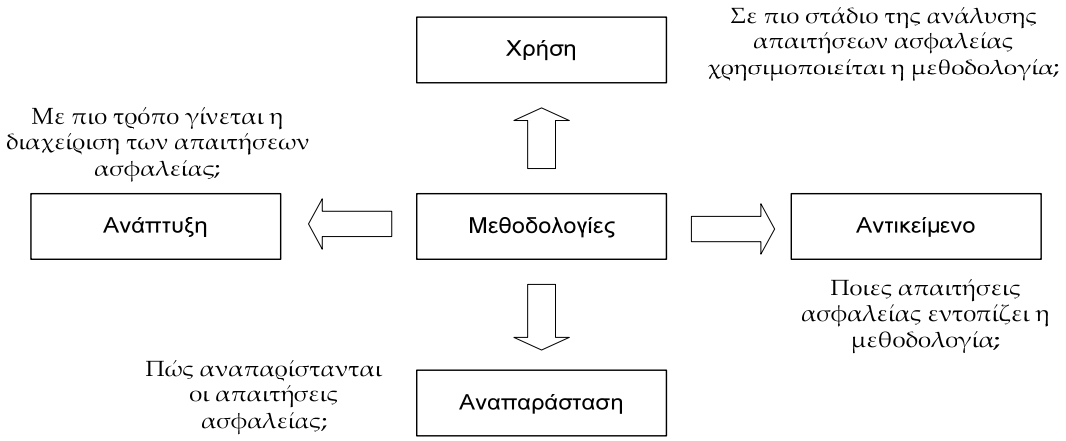
3.10.1. Μεθοδολογικό Πλαίσιο Σύγκρισης

Στην παρούσα ενότητα αναλύονται οι προαναφερθείσες μεθοδολογίες, με σκοπό την ανάδειξη των χαρακτηριστικών τους όσον αφορά στη σχεδίαση και υλοποίηση των απαιτήσεων της ασφάλειας και ιδιωτικότητας σε ένα σύστημα.

Για το σκοπό της ανάλυσης χρησιμοποιήθηκε ένα πλαίσιο το οποίο εξετάζει τις μεθοδολογίες υπό τέσσερις οπτικές, οι οποίες βασίζονται στις τέσσερις βασικές παραμέτρους που συμμετέχουν στη σχεδίαση συστημάτων:

- *Χρήση:* Σε πιο στάδιο της ανάλυσης απαιτήσεων ασφαλείας χρησιμοποιείται η μεθοδολογία;
- *Αντικείμενο:* Ποιες απαιτήσεις ασφαλείας εντοπίζει η μεθοδολογία;
- *Αναπαράσταση:* Πώς αναπαρίστανται οι απαιτήσεις ασφαλείας;
- *Ανάπτυξη:* Με πιο τρόπο γίνεται η διαχείριση των απαιτήσεων ασφαλείας;

Διαγραμματικά το πλαίσιο απεικονίζεται στο Σχήμα 3.1.



Σχήμα 3.1. Πλαίσιο Σύγκρισης Μεθοδολογιών

Κάθε πλευρά αναλύεται σε περαιτέρω κριτήρια. Συγκεκριμένα, στην κατηγορία της χρήσης εξετάζονται τα ακόλουθα κριτήρια: α) Προσδιορισμός των απαιτήσεων ασφαλείας, β) Διαχείριση απαιτήσεων ασφαλείας, γ) Παραγωγή πολιτικών συστήματος. Αναλυτικότερα, οι μεθοδολογίες εξετάζονται για τη χρήση ή μη μεθόδων προσδιορισμού των απαιτήσεων ασφαλείας, κατά πόσο καθορίζουν και επαληθεύουν τις απαιτήσεις αυτές, καθώς και αν καθορίζονται πολιτικές ασφαλείας από τις απαιτήσεις αυτές.

Στη δεύτερη κατηγορία εξετάζεται το αντικείμενο των μεθοδολογιών υπό τα ακόλουθα κριτήρια: α) Απαιτήσεις ασφαλείας του οργανισμού, β) Πολιτικές συστήματος. Πολλές μεθοδολογίες έχουν ως

αντικείμενο μόνο τον προσδιορισμό των απαιτήσεων ασφαλείας και ιδιωτικότητας. Άλλες, όμως, προχωρούν και στον καθορισμό πολιτικών ασφαλείας.

Η κατηγορία της αναπαράστασης εξετάζει τον τρόπο με τον οποίο εκφράζονται τα ζητήματα ασφαλείας. Συνήθως υπάρχουν δύο τρόποι αναπαράστασης: η διαγραμματική και η φορμαλιστική. Από αυτούς τους τρόπους προκύπτουν και τα κριτήρια της κατηγορίας αυτής: διαγραμματική αναπαράσταση, φορμαλιστική γλώσσα.

Η κατηγορία της ανάπτυξης εξετάζει τον τρόπο με τον οποίο τα ζητήματα ασφαλείας αναπτύσσονται και χρησιμοποιούνται. Εξετάζεται η ύπαρξη εργαλείων μοντελοποίησης, καθώς και η παροχή καθοδήγησης για την όλη διαδικασία μοντελοποίησης. Τα κριτήρια της κατηγορίας αυτής είναι: α) καθοδήγηση και β) εργαλεία.

3.10.2. Ανάλυση

Αναφορικά με τη κατηγορία «χρήση» του πλαισίου σύγκρισης, συνάγεται ότι η πλειονότητα των μεθοδολογιών επικεντρώνεται στη διαχείριση των απαιτήσεων ασφαλείας, π.χ. ενδιαφέρονται για τον τρόπο καθορισμού και επικύρωσης των απαιτήσεων. Ωστόσο, λίγες είναι αυτές που παρέχουν ένα δομημένο τρόπο εύρεσης των απαιτήσεων ασφαλείας από διάφορες πηγές (π.χ. από τους υπεύθυνους του οργανισμού, τα έγγραφα του οργανισμού, κ.λπ.). Επίσης, λίγες μεθοδολογίες υλοποιούν έναν τρόπο μετάφρασης των απαιτήσεων ασφαλείας σε πολιτικές ασφαλείας του συστήματος. Συγκεκριμένα, η μεθοδολογία *i** και η M-N υποστηρίζουν την εύρεση και διαχείριση των απαιτήσεων ασφαλείας, αλλά δεν προτείνουν έναν τρόπο μετάφρασης των απαιτήσεων αυτών σε αντίστοιχες πολιτικές ασφαλείας. Η μέθοδος GBRAM είναι η μόνη που καλύπτει και τα τρία κριτήρια. Η RBAC επικεντρώνεται στον καθορισμό

των πολιτικών ασφαλείας χωρίς να περιγράφει σαφείς μεθόδους εύρεσης και διαχείρισης των απαιτήσεων ασφαλείας.

Αναφορικά με την κατηγορία «αντικείμενο», σχεδόν όλες οι μεθοδολογίες, με εξαίρεση τη GBRAM και τη RBAC, επικεντρώνονται μόνο στις απαιτήσεις ασφαλείας. Η GBRAM, ως επόμενο βήμα, καθορίζει πολιτικές προερχόμενες από τις απαιτήσεις, ενώ το αντικείμενο της RBAC είναι ο καθορισμός των πολιτικών ασφαλείας. Ωστόσο, η αναγνώριση ρόλων που χρησιμοποιεί η RBAC προέρχεται από το χώρο του καθορισμού απαιτήσεων.

Αναφορικά με την κατηγορία «αναπαράσταση», οι περισσότερες από τις προαναφερθείσες μεθοδολογίες χρησιμοποιούν ένα γραφικό τρόπο αναπαράστασης των μοντέλων τους. Οι μεθοδολογίες NFR, *i**, KAOS, και Tropos, χρησιμοποιούν τεχνολογίες διαγραμματικής τεχνικής ανάλυσης για να εκφράσουν τις σχέσεις των στόχων με τους υπό-στόχους. Πέραν της διαγραμματικής αναπαράστασης, κάποιες από τις μεθοδολογίες χρησιμοποιούν και μια φορμαλιστική γλώσσα με σκοπό τη φορμαλιστική έκφραση των μοντέλων τους. Οι NFR και *i** χρησιμοποιούν τη γλώσσα Telos. Η Tropos χρησιμοποιεί τη γλώσσα Formal Tropos, η οποία ορίζει έναν τρόπο αναπαράστασης με τη χρήση κειμένου για την περιγραφή των μοντέλων της. Η μεθοδολογία M-N, καθώς και η GBRAM, δε χρησιμοποιούν ούτε διαγραμματική ούτε φορμαλιστική αναπαράσταση για τα μοντέλα τους. Η M-N χρησιμοποιεί μία ανεπίσημη προσέγγιση με τη χρήση κειμένου για την αναπαράσταση των μοντέλων του. Η GBRAM ορίζει πίνακες, όπου κάθε στόχος συνδυάζεται με έναν αριθμό εμποδίων που εμποδίζουν την υλοποίησή του και μία σειρά σεναρίων για την επίλυση των εμποδίων αυτών. Η RBAC δε χρησιμοποιεί, επίσης, κανέναν από τους προαναφερθέντες τρόπους αναπαράστασης. Λογικές εκφράσεις χρησιμοποιούνται μόνο για τη μοντελοποίηση των συνθηκών των πολιτικών ασφαλείας του συστήματος.

Αναφορικά με την κατηγορία «ανάπτυξη», οι περισσότερες μεθοδολογίες χρησιμοποιούν εργαλεία μοντελοποίησης για να βοηθήσουν τον υπεύθυνο υλοποίησης του συστήματος να αποτυπώσει τα παραγόμενα μοντέλα. Συγκεκριμένα, το NFR Assistant, το *i** Organizational Modeling Environment, το graphical Tropos και το KAOS Observier είναι εργαλεία ανάπτυξης των αντίστοιχων μεθοδολογιών. Ενώ αυτά τα εργαλεία βοηθούν τον υπεύθυνο υλοποίησης στην ορθή δημιουργία των μοντέλων των απαιτήσεων ασφαλείας, δεν του προσφέρουν αρκετή καθοδήγηση ώστε να ξεπερνά τυχόν προβλήματα κατά τη φάση της δημιουργίας των μοντέλων. Οι μεθοδολογίες M-N, GBRAM και RBAC, δεν παρέχουν εργαλεία μοντελοποίησης, αλλά προσφέρουν, σε ικανοποιητικό βαθμό, καθοδήγηση, με κανόνες και διαδικασίες, για τα μοντέλα τους. Η καθοδήγηση βοηθά τον υπεύθυνο υλοποίησης να αντεπεξέλθει σε προβλήματα, όπως ασυμβατότητες μεταξύ των στόχων ασφαλείας ή αλλαγές στα μοντέλα των απαιτήσεων.

Η μεθοδολογία B-S, καθώς και η επέκτασή της από τους Hong et.al είναι πολύ εύκολες στη χρήση, έχουν χαμηλό κόστος εφαρμογής και δεν απαιτούν πολύ χρόνο για την εφαρμογή τους. Παρόλα αυτά υπάρχουν αρκετά μειονεκτήματα. Αρχικά, δεν προτείνουν κανέναν τρόπο εύρεσης τεχνολογιών για την υλοποίηση των απαιτήσεων ασφαλείας. Υπάρχει κενό μεταξύ της σχεδίασης και της υλοποίησης, μιας και δεν υπάρχει κανένας τρόπος καθοδήγησης στην υλοποίηση των απαιτήσεων ασφαλείας. Επίσης, οι μεθοδολογίες αυτές, παράγουν ένα στατικό σύνολο απαιτήσεων και αφήνουν στο σχεδιαστή τη διαδικασία του επαναπροσδιορισμού των απαιτήσεων, μιας και συμπεριλαμβάνουν τη φάση της επανάληψης στην όλη διαδικασία του σχεδιασμού.

Σύμφωνα με τα μειονεκτήματα αυτά, οι παραπάνω μεθοδολογίες είναι πιθανότερο να εφαρμοστούν μία φορά στο τέλος της φάσης της σχεδίασης, όπου η φάση της επανάληψης δεν είναι ζωτικής σημασίας. Η

STRAP συνδυάζει επιτυχώς τεχνικές ανάλυσης στόχων και σημασιολογικές τεχνικές για την εύρεση απαιτήσεων ιδιωτικότητας. Το βασικό της μειονέκτημα είναι ότι δεν υπάρχει σύνδεση μεταξύ των φάσεων της σχεδίασης και της υλοποίησης, με αποτέλεσμα να μην προτείνονται τεχνολογίες υλοποίησης των απαιτήσεων ιδιωτικότητας που αναγνωρίστηκαν στη φάση της σχεδίασης.

Στον Πίνακα 3.1 παρουσιάζονται συνοπτικά τα αποτελέσματα της προαναφερθείσας ανάλυσης.

Πίνακας 3.1. Σύγκριση Μεθοδολογιών Απαιτήσεων Ασφαλείας

		NFR	*i**	Tropos	KAOS	M-N	GBRAM	RBAC	B-S	STRAP
ΧΡΗΣΗ	Προσδιορισμός των ΑΑ		✓	✓		✓	✓		✓	✓
	Διαχείριση ΑΑ	✓	✓	✓	✓	✓	✓		✓	✓
	Παραγωγή πολιτικών συστήματος						✓	✓		
ΑΝΤΙΚΕΙ ΜΕ-ΝΟ	ΑΑ του οργανισμού	✓	✓	✓	✓	✓	✓		✓	✓
	Πολιτικές Συστήματος						✓	✓		
ΑΝΑΠΑΡΑ-ΣΤΑΣΗ	Διαγραμματική Αναπαράσταση	✓	✓	✓	✓					
	Φορμαλιστική Αναπαράσταση	✓	✓	✓	✓					
ΑΝΑΠΤ Υ-ΞΗ	Καθοδήγηση					✓	✓	✓	✓	✓
	Εργαλεία	✓	✓	✓	✓					

3.11. Συμπεράσματα

Στο κεφάλαιο αυτό περιγράφηκαν οι βασικές μεθοδολογίες από το χώρο της σχεδίασης συστημάτων. Επιλέχθηκαν οι συγκεκριμένες μεθοδολογίες διότι σε σχέση με άλλες μεθοδολογίες σχεδίασης και ανάλυσης απαιτήσεων, ενσωματώνουν κατάλληλες έννοιες για τη σαφή αναπαράσταση διαφόρων απαιτήσεων ασφαλείας, ενώ μελετούν επίσης και το τρόπο που οι απαιτήσεις αυτές μεταφράζονται σε συγκεκριμένες πολιτικές για το υπό ανάπτυξη σύστημα. Στις παραγράφους 3.1-3.9 περιγράφονται οι μεθοδολογίες αυτές. Στη παράγραφο 3.10 παρουσιάζεται ένα μεθοδολογικό πλαίσιο σύγκρισης, τα αποτελέσματα του οποίου αναλύονται στην ίδια παράγραφο.

Όπως παρουσιάστηκε και στην ανάλυση της σύγκρισης των μεθοδολογιών, συμπεραίνεται ότι τα ζητήματα ασφαλείας και ιδιωτικότητας δεν λαμβάνονται υπόψη εξίσου σε όλες τις φάσεις τις σχεδίασης συστημάτων. Οι περισσότερες μεθοδολογίες δεν προχωρούν την ανάλυσή τους μέχρι το επίπεδο της υλοποίησης, με αποτέλεσμα να μη παρέχεται σωστή καθοδήγηση στον υπεύθυνο υλοποίησης του συστήματος. Οι απαιτήσεις ασφαλείας και ιδιωτικότητας πρέπει να αναλύονται εκτενώς κατά τη σχεδίαση, ώστε όποιες αδυναμίες και αν υπάρξουν, να λυθούν σε αυτή τη φάση και όχι στην υλοποίηση, όπου θα απαιτηθεί και περισσότερος χρόνος και περισσότερο κόστος για τον επανασχεδιασμό του συστήματος και τη λύση των αδυναμιών του. Διαφαίνεται λοιπόν η ανάγκη ύπαρξης μιας μεθοδολογίας που θα αντιμετωπίζει ξεχωριστά τις απαιτήσεις ιδιωτικότητας κατά τη φάση της σχεδίασης του συστήματος.

Στο επόμενο κεφάλαιο περιγράφονται οι τεχνολογίες ενίσχυσης της ιδιωτικότητας που χρησιμοποιούνται από τους υπεύθυνους υλοποίησης συστημάτων για την ικανοποίηση των απαιτήσεων ιδιωτικότητας.

4. Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας

Το κεφάλαιο αυτό περιγράφει μια σειρά από τεχνολογίες, αρχιτεκτονικές, πρωτόκολλα και εργαλεία (στο εξής θα αναφέρονται όλα μαζί ως «τεχνολογίες») τα οποία υποστηρίζουν την υλοποίηση των απαιτήσεων ιδιωτικότητας. Οι τεχνολογίες αυτές, όπως αναφέρεται παρακάτω, χρησιμοποιούνται από την προτεινόμενη μεθοδολογία ως πιθανές λύσεις ικανοποίησης των απαιτήσεων ιδιωτικότητας του εκάστοτε συστήματος που μελετάται.

Ανάλογα με τη λειτουργία τους εντάσσονται οι τεχνολογίες σε κατηγορίες. Αυτές είναι (Group, META 2005):

α) Διαχειριστικά Εργαλεία (Administrative Tools)

β) Πληροφοριακά Εργαλεία (Informational Tools)

γ) Προϊόντα, Υπηρεσίες και Αρχιτεκτονικές Ιδιωτικότητας (Privacy Products, Services and Architectures)

δ) Εργαλεία Ψευδωνυμίας (Pseudonymizer Tools)

ε) Εργαλεία διαγραφής ιχνών και αποδεικτικών (Track and Evidence Erasers)

στ) Εργαλεία Κρυπτογράφησης (Encryption Tools)

Ακολούθως, περιγράφονται τα βασικά χαρακτηριστικά των κατηγοριών αυτών, καθώς και οι τεχνολογίες που εντάσσονται σε κάθε μια.

4.1. Διαχειριστικά Εργαλεία

Στην κατηγορία αυτή εντάσσονται οι τεχνολογίες γενικού σκοπού, αλλά και οι τεχνολογίες ειδικού σκοπού για τη διαχείριση της ιδιωτικότητας σε έναν οργανισμό. Οι τεχνολογίες γενικού σκοπού υποστηρίζουν λειτουργίες που παρέχονται και από άλλες τεχνολογίες ασφάλειας (π.χ. η διαχείριση της ιδιωτικότητας παρέχεται και από το γενικό πρόγραμμα διαχείρισης της ασφάλειας ενός συστήματος). Οι τεχνολογίες ειδικού σκοπού καλύπτουν ειδικά τη διαχείριση της ιδιωτικότητας σε ένα οργανισμό και εγκαθίστανται και λειτουργούν ταυτόχρονα με ένα σύστημα διαχείρισης. Οι τεχνολογίες αυτές ανήκουν στην κατηγορία των τεχνολογιών ενίσχυσης της ιδιωτικότητας. Μερικές από τις πιο αντιπροσωπευτικές τεχνολογίες κάθε κατηγορίας παρουσιάζονται στις επόμενες ενότητες.

4.1.1. Διαχείριση Ταυτότητας (Identity Management)

Η συγκεκριμένη τεχνολογία δεν μπορεί να χαρακτηριστεί ως ενιαία τεχνολογία, αλλά ως συνδυασμός συνεργαζόμενων τεχνολογικών λύσεων. Η διαχείριση ταυτότητας μπορεί να υλοποιηθεί με ποικιλία εναλλακτικών τρόπων, οι οποίοι χρησιμοποιούνται είτε μεμονωμένα είτε σε συνδυασμό με σκοπό την προστασία της ιδιωτικότητας.

Η διαχείριση ταυτότητας θεωρείται τεχνολογία υποστήριξης της ιδιωτικότητας, αφού οι χρήστες που χρησιμοποιούν δικτυακές υπηρεσίες πρέπει να μπορούν να αποδείξουν την ταυτότητά τους για να αντιμετωπιστεί η παραβίαση της ιδιωτικότητας από άλλους χρήστες δια της επίτευξης μη εξουσιοδοτημένης πρόσβασης άλλων οντοτήτων σε δεδομένα του χρήστη.

Βασικό σκοπό των συστημάτων διαχείρισης ταυτότητας αποτελεί η απλοποίηση του χειρισμού των ταυτοτήτων του χρήστη, συνεχίζοντας όμως να προστατεύουν την ιδιωτικότητά του. Επομένως, οι τεχνολογίες που υποστηρίζουν τη διαχείριση ταυτότητας συχνά αποτελούν μέρος ενός ευρύτερου πλαισίου προστασίας της ιδιωτικότητας. Από τη στιγμή που το πλαίσιο αυτό θα δημιουργηθεί, ο χρήστης μπορεί να πιστοποιείται σε διάφορες υπηρεσίες μέσω διαφόρων τεχνικών προστατεύοντας έτσι την ταυτότητά του, ενδεχομένως δια της ανωνυμίας, διασφαλίζοντας την προστασία της ιδιωτικότητάς του.

4.1.2. Βιομετρία (Biometrics)

Ένας τρόπος αναγνώρισης της ταυτότητας των χρηστών είναι η χρήση βιομετρικών τεχνικών. Η διαδικασία της αναγνώρισης μπορεί να γίνει χωρίς την αποθήκευση των βιολογικών δεδομένων του χρήστη, αλλά με τη σύγκριση μιας κρυπτογραφημένης έκδοσης δεδομένων με το αποτέλεσμα του βιολογικού δεδομένου που θα δοθεί. Αν αυτά σχετίζονται μοναδικά, τότε επιτυγχάνεται η αναγνώριση του χρήστη ενώ ταυτόχρονα δεν παραβιάζεται η ιδιωτικότητά του, μιας και η όλη διαδικασία δε συνδέει το χρήστη με τα προσωπικά του δεδομένα.

4.1.3. Έξυπνες Κάρτες (Smart Cards)

Οι έξυπνες κάρτες χρησιμοποιούνται για την αναγνώριση των χρηστών συμπεριλαμβάνοντας τεχνικές κρυπτογραφίας είτε στη κάρτα είτε στον αναγνώστη. Παρόλα αυτά πρέπει να επισημανθεί ότι η όλη διαδικασία αναγνώρισης αφορά στην κάρτα και όχι στο χρήστη της. Από τη στιγμή που η κάρτα δεν περιέχει πληροφορίες που χαρακτηρίζουν

αυτόν που τη φέρει, μπορεί να χρησιμοποιηθεί για να υποστηρίξει την ανωνυμία των χρηστών.

4.1.4. Διαχείριση Δικαιωμάτων (Permission Management)

Η τεχνολογία αυτή συνδέεται με εκείνη της διαχείρισης ταυτότητας, διότι μία επιτυχημένη αναγνώριση του χρήστη συνοδεύεται και από τα αντίστοιχα δικαιώματα που θα του αποδοθούν. Συχνά τα δικαιώματα που θα έχει ένας χρήστης εξαρτώνται κυρίως από το ρόλο του χρήστη στο συγκεκριμένο σύστημα, παρά από τη ταυτότητα αυτού.

Διατηρώντας τα δικαιώματα ενός χρήστη ξεχωριστά από τα δεδομένα της ταυτότητάς του μπορεί να οδηγήσει στην προστασία της ιδιωτικότητάς του, αφού η διαδικασία της αναγνώρισης θα γίνεται σε διαφορετική στιγμή και σημείο (π.χ. σε διαφορετικό κόμβο του δικτύου) από αυτή της ανάθεσης των δικαιωμάτων.

4.1.5. Εργαλεία Παρακολούθησης και Ελέγχου (Monitoring and Audit Tools)

Εργαλεία διαχείρισης ελέγχου και παρακολούθησης της ασφάλειας των πληροφοριακών συστημάτων είναι ευρέως διαδεδομένα τα τελευταία χρόνια. Τα εργαλεία που χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο της ιδιωτικότητας συχνά καλύπτονται, λειτουργικά, από αντίστοιχα εργαλεία που μεριμνούν για την ασφάλεια του συστήματος. Παρόλα αυτά, τα εργαλεία ελέγχου και παρακολούθησης της ιδιωτικότητας μπορούν να χρησιμοποιηθούν για να καλύψουν επιπλέον απαιτήσεις ιδιωτικότητας.

4.2. Πληροφοριακά Εργαλεία

Οι ενέργειες της αύξησης της γνώσης ή της δημιουργίας πολιτικών ιδιωτικότητας και ο έλεγχος συμμόρφωσης με αυτές αποτελούν παθητικές μορφές προστασίας της ιδιωτικότητας. Παρόλα αυτά συχνά αποτελούν μέρος των ενεργειών ενός ευρύτερου πλαισίου για την προστασία της ιδιωτικότητας, το οποίο υποστηρίζει ότι οι ενέργειες προστασίας της ιδιωτικότητας απαιτούν δομημένες πολιτικές και αρχές στη φάση της σχεδίασης, της υλοποίησης καθώς και στη φάση της λειτουργίας όπου γίνονται και οι συχνοί έλεγχοι και ανασκοπήσεις για την επιβεβαίωση της συμμόρφωσης με τις αρχές του συστήματος.

Στην κατηγορία αυτή ανήκουν όλες οι τεχνολογίες που υποστηρίζουν τη δημιουργία και διαχείριση των πολιτικών[1] προστασίας καθώς και αυτές που υποστηρίζουν τον έλεγχο της συμμόρφωσης μεταξύ των αρχών, των πολιτικών και των υπηρεσιών-συστημάτων.

4.2.1. Γεννήτορες Πολιτικών Ιδιωτικότητας (Privacy Policy Generators)

Οι γεννήτορες πολιτικών ιδιωτικότητας είναι τεχνολογίες που χρησιμοποιούνται για να δημιουργούν πολιτικές προστασίας της ιδιωτικότητας. Τυπική περίπτωση αποτελεί η προσέγγιση, σύμφωνα με την οποία ο ίδιος ο χρήστης χρησιμοποιεί σχετική τεχνολογία για να ορίσει τις πολιτικές προστασίας της ιδιωτικότητάς του στο Διαδίκτυο, ώστε όταν επισκέπτεται διάφορες ιστοσελίδες να μπορεί να προσπελάσει

[1] Πολιτική ονομάζεται ένα σύνολο κανόνων που ορίζεται με σκοπό τη καθοδήγηση κατά τη διαδικασία λήψης αποφάσεων

μόνον αυτές που συμμορφώνονται με τις πολιτικές που έχει δηλώσει. Οι τεχνολογίες αυτές καλύπτουν έμμεσα τις απαιτήσεις ιδιωτικότητας.

4.2.2. Αναγνώστες/Επαληθευτές Πολιτικών Ιδιωτικότητας (Privacy Policy Readers/Validators)

Επιπλέον των εργαλείων δημιουργίας πολιτικών ιδιωτικότητας υπάρχουν και εργαλεία ανάγνωσης/ελέγχου των πολιτικών αυτών. Στο προαναφερόμενο παράδειγμα του Διαδικτύου, τα εργαλεία ελέγχουν τη συμβατότητα μεταξύ των πολιτικών της ιστοσελίδας και αυτών του χρήστη. Τα εργαλεία αυτά δεν θα αποφανθούν για το αν η σελίδα είναι επιτρεπτή για το χρήστη ή όχι, αλλά θα τον καθοδηγήσουν στη λήψη εκείνων των αποφάσεων που αφορούν την προστασία της ιδιωτικότητάς του. Για το λόγο αυτό, και τα συγκεκριμένα εργαλεία, όπως και τα προηγούμενα, δεν αποτελούν εργαλεία ενεργητικής προστασίας της ιδιωτικότητας.

4.2.3. Εξέταση Συμμόρφωσης με τις απαιτήσεις Ιδιωτικότητα (Privacy Compliance Scanning)

Οι τεχνολογίες της κατηγορίας αυτής χρησιμοποιούνται για να ελέγξουν αν η ισχύουσα πολιτική προστασίας της ιδιωτικότητας ενός οργανισμού υποστηρίζεται πραγματικά στις ίδιες τις εφαρμογές που προσφέρει. Για παράδειγμα, η ιστοσελίδα ενός οργανισμού μπορεί να εξεταστεί για να διαπιστωθεί αν ταιριάζει με τις πολιτικές προστασίας της ιδιωτικότητας του οργανισμού. Μετά, οι πολιτικές του χρήστη συγκρίνονται με αυτές του οργανισμού και, τελικά, αφού ενημερωθεί ο χρήστης αποφασίζει αν διακυβεύεται η ιδιωτικότητα του ή όχι και ανάλογα πράττει.

4.3. Προϊόντα, Υπηρεσίες και Αρχιτεκτονικές Ιδιωτικότητας

Στην κατηγορία αυτή ανήκουν τεχνολογίες που ως επί το πλείστον παρέχουν ανώνυμη πρόσβαση σε διάφορες υπηρεσίες και στο Διαδίκτυο. Κύριος στόχος των τεχνολογιών αυτών είναι να επιτρέπουν στο χρήστη να αποκτά πρόσβαση στις διάφορες υπηρεσίες χωρίς να αποκαλύπτει την πραγματική του ταυτότητα. Η διατήρηση της ανωνυμίας του χρήστη βασίζεται σε ένα σύνολο από συνεργαζόμενες τρίτες οντότητες, η επικοινωνία των οποίων υποστηρίζεται από μηχανισμούς κρυπτογραφίας έτσι ώστε να διατηρείται η ανωνυμία του χρήστη ακόμη και αν μία από αυτές αποκαλυφθεί σε κάποιο κακόβουλο χρήστη ή λογισμικό.

4.3.1. Ψευδώνυμα για την Περιήγηση στο Διαδίκτυο (Browsing Pseudonyms)

Κατά την περιήγησή του στο Διαδίκτυο, ο χρήστης αφήνει ίχνη σε κάθε σημείο που επισκέπτεται και ειδικά στα σημεία όπου υπάρχουν συσκευές για την παροχή της επικοινωνίας, εξυπηρετητές, ή άλλοι κεντρικοί κόμβοι. Τα ίχνη αυτά δεν ελέγχονται από καμία συγκεκριμένη αρχή και ο χρήστης δεν μπορεί να τα διαγράψει, διότι οι μηχανισμοί του Διαδικτύου βασίζονται σε αυτά για να παρέχουν τις διάφορες υπηρεσίες τους αλλά και για την επικοινωνία τους με το χρήστη.

Για το λόγο αυτό έχουν αναπτυχθεί διάφορες τεχνολογίες οι οποίες παρέχουν στους χρήστες «ψευδείς διευθύνσεις Διαδικτύου». Έτσι, οι χρήστες μπορούν να επισκέπτονται διάφορες ιστοσελίδες και να έχουν πρόσβαση σε διάφορες υπηρεσίες, δίχως να αποκαλύπτουν την πραγματική τους διεύθυνση.

4.3.2. Εικονικές Διευθύνσεις Ηλεκτρονικού Ταχυδρομείου (Virtual Email Addresses)

Το πρόβλημα που περιγράφηκε προηγουμένως για την περιήγηση στο Διαδίκτυο απαντάται και στην αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν ο χρήστης στέλνει ένα ηλεκτρονικό μήνυμα τα ίχνη του παραμένουν σε πολλούς ενεργούς κόμβους του Διαδικτύου και σε μερικούς από αυτούς διατηρείται αντίγραφο του μηνύματος μετά την προώθησή του. Για να αποσταλεί ένα μήνυμα ανώνυμα θα πρέπει να αλλάξει η διεύθυνση του αποστολέα ώστε να μην καταγράφεται η πραγματική. Επίσης, δεδομένα που αφορούν στην αποστολή και στη λήψη του μηνύματος θα πρέπει να είναι πλασματικά.

Για το σκοπό αυτό έχουν δημιουργηθεί διάφορες τεχνολογίες, οι οποίες προσφέρουν στο χρήστη εικονικές διευθύνσεις ηλεκτρονικού ταχυδρομείου, με διάφορες διαβαθμίσεις για την προστασία της ανωνυμίας, έτσι ώστε να μπορεί να επικοινωνεί μέσω ηλεκτρονικού ταχυδρομείου χωρίς να αποκαλύπτει την πραγματική του ταυτότητα.

4.3.3. Έμπιστες Τρίτες Οντότητες (Trusted Third Parties)

Η χρήση τρίτων έμπιστων οντοτήτων για την παράδοση ψηφιακών πιστοποιητικών και κλειδιών σε υπηρεσίες που χρησιμοποιούν Υποδομή Δημοσίου Κλειδιού είναι ευρέως γνωστή. Στην Υποδομή Δημοσίου Κλειδιού κάθε οντότητα κατέχει ένα ζεύγος κλειδιών (ένα ιδιωτικό και ένα δημόσιο). Με το δημόσιο κλειδί κρυπτογραφούνται τα δεδομένα που αποστέλλονται και τα οποία μπορούν να αποκρυπτογραφηθούν μόνο από το κάτοχο του ιδιωτικού κλειδιού. Έτσι, κάθε οντότητα που επιθυμεί να στείλει κάτι σε μια άλλη κρυπτογραφεί τα δεδομένα με το δημόσιο κλειδί της οντότητας-παραλήπτη και μόνο η τελευταία μπορεί να τα δει, αφού

κατέχει το αντίστοιχο ιδιωτικό κλειδί. Οι έμπιστες τρίτες οντότητες είναι υπεύθυνες για τη παραγωγή των κλειδιών στις οντότητες και για την προστασία των προσωπικών δεδομένων των οντοτήτων, μιας και εκείνες μόνο αποκαλύπτουν τα προσωπικά στοιχεία των κατόχων των κλειδιών. Παραδείγματα τρίτων έμπιστων οντοτήτων αποτελούν οι αρχές δήλωσης προσωπικών δεδομένων, οι αρχές πιστοποίησης, οι αρχές επικύρωσης, η συμβολαιογραφία καθώς και οι αρχές παροχής ανωνυμίας και ψευδωνυμίας.

4.3.4. Κλειδιά Αντικαταστάτες (Surrogate Keys)

Τα κλειδιά χρησιμοποιούνται σε μεγάλες βάσεις δεδομένων για να αντιστοιχούν πεδία με δεδομένα. Σε περίπτωση κλοπής των κλειδιών αυτών είναι ξεκάθαρο ότι τα δεδομένα των χρηστών τίθενται σε κίνδυνο με αποτέλεσμα να διακυβεύεται η προστασία της ιδιωτικότητάς τους. Για το λόγο αυτό έχει αναπτυχθεί μία σειρά από τεχνολογίες οι οποίες σκοπό έχουν να παράγουν κλειδιά-αντικαταστάτες. Τα κλειδιά αυτά αντικαθιστούν τα αρχικά κλειδιά που χρησιμοποιούνται για την αντιστοίχιση των πεδίων με τα ευαίσθητα δεδομένα που αποθηκεύονται σε αυτά. Έτσι προστατεύεται η ιδιωτικότητα των χρηστών αφού είναι πιο δύσκολο για κάποιον τρίτο να οδηγηθεί στα προσωπικά δεδομένα ενός χρήστη ακόμη και αν αποκαλύψει το κλειδί-αντικαταστάτη.

Τα κλειδιά αυτά χρησιμοποιούνται σε δεδομένα που περιγράφουν συναλλαγές πελατών και σκοπός τους είναι να ελαχιστοποιήσουν τον υπολογιστικό χρόνο που απαιτείται για να γίνει αντιστοίχηση των νέων δεδομένων με αυτά που υπάρχουν ήδη στη βάση για κάθε χρήστη. Επίσης, οι τεχνολογίες αυτές μπορούν να εμποδίσουν το συνδυασμό δεδομένων από διαφορετικές βάσεις αποτρέποντας έτσι το ενδεχόμενο παραβίασης της ιδιωτικότητας.

4.3.5. Τεχνολογία Crowds

Από τις αρχές του 1997 στα εργαστήρια AT&T άρχισε να εφαρμόζεται ένας νέος μηχανισμός, με το όνομα Crowds, για την προστασία της ανωνυμίας των χρηστών που επιθυμούν να υποβάλουν αιτήσεις στους εξυπηρετητές των δικτυακών χώρων (web servers) που επισκέπτονται και να λάβουν τις αντίστοιχες απαντήσεις. Η ονομασία του συστήματος οφείλεται στην ιδέα ότι η «ανάμιξη» ενός ατόμου σε ένα πλήθος προσφέρει δυνατότητες απόκρυψης των ενεργειών του στις ενέργειες των μελών του πλήθους. Με την ένταξή του στο πλήθος, ένα άτομο γίνεται απρόσωπο μέλος του (Reiter, M. and Rubin, A. 1999).

Η λειτουργία του Crowds ουσιαστικά βασίζεται, όπως αναφέρθηκε, στην ύπαρξη ενός συνόλου χρηστών, στο «πλήθος». Τα μέλη που έχουν ενταχθεί σε ένα πλήθος, εκπροσωπούνται σ' αυτό μέσω μιας διεργασίας που εκτελείται τοπικά στον υπολογιστή τους και αποκαλείται jondo –από το όνομα «John Doe» που εκφράζει την εικόνα ενός απρόσωπου συμμετόχου. Μόλις ο χρήστης εκκινήσει τη διεργασία jondo στον υπολογιστή του επιλέγει εκείνη ως το δικτυακό του πληρεξούσιο (web proxy) προσδιορίζοντας στον περιηγητή τη μηχανή και τον αριθμό θύρας της jondo ως τον πληρεξούσιο για όλες τις υπηρεσίες. Έτσι, κάθε αίτηση προερχόμενη από τον περιηγητή προωθείται απευθείας στη διεργασία jondo.

Με τη λειτουργία της jondo διεργασίας στη μηχανή του χρήστη και την ένταξή της στο πλήθος, ξεκινά η εγκαθίδρυση ενός τυχαίου μονοπατιού από jondos που εκτελούνται στις μηχανές άλλων μελών του πλήθους. Μέσω αυτού του πλήθους θα μεταφέρονται οι συναλλαγές των χρηστών τους προς και από τους επιθυμητούς εξυπηρετητές δικτυακών χώρων. Επακόλουθες αιτήσεις που ξεκινούν από την ίδια jondo, ακολουθούν το ίδιο μονοπάτι –εκτός ίσως αν πηγαίνουν σε διαφορετικό

τελικό εξυπηρετητή – και οι απαντήσεις του εξυπηρετητή διασχίζουν το ίδιο μονοπάτι όπως οι αιτήσεις, αλλά με αντίστροφη πορεία. Κάθε επικοινωνία στο μονοπάτι είναι κρυπτογραφημένη με ένα κλειδί μονοπατιού, το οποίο κατέχει κάθε jondo που βρίσκεται στο μονοπάτι (Reiter, M. and Rubin, A. 1998; Gritzalis, S. 2004).

4.3.6. Onion Routing

Το onion routing (Reed, M., Syverson, P. and Goldschlang, D. 1998; Goldschlang, D., Syverson, P. and Reed, M. 1999) είναι αρχιτεκτονική για υποστήριξη ιδιωτικής επικοινωνίας σε δημόσιο δίκτυο. Προσφέρει ανωνυμία σύνδεσης – απόκρυψη όχι μόνο του περιεχομένου της επικοινωνίας με κρυπτογράφησή του, αλλά και της ταυτότητας των μελών που επικοινωνούν – αντιμετωπίζοντας επιθέσεις «ωτακουστή» και ανάλυσης κίνησης[2] (traffic analysis). Οι ανώνυμες συνδέσεις που δημιουργούνται είναι αμφίδρομες, σχεδόν πραγματικού χρόνου και η κίνηση σ' αυτές γίνεται με ή χωρίς σύνδεση.

Η λειτουργία του Onion Routing στηρίζεται στη δυναμική δημιουργία ανώνυμων συνδέσεων μέσα από ένα δίκτυο μικτών Chaum (Chaum mixes) ή αλλιώς onion δρομολογητών, όπως ονομάζονται στην τεχνολογία αυτή, οι οποίοι συνδέονται με μεγάλης διάρκειας μόνιμες TCP συνδέσεις.

Ένας onion δρομολογητής (onion router) είναι ουσιαστικά μια συσκευή αποθήκευσης και προώθησης, η οποία δέχεται πλήθος μηνυμάτων σταθερού μεγέθους από διάφορες πηγές. Στα μηνύματα αυτά

[2] Ανάλυση κίνησης είναι η διαδικασία όπου κάποιος κακόβουλος χρήστης παρακολουθεί τα μηνύματα που διακινούνται σε ένα δίκτυο με στόχο την κλοπή ή/και παραποίησή τους

εκτελεί κρυπτογραφικές μετατροπές και στη συνέχεια τα προωθεί στον επόμενο προορισμό με τυχαία σειρά προκειμένου να μειωθεί η συσχέτιση από εισβολείς του δικτύου.

Το δίκτυο των onion δρομολογητών είναι κατανεμημένο, με ανοχή λαθών και πολλαπλά πεδία διαχείρισης, με τρόπο που ένα onion από μόνο του δεν μπορεί να διακόψει το δίκτυο ή να θέσει σε κίνδυνο την ιδιωτικότητα. Έτσι η συνεργασία μεταξύ κακόβουλων onion δρομολογητών είναι καταδικασμένη σε αποτυχία.

Μια ανώνυμη σύνδεση είναι ανεξάρτητη από πρωτόκολλο και περιλαμβάνει τρεις φάσεις:

1. Εγκαθίδρυση σύνδεσης, κατά την οποία ο εκκινητής στέλνει το onion με τις ιδιότητες της σύνδεσης χρησιμοποιώντας κρυπτογραφία δημόσιου κλειδιού, με χαμηλή επιβάρυνση. Σε αυτό το σημείο καθορίζεται αυστηρά και η διαδρομή.

2. Μεταφορά δεδομένων και στις δύο κατευθύνσεις, ώστε τα δεδομένα προ-κρυπτογραφούνται όπως έχει συμφωνηθεί κατά την εγκατάσταση και κάθε onion δρομολογητής αφαιρεί ένα επίπεδο κρυπτογράφησης.

3. Αποσύνδεση (connection tear-down)

4.3.7. Dc-Nets

Το δίκτυο Dc-Net (Chaum, D. 1985; Chaum, D. 1988) επιτρέπει στους χρήστες που συμμετέχουν σε αυτό να αποστέλλουν και να λαμβάνουν μηνύματα ανώνυμα μέσω οποιουδήποτε δικτύου και αν είναι συνδεδεμένοι. Μπορεί να χρησιμοποιηθεί για να προσφέρει απόλυτη ανωνυμία στον αποστολέα.

Η τεχνολογία αυτή βασίζεται στην τεχνική της «δυαδικής επιθετικής αποστολής» (binary superposed sending). Κάθε χρήστης-

σταθμός του δικτύου δημιουργεί τουλάχιστον ένα κλειδί-ψηφίο για κάθε ψηφίο του μηνύματος και στέλνει το κάθε κλειδί-ψηφίο σε έναν άλλο χρήστη-σταθμό του δικτύου μέσω ενός ασφαλούς καναλιού επικοινωνίας.

Για κάθε μία αποστολή ενός κλειδιού-ψηφίου, κάθε χρήστης-σταθμός προσθέτει το υπόλοιπο της διαίρεσης του ψηφίου με το 2 σε όλα τα κλειδιά-ψηφία που έχει καθώς και στα ψηφία του μηνύματος, εάν υπάρχει μήνυμα φυσικά. Οι χρήστες-σταθμοί που δεν επιθυμούν να στείλουν κάποιο μήνυμα αποστέλλουν μηδενικά αθροίζοντας τα σύνολα των δικών τους κλειδιών-ψηφίων που από τη στιγμή που δεν επιθυμούν να στείλουν κάτι είναι βεβαίως μηδέν. Τα σύνολα αυτά αποστέλλονται στο δίκτυο αφού προστεθεί πάλι το υπόλοιπο της διαίρεσης αυτών με το 2.

Το αποτέλεσμα μοιράζεται σε όλους τους χρήστες-σταθμούς του δικτύου και ισούται με το άθροισμα όλων των ψηφίων των μηνυμάτων. Αν ένας χρήστης-σταθμός στείλει ένα μήνυμα, το μήνυμα παραδίδεται επιτυχώς ως το αποτέλεσμα του συνολικού αθροίσματος ψηφίων για τον κάθε σταθμό.

4.3.8. Mix-Nets

Τα δίκτυα Mix-Nets (Chaum, D. 1981; Pfitzmann, A. and Waidner, M. 1987) χρησιμοποιούνται για τη διαφύλαξη της μη-συνδεσιμότητας του αποστολέα και του παραλήπτη, καθώς και της ανωνυμίας του αποστολέα έναντι του παραλήπτη και κατ' επιλογή για την ανωνυμία του παραλήπτη (Fischer-Hubner, S. 2001).

Ένα mix είναι ένας σταθμός δικτύου ο οποίος συλλέγει διάφορα μηνύματα ίσου μεγέθους από αποστολείς, απορρίπτει τα μηνύματα που έχει λάβει παραπάνω από μία φορές, αλλάζει την κωδικοποίησή τους και τα προωθεί στους παραλήπτες τους με διαφορετική σειρά από αυτή που τα παρέλαβε.

Χρησιμοποιώντας ένα μόνο mix ανάμεσα σε έναν αποστολέα και έναν παραλήπτη, ένας κακόβουλος χρήστης δεν μπορεί να καταλάβει πως ο συγκεκριμένος αποστολέας επικοινωνεί με το συγκεκριμένο παραλήπτη αλλά μπορεί να καταλάβει τη σχέση του αποστολέα με το mix όπως και τη σχέση του παραλήπτη με το mix. Για το λόγο αυτό, μία αλυσίδα από σταθμούς mix αυξάνουν την ασφάλεια της επικοινωνίας.

Χρησιμοποιώντας μία αλυσίδα από σταθμούς mix, ένας εισβολέας που έχει πρόσβαση σε όλες τις γραμμές επικοινωνίας μπορεί να εντοπίσει και να παρακολουθήσει ένα μήνυμα μέσα στο δίκτυο των σταθμών mix μόνο αν αυτός/ή έχει τη συνεργασία όλων των σταθμών από τους οποίους θα περάσει το μήνυμα ή μπορεί να παραβιάσει τους αλγόριθμους κρυπτογραφίας που εφαρμόζουν οι σταθμοί mix για να κρυπτογραφήσουν το μήνυμα.

4.3.9. Hordes

Το Hordes (Shields, C. and Levine, B. 2000) χρησιμοποιεί πολλαπλούς αντιπροσώπους ή εξουσιοδοτημένους εξυπηρετητές, παρόμοιους με εκείνους της τεχνολογίας Crowds, για να δρομολογεί ανώνυμα ένα πακέτο προς τον αποκρινόμενο, αλλά επιπλέον εφαρμόζει υπηρεσίες πολλαπλής δρομολόγησης ώστε να μεταφέρει την απάντηση ανώνυμα στον ιδρυτή. Τα αποτελέσματα κάποιων εφαρμογών, σχετικά με την απόδοση, έδειξαν ότι το Hordes έχει λίγη περισσότερη από τη μισή καθυστέρηση δρομολόγησης του Crowds, δεν απαιτεί μεγάλους πίνακες δρομολόγησης στους υπολογιστές, δεν είναι αντικείμενο παθητικών επιθέσεων ιχνηλάτησης, συχνά χρησιμοποιεί λιγότερες πηγές δικτύου και απαιτεί μικρότερο ποσό εργασίας από τις συνεργαζόμενες jondos.

Το Hordes έχει σχεδιαστεί ώστε να τοποθετεί πολλούς συμμετέχοντες στην ίδια ομάδα λήψης δεδομένων. Η χρήση πολλαπλής

δρομολόγησης για ανώνυμη παραλαβή προσφέρει ανωνυμία με πολλούς τρόπους. Καταρχήν, η IP διεύθυνση του προορισμού στα πακέτα απάντησης είναι η διεύθυνση της multicast ομάδας και όχι κάποιου υπολογιστή. Έπειτα, είναι δύσκολο να προσδιοριστεί το σύνολο των μελών της ομάδας. Ακόμα και αν αποκαλυφθούν τα μέλη ενός συνόλου, εξακολουθεί να υπάρχει ανωνυμία στο σύνολο παραλαβής.

Το Hordes χρησιμοποιεί τη multicast επικοινωνία για το αντίστροφο μονοπάτι μιας ανώνυμης σύνδεσης, αποκτώντας έτσι πολλά πλεονεκτήματα. Πρώτον, το σύνολο των μελών μιας ομάδας της πολλαπλής δρομολόγησης δεν είναι γνωστό σε καμία οντότητα, ενώ χρειάζεται η συνεργασία όλων των δρομολογητών του δέντρου για να προσδιοριστεί το σύνολο των παραληπτών. Έχει αποδειχτεί στο παρελθόν ότι είναι αδύνατον να επιτευχθεί μια τέτοια συνεργασία δια μήκους πολλαπλών πεδίων διαχείρισης. Δεύτερον, ακόμα και αν προσδιοριστούν τα μέλη μιας συγκεκριμένης multicast ομάδας, ο πραγματικός ιδρυτής μιας σύνδεσης παραμένει ακαθόριστος μέσα στην ομάδα, εκτός αν είναι το μόνο της μέλος. Πέραν της ανωνυμίας, το Hordes προσφέρει μη-συνδεσιμότητα μεταξύ του αποστολέα και του παραλήπτη. Παρόμοια τεχνολογία σε σχέση με το πρωτόκολλο Hordes είναι η τεχνολογία Anonymizer (Boyan, J. 1997).

4.3.10. GNUnet's Anonymity Protocol-GAP

Το πρωτόκολλο GAP δημιουργήθηκε για να υποστηρίξει την ασφαλή λειτουργία του δικτύου GNUnet. Το δίκτυο GNUnet είναι ένα ομότιμο δίκτυο που παρέχει ανεύρεση ομότιμων σταθμών, κρυπτογράφηση συνδέσμων μεταξύ των σταθμών, καθώς και ομαδοποίηση μηνυμάτων. Προτάθηκε από τους (Bennett, K. and Grothoff, C. 2003) και υποστηρίζει ανώνυμες συναλλαγές δεδομένων.

Στόχος του πρωτοκόλλου είναι η απόκρυψη της ταυτότητας του σταθμού που ξεκινά μία επικοινωνία με έναν παραλήπτη από όλους τους άλλους σταθμούς του δικτύου συμπεριλαμβανομένων και των δρομολογητών του δικτύου, ενεργών και παθητικών κακόβουλων σταθμών, καθώς ακόμη και του παραλήπτη που συμμετέχει στην επικοινωνία αυτή (Gritzalis, S. 2004).

Η επικοινωνία μεταξύ όλων των σταθμών του δικτύου είναι εμπιστευτική. Ένας σταθμός που δεν ανήκει στο δίκτυο δεν μπορεί να παρατηρήσει τα πραγματικά δεδομένα που «ταξιδεύουν» μέσα σε αυτό. Τα μηνύματα και τα δεδομένα δεν μπορούν να αναγνωρισθούν μιας και το πρωτόκολλο φροντίζει να προσθέτει στοιχεία στα μηνύματα έτσι ώστε όλα να είναι τα ίδια σε μέγεθος.

Η σημαντικότερη διαφορά του πρωτοκόλλου GAP σε σχέση με τις προαναφερόμενες τεχνολογίες που χρησιμοποιούν διάφορους ενδιάμεσους σταθμούς, είναι ότι οι δεύτερες πάντα πριν περάσουν στον επόμενο σταθμό επανεγγράφουν τον κώδικα που χρειάζεται, ενώ το GAP απλά καθορίζει μια διεύθυνση-επιστροφής άσχετη με αυτή του τρέχοντος κάθε φορά σταθμού με αποτέλεσμα το δίκτυο να μπορεί να επαναδρομολογεί δεδομένα με πιο αποτελεσματικό τρόπο.

Το μεγαλύτερο μειονέκτημα του πρωτοκόλλου GAP είναι ότι έχει δημιουργηθεί και παραμετροποιηθεί για να καλύπτει τις ανάγκες του δικτύου GNUnet.

4.3.11. Tor

Η αρχιτεκτονική Tor (Dingledine, R., Mathewson, N. and Syverson, P. 2004) βασίζεται στην αρχιτεκτονική onion routing που περιγράφηκε προηγουμένως. Ωστόσο, η αρχιτεκτονική Tor παρουσιάζει αρκετές βελτιώσεις σε σχέση με αυτή του onion routing. Πρωτίστως, η Tor

ικανοποιεί καλύτερα και ασφαλέστερα τον τρόπο προώθησης των μηνυμάτων του αποστολέα από σταθμό σε σταθμό χρησιμοποιώντας ένα δυναμικό τρόπο δημιουργίας του μονοπατιού μεταξύ των σταθμών, ενώ ο κάθε σταθμός διαπραγματεύεται κλειδιά για την κρυπτογράφηση των δεδομένων που ισχύουν μόνο μεταξύ αυτού και του επόμενου του. Άπαξ και διαγραφούν τα κλειδιά αυτά, οι σταθμοί δεν μπορούν να αποκρυπτογραφήσουν προηγούμενη κυκλοφορία δεδομένων, προστατεύοντας έτσι τα δεδομένα.

Επιπλέον, η αρχιτεκτονική Tor χρησιμοποιεί τη διεπαφή ενός συγκεκριμένου SOCKS[3] πληρεξουσίου επιτρέποντας στους χρήστες να μπορούν να χρησιμοποιούν τα περισσότερα TCP-προγράμματα χωρίς να κάνουν αλλαγές. Η Tor βελτιώνει την αποτελεσματικότητα και την ανωνυμία πολυπλέκοντας πολλές σειρές TCP πακέτων δεδομένων σε κάθε κύκλωμα επικοινωνίας ενώ το onion routing δημιουργεί ξεχωριστό κύκλωμα για κάθε αίτημα που γίνεται στο επίπεδο εφαρμογής του TCP. Αυτή η τεχνολογία έχει τη δυνατότητα ρύθμισης της κυκλοφορίας των πακέτων ώστε να αποφεύγεται η κυκλοφορία και ο συνωστισμός με αποτέλεσμα τη δημιουργία καθυστερήσεων στο δίκτυο. Συγκεκριμένα, οι σταθμοί που βρίσκονται στις άκρες του δικτύου ελέγχουν όλη την κυκλοφορία και διοχετεύουν τα πακέτα με τέτοιο ρυθμό ώστε να αποφεύγονται καθυστερήσεις και συνωστισμοί, κάτι που οι άλλες τεχνολογίες δεν το κάνουν.

Άλλο πλεονέκτημα της αρχιτεκτονικής Tor είναι ο έλεγχος ακεραιότητας από άκρο σε άκρο. Κάθε σταθμός του δικτύου έχει τη

[3] Το SOCKS είναι ένα πρωτόκολλο Διαδικτύου που επιτρέπει σε εφαρμογές πελάτη-εξυπηρετητή να χρησιμοποιούν με διαφάνεια υπηρεσίες που προσφέρονται από λογισμικά αναχωμάτων (firewalls)

δυνατότητα να αλλάξει τα δεδομένα πριν τα προωθήσει στον επόμενο. Η onion routing δεν έκανε κανένα έλεγχο ακεραιότητας των δεδομένων πριν τη μετάβαση στον επόμενο σταθμό. Η Tor ελέγχει την ακεραιότητα των δεδομένων όχι από σταθμό σε σταθμό αλλά τα δεδομένα που έλαβε ο πρώτος σταθμός της Tor με αυτά που εξάγει ο τελευταίος πριν παραδοθούν στον παραλήπτη.

Επιπλέον η Tor παρέχει ένα μηχανισμό με χρήση εξυπηρετητών «τοπολογικά» προστατευμένων για τη προστασία της ανωνυμίας του παραλήπτη που ανταποκρίνεται. Συγκεκριμένα, οι χρήστες που θα χρησιμοποιήσουν το δίκτυο διαπραγματεύονται ένα σημείο συνάντησης από όπου και συνδέονται με κρυφούς εξυπηρετητές προσφέροντας μεγαλύτερη ασφάλεια και προστασία της ιδιωτικότητας των χρηστών. Ενώ στην αρχιτεκτονική onion routing περιλαμβάνονται τα «απαντητικά onions» που μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός κυκλώματος επικοινωνίας με έναν κρυφό εξυπηρετητή, τα onions αυτά δεν προσέφεραν ασφάλεια στην προώθηση μηνυμάτων και αχρηστεύονταν όταν ένας από τους σταθμούς στο μονοπάτι του κυκλώματος κατέρρεε ή άλλαζε κλειδιά. Στην αρχιτεκτονική Tor τα απαντητικά onion δεν απαιτούνται πλέον.

4.4. Εργαλεία Ψευδωνυμίας

Οι τεχνολογίες που ανήκουν στην κατηγορία αυτή είναι εργαλεία τα οποία χρησιμοποιούνται σε συνδυασμό με άλλες διαδικτυακές εφαρμογές. Συνήθως έχουν ρόλο πρόσθετου χαρακτηριστικού στις εφαρμογές αυτές φροντίζοντας για την προστασία της ιδιωτικότητας των χρηστών.

Βασική υπηρεσία των εργαλείων αυτών είναι η ψευδωνυμία. Συνήθως αυτό επιτυγχάνεται με αντικατάσταση του πραγματικού

ονόματος του χρήστη με μια ουδέτερη μοναδική ταυτότητα που χρησιμοποιείται για μια συγκεκριμένη συναλλαγή.

Στο χώρο των βάσεων δεδομένων υπάρχουν πεδία τα οποία περιέχουν ευαίσθητα προσωπικά δεδομένα. Στην ενότητα αυτή παρουσιάζονται εργαλεία τα οποία επαναδημιουργούν τις βάσεις αυτές χρησιμοποιώντας κλειδιά για να συνδέσουν διάφορους πίνακες και πεδία δεδομένων καταφέρνοντας έτσι να προστατέψουν τα προσωπικά δεδομένα των χρηστών. Τα κλειδιά, όπως και οι ουδέτερες μοναδικές ταυτότητες, είναι ένας άλλος τρόπος προστασίας της ιδιωτικότητας.

4.4.1. CRM Personalization

Μια σειρά από εργαλεία προσφέρονται για την προστασία της ανωνυμίας των χρηστών του Διαδικτύου κυρίως αυτών που χρησιμοποιούν το Διαδίκτυο για την πραγματοποίηση αγορών και τη χρήση συναφών υπηρεσιών. Τα περισσότερα από αυτά τα εργαλεία ανήκουν σε μια ευρύτερη ομάδα εργαλείων που ονομάζεται Customer Relationship Management.

Η κατηγορία αυτή περιλαμβάνει τεχνολογίες που υλοποιούν ανώνυμες συναλλαγές μεταξύ των πελατών και των διαδικτυακών καταστημάτων. Επίσης παρέχουν λύσεις όπως δημιουργία προφίλ των πελατών στα διάφορα καταστήματα βάση των προτιμήσεών τους χωρίς τα ίδια τα καταστήματα να μπορούν να ξέρουν ποιος πραγματικά είναι ο πελάτης και τα προσωπικά δεδομένα αυτού.

4.4.2. Διαχείριση Δεδομένων Εφαρμογών (Application Data Management)

Πολλές εφαρμογές δημιουργούνται στηριζόμενες σε βάσεις δεδομένων με τις οποίες συνδέονται μέσω ενός πεδίου-κλειδιού το οποίο περιέχει μοναδικό αναγνωριστικό για κάθε χρήστη της βάσης. Αυτή η λογική σχεδιασμού συστημάτων μπορεί να αποβεί πολύ επικίνδυνη για την ιδιωτικότητα των χρηστών μιας και κάθε φορά που γίνεται εισαγωγή ή εξαγωγή δεδομένων, αυτά πρέπει να συνοδεύονται και από την ταυτότητα του χρήστη ώστε να υπάρχει επιβεβαίωση ότι μεταφέρονται τα σωστά δεδομένα. Στις περιπτώσεις αυτές το πεδίο που περιέχει το αναγνωριστικό του χρήστη μπορεί να αντικατασταθεί από διάφορα άλλα κλειδιά τα οποία θα συνδέουν τους διάφορους πίνακες δεδομένων μεταξύ των εφαρμογών και των βάσεων χωρίς να αναφέρονται πουθενά τα αναγνωριστικά στοιχεία του χρήστη.

Κάποια εργαλεία προσφέρουν υπηρεσίες αντικατάστασης των αναγνωριστικών των χρηστών με τυχαία κλειδιά επιτυγχάνοντας έτσι διαλειτουργικότητα μεταξύ των εφαρμογών χωρίς τον κίνδυνο της αποκάλυψης προσωπικών δεδομένων των χρηστών κατά τη διάρκεια της ανταλλαγής δεδομένων.

Η διαχείριση δεδομένων εφαρμογών χρησιμοποιεί κλειδιά αντικαταστάτες (όπως περιγράφηκαν στην ενότητα 4.3.4). Ο στόχος όμως της συγκεκριμένης κατηγορίας εκτός από τη προστασία της μη-συνδεσιμότητας είναι και η προστασία της ψευδωνυμίας μιας και οι τεχνολογίες που ανήκουν στη συγκεκριμένη κατηγορία επικεντρώνονται στη διαχείριση των δεδομένων κατά την έξοδό τους από τη βάση.

4.5. Εργαλεία Διαγραφής Ιχνών και Αποδεικτικών

Όταν οι χρήστες επικοινωνούν ή χρησιμοποιούν υπηρεσίες μέσω του Διαδικτύου πάντοτε αφήνουν ίχνη των δραστηριοτήτων τους σε διάφορα σημεία κατά μήκος της ψηφιακής τους διαδρομής. Κάποια από αυτά τα ίχνη αποθηκεύονται για καθαρά διαχειριστικούς λόγους (π.χ. χρεώσεις), ενώ άλλα αποθηκεύονται με σκοπό την εξυπηρέτηση του χρήστη ή του παρόχου υπηρεσιών Διαδικτύου του χρήστη.

Στην κατηγορία των εργαλείων διαγραφής ιχνών και αποδεικτικών ανήκουν εργαλεία τα οποία εξυπηρετούν και τους χρήστες αλλά και τους παρόχους και σκοπό έχουν τη διαγραφή των ιχνών και του ιστορικού των δραστηριοτήτων τους. Τα εργαλεία αυτά συνήθως δεν θεωρούνται τεχνολογίες που ενισχύουν την ιδιωτικότητα, μπορούν όμως να χρησιμοποιηθούν σε συνδυασμό με άλλες τεχνολογίες και να προστατεύσουν την ιδιωτικότητα των χρηστών.

4.5.1. Εύρεση και Απομάκρυνση λογισμικού υποκλοπής Spyware (Spyware Detection and Removal)

Ο όρος spyware αναφέρεται στην κατηγορία του λογισμικού που κρύβεται στον υπολογιστή ενός χρήστη και υποκλέπτει και αναφέρει στο δημιουργό του όλες τις ενέργειες και δραστηριότητες του χρήστη. Χρησιμοποιεί συνήθως τεχνικές γνωστών κατηγοριών ιομορφικού λογισμικού για την αναπαραγωγή και εγκατάστασή του στον υπολογιστή του κάθε χρήστη και είναι ικανό να ενημερώνει το δημιουργό του για πληροφορίες που αφορούν τον υπολογιστή του χρήστη ή και άλλους υπολογιστές στους οποίους συνδέεται ο χρήστης αυτός (π.χ. τράπεζες, εμπορικές ιστοσελίδες, κ.α.).

4.5.2. Εργαλεία καθαρισμού των φυλλομετρητών ιστοσελίδων (Browser Cleaning Tools)

Κάθε φυλλομετρητής ιστοσελίδων, που λειτουργεί κανονικά και χωρίς προβλήματα σε έναν υπολογιστή, αποθηκεύει σημαντική ποσότητα πληροφοριών. Οι πληροφορίες αυτές αφορούν κυρίως διευθύνσεις που έχει επισκεφτεί ο χρήστης καθώς και αντίγραφα δεδομένων που έχουν ανακτηθεί από διάφορες ιστοσελίδες. Επίσης, ο κάθε φυλλομετρητής, επιτρέπει σε κάθε ιστοσελίδα να αποθηκεύσει σε ένα ειδικό αρχείο, γνωστό ως cookie, πληροφορίες που αφορούν την επίσκεψη του χρήστη σε αυτήν, έτσι ώστε να μπορεί την επόμενη φορά που θα την επισκεφτεί να λάβει καλύτερες υπηρεσίες, όπως ταχύτερη αυθεντικοποίηση, προσωποποιημένες διαφημίσεις κ.λπ. Όλες αυτές οι πληροφορίες που αποθηκεύονται μπορούν να θέσουν σε κίνδυνο την ιδιωτικότητα του χρήστη αφού μπορεί να περιέχουν ευαίσθητα δεδομένα που ο ίδιος δεν θέλει να αποκαλυφτούν.

Για το σκοπό αυτό έχουν αναπτυχθεί εργαλεία τα οποία φροντίζουν να διαγράφουν όλες αυτές τις αποθηκευμένες πληροφορίες.

4.5.3. Εργαλεία Διαγραφής Ιχνών (Activity Traces Erasor)

Πέραν των φυλλομετρητών, οι περισσότεροι υπολογιστές αποθηκεύουν πληροφορίες σχετικά με τη χρήση τους και τις ενέργειες στις οποίες προχωρούν οι χρήστες χρησιμοποιώντας τους. Συνήθως το λειτουργικό σύστημα και οι εφαρμογές που είναι εγκατεστημένες στον υπολογιστή αποθηκεύουν αρχεία με τις ενέργειες που έχουνε γίνει (log files).

Όπως και στην προηγούμενη περίπτωση, όλες αυτές οι πληροφορίες που αποθηκεύονται μπορούν να θέσουν σε κίνδυνο την

ιδιωτικότητα του χρήστη αφού μπορεί να περιέχουν ευαίσθητα δεδομένα που ο ίδιος δεν επιθυμεί να αποκαλυφτούν.

Για το σκοπό αυτό έχουν αναπτυχθεί εργαλεία τα οποία φροντίζουν να διαγράφουν όλες αυτές τις αποθηκευμένες πληροφορίες.

4.5.4. Εργαλεία Διαγραφής Δεδομένων Αποθηκευμένων σε Σκληρούς Δίσκους (Hard Disk Data Erasor)

Όταν κάποιος χρήστης αντικαθιστά το σκληρό δίσκο του υπολογιστή του ή τον αφαιρεί για να τον παραδώσει για επισκευή, τα δεδομένα που βρίσκονται στο δίσκο αυτό είναι σε κίνδυνο ακόμα και αν ο υπόλοιπος υπολογιστής είναι ανενεργός. Ακόμη και αν τα δεδομένα του δίσκου διαγραφούν από το χρήστη, αυτά παραμένουν ορατά για έναν τεχνικό με χρήση κατάλληλων εργαλείων.

Σε αυτές τις περιπτώσεις πρέπει ο χρήστης να είναι σίγουρος ότι τα δεδομένα που διαγράφει από το σκληρό του δίσκο, όντως έχουν διαγραφεί και δεν μπορούν να ανακτηθούν από κανέναν άλλον. Για την αποτελεσματική διαγραφή των δεδομένων ακολουθείται μια συγκεκριμένη διαδικασία, η οποία υποβοηθείται από εργαλεία που έχουν αναπτυχθεί και ανήκουν στην κατηγορία αυτή.

4.6. Εργαλεία Κρυπτογράφησης

Η χρήση της κρυπτογραφίας για τη διασφάλιση της μυστικότητας επιλεγμένων πληροφοριών συναντάται συχνά στις τεχνολογίες προστασίας της ιδιωτικότητας. Χρησιμοποιώντας τεχνολογίες κρυπτογράφησης επιτυγχάνεται η ροή ευαίσθητων δεδομένων μέσα από ανασφαλή δίκτυα και εξυπηρετητές ενώ ακόμη και η αποκάλυψη της ταυτότητας χρηστών σε τρίτες οντότητες μπορεί να αποφευχθεί.

Με τη χρήση δε πολλαπλών επιπέδων κρυπτογράφησης η προστασία των δεδομένων διαφυλάσσεται ακόμα και αν μερικά από τα επίπεδα αυτά πάψουν να είναι κρυπτογραφημένα.

Παρόλο που οι τεχνολογίες κρυπτογράφησης έχουν εφευρεθεί πολύ πριν τις σύγχρονες ανησυχίες για προστασία της ιδιωτικότητας, θεωρούνται τεχνολογίες ενίσχυσης της ιδιωτικότητας μιας και συμβάλλουν στην προστασία των προσωπικών δεδομένων των χρηστών.

4.6.1. Κρυπτογράφηση Ηλεκτρονικού Ταχυδρομείου (Encrypting Email)

Όπως αναφέρθηκε και σε προηγούμενη ενότητα, υπάρχει πάντοτε η πιθανότητα όταν αποστέλλει ο χρήστης ένα ηλεκτρονικό μήνυμα αυτό να παρακολουθείται από τρίτες οντότητες και επίσης να κρατείται αντίγραφο του μηνύματος από τους διάφορους υπολογιστές που διέρχεται μέχρι να καταλήξει στον παραλήπτη του.

Για να διαφυλαχθεί το περιεχόμενο του μηνύματος, όπως επίσης και τα τυχόν συνημμένα αρχεία που μπορεί να το συνοδεύουν, εφαρμόζονται διάφορες τεχνικές κρυπτογράφησης σε αυτό, εμποδίζοντας έτσι μη εξουσιοδοτημένες οντότητες να είναι σε θέση να ανακτήσουν το περιεχόμενο του μηνύματος ακόμη και αν επιτύχουν την υποκλοπή του περιεχομένου ή των συνημμένων αρχείων.

4.6.2. Κρυπτογράφηση Συναλλαγών (Encrypting Transactions)

Όταν ο χρήστης περιηγείται στο Διαδίκτυο χρησιμοποιεί το πρωτόκολλο μεταφοράς υπερκειμένου (http) το οποίο δεν παρέχει καμία ασφάλεια στην επικοινωνία και τις συναλλαγές με τους διάφορους δικτυακούς τόπους.

Στις περιπτώσεις συναλλαγών που περιλαμβάνουν ευαίσθητα προσωπικά ή οικονομικά δεδομένα μπορεί εναλλακτικά να χρησιμοποιηθεί ένα ασφαλές πρωτόκολλο αντί του πρωτοκόλλου μεταφοράς υπερκειμένου. Ένα από τα πιο γνωστά ασφαλή πρωτόκολλα είναι το Secure Socket Layer (SSL), το οποίο περιλαμβάνει κρυπτογράφηση του περιεχομένου της συναλλαγής, διασφάλιση της ακεραιότητας των μηνυμάτων, καθώς επίσης και αυθεντικοποίηση, προαιρετικά αμφοτέρων, των μελών που συμμετέχουν στη συναλλαγή.

4.6.3. Κρυπτογράφηση Εγγράφων (Encrypting Documents)

Όταν αποθηκεύονται ή αποστέλλονται ψηφιακά έγγραφα που περιέχουν προσωπικά δεδομένα και πληροφορίες, γεννάται η απαίτηση, μεταξύ άλλων, της προστασίας της εμπιστευτικότητας των εγγράφων αυτών.

Η κρυπτογράφηση εγγράφων χρησιμοποιείται συχνά για την προστασία της ιδιωτικότητας ειδικά όταν ένα έγγραφο αποθηκεύεται ή αποστέλλεται ηλεκτρονικά χρησιμοποιώντας ανασφαλείς υποδομές που δεν μπορούν να εγγυηθούν την προστασία των εγγράφων και των πληροφοριών μέχρι την παράδοσή τους στους αντίστοιχους παραλήπτες.

4.7. Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκαν μια σειρά από τεχνολογίες, αρχιτεκτονικές, πρωτόκολλα και εργαλεία ενίσχυσης της ιδιωτικότητας. Οι υπεύθυνοι υλοποίησης συστημάτων χρησιμοποιούν τις τεχνολογίες αυτές είτε ανεξάρτητα είτε σε συνδυασμό με άλλο λογισμικό για να ικανοποιήσουν τις απαιτήσεις ιδιωτικότητας. Όπως γίνεται αντιληπτό και

από τις περιγραφές των τεχνολογιών, κάθε μια ικανοποιεί συγκεκριμένες απαιτήσεις ιδιωτικότητας και όχι το σύνολο τους.

Οι τεχνολογίες όμως αυτές δεν συνδέονται με το περιεχόμενο του υπό-ανάπτυξη, κάθε φορά συστήματος. Στη φάση της σχεδίασης πρέπει να γίνει σωστή ανάλυση των απαιτήσεων και να καθοδηγηθεί σωστά ο υπεύθυνος υλοποίησης έτσι ώστε η επιλογή των τεχνολογιών ενίσχυσης της ιδιωτικότητας να ταιριάζει και με τους στόχους του υπό-ανάπτυξη συστήματος.

Στο κεφάλαιο 5 περιγράφεται η μεθοδολογία PriS. Σκοπός της είναι η ενσωμάτωση και ανάλυση των απαιτήσεων ιδιωτικότητας κατά τη φάση της σχεδίασης. Στο τέλος η PriS αναφέρεται στις τεχνολογίες ενίσχυσης της ιδιωτικότητας και προτείνει ποιες από αυτές μπορούν να υλοποιήσουν τις απαιτήσεις ιδιωτικότητας σε σχέση πάντοτε με το σύστημα που μελετάται και αναλύεται.

5. Η Μεθοδολογία PriS

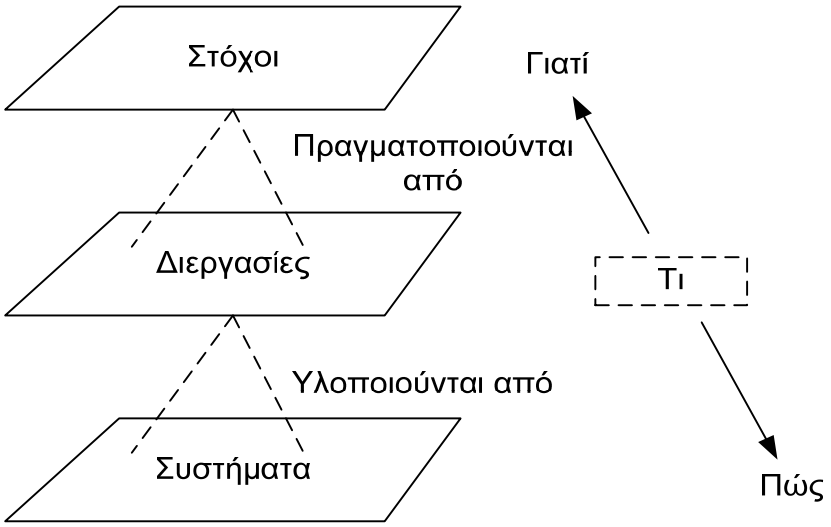
Σε αυτό το κεφάλαιο αναπτύσσεται η μεθοδολογία PriS (Privacy Safeguard), σκοπός της οποίας είναι η ενσωμάτωση των βασικών απαιτήσεων ιδιωτικότητας στη διαδικασία της σχεδίασης συστημάτων. Η PriS αναπαριστά τις απαιτήσεις της ιδιωτικότητας (privacy requirements) ως στόχους (goals) του συστήματος και χρησιμοποιεί πρότυπα διεργασιών ιδιωτικότητας (privacy process patterns) (από εδώ και στο εξής θα αναφέρονται ως *πρότυπα ιδιωτικότητας*) για να περιγράψει την επίδραση των στόχων ιδιωτικότητας στις διεργασίες του συστήματος και στα αντίστοιχα συστήματα λογισμικού που υλοποιούν τις διεργασίες αυτές.

5.1. Το εννοιολογικό μοντέλο της PriS

Η PriS είναι μια μεθοδολογία ανάλυσης απαιτήσεων ιδιωτικότητας. Περιλαμβάνει μια σειρά από έννοιες που σκοπό έχουν αφενός μεν την εφαρμογή των απαιτήσεων αυτών στις δραστηριότητες ενός οργανισμού, αφετέρου δε την παροχή ενός συστηματικού τρόπου εύρεσης ορθών μοντέλων συστημάτων τα οποία και να υλοποιούν τις απαιτήσεις αυτές.

Το εννοιολογικό μοντέλο που χρησιμοποιεί η PriS βασίζεται στη μεθοδολογία EKD Enterprise Knowledge Development (Loucopoulos, P. and Kavakli, E. 1997; Loucopoulos, P. 2000). Η EKD παρέχει ένα συστηματικό τρόπο ανάπτυξης και τεκμηρίωσης της γνώσης που υπάρχει σε έναν οργανισμό. Η EKD υποβοηθά τους οργανισμούς και τις επιχειρήσεις να αντιληφθούν τις διαδικασίες που ακολουθούν και τη γνώση που έχουν, καθώς επίσης και τις αλλαγές που πρέπει να γίνουν σε περίπτωση που κάποια αιτία τροποποιήσει τον τρόπο διαχείρισης ή εφαρμογής αυτής της γνώσης. Για παράδειγμα, η εισαγωγή ενός νέου πληροφοριακού

συστήματος σε μια επιχείρηση μπορεί να επιφέρει ιδιαίτερες αλλαγές. Η EKD καταγράφει και τεκμηριώνει την υπάρχουσα γνώση, ενώ παράλληλα, βοηθώντας τις επιχειρήσεις να αντιληφθούν την ανάγκη για αλλαγές και βελτιώσεις, βοηθά στην εφαρμογή των αναγκαίων αλλαγών. Στο Σχήμα 5.1 παρουσιάζεται ο τρόπος λειτουργίας της EKD.



Σχήμα 5.1. Το εννοιολογικό μοντέλο της EKD

Η αποτύπωση της γνώσης ενός οργανισμού[4] με τη μεθοδολογία EKD επιτυγχάνεται με την αποτύπωση των:

α) στόχων του οργανισμού, οι οποίοι εκφράζουν τις αντικειμενικές προθέσεις στις οποίες στηρίζεται και στοχεύει η όλη λειτουργία του

β) «φυσικών» διεργασιών, οι οποίες επιτυγχάνουν να μετατρέψουν τους «θεωρητικούς» στόχους σε «πραγματικές» λειτουργίες

γ) συστημάτων λογισμικού, τα οποία υποστηρίζουν τη λειτουργία των παραπάνω διεργασιών.

[4] Οργανισμός ορίζεται ο φορέας στον οποίο θα παρέχονται κάποιες υπηρεσίες δια μέσου του Πληροφοριακού Συστήματος

Η μεθοδολογία EKD χρησιμοποιεί τους στόχους ως μέσο ανάλυσης των απαιτήσεων στην τεχνολογία λογισμικού. Μια ανασκόπηση των μεθοδολογιών που χρησιμοποιούν αντίστοιχο τρόπο προσέγγισης περιλαμβάνεται στο (Kavakli, E. 2004).

Όπως φαίνεται στο Σχήμα 5.1, οι διεργασίες αναφέρονται στο «ΤΙ» γίνεται, οι στόχοι αιτιολογούν «ΓΙΑΤΙ» υπάρχουν οι διεργασίες αυτές, ενώ τα συστήματα περιγράφουν το «ΠΩΣ» οι διεργασίες μπορούν να υλοποιηθούν από διάφορες αρχιτεκτονικές συστημάτων. Με αυτό τον τρόπο επιτυγχάνεται η διασύνδεση μεταξύ του σκοπού για τον οποίο αναπτύσσεται το σύστημα και της δομής του προς υλοποίηση συστήματος.

Επεκτείνοντας το παραπάνω μοντέλο, η μεθοδολογία PriS συμβολίζει τις απαιτήσεις της ιδιωτικότητας ως έναν ειδικό τύπο στόχου, το στόχο της ιδιωτικότητας. Οι απαιτήσεις αυτές περιορίζουν την όλη διαδικασία της μετατροπής των στόχων του οργανισμού στις ανάλογες διεργασίες με βάση τις παραμέτρους ιδιωτικότητας που εκφράζουν. Στο Σχήμα 5.2 αποτυπώνεται το εννοιολογικό μοντέλο της PriS.

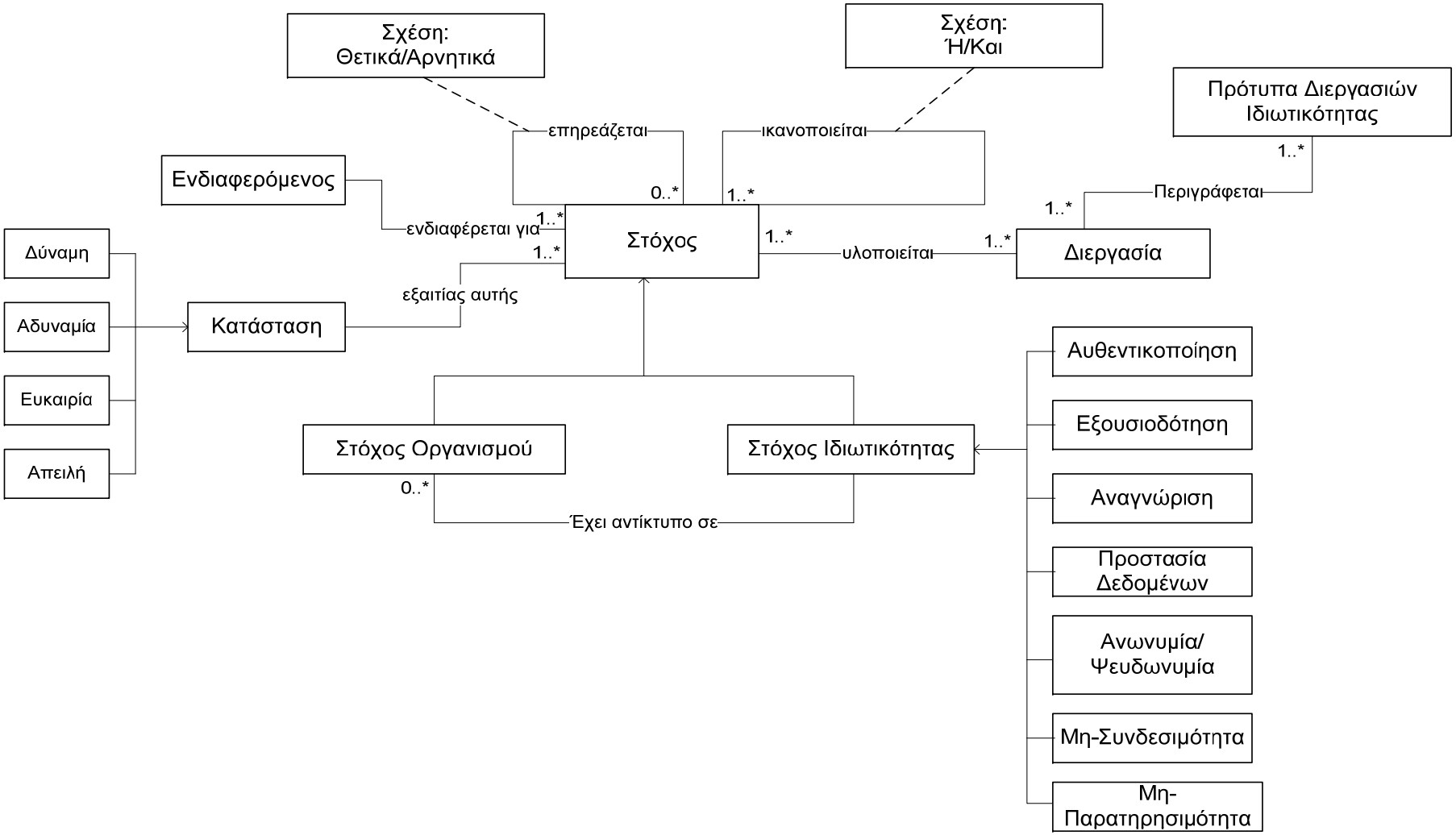
Βασική οντότητα του μοντέλου είναι ο *στόχος*. Οι στόχοι είναι επιθυμητές καταστάσεις γεγονότων οι οποίες πρέπει να επιτευχθούν. Οι στόχοι εκφράζονται από τους *ενδιαφερόμενους*, δηλαδή καθένας που έχει ενδιαφέρον για τη σχεδίαση και χρήση του συστήματος. Επίσης στόχοι δημιουργούνται ως αντίδραση σε συγκεκριμένες *καταστάσεις* όπως *δύναμης, αδυναμίας, ευκαιρίας* ή *απειλής*.

Όπως φαίνεται στο Σχήμα 5.2 υπάρχουν δύο τύποι στόχων. Οι *στόχοι οργανισμού* και οι *στόχοι ιδιωτικότητας*. Οι στόχοι του οργανισμού αντιπροσωπεύουν τους σκοπούς που θέλει να υλοποιήσει ο οργανισμός με το προς σχεδίαση και ανάπτυξη σύστημα. Οι στόχοι ιδιωτικότητας δημιουργούνται από διάφορα ζητήματα προστασίας της ιδιωτικότητας. Οκτώ είναι οι τύποι των στόχων ιδιωτικότητας, με βάση τις βασικές

παραμέτρους ιδιωτικότητας που αναφέρθηκαν προηγουμένως, η *αυθεντικοποίηση (authentication)*, η *εξουσιοδότηση (authorization)*, η *αναγνώριση (identification)*, η *προστασία δεδομένων (data protection)*, η *ανωνυμία (anonymity)*, η *ψευδωνυμία (pseudonymity)*, η *μη-συνδεσιμότητα (unlinkability)* και η *μη-παρατηρησιμότητα (unobservability)*.

Οι στόχοι ιδιωτικότητας μπορεί να έχουν αντίκτυπο στους στόχους του οργανισμού. Για παράδειγμα, ας αναλογιστούμε το στόχο οργανισμού ενός διαδικτυακού φαρμακείου ο οποίος αναφέρει το εξής: «Σε όλους τους πελάτες που χρησιμοποιούν το Διαδίκτυο για να παραγγείλουν φάρμακα θα γίνονται καλές τιμές». Επίσης ένας στόχος ιδιωτικότητας που πρέπει να ληφθεί υπόψη και να υλοποιηθεί από τον οργανισμό είναι ο εξής: «Διαφύλαξη της μη-συνδεσιμότητας των πελατών». Όπως είναι αντιληπτό ο στόχος ιδιωτικότητας σαφώς και έχει αντίκτυπο στον πρώτο στόχο που αναφέρθηκε: είναι η δημιουργία ενός νέου στόχου ο οποίος αναφέρει το εξής: «Καμία τρίτη οντότητα δεν θα πρέπει να έχει τη δυνατότητα να συνδέσει έναν πελάτη με τα φάρμακα που αυτός/ή παρήγγειλε». Γενικά ένας στόχος ιδιωτικότητας μπορεί να προκαλέσει την αλλαγή και βελτίωση των στόχων του οργανισμού ή ακόμη και τη δημιουργία νέων στόχων. Με αυτό τον τρόπο τα ζητήματα της ιδιωτικότητας ενσωματώνονται στην όλη σχεδίαση του συστήματος.

Οι στόχοι πραγματοποιούνται από τις διεργασίες οι οποίες με τη σειρά τους περιγράφονται από πρότυπα ιδιωτικότητας ανάλογα με τις απαιτήσεις ιδιωτικότητας που υλοποιούν. Όμως, οι στόχοι δεν μπορούν να αντιστοιχισθούν απευθείας στις διεργασίες. Η διαδικασία της μετάβασης από τους στόχους στις διεργασίες περιλαμβάνει τη διαδικασία του *τελεολογικού μετασχηματισμού* των γενικών στόχων του οργανισμού σε ένα ή περισσότερους υπό-στόχους οι οποίοι αποτελούν το μέσο για να αποκτηθεί η σύνδεση μεταξύ των γενικών στόχων και των διεργασιών.



Σχήμα 5.2. Το εννοιολογικό μοντέλο της PriS

Κατά τη διάρκεια αυτής της διαδικασίας, σε κάθε βήμα της, εισάγονται νέοι στόχοι οι οποίοι εντάσσονται μαζί με τους αρχικούς, μέσω *αιτιολογικών σχέσεων* σχηματίζοντας έτσι μια *ιεραρχία* από στόχους. Κάθε υπό-στόχος μπορεί να συνεισφέρει στην επίτευξη ενός ή περισσότερων στόχων, όποτε το αποτέλεσμα στην ουσία είναι ένας γράφος, παρά μία ιεραρχία. Όπως φαίνεται και από το Σχήμα 5.2, ο τύπος της συσχέτισης που ορίζει την ανάλυση του κάθε στόχου μεταξύ των υπο-στόχων είναι του τύπου *ή/και*. Η συσχέτιση και δηλώνει ότι η επίτευξη ενός στόχου εξαρτάται από την επίτευξη ενός συνδυασμού υπό-στόχων. Η συσχέτιση ή δηλώνει ότι η επίτευξη ενός στόχου εξαρτάται από ένα σύνολο εναλλακτικών στόχων.

Επιπλέον της συσχέτισης της ικανοποίησης, μεταξύ ενός στόχου και των υπο-στόχων, υπάρχει και ακόμη ένας τύπος: ο τύπος της *επιρροής*. Ο τύπος αυτός αποτελείται από δύο μέρη. Από τη *θετική* και την *αρνητική* επιρροή. Η σχέση της θετικής επιρροής μεταξύ δύο στόχων δηλώνει ότι η επίτευξη του ενός υποστηρίζει την επίτευξη του άλλου. Ωστόσο, το αντίθετο δεν είναι απαραίτητα αληθές. Επιπλέον η συσχέτιση της αρνητικής επιρροής μεταξύ δύο στόχων δηλώνει ότι η επίτευξη του ενός εμποδίζει την επίτευξη του άλλου.

5.2. Ο τρόπος εργασίας της PriS

Η μεθοδολογική προσέγγιση της PriS, όσον αφορά τον τρόπο με τον οποίο επεξεργάζεται τις απαιτήσεις ιδιωτικότητας του συστήματος, περιλαμβάνει τα ακόλουθα στάδια:

α) Προσδιορισμός των απαιτήσεων ιδιωτικότητας στο υπό ανάπτυξη σύστημα

β) Ανάλυση της επίδρασης των απαιτήσεων ιδιωτικότητας στις διεργασίες του οργανισμού

γ) Διαμόρφωση των διεργασιών που επηρεάζονται από τις απαιτήσεις ιδιωτικότητας, με χρήση προτύπων ιδιωτικότητας

δ) Επιλογή των τεχνολογιών που υποστηρίζουν την υλοποίηση των προαναφερθέντων προτύπων ιδιωτικότητας

5.2.1. Προσδιορισμός των απαιτήσεων ιδιωτικότητας

Το πρώτο στάδιο αφορά στον προσδιορισμό των απαιτήσεων ιδιωτικότητας του συγκεκριμένου οργανισμού. Περιλαμβάνει την καταγραφή απόψεων από επιλεγμένα στελέχη του οργανισμού που έχουν την ευθύνη λήψης αποφάσεων όπως διευθυντές, αναλυτές συστημάτων, χρήστες, αποφασίζοντες για τη στρατηγική του οργανισμού κ.λπ. Στόχος είναι η ανάλυση των απόψεων σχετικά με τη λειτουργία του οργανισμού, ο καθορισμός των ζητημάτων που αφορούν στην ιδιωτικότητα και ο εντοπισμός των απαιτήσεων ιδιωτικότητας που πρέπει να ληφθούν υπόψη για τη σωστή λειτουργία του οργανισμού.

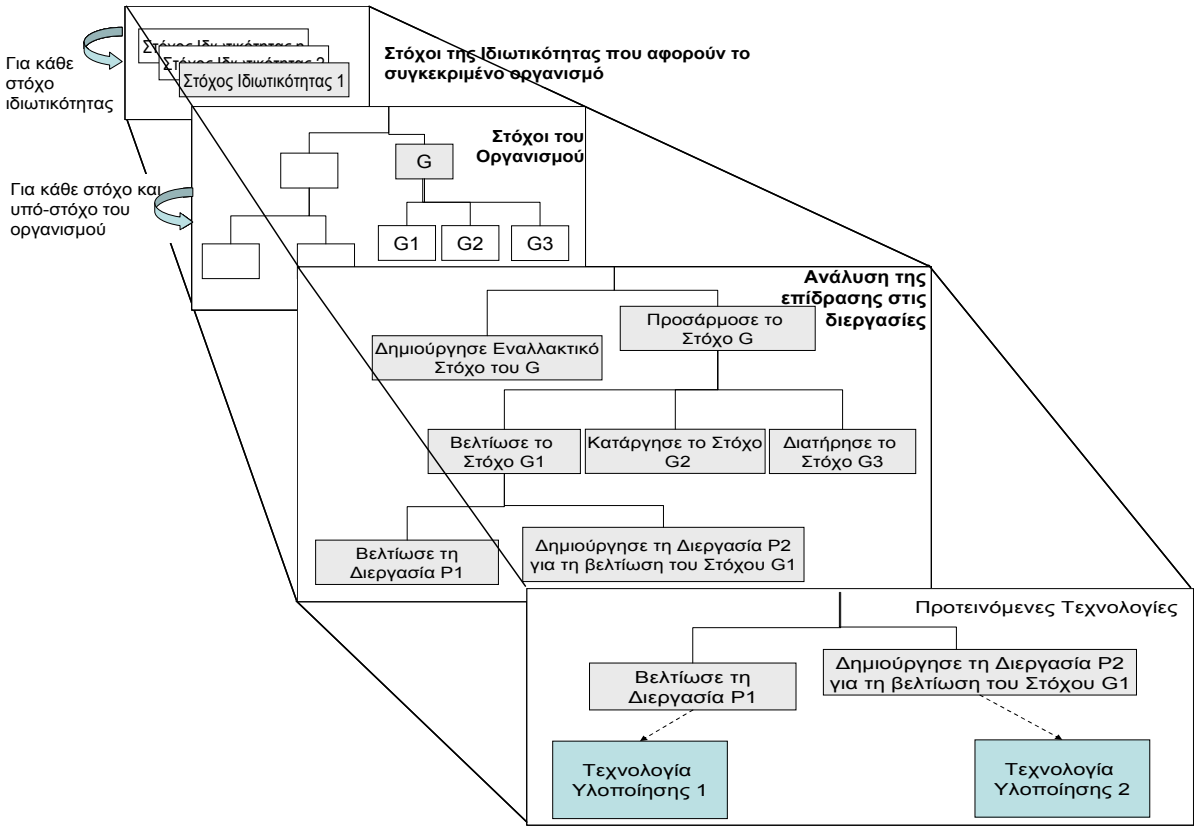
Ο προσδιορισμός των θεμάτων που αφορούν στην ιδιωτικότητα, για το συγκεκριμένο οργανισμό, βασίζεται στις απαιτήσεις ιδιωτικότητας που αναφέρθηκαν στο κεφάλαιο 2. Βασικός σκοπός του παρόντος σταδίου είναι να αποφασιστεί ποιες από τις προαναφερθείσες απαιτήσεις ιδιωτικότητας αφορούν στο υπό-ανάπτυξη σύστημα και με ποιον τρόπο θα ενσωματωθούν στην υπάρχουσα ιεραρχία των στόχων, που καθορίζουν το πλαίσιο λειτουργίας του οργανισμού.

5.2.2. Ανάλυση της επίδρασης των απαιτήσεων ιδιωτικότητας στις διεργασίες του οργανισμού

Το δεύτερο στάδιο αφορά στην ανάλυση της επίδρασης των απαιτήσεων ιδιωτικότητας στις διεργασίες και στα συστήματα που τις

υποστηρίζουν. Στο στάδιο αυτό περιλαμβάνονται δύο φάσεις. Στην πρώτη φάση αναγνωρίζεται η επίδραση των απαιτήσεων ιδιωτικότητας στους γενικότερους στόχους του οργανισμού, ενώ στη δεύτερη φάση αναλύεται η επίδραση των αλλαγών των διεργασιών που τις υλοποιούν εξαιτίας των απαιτήσεων ιδιωτικότητας. Μια περίληψη της όλης αυτής διαδικασίας φαίνεται στο Σχήμα 5.3.

Για κάθε απαίτηση ιδιωτικότητας που έχει προσδιορισθεί από το προηγούμενο στάδιο και συμπεριληφθεί στους στόχους του οργανισμού, εντοπίζεται η επίδραση που αυτή μπορεί να έχει στους στόχους του οργανισμού. Η επίδραση αυτή μπορεί να οδηγήσει στην εισαγωγή νέων στόχων ή στη βελτίωση των ήδη υπαρχόντων. Η εισαγωγή νέων στόχων, δευτερογενώς, μπορεί να οδηγήσει στην εισαγωγή νέων διεργασιών, ενώ η βελτίωση των ήδη υπαρχόντων στόχων μπορεί να οδηγήσει στην βελτίωση αντίστοιχων διεργασιών.



Σχήμα 5.3. Ανάλυση της επίδρασης των απαιτήσεων ιδιωτικότητας στις διεργασίες του οργανισμού

Η διαδικασία αυτή επαναλαμβάνεται για κάθε νέα απαίτηση ιδιωτικότητας και για όλους τους στόχους του οργανισμού κάθε φορά. Το αποτέλεσμα αυτού του σταδίου είναι ο προσδιορισμός εναλλακτικών λύσεων όσον αφορά τον τρόπο με τον οποίο θα μπορέσουν να ικανοποιηθούν οι απαιτήσεις ιδιωτικότητας που τέθηκαν στην αρχή. Ουσιαστικά καταγράφεται ένα σύνολο στόχων, οι οποίοι συσχετίζονται με τον τύπο συσχέτισης και/ή (and/or).

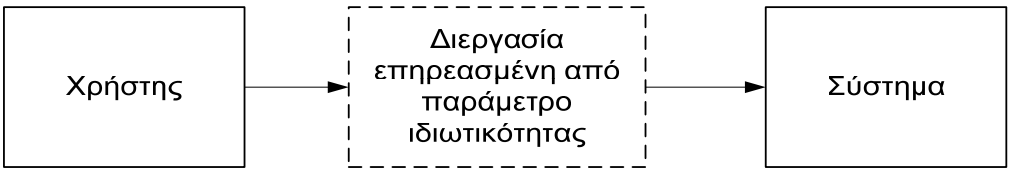
5.2.3. Διαμόρφωση των διεργασιών που επηρεάζονται από τις απαιτήσεις ιδιωτικότητας, με χρήση προτύπων ιδιωτικότητας

Μετά τον εντοπισμό των διεργασιών που επηρεάζονται από τις απαιτήσεις ιδιωτικότητας, ακολουθεί η διαμόρφωση των συγκεκριμένων διεργασιών με βάση τα πρότυπα (patterns) ιδιωτικότητας. Τα πρότυπα αυτά είναι γενικευμένα μοντέλα διεργασιών τα οποία περιέχουν ενέργειες, καθώς και ροές δεδομένων μεταξύ των ενεργειών και παρουσιάζουν τον τρόπο με τον οποίο θα πρέπει να λειτουργεί ένας οργανισμός σε συγκεκριμένο, κάθε φορά, τμήμα του (Kalloniatis, C., Kavakli, E. and Gritzalis, S. 2007).

Ένα πρότυπο περιγράφει μια γενική λύση σε ένα κοινό πρόβλημα από το οποίο μπορεί να καθοριστεί μια συγκεκριμένη λύση σε ένα συγκεκριμένο πρόβλημα. Το πρότυπο διεργασίας είναι ένα πρότυπο που περιγράφει ένα τρόπο προσέγγισης, μέσω μιας σειράς ενεργειών, για την επιτυχή ανάπτυξη λογισμικού. Είναι απαραίτητα διότι χρησιμοποιούνται για να περιγράψουν το τρόπο που απεικονίζονται οι απαιτήσεις του συστήματος στις διεργασίες. Συγκεκριμένα, κάθε πρότυπο διεργασίας εξειδικεύεται σε κάθε περίπτωση χρήσης ανάλογα με το περιβάλλον του οργανισμού για το οποίο θα αναπτυχθεί το πληροφοριακό σύστημα και έτσι δεν χρειάζεται κάθε φορά να υλοποιούνται από την αρχή οι

διεργασίες για τις οποίες έχουν περιγραφεί ήδη τα πρότυπα τους. Επίσης βοηθούν στην υλοποίηση των διεργασιών μέσω των διακριτών ενεργειών που τις υλοποιούν. Σαφέστατα, είναι πιο εύκολο για τον υπεύθυνο υλοποίησης του συστήματος να ικανοποιήσει τις απαιτήσεις των διαδικασιών γνωρίζοντας αναλυτικά τις ενέργειες που υλοποιούνται από την κάθε διαδικασία. Επιπρόσθετα με τη βοήθεια των προτύπων διεργασιών ελέγχεται ευκολότερα αν η μέθοδος είναι υλοποιήσιμη ή οχί.

Συγκεκριμένα, η PriS ορίζει επτά πρότυπα ιδιωτικότητας που αντιστοιχούν στις απαιτήσεις ιδιωτικότητας που έχουν αναφερθεί σε προηγούμενα κεφάλαια[5]. Κάθε πρότυπο ορίζεται σε δύο επίπεδα. Το πρώτο επίπεδο, όπως φαίνεται και στο Σχήμα 5.4, είναι πιο αφαιρετικό και είναι ταυτόσημο για όλα τα πρότυπα ιδιωτικότητας της PriS. Για το λόγο αυτό δεν αναφέρεται σε κάθε ένα από τα πρότυπα ιδιωτικότητας που ακολουθούν.



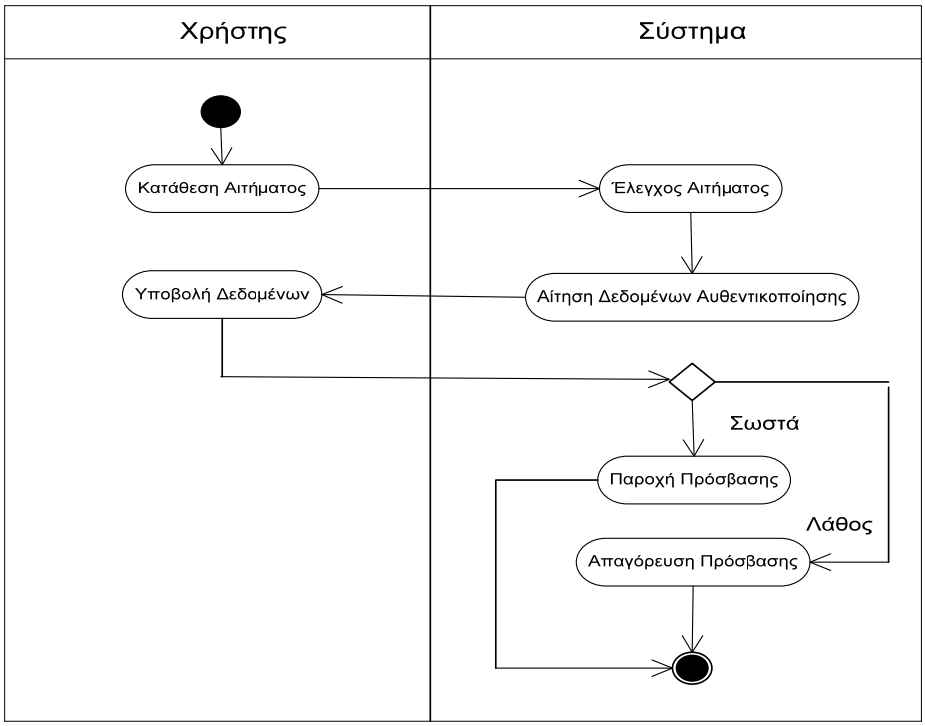
Σχήμα 5.4. Πρώτο Επίπεδο Προτύπου Ιδιωτικότητας

Το επίπεδο αυτό περιγράφει τη γενική περίπτωση όπου ένας χρήστης σχετίζεται με το σύστημα μέσω μιας συγκεκριμένης διεργασίας η οποία «περιορίζεται από μια απαίτηση ιδιωτικότητας». Το σύστημα είναι

[5] Επειδή η ψευδωνυμία μπορεί να θεωρηθεί ένας τρόπος υλοποίησης υπηρεσίας ανωνυμίας, μπορούν να καλυφθούν αμφότερα σε ένα πρότυπο. Για το λόγο αυτό υπάρχουν οκτώ απαιτήσεις και επτά πρότυπα.

συνήθως ένα «πληροφοριακό σύστημα», αλλά θα μπορούσε να είναι ένα άλλο άτομο ή ακόμη και μια άλλη διεργασία ή υπηρεσία.

Στο δεύτερο επίπεδο αναλύονται οι διεργασίες που επηρεάζονται από απαιτήσεις ιδιωτικότητας. Κάθε διεργασία αναλύεται με βάση την αντίστοιχη απαίτηση ιδιωτικότητας που την «περιορίζει». Στο Σχήμα 5.5 αναλύεται το πρότυπο ιδιωτικότητας της διεργασίας που επηρεάζεται από την απαίτηση της *αυθεντικοποίησης*.

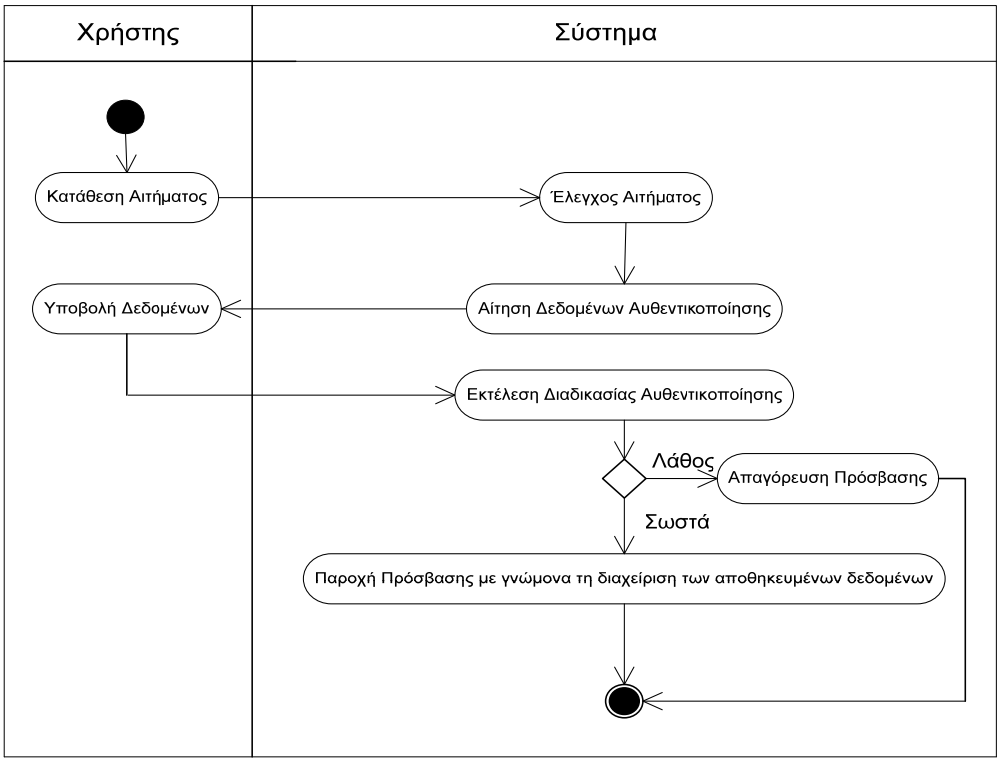


Σχήμα 5.5. Πρότυπο Αυθεντικοποίησης

Κάθε πρότυπο αποτελείται από μια σειρά ενεργειών (εκφρασμένη σε UML) βάση της οποίας πραγματοποιείται η αντίστοιχη διεργασία.

Όπως φαίνεται στο παραπάνω σχήμα, ο χρήστης καταθέτει ένα αίτημα στο σύστημα. Το σύστημα ελέγχει το αίτημα αυτό ώστε να αποφασιστεί αν απαιτούνται δεδομένα αυθεντικοποίησης. Αν πράγματι αυτά απαιτούνται, τότε το σύστημα ζητά από το χρήστη να τα εισάγει. Αν αυτά είναι έγκυρα τότε ο χρήστης αποκτά πρόσβαση στα δεδομένα και τις υπηρεσίες που ζήτησε, ενώ σε αντίθετη περίπτωση το σύστημα του απαγορεύει την πρόσβαση.

Το πρότυπο ιδιωτικότητας για την απαίτηση της *εξουσιοδότησης* παρουσιάζεται στο Σχήμα 5.6. Σύμφωνα με την απαίτηση αυτή, τα προσωπικά δεδομένα των χρηστών μπορούν να προσπελαστούν μόνον από εξουσιοδοτημένους χρήστες. Για το λόγο αυτό, αρχικά, όταν ο χρήστης καταθέτει ένα αίτημα στο σύστημα, ελέγχεται η φύση του αιτήματος και προσδιορίζεται αν για τη συγκεκριμένη πρόσβαση ή υπηρεσία, απαιτείται από το χρήστη να αναγνωρισθεί πριν εισέλθει στο σύστημα. Σε περίπτωση που ο χρήστης καταθέτει ένα αίτημα στο σύστημα το οποίο δεν αφορά χρήση προσωπικών δεδομένων άλλων χρηστών ή δεν παραβιάζει κανόνες ασφαλείας του συστήματος, το σύστημα δεν πρέπει να ζητά από το χρήστη προσωπικά στοιχεία (π.χ. στοιχεία αυθεντικοποίησης) αλλά θα πρέπει να του προσφέρει απευθείας την υπηρεσία ή την πρόσβαση στα δεδομένα που ζήτησε.

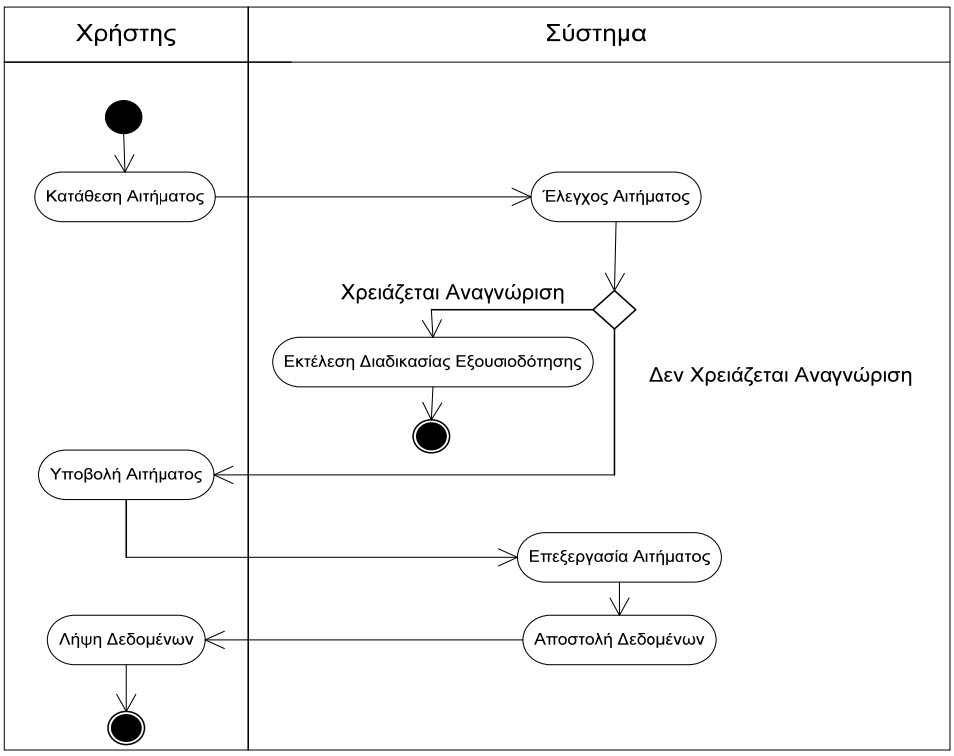


Σχήμα 5.6. Πρότυπο Εξουσιοδότησης

Σε αντίθετη περίπτωση, όποτε ο χρήστης ζητά πρόσβαση σε υπηρεσίες που μόνον εξουσιοδοτημένοι χρήστες επιτρέπεται να έχουν, το

σύστημα οδηγεί το χρήστη στη διεργασία της αυθεντικοποίησης έτσι ώστε να ελεγχθεί η εγκυρότητά του και σε περίπτωση θετικής έκβασης να του αποδοθούν από το σύστημα τα δικαιώματα που προβλέπονται, αφού για κάθε χρήστη υπάρχουν (έχουν προκαθοριστεί) συγκεκριμένα δικαιώματα όσον αφορά στις ενέργειες και στις δυνατότητες πρόσβασης.

Το πρότυπο ιδιωτικότητας που αναφέρεται στην απαίτηση της *αναγνώρισης* παρουσιάζεται στο Σχήμα 5.7. Ο ρόλος του συγκεκριμένου προτύπου είναι διττός. Σκοπός του είναι να προστατέψει αφενός μεν το χρήστη που αιτείται πρόσβασης σε δεδομένα ή υπηρεσίες του συστήματος και αφετέρου δε τα προσωπικά δεδομένα των χρηστών που βρίσκονται αποθηκευμένα στο σύστημα. Ακολούθως το πρότυπο φροντίζει ώστε μόνον εξουσιοδοτημένοι χρήστες να επιτρέπεται να εισέλθουν στο σύστημα και να έχουν πρόσβαση στις αντίστοιχες υπηρεσίες, τα προσωπικά δεδομένα των άλλων χρηστών και του συστήματος γενικότερα.



Σχήμα 5.7. Πρότυπο Αναγνώρισης

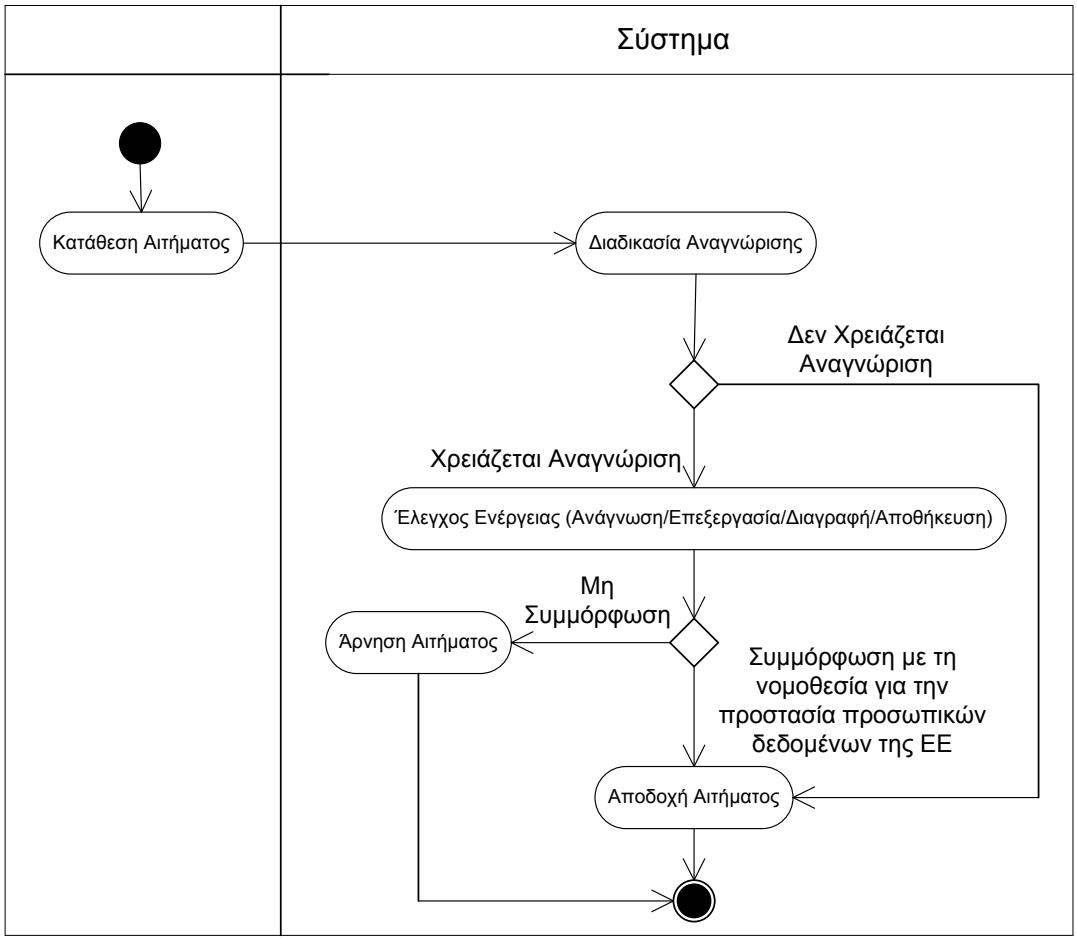
Όπως φαίνεται στο Σχήμα 5.7, όταν ο χρήστης καταθέσει ένα αίτημα προς το σύστημα, πρώτα ελέγχεται αν για την υλοποίησή του απαιτείται η αναγνώριση του χρήστη. Αυτό είναι σημαντικό διότι στο σύστημα θα πρέπει να έχει δηλωθεί για ποιες υπηρεσίες και δεδομένα απαιτείται η αναγνώριση του χρήστη και σε ποια όχι. Η απαίτηση χρήσης προσωπικών δεδομένων χρηστών για υπηρεσίες και παροχή δεδομένων που δεν απαιτείται δε συνάδει με τις απαιτήσεις περί προστασίας προσωπικών δεδομένων.

Σε περίπτωση που δεν απαιτείται αναγνώριση, το σύστημα ικανοποιεί το αίτημα του χρήστη χωρίς να ζητήσει κανένα αναγνωριστικό στοιχείο. Σε περίπτωση που θα χρειαστεί αναγνώριση, τότε ενεργοποιείται η διεργασία της εξουσιοδότησης όπως φαίνεται και στο σχήμα. Διευκρινίζεται ότι το πρότυπο της αναγνώρισης σε καμία περίπτωση δεν αντικαθιστά την ανωνυμία. Υπάρχει σαφής διαφοροποίηση ανάμεσα στη μη αποστολή εκ μέρους του χρήστη των προσωπικών του δεδομένων, από την ύπαρξη τεχνολογιών προστασίας της ανωνυμίας κάθε φορά που αιτείται κάποιας υπηρεσίας από ένα σύστημα. Η αναγνώριση ξεχωρίζει ποιες υπηρεσίες μπορεί να διαθέσει το σύστημα σε εξουσιοδοτημένους χρήστες και ποιες όχι. Για τις υπηρεσίες που δεν χρειάζονται αναγνώριση, το σύστημα δεν ζητά κανένα στοιχείο από το χρήστη. Δεν φροντίζει όμως και για τη προστασία των δεδομένων του κατά τη διάρκεια της επικοινωνίας του με αυτό.

Στο Σχήμα 5.8 παρουσιάζεται το πρότυπο ιδιωτικότητας που αναφέρεται στην απαίτηση της *προστασίας δεδομένων*. Σκοπός αυτού του προτύπου είναι να διασφαλιστεί ότι σε κάθε συναλλαγή που περιλαμβάνονται προσωπικά δεδομένα διαφυλάσσονται οι απαιτήσεις προστασίας της ιδιωτικότητας όπως αυτές έχουν θεσπιστεί από τον ίδιο τον οργανισμό σε συμμόρφωση με το ισχύον νομοθετικό πλαίσιο, όπως

την Οδηγία 95/46/EU που αναφέρεται στην κατοχή προσωπικών δεδομένων και στην ελεύθερη διακίνηση τους (EU, Directive. 1995).

Συγκεκριμένα, όταν ένας χρήστης, εντός ή εκτός του συστήματος, προσπαθεί να προσπελάσει ιδιωτικά δεδομένα, η διεργασία της αναγνώρισης ενεργοποιείται σύμφωνα με το αντίστοιχο πρότυπο ώστε να γίνει γνωστό στο σύστημα ποιος είναι ο συγκεκριμένος χρήστης και

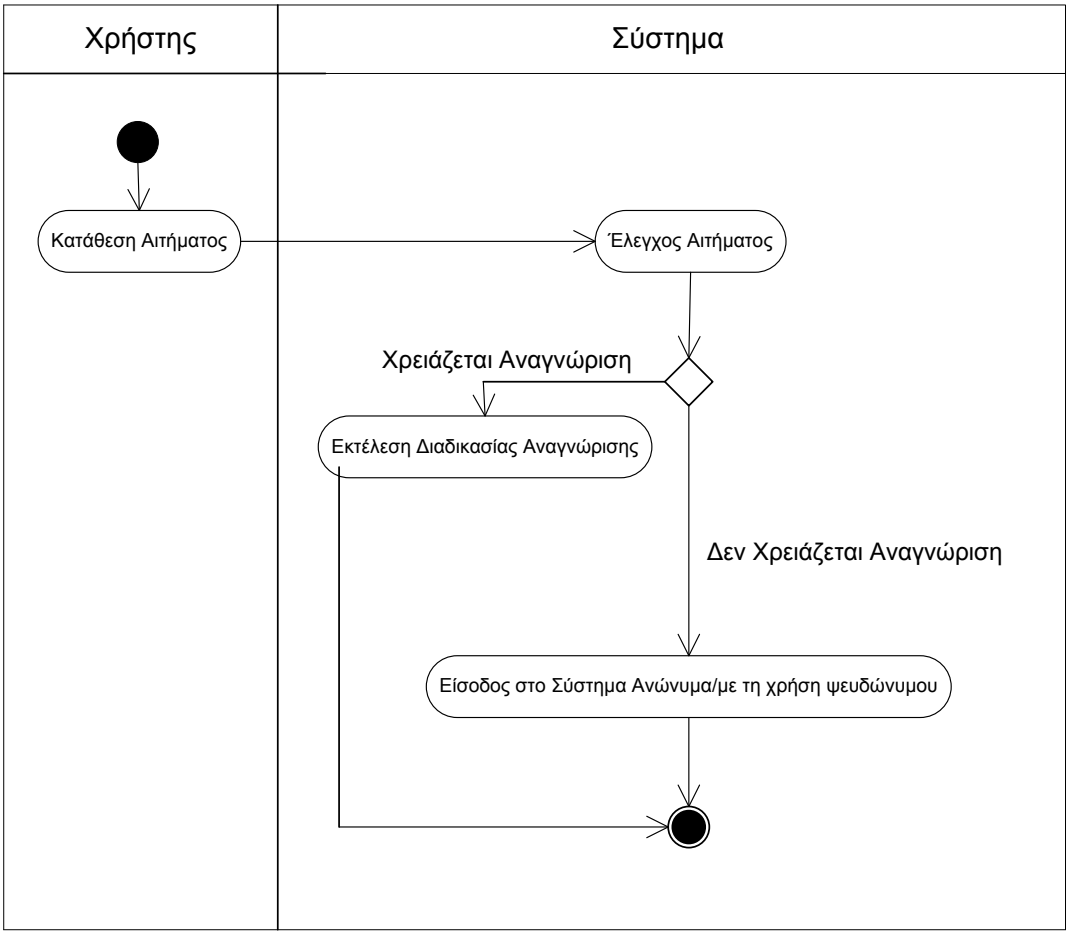


Σχήμα 5.8. Πρότυπο Προστασίας Δεδομένων

ανάλογα να του δοθούν τα δικαιώματα που έχει όσον αφορά την ανάγνωση, επεξεργασία, διαγραφή και αποθήκευση προσωπικών δεδομένων. Στη συνέχεια, όταν ο χρήστης ζητήσει να κάνει μία από τις παραπάνω ενέργειες, ελέγχεται αν το αίτημά του είναι σύμφωνο με το προβλεπόμενο πλαίσιο προστασίας της ιδιωτικότητας που έχει θεσπίσει ο

συγκεκριμένος οργανισμός και ανάλογα το αίτημά του είτε γίνεται δεκτό είτε απορρίπτεται. Στην πραγματικότητα λοιπόν υπάρχουν δύο έλεγχοι πριν ο χρήστης καταφέρει τελικά να προσπελάσει και να επεξεργαστεί προσωπικά δεδομένα που είναι αποθηκευμένα στο σύστημα.

Το επόμενο πρότυπο αφορά στην ανωνυμία και στην ψευδωνυμία. Όπως έχει προαναφερθεί η ψευδωνυμία μπορεί να θεωρηθεί ως μέρος της ανωνυμίας και γι' αυτό το λόγο υλοποιούνται και οι δύο απαιτήσεις σε ένα κοινό πρότυπο ιδιωτικότητας όπως φαίνεται και στο Σχήμα 5.9.



Σχήμα 5.9. Πρότυπο Ανωνυμίας/Ψευδωνυμίας

Συγκεκριμένα ο χρήστης καταθέτει ένα αίτημα το οποίο και ελέγχεται για να αποφασιστεί αν χρειάζεται να γίνει αναγνώριση του χρήστη ή όχι με γνώμονα πάντοτε το περιεχόμενο που θέλει να προσπελάσει ή την υπηρεσία στην οποία ζητά πρόσβαση. Αν η

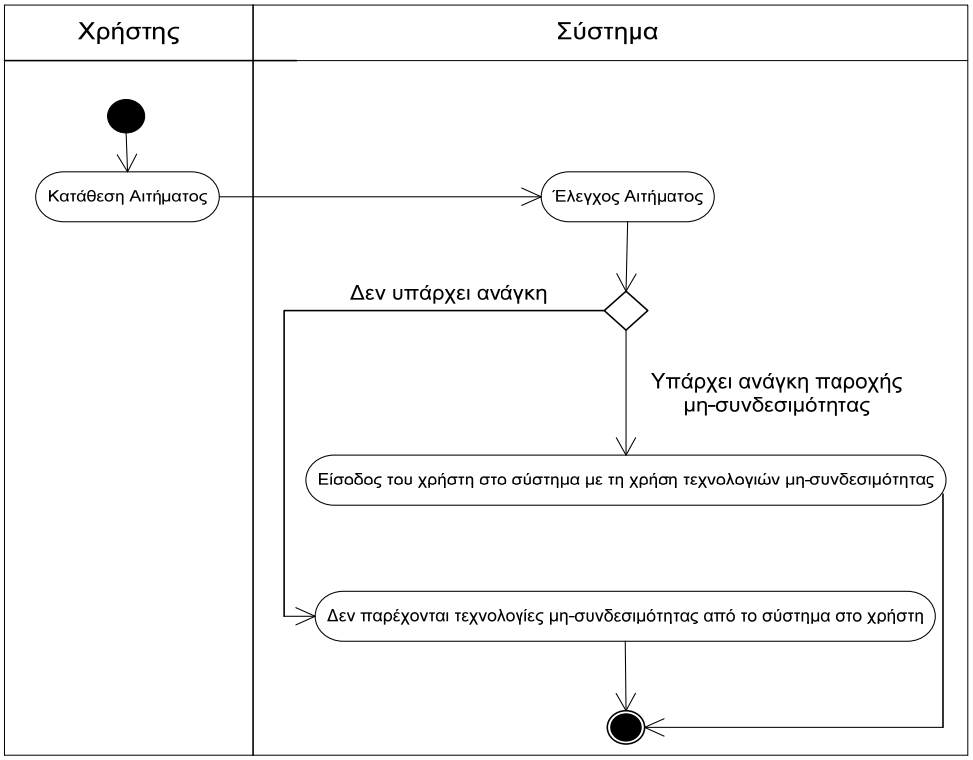
αναγνώριση του χρήστη είναι απαραίτητη τότε ενεργοποιείται η αντίστοιχη διεργασία της αναγνώρισης η οποία και περιλαμβάνει τις ανάλογες ενέργειες όπως περιγράφηκαν προηγουμένως.

Στην περίπτωση που δεν χρειάζεται αναγνώριση, ο χρήστης, αφενός μεν λαμβάνει τις πληροφορίες που ζήτησε χωρίς να δώσει κανένα από τα προσωπικά του στοιχεία, αφετέρου δε κατά τη διάρκεια των συναλλαγών του με το σύστημα εφαρμόζονται και διάφορες τεχνολογίες που σκοπό έχουν να προστατέψουν την ανωνυμία του. Γίνεται αντιληπτό λοιπόν ότι η αναγνώριση μπορεί να είναι μέρος της ανωνυμίας ανάλογα με το αν θα χρειαστούν ή όχι προσωπικά δεδομένα του χρήστη προς επεξεργασία.

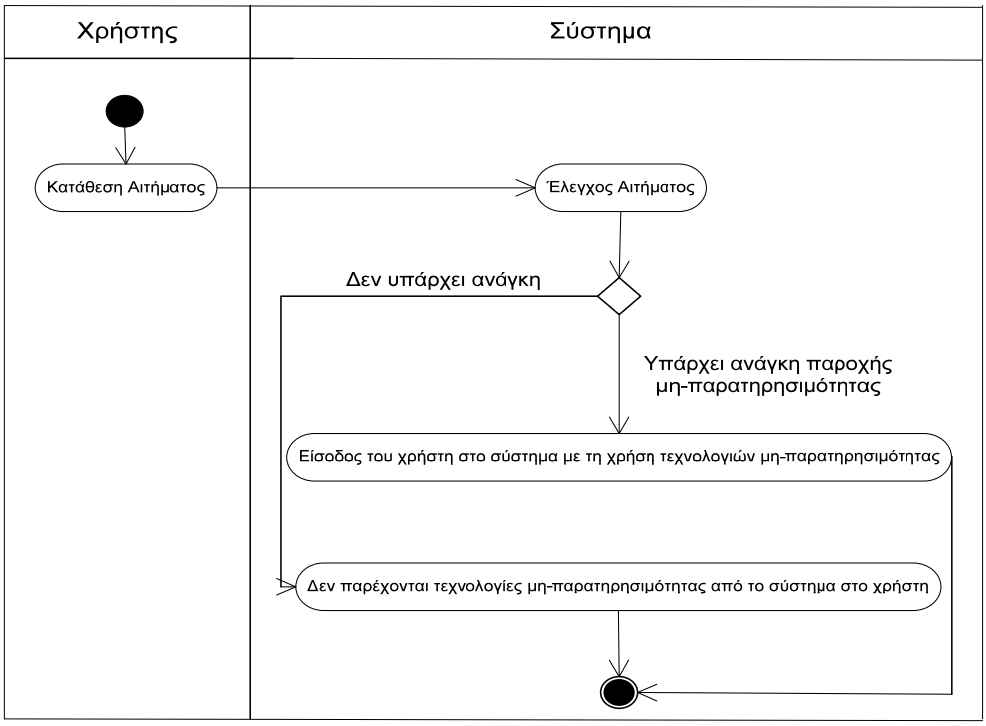
Η ανωνυμία είναι μια απαίτηση που πρέπει να υλοποιείται σε περιπτώσεις που δεν χρειάζεται να αποκαλύπτεται η ταυτότητα του χρήστη που ζητά να χρησιμοποιήσει μια υπηρεσία για την οποία τρίτες οντότητες, όπως άλλοι χρήστες, άλλα συστήματα, κακόβουλοι παρατηρητές κ.λπ. δεν θα πρέπει να μπορούν να αντιληφθούν ποιος τη χρησιμοποιεί και για ποιο σκοπό. Οι τεχνολογίες χρησιμοποιούνται για να προστατέψουν την ανωνυμία του χρήστη όχι μόνο τη στιγμή που αιτείται μιας υπηρεσίας ή αιτείται πρόσβασης σε συγκεκριμένα δεδομένα αλλά καθ' όλη τη διάρκεια της επικοινωνίας. Η ψευδωνυμία χρησιμοποιείται συνήθως όπου δεν μπορεί να χρησιμοποιηθεί η ανωνυμία, αλλά και πάλι με στόχο την προστασία της ανωνυμίας του χρήστη.

Τα πρότυπα ιδιωτικότητας των απαιτήσεων της μη-συνδεσιμότητας και της μη-παρατηρησιμότητας παρουσιάζονται στα ακόλουθα σχήματα 5.10 και 5.11 αντίστοιχα. Τα δύο αυτά πρότυπα έχουν όμοια δομή. Ο χρήστης καταθέτει ένα αίτημα. Με βάση τις απαιτήσεις του συστήματος εάν η μία ή και οι δύο απαιτήσεις πρέπει να υλοποιηθούν τότε ανάλογες τεχνολογίες χρησιμοποιούνται τη στιγμή που ο χρήστης συνδέεται στο σύστημα. Έτσι καθ' όλη τη διάρκεια της συναλλαγής του οι τεχνολογίες

αυτές θα ικανοποιούν τις αντίστοιχες απαιτήσεις της μη-συνδεσιμότητας και της μη- παρατηρησιμότητας.



Σχήμα 5.10. Πρότυπο μη-συνδεσιμότητας



Σχήμα 5.11. Πρότυπο μη-παρατηρησιμότητας

5.2.4. Επιλογή των τεχνολογιών που υποστηρίζουν την υλοποίηση των προαναφερθέντων προτύπων ιδιωτικότητας

Στο τελευταίο στάδιο προσδιορίζεται ποια είναι η πιο ενδεδειγμένη τεχνολογία που μπορεί να υλοποιήσει τις διεργασίες που επηρεάζονται από τις παραμέτρους της ιδιωτικότητας όπως αυτές έχουν ήδη οριστεί από τα προηγούμενα στάδια. Με βάση τα πρότυπα ιδιωτικότητας προτείνονται οι κατάλληλες αρχιτεκτονικές και τεχνολογίες που υποστηρίζουν και υλοποιούν τις παραπάνω διεργασίες.

Συγκεκριμένα, κάθε πρότυπο ιδιωτικότητας περιγράφει τις συγκεκριμένες ενέργειες που πρέπει να υλοποιηθούν για να υποστηριχθεί η αντίστοιχη διεργασία από το σύστημα. Με αυτόν τον τρόπο γίνεται μια υπόδειξη προς τον υπεύθυνο της υλοποίησης του συστήματος, δηλώνοντας το σημείο στο οποίο πρέπει να εφαρμοστεί η προτεινόμενη τεχνολογία ιδιωτικότητας έτσι ώστε να διασφαλιστεί η υλοποίηση της αντίστοιχης παραμέτρου ιδιωτικότητας στη συγκεκριμένη διεργασία. Η αντιστοιχία μεταξύ των προτύπων ιδιωτικότητας και των τεχνολογιών που τα υλοποιούν περιλαμβάνεται στον Πίνακα 5.1.

Όπως φαίνεται και στον πίνακα αυτό, σε κάθε κατηγορία τεχνολογιών ενίσχυση της ιδιωτικότητας ανήκει μια σειρά από μεθοδολογίες και τεχνολογίες, ενώ καταγράφεται ποιες από αυτές υλοποιούν κάθε πρότυπο ιδιωτικότητας (Welfare, US Department of Health Education and 1973; Group, META 2005).

Αξιοποιώντας τον πίνακα αυτόν, ο υπεύθυνος για την υλοποίηση του συστήματος, μπορεί να επιλέξει για κάθε πρότυπο ιδιωτικότητας τις τεχνολογίες εκείνες που θεωρεί ως βέλτιστες, πάντοτε βασιζόμενος στις απαιτήσεις ιδιωτικότητας που πρέπει να υλοποιηθούν, καθώς και στο συγκεκριμένο πλαίσιο αρμοδιοτήτων του οργανισμού στον οποίο θα ενσωματωθεί το υπό-ανάπτυξη σύστημα.

Πίνακας 5.1. Αντιστοίχηση Προτύπων Ιδιωτικότητας - Τεχνολογιών Υλοποίησης

Πρότυπα Διεργασιών Ιδιωτικότητας	Διαχειριστικά Εργαλεία					Πληροφοριακά Εργαλεία			Προϊόντα, υπηρεσίες και αρχιτεκτονικές Ανωνυμίας										Εργαλεία Ψευδωνυμίας		Εργαλεία Διαγραφής Ιχνών και Αποδεικτικών				Εργαλεία Κρυπτογράφησης		
	Identity Management	Biometrics	Smart Cards	Permission Management	Monitoring and Audit tools	Privacy Policy Generators	Privacy Policy Readers /Validators	Privacy Compliance Scanning	Browsing Pseudonyms	Virtual Email Addresses	Trusted Third Parties	Surrogate Keys	Crowds	Onion Routing	DC-Nets	Mix-Nets	Hordes	GAP	Tor	CRM Personalization	Application Data Management	Spyware Detection and Removal	Browser Cleaning Tools	Activity Traces eraser	Harddisk data eraser	Encrypting Email	Encrypting Transactions	Encrypting Documents
Αυθεντικοποίηση	X	X	X	X	X																							
Εξουσιοδότηση	X	X	X	X	X																							
Αναγνώριση	X	X	X	X	X																							
Προστασία Δεδομένων	X	X	X	X	X	X	X	X																				X
Ανωνυμία ή/και Ψευδωνυμία	X	X	X	X					X	X	X		X	X	X	X	X	X	X	X	X	X			X			
Μη-Συνδεσιμότητα											X	X		X		X	X	X	X	X	X	X	X	X	X			
Μη-Παρατηρησιμότητα			X	X	X												X	X	X			X	X	X	X	X	X	X

Επομένως, δεν προτείνεται μία μόνο συγκεκριμένη λύση, αλλά εντοπίζονται μια σειρά από τεχνικές που μπορούν να υλοποιήσουν τα πρότυπα ιδιωτικότητας που ορίστηκαν στο προηγούμενο στάδιο. Ο υπεύθυνος υλοποίησης του συστήματος είναι εκείνος που θα επιλέξει ποια αρχιτεκτονική είναι καλύτερο να εφαρμοστεί στο υπό-ανάπτυξη σύστημα βασιζόμενος σε παράγοντες και προτεραιότητες που έχει θέσει ο οργανισμός, όπως κόστος, αποδοτικότητα του νέου συστήματος, πολυπλοκότητα υλοποίησης, κ.λπ.

5.3. Συμπεράσματα

Στο κεφάλαιο αυτό αναπτύχθηκε η μεθοδολογία PriS στόχος της οποίας είναι η ανάλυση των απαιτήσεων ιδιωτικότητας. Η PriS βοηθά τόσο στην εφαρμογή των απαιτήσεων στις δραστηριότητες ενός οργανισμού όσο και στη παροχή ενός συστηματικού τρόπου εύρεσης

ορθών μοντέλων συστημάτων για την υλοποίηση των απαιτήσεων. Το εννοιολογικό μοντέλο της PriS εξελίσσει αυτό της μεθοδολογίας EKD για την αποτύπωση της γνώσης του οργανισμού. Ειδικότερα, η PriS χρησιμοποιεί ένα ειδικό τύπο στόχου για να συμβολίσει τις απαιτήσεις ιδιωτικότητας, τον στόχο ιδιωτικότητας. Οι στόχοι υλοποιούνται από διεργασίες και αυτές αναλύονται σε πρότυπα ιδιωτικότητας τα οποία περιγράφουν τις ενέργειες που πρέπει να γίνουν σε κάθε διεργασία για να υλοποιηθεί η αντίστοιχη απαίτηση ιδιωτικότητας. Τέλος προτείνονται μια σειρά από τεχνολογίες για την υλοποίηση των προτύπων ιδιωτικότητας.

Ο τρόπος λειτουργίας της PriS, όπως περιγράφεται, υποθέτει ότι οι στόχοι ιδιωτικότητας αποτελούν στρατηγικούς στόχους του οργανισμού και άρα εμφανίζονται στο υψηλότερο επίπεδο της ιεραρχίας των στόχων. Σε διαφορετική περίπτωση, όταν δηλαδή ένας στόχος ιδιωτικότητας ανακαλυφθεί κατά την ανάλυση των στόχων σε χαμηλότερο επίπεδο, τότε τα βήματα β,γ, και δ της μεθοδολογίας εφαρμόζονται σε κάθε «κλαδί» της ιεραρχίας των στόχων που επηρεάζεται.

Στη παράγραφο 5.1 παρουσιάστηκε το εννοιολογικό μοντέλο της μεθοδολογίας ενώ στη παράγραφο 5.2 αναλύθηκε ο τρόπος λειτουργίας της. Στο επόμενο κεφάλαιο παρουσιάζεται το φορμαλιστικό μοντέλο της PriS.

6. Το φορμαλιστικό μοντέλο της PriS

Το κεφάλαιο αυτό ορίζει με φορμαλιστικό τρόπο τα βασικά στάδια της προτεινόμενης μεθοδολογίας που περιγράφηκε στο προηγούμενο κεφάλαιο. Στόχος είναι η σαφής απεικόνιση των εννοιών που χρησιμοποιεί η PriS, καθώς και των βασικών σταδίων της μεθοδολογίας ούτως ώστε να είναι δυνατή η ανάπτυξη ενός εργαλείου που να υποστηρίζει τις ενέργειες αυτές.

6.1. Βήμα 1ο - Προσδιορισμός των απαιτήσεων-στόχων ιδιωτικότητας στο υπό-ανάπτυξη σύστημα

Η βασική δομή αναπαράστασης που χρησιμοποιείται στο εννοιολογικό μοντέλο της PriS είναι αυτή της ιεραρχίας των στόχων, ή ακριβέστερα του γράφου στόχων αφού πέρα από τις σχέσεις Ή/ΚΑΙ είναι δυνατή και η ύπαρξη σχέσεων μεταξύ στόχων του ίδιου επιπέδου (σχέση ΕΠΗΡΕΑΖΕΙ).

Με βάση αυτό, το μοντέλο στόχων ορίζεται ως ένας κατευθυνόμενος γράφος (directed graph):

Ορισμός 1: Ορίζεται ως V = (G,E) ένας κατευθυνόμενος γράφος ο οποίος περιγράφει το μοντέλο των στόχων.

$$V = (\{G_1, G_2, G_3, \ldots\ldots\ldots, G_{v-1}, G_v\}, \{ E_1, E_2, E_3, \ldots\ldots\ldots, E_{m-1}, E_m\})$$

όπου, $G_1 \ldots G_v$ είναι το σύνολο των στόχων και υπό-στόχων του συστήματος όπως αυτοί έχουν αναγνωρισθεί από τους *ενδιαφερόμενους* του συστήματος και $E_1 \ldots E_m$ το σύνολο των συνδέσεων μεταξύ των στόχων.

Στο σύνολο Ε ανήκουν όλες οι συσχετίσεις μεταξύ των στόχων της ιεραρχίας. Κάθε συσχέτιση ορίζεται από το ζευγάρι των στόχων που συνδέει καθώς και το τύπο της συσχέτισης τους. Πρώτα αναφέρεται ο πιο γενικός στόχος και έπειτα ακολουθεί ο στόχος που τον αναλύει/συγκεκριμενοποιεί. Στο τέλος αναφέρεται η τιμή του τύπου της συσχέτισης που μπορεί να είναι: Ή, ΚΑΙ, ΕΠΗΡΕΑΖΕΙ_ΘΕΤΙΚΑ, ΕΠΗΡΕΑΖΕΙ_ΑΡΝΗΤΙΚΑ. Κάθε τύπος συσχέτισης εκφράζεται με ένα αριθμό από το 1 έως το 4. Με 1 η συσχέτιση τύπου Ή, με 2 η συσχέτιση τύπου ΚΑΙ, με 3 η συσχέτιση ΕΠΗΡΕΑΖΕΙ_ΘΕΤΙΚΑ και με 4 η συσχέτιση ΕΠΗΡΕΑΖΕΙ_ΑΡΝΗΤΙΚΑ. Για παράδειγμα η σχέση $e_i=(G_1, G_2, 2)$ ορίζει τη σύνδεση του στόχου G_1 με το στόχο G_2 και ειδικότερα ότι ο στόχος G_1 αναλύεται στο στόχο G_2 και ο τύπος συσχέτισής τους είναι ο ΚΑΙ. Σε μια σύνδεση ο πρώτος, πιο γενικός στόχος ονομάζεται *στόχος_γονέας* και ο δεύτερος, ο πιο συγκεκριμένος, *στόχος_παιδί*. Έτσι δηλώνεται και το επίπεδό τους στην ιεραρχία του μοντέλου μιας και όπως είναι φυσικό οι στόχοι γονείς είναι πάντοτε σε υψηλότερο επίπεδο από τους στόχους_παιδιά.

Η ιεραρχία των στόχων, στο φορμαλιστικό μοντέλο, μπορεί να οριστεί από το σύνολο των συσχετίσεών τους. Για παράδειγμα, ο στόχος γονέας της ιεραρχίας (ο πιο γενικός στόχος) μπορεί να αναγνωρισθεί μέσω των συσχετίσεων αφού σε καμία δεν θα συμμετέχει ως στόχος_παιδί. Επίσης όλοι οι τελικοί στόχοι του μοντέλου αναγνωρίζονται από το γεγονός ότι δεν συμμετέχουν σε καμία συσχέτιση ως στόχοι_παιδιά.

Ακολούθως πρέπει να καθοριστεί ποιοι από τους στόχους της ιεραρχίας επηρεάζονται και από ποιες απαιτήσεις ιδιωτικότητας. Για το λόγο αυτό έχουν ορισθεί επτά μεταβλητές, οι *μεταβλητές ιδιωτικότητας (privacy variables)*, στο εξής PV, οι οποίες αντιστοιχούν στις επτά

απαιτήσεις ιδιωτικότητας όπως φαίνονται και στο Πίνακα 6.1. Οι μεταβλητές αυτές μπορεί να λάβουν μόνο δύο τιμές, 0 ή 1.

Πίνακας 6.1. Μεταβλητές Ιδιωτικότητας που εκφράζουν τις αντίστοιχες απαιτήσεις ιδιωτικότητας

Μεταβλητές Ιδιωτικότητας	Απαιτήσεις Ιδιωτικότητας
PV1	Αυθεντικοποίηση
PV2	Εξουσιοδότηση
PV3	Αναγνώριση
PV4	Προστασία Δεδομένων
PV5	Ανωνυμία και Ψευδωνυμία
PV6	Μη-Συνδεσιμότητα
PV7	Μη-Παρατηρησιμότητα

Με βάση τα παραπάνω, ισχύει ο ακόλουθος ορισμός για κάθε στόχο της ιεραρχίας.

Ορισμός 2: Κάθε απαίτηση ιδιωτικότητας εκφράζεται από μία μεταβλητή, τη μεταβλητή ιδιωτικότητας, η οποία μπορεί να λάβει μόνο δύο τιμές. Την τιμή 0 ή τη τιμή 1. Σε κάθε στόχο G_i εκχωρούνται επτά τιμές οι οποίες και αντιπροσωπεύουν τις απαιτήσεις ιδιωτικότητας που επηρεάζουν το συγκεκριμένο στόχο.

$$G_i = \{PV1, PV2, PV3, PV4, PV5, PV6, PV7\}, PV_i \in \{0,1\}$$

Κάθε στόχος έχει επτά τιμές οι οποίες ερμηνεύονται με τη σειρά που ορίσθηκαν παραπάνω. Όταν μια μεταβλητή ιδιωτικότητας είναι ίση με 0 σημαίνει ότι η αντίστοιχη απαίτηση ιδιωτικότητας δεν επηρεάζει το συγκεκριμένο στόχο, ενώ αν έχει την τιμή 1 τον επηρεάζει.

Αν ο στόχος G_i δεν είναι τελικός στόχος, δηλαδή έχει στόχους_παιδιά, τότε οι απαιτήσεις ιδιωτικότητας που επηρεάζουν το στόχο αυτό επηρεάζουν τους στόχους_παιδιά αυτού ανάλογα με το τύπο της συσχέτισής τους.

Η υλοποίηση της ιεραρχίας των στόχων καθώς και ο χειρισμός των απαιτήσεων ιδιωτικότητας σε αυτό βασίζεται στις παρακάτω συναρτήσεις και διαδικασίες.

I. Δημιουργία Πίνακα Γειτνίασης (Adjacency Matrix)

Για να αναπαρασταθεί το μοντέλο της ιεραρχίας των στόχων κατασκευάζεται ο ακόλουθος πίνακας ο οποίος ονομάζεται «πίνακας γειτνίασης» (adjacency matrix). Στον πίνακα αυτό συμμετέχουν όλοι οι στόχοι του μοντέλου.

Κάθε κελί λαμβάνει μια τιμή από το 0 έως το 4. Στα κελιά που υπάρχει η τιμή 0 δηλώνεται ότι ο στόχος που αναφέρεται στη γραμμή του πίνακα δεν συσχετίζεται με το στόχο που αναφέρεται στη στήλη του. Στα κελιά που υπάρχει τιμή διάφορη του μηδενός, εμφανίζεται μια τιμή ανάμεσα στο ένα και το τέσσερα. Αυτό σημαίνει ότι ο στόχος που βρίσκεται στη γραμμή συνδέεται με το στόχο που βρίσκεται στη στήλη. Η τιμή δηλώνει και τον τύπο της συσχέτισης όπως ορίστηκε προηγουμένως. Επίσης ο στόχος της γραμμής είναι ο στόχος_γονέας ενώ στόχος της στήλης είναι ο στόχος_παιδί.Ένα παράδειγμα ενός πίνακα γειτνίασης βρίσκεται στο πίνακα 6.2.

Πίνακας 6.2. Πίνακας Γειτνίασης

	G_1	G_2	...	G_n
G_1	0	2	0	0
G_2	0	0	0	1
...	1	1	0	3
G_n	0	0	0	0

II. Assign_pv (G_i) = (PV1,PV2, PV3, PV4, PV5, PV6, PV7)

Η διαδικασία αυτή αναθέτει σε κάθε στόχο της ιεραρχίας επτά τιμές που αντιστοιχούν στις επτά μεταβλητές ιδιωτικότητας του κάθε στόχου ανάλογα με τις απαιτήσεις ιδιωτικότητας που τον επηρεάζουν. Μέσω της διαδικασίας αυτής, περιγράφεται το αντίκτυπο των στόχων ιδιωτικότητας στους στόχους του οργανισμού (σχέση «ΕΧΕΙ_ΑΝΤΙΚΤΥΠΟ_ΣΕ» στο εννοιολογικό μοντέλο του σχήματος 5.2). Για παράδειγμα, αν ο στόχος G_5 επηρεάζεται από τις απαιτήσεις της αυθεντικοποίησης και της μη-συνδεσιμότητας τότε η διαδικασία Assign_pv θα συντασσόταν ως εξής:

$$\text{Assign\_pv } (G_5) = (1,0,0,0,0,1,0)$$

III. Συνάρτηση Read_pv (G_i)

Η συνάρτηση αυτή λαμβάνει ως παράμετρο εισόδου το όνομα ενός στόχου και επιστρέφει τις τιμές των επτά μεταβλητών ιδιωτικότητας που του έχουν ανατεθεί. Έτσι μέσω της συγκεκριμένης συνάρτησης είναι πάντοτε γνωστό, για κάθε στόχο της ιεραρχίας, αν επηρεάζεται και από ποιες απαιτήσεις ιδιωτικότητας. Είναι ευνόητο πως οι στόχοι που δεν επηρεάζονται καθόλου από παραμέτρους ιδιωτικότητας έχουν σε όλες τις μεταβλητές την τιμή 0. Για παράδειγμα αν καλέσουμε τη συνάρτηση Read_pv() με παράμετρο εισόδου το στόχο G_7 και μας επιστρέψει τις ακόλουθες τιμές (1,0,0,0,0,0,1), αυτό σημαίνει ότι ο συγκεκριμένος στόχος είναι σχετικός με την ικανοποίηση των παραμέτρων ιδιωτικότητας για το συγκεκριμένο οργανισμό και συγκεκριμένα επηρεάζεται από τις απαιτήσεις της αυθεντικοποίησης και της μη-παρατηρησιμότητας.

6.2. Βήμα 2ο - Ανάλυση της επίδρασης των απαιτήσεων-στόχων ιδιωτικότητας στις διεργασίες του οργανισμού

Οι διεργασίες υλοποιούν τους τελικούς στόχους της ιεραρχίας που ορίσθηκαν στο προηγούμενο βήμα. Κάθε διεργασία μπορεί να υλοποιεί έναν ή και περισσότερους τελικούς στόχους. Ο φορμαλιστικός ορισμός των διεργασιών στη PriS δίνεται παρακάτω.

Ορισμός 3: Κάθε διεργασία ανήκει σε ένα σύνολο από διεργασίες, το σύνολο P.

$$P = \{P_1, P_2, P_3, \ldots\ldots\ldots, P_{v-1}, P_v\}$$

Το σύνολο P περιλαμβάνει όλες τις διεργασίες που έχει αναγνωρισθεί ότι υλοποιούν τους τελικούς στόχους του συστήματος.

Αρχικά θα πρέπει να αναγνωρισθούν και να συνδεθούν οι τελικοί στόχοι που επηρεάζονται από απαιτήσεις ιδιωτικότητας με τις αντίστοιχες διεργασίες που τους υλοποιούν. Για το σκοπό αυτό ορίζεται η διαδικασία Match_G_P(G_i)=P_k. Η διαδικασία αυτή λαμβάνει ως παράμετρο εισόδου τον τελικό στόχο που επηρεάζεται από παραμέτρους ιδιωτικότητας και θέτει σε αυτόν το όνομα της διεργασίας που τον υλοποιεί. Έτσι δημιουργείται ένας σύνδεσμος μεταξύ των τελικών στόχων και των αντίστοιχων διεργασιών που τους υλοποιούν (Σχέση ΥΛΟΠΟΙΕΙΤΑΙ στο εννοιολογικό μοντέλο του σχήματος 5.2). Στο τέλος αυτής της φάσης δύο ενέργειες έχουν επιτευχθεί: [α] Η αναγνώριση των διεργασιών σχετικών με την υλοποίηση των παραμέτρων ιδιωτικότητας του συστήματος και [β] η σύνδεση αυτών με τους τελικούς στόχους της ιεραρχίας που επηρεάζονται από παραμέτρους ιδιωτικότητας.

Στη συνέχεια αναγνωρίζονται τα πρότυπα ιδιωτικότητας που πρέπει να εφαρμοστούν στις διεργασίες που αναφέρθηκαν προηγουμένως αφενός μεν για να γίνει η σωστή διαμόρφωση και ανάλυση των διεργασιών και αφετέρου για να μπορέσει μετά η μεθοδολογία να προτείνει τις σωστές τεχνικές υλοποίησης των διεργασιών αυτών.

Για την υλοποίηση αυτής της ενέργειας απαιτείται αντιστοίχηση του κάθε προτύπου ιδιωτικότητας σε μια μεταβλητή, τη *μεταβλητή προτύπου διεργασίας (process pattern variable)*, στο εξής PP. Στον Πίνακα 6.3 παρουσιάζεται η αντιστοιχία αυτή.

Πίνακας 6.3. Αντιστοίχηση των πρότυπων ιδιωτικότητας σε αντίστοιχες μεταβλητές

Μεταβλητές Προτύπων Ιδιωτικότητας	**Πρότυπα Ιδιωτικότητας**
PP1	Πρότυπο Αυθεντικοποίησης
PP2	Πρότυπο Εξουσιοδότησης
PP3	Πρότυπο Αναγνώρισης
PP4	Πρότυπο Προστασίας Δεδομένων
PP5	Πρότυπο Ανωνυμίας & Ψευδωνυμίας
PP6	Πρότυπο Μη-Συνδεσιμότητας
PP7	Πρότυπο Μη-Παρατηρησιμότητας

Οι μεταβλητές προτύπων ιδιωτικότητας ακολουθούν την ίδια λογική με τις μεταβλητές ιδιωτικότητας που περιγράφηκαν προηγουμένως. Πιο συγκεκριμένα, σε κάθε διεργασία ανατίθενται επτά τιμές που αντιστοιχούν στις επτά μεταβλητές προτύπων ιδιωτικότητας. Κάθε μεταβλητή μπορεί να λάβει δύο τιμές, 0 ή 1. Αν λάβει την τιμή 0 σημαίνει ότι το συγκεκριμένο πρότυπο δε θα εφαρμοστεί στη συγκεκριμένη διεργασία, ενώ αν λάβει την τιμή 1 συμβαίνει το αντίθετο.

Με βάση αυτά φτάνουμε στον ακόλουθο ορισμό που ισχύει για κάθε διεργασία.

Ορισμός 4: Κάθε πρότυπο ιδιωτικότητας εκφράζεται από μία μεταβλητή, τη μεταβλητή προτύπου ιδιωτικότητας η οποία μπορεί να λάβει μόνο δύο τιμές. Την τιμή 0 ή την τιμή 1. Σε κάθε διεργασία P_i εκχωρούνται επτά τιμές, οι οποίες και δηλώνουν τα πρότυπα ιδιωτικότητας που θα εφαρμοστούν στην κάθε διεργασία.

$$P_i = \{PP1,PP2,PP3,PP4,PP5,PP6,PP7\} , PP_i \in \{0,1\}$$

6.3. Βήμα 3ο - Διαμόρφωση των διεργασιών που επηρεάζονται από τις απαιτήσεις-στόχους ιδιωτικότητας με χρήση προτύπων ιδιωτικότητας

Στο προηγούμενο βήμα αναφέρθηκε ότι σε κάθε διεργασία ανατίθεται ένας αριθμός από πρότυπα ιδιωτικότητας. Τα πρότυπα αυτά επιλέγονται για κάθε διεργασία ξεχωριστά ανάλογα με τις απαιτήσεις ιδιωτικότητας που επηρεάζουν τους τελικούς στόχους, οι οποίοι στόχοι υλοποιούνται από τις διεργασίες αυτές. Για να καθοριστούν οι απαιτήσεις ιδιωτικότητας που περιορίζουν κάθε στόχο, αρκεί να μελετηθούν οι τιμές των μεταβλητών ιδιωτικότητας, όπως προαναφέρθηκε.

Παρόλο που ο ορισμός της τιμής των μεταβλητών ιδιωτικότητας γίνεται απευθείας, ως ένα σύνολο επτά στοιχείων, στην πραγματικότητα υπάρχει και μια κατηγοριοποίηση των τιμών αυτών. Συγκεκριμένα, οι πρώτες τέσσερις τιμές σχετίζονται με θέματα αναγνώρισης, ενώ οι τελευταίες τρεις με θέματα ανωνυμίας. Με άλλα λόγια, οι πρώτες τέσσερις απαιτήσεις φροντίζουν για την προστασία της ιδιωτικότητας με την επικέντρωση στην αναγνώριση του κάθε χρήστη και την κατοχύρωση

πρόσβασης ανάλογα με τα δικαιώματα που έχει και τα δεδομένα που προσπαθεί να προσπελάσει. Η προστασία της ιδιωτικότητας με βάση την αναγνώριση στηρίζεται στο γεγονός ότι κανένας χρήστης δεν μπορεί να παραβιάσει το απόρρητο και τα προσωπικά δεδομένα του άλλου εκτός αν το δικαιούται ή έχει πρόσβαση σε αυτό. Οι τελευταίες τρεις απαιτήσεις φροντίζουν για την προστασία της ιδιωτικότητας με την επικέντρωση στην προστασία της ανωνυμίας των χρηστών ή στην προστασία των δεδομένων των χρηστών από την αποκάλυψη σε επικίνδυνες τρίτες οντότητες που σκοπό έχουν να υποκλέψουν και να εκμεταλλευτούν προσωπικά δεδομένα.

Με βάση την παραπάνω κατηγοριοποίηση, οι τιμές των επτά μεταβλητών ιδιωτικότητας του κάθε τελικού στόχου, εξετάζονται ξεχωριστά και εφαρμόζονται διαφορετικοί κανόνες σε κάθε περίπτωση για να γίνει η επιλογή των προτύπων ιδιωτικότητας που θα εφαρμοστούν σε κάθε διεργασία.

Συγκεκριμένα, όσον αφορά στις τέσσερις πρώτες απαιτήσεις ιδιωτικότητας, η επιλογή του προτύπου ιδιωτικότητας που θα εφαρμοστεί εξαρτάται αποκλειστικά από το ποια μεταβλητή είναι η τελευταία στη σειρά των τεσσάρων που έχει τιμή ίση με 1. Με άλλα λόγια, όταν εξετάζονται οι πρώτες τέσσερις μεταβλητές ιδιωτικότητας, εφαρμόζεται πάντοτε το αντίστοιχο πρότυπο ιδιωτικότητας της τελευταίας μεταβλητής που έχει τιμή ίση με 1. Αυτό συμβαίνει διότι, όπως προαναφέρθηκε στο κεφάλαιο με τα πρότυπα ιδιωτικότητας, τα πρώτα τέσσερα πρότυπα (της αυθεντικοποίησης, της εξουσιοδότησης, της αναγνώρισης και της προστασίας δεδομένων) είναι έτσι δομημένα ώστε το επόμενο στη σειρά περιέχει και το προηγούμενο. Έτσι, στην περίπτωση που ένας τελικός στόχος πρέπει να υλοποιήσει τις απαιτήσεις της αυθεντικοποίησης και της προστασίας δεδομένων, από τη στιγμή που η προστασία δεδομένων έπεται της αυθεντικοποίησης, το πρότυπο ιδιωτικότητας που θα

εφαρμοστεί στη διεργασία που θα υλοποιήσει το τελικό στόχο θα είναι αυτό της προστασίας δεδομένων μιας και αυτό καλύπτει και το πρότυπο της αυθεντικοποίησης. Το συγκεκριμένο παράδειγμα που αναφέρθηκε περιγράφεται φορμαλιστικά ως ακολούθως:

$G_i = \{1,0,0,1,0,0,0\}$	Οι απαιτήσεις ιδιωτικότητας που επηρεάζουν το στόχο G_i
Match_G_P $(G_i) = P_k$	Η διεργασία P_k υλοποιεί το στόχο G_i
$P_k = \{0,0,0,1,0,0,0\}$	Τα πρότυπα ιδιωτικότητας που εφαρμόζονται στην διεργασία P_k

Ο Πίνακας 6.4 παρουσιάζει τα πρότυπα ιδιωτικότητας που εφαρμόζονται στις διεργασίες ανάλογα με τις τιμές των μεταβλητών ιδιωτικότητας των τελικών στόχων που υλοποιούνται από τις διεργασίες αυτές.

Όπως φαίνεται στον πίνακα αυτόν, το πρότυπο ιδιωτικότητας που εφαρμόζεται σε κάθε διεργασία, πάντα όσον αφορά τις πρώτες τέσσερις απαιτήσεις ιδιωτικότητας, είναι πάντοτε το τελευταίο στη σειρά όπου η αντίστοιχη μεταβλητή ιδιωτικότητας έχει τη τιμή 1.

Η επιλογή των αντίστοιχων προτύπων ιδιωτικότητας που εφαρμόζονται στις διεργασίες με βάση τις τελευταίες τρεις απαιτήσεις ιδιωτικότητας (ανωνυμία & ψευδωνυμία, μη-συνδεσιμότητα, μη-παρατηρησιμότητα) εξαρτάται αποκλειστικά από την τιμή της κάθε μιας μεταβλητής ιδιωτικότητας των τελικών στόχων.

Πιο συγκεκριμένα, για κάθε μία από τις τρεις τελευταίες μεταβλητές ιδιωτικότητας που ανατίθεται σε ένα στόχο και έχει τιμή 1 εφαρμόζεται το αντίστοιχο πρότυπο ιδιωτικότητας στη διεργασία που υλοποιεί τον τελικό στόχο με τη συγκεκριμένη απαίτηση.

Πίνακας 6.4. Επιλογή προτύπων ιδιωτικότητας με βάση τις πρώτες τέσσερις τιμές των μεταβλητών ιδιωτικότητας

PV1	PV2	PV3	PV4	Πρότυπο Ιδιωτικότητας
1	0	0	0	Αυθεντικοποίηση
0	1	0	0	Εξουσιοδότηση
1	1	0	0	Εξουσιοδότηση
0	0	1	0	Αναγνώριση
0	1	1	0	Αναγνώριση
1	0	1	0	Αναγνώριση
1	1	1	0	Αναγνώριση
0	0	0	1	Προστασία Δεδομένων
…	…	…	1	Προστασία Δεδομένων[6]

Ωστόσο, υπάρχουν τέσσερις περιπτώσεις στις οποίες δεν ισχύει ο γενικός αυτός κανόνας εφαρμογής των προτύπων με βάση τις τιμές της κάθε απαίτησης αλλά εφαρμόζεται το πρότυπο εκείνο που προκύπτει από το συνδυασμό και των τριών τιμών. Οι τέσσερις αυτές περιπτώσεις παρουσιάζονται στο παρακάτω Πίνακα 6.5.

Συνδυάζοντας τις παραπάνω περιπτώσεις και κανόνες επιστρέφονται ως αποτέλεσμα οι τιμές των επτά μεταβλητών προτύπων ιδιωτικότητας. Για παράδειγμα, έστω ότι ο τελικός στόχος G_i έχει τις ακόλουθες επτά τιμές στις μεταβλητές ιδιωτικότητας που του έχουν ανατεθεί: (0,1,0,1,0,1,0). Αυτό σημαίνει ότι ο στόχος αυτός ικανοποιεί τις

[6] Οι τελείες στις πρώτες τρεις μεταβλητές υποδηλώνουν ότι, ανεξάρτητα με τις τιμές τους, από τη στιγμή που η τέταρτη μεταβλητή, αυτή της προστασίας δεδομένων, είναι ίση με 1 τότε το προτεινόμενο πρότυπο διεργασίας θα είναι αυτό της προστασίας δεδομένων.

απαιτήσεις της εξουσιοδότησης, της προστασίας δεδομένων και της μη-συνδεσιμότητας. Έστω επίσης ότι η διεργασία P_k υλοποιεί το στόχο G_i. Στην περίπτωση αυτή και με βάση τις περιπτώσεις και τους κανόνες που προαναφέρθηκαν, τα πρότυπα ιδιωτικότητας που θα εφαρμοστούν στη συγκεκριμένη διεργασία είναι δύο: το πρότυπο της προστασίας δεδομένων και το πρότυπο της μη-συνδεσιμότητας.

Πίνακας 6.5. Επιλογή προτύπων ιδιωτικότητας βάση των τελευταίων τριών τιμών των μεταβλητών ιδιωτικότητας

PV5	PV6	PV7	Πρότυπο Ιδιωτικότητας
1	0	0	Ανωνυμία & Ψευδωνυμία
0	1	0	Μη-Συνδεσιμότητα
0	0	1	Μη-Παρατηρησιμότητα
0	1	1	Μη-Παρατηρησιμότητα

Όπως όμως προαναφέρθηκε, κάθε διεργασία μπορεί να υλοποιεί περισσότερους από έναν τελικούς στόχους. Στην περίπτωση αυτή υπάρχει ένα ενδιάμεσο βήμα πριν την επιλογή των προτύπων ιδιωτικότητας που θα εφαρμοστούν στη διεργασία. Συγκεκριμένα, δεν είναι δυνατόν να εφαρμοστούν οι κανόνες που αναφέρθηκαν προηγουμένως στην επιλογή των προτύπων ιδιωτικότητας όταν υπάρχουν δύο ή περισσότεροι τελικοί στόχοι μιας και δεν μπορεί άμεσα να εξαχθεί ο ορθός συνδυασμός τιμών εφόσον δεν υπάρχουν επτά τιμές αλλά υπάρχουν τόσες επτάδες τιμών όσοι και οι τελικοί στόχοι που υλοποιούνται από την ίδια διεργασία. Στην περίπτωση αυτή λοιπόν δημιουργείται ένας ιδεατός στόχος ονόματι G' ο οποίος αποτελεί την διάζευξη των τιμών των στόχων που υλοποιούνται από την ίδια διεργασία. Το αποτέλεσμα της ένωσης είναι ότι ο στόχος G' θα περιέχει πάντοτε, για κάθε τιμή μεταβλητής ιδιωτικότητας, τη μέγιστη τιμή που βρήκε από τους στόχους που συμμετείχαν στην διάζευξη. Για

παράδειγμα, ας θεωρηθεί ότι ο στόχος G_i με τιμές στις μεταβλητές ιδιωτικότητας (0,1,0,0,1,0,0) και ο στόχος G_t με τιμές (1,1,0,1,1,0,1) υλοποιούνται από την ίδια διεργασία, την P_k. Στην περίπτωση αυτή για να αποφασιστεί ποια πρότυπα ιδιωτικότητας θα εφαρμοστούν στη διεργασία P_k θα πρέπει πρώτα να προηγηθεί η δημιουργία ενός στόχου, του G' με τιμές τις μεγαλύτερες για κάθε επιμέρους τιμή ανάμεσα στους στόχους G_i και G_t. Δηλαδή οι τιμές του G' θα ήταν οι (1,1,0,1,1,0,1). Η επιλογή των προτύπων θα γίνει με βάση τις τιμές του ιδεατού στόχου με αποτέλεσμα να εφαρμοστούν στη διεργασία P_k τα πρότυπα εκείνα που θα ικανοποιούν και το στόχο G_i αλλά και το στόχο G_t.

Ορισμός 5: $\forall G_i \in G$, που υλοποιείται από τη διεργασία P_k, ένας νέος στόχος G' δημιουργείται και ορίζεται ως εξής:

$$G' = G^i \vee G^j \vee \ldots \vee G^k$$

$$PV'_l = [PV^i_l \vee PV^j_l \vee \ldots \vee PV^k_l]$$

όπου

κ = αριθμός των τελικών στόχων που υλοποιούνται από την ίδια διεργασία

l = 1,2,..,7 (οι επτά μεταβλητές ιδιωτικότητας του κάθε στόχου)

Με βάση τον παραπάνω ορισμό, λαμβάνονται πάντοτε οι μέγιστες τιμές των μεταβλητών ιδιωτικότητας των τελικών στόχων που υλοποιούνται από την ίδια διεργασία και δημιουργείται ένας ιδεατός στόχος G', ο οποίος αποτελείται από τις μέγιστες τιμές των μεταβλητών ιδιωτικότητας των τελικών στόχων. Με βάση τις τιμές αυτές γίνεται και η επιλογή των προτύπων ιδιωτικότητας.

Εκτός από τη διαδικασία Match_G_P που παρουσιάσθηκε προηγουμένως και σκοπός της είναι η σύνδεση ενός τελικού στόχου με την αντίστοιχη διεργασία που τον υλοποιεί, υπάρχουν και άλλες διαδικασίες και συναρτήσεις που πρέπει να ορισθούν για να μπορέσει να

υλοποιηθεί ο παραπάνω περιγραφικός τρόπος λειτουργίας του φορμαλιστικού μοντέλου της PriS.

i) Διαδικασία Init(P_k)

Σκοπός της διαδικασίας αυτής είναι η αρχικοποίηση των τιμών των μεταβλητών προτύπων ιδιωτικότητας μιας διεργασίας. Συγκεκριμένα, λαμβάνει ως παράμετρο εισόδου το όνομα μιας διεργασίας και αναθέτει σε όλες τις μεταβλητές προτύπων ιδιωτικότητας αυτής την τιμή 0 ως αρχική τιμή.

ii) Συνάρτηση Get_pr(i, Read_pv(Gi))

Σκοπός της συνάρτησης Get_pr είναι η εύρεση, ανάγνωση και επιστροφή της τιμής μιας συγκεκριμένης μεταβλητής ιδιωτικότητας ενός συγκεκριμένου στόχου. Με άλλα λόγια, η συνάρτηση αυτή λαμβάνει ως παραμέτρους εισόδου έναν αριθμό από 1-7, ο οποίος αποθηκεύεται σε μια μεταβλητή i καθώς και το όνομα ενός στόχου και επιστρέφει την τιμή της i-ης μεταβλητής ιδιωτικότητας αυτού του στόχου.

iii) Συνάρτηση Locate_pp(Gi)

Σκοπός της συνάρτησης αυτής είναι ο καθορισμός των προτύπων ιδιωτικότητας που αντιστοιχούν σε μια διεργασία με βάση τις παραμέτρους ιδιωτικότητας του τελικού στόχου. Πιο συγκεκριμένα, η συνάρτηση αυτή λαμβάνει ως παράμετρο εισόδου το όνομα ενός τελικού στόχου (ή αν είναι πολλοί λαμβάνει ως είσοδο τον ιδεατό στόχο G') και επιστρέφει ως αποτέλεσμα τα πρότυπα ιδιωτικότητας που θα εφαρμοστούν στη διεργασία που θα υλοποιήσει το στόχο ή τους στόχους αυτούς. Η συνάρτηση αυτή επιστρέφει τέσσερις τιμές σε τέσσερις

μεταβλητές με τα εξής ονόματα: id, an, unlink, unob. Η μεταβλητή id λαμβάνει μια τιμή από το 1 έως το 4 ανάλογα με το πιο από τα τέσσερα πρώτα πρότυπα ιδιωτικότητας θα εφαρμοστεί. Η μεταβλητή an λαμβάνει τη τιμή 1 αν πρόκειται να εφαρμοστεί το πρότυπο της ανωνυμίας/ψευδωνυμίας και 0 αν όχι. Με την ίδια λογική οι μεταβλητές unlink και unob λαμβάνουν τη τιμή 0 ή 1 στις περιπτώσεις εφαρμογής του προτύπου της μη-συνδεσιμότητας και της μη-παρατηρησιμότητας αντίστοιχα. Στη συνέχεια αναφέρεται πώς από τις μεταβλητές αυτές επιλέγονται τα πρότυπα ιδιωτικότητας που θα εφαρμοστούν.

Για να γίνει πιο κατανοητός ο τρόπος λειτουργίας της συνάρτησης Locate_pp() παρατίθεται ο αλγόριθμός της:

```
Locate_pp(Gi)

an=0
id=0
for i=1 to 4
        if Get_pr(i,Read_pv(Gi)) = 1 then id=i
end for
if Get_pr(5,Read_pv(Gi)) = 1 then
        an=1
end if
if Get_pr(6,Read_pv(Gi)) = 1 and Get_pv(7,Read_pv(Gi)) = 1 then
        unlink=0
        unob=1
else
        unlink=Get_pr(6,Read_pv(Gi))
        unob=Get_pr(7,Read_pv(Gi))
end if
```

Συγκεκριμένα, η συνάρτηση Locate_pp() χρησιμοποιεί τέσσερις μεταβλητές που σκοπό έχουν να αποθηκεύσουν το αποτέλεσμα της

συνάρτησης, δηλαδή ποια πρότυπα ιδιωτικότητας θα εφαρμοστούν και ποια όχι. Οι μεταβλητές αυτές, όπως προαναφέρθηκε, είναι οι id, an, unlink, unob. Η μεταβλητή id χρησιμοποιείται για τις πρώτες τέσσερις απαιτήσεις. Όπως προαναφέρθηκε, η επιλογή των προτύπων ιδιωτικότητας για τις πρώτες τέσσερις απαιτήσεις εξαρτάται πάντοτε από την τελευταία απαίτηση στη σειρά που έχει τιμή ίση με 1. Σκοπός της μεταβλητής id είναι να κρατήσει ποια είναι η τελευταία από τις πρώτες τέσσερις απαιτήσεις που έχει αυτή την τιμή. Έτσι, η συγκεκριμένη μεταβλητή, λαμβάνει πάντοτε μια τιμή από το 0 έως το 4. Η μεταβλητή an λαμβάνει τιμή 1 αν θα εφαρμοστεί πρότυπο ανωνυμίας/ψευδωνυμίας και 0 σε αντίθετη περίπτωση. Το ίδιο ισχύει και για τις μεταβλητές unlink και unob για τα πρότυπα της μη-συνδεσιμότητας και μη-παρατηρησιμότητας, αντίστοιχα. Υπάρχουν και οι εξαιρέσεις που αναφέρθηκαν στον Πίνακα 6.4 τις οποίες λαμβάνει υπόψη η συνάρτηση κατά τη φάση της επιλογής των προτύπων.

Ειδικότερα, ξεκινώντας η συνάρτηση Locate_pp(), αρχικοποιεί τις τέσσερις μεταβλητές που αναφέρθηκαν με την τιμή 0. Έπειτα, με τη χρήση της συνάρτησης Get_pr() διαβάζει μία-μία τις τιμές των πρώτων τεσσάρων μεταβλητών ιδιωτικότητας (μεταβλητές PV) του τελικού στόχου που έχει λάβει ως όρισμα (G_i) και διατηρεί στη μεταβλητή id τη σειρά της τελευταίας απαίτησης που έχει τιμή ίση με 1. Έτσι, για τις πρώτες τέσσερις απαιτήσεις ιδιωτικότητας θα εφαρμοστεί, στη διεργασία που θα τον υλοποιήσει, το πρότυπο που αντιστοιχεί στην τελευταία απαίτηση που είχε τιμή 1.

Όσον αφορά την απαίτηση της ανωνυμίας και ψευδωνυμίας η συνάρτηση ελέγχει την αντίστοιχη τιμή της μεταβλητής ιδιωτικότητας και αν είναι ίση με 1 τότε και η μεταβλητή an λαμβάνει την τιμή 1 δηλώνοντας ότι θα εφαρμοστεί το αντίστοιχο πρότυπο ιδιωτικότητας στη διεργασία που θα υλοποιήσει το συγκεκριμένο τελικό στόχο.

Για τις περιπτώσεις της μη-συνδεσιμότητας και μη-παρατηρησιμότητας ισχύει ότι και στην περίπτωση της ανωνυμίας-ψευδωνυμίας με τη διαφορά ότι η συνάρτηση Locate_pp() ελέγχει και την περίπτωση όπου αν και οι δύο τελευταίες μεταβλητές έχουν τιμή ίση με 1 τότε δεν εφαρμόζονται και τα δύο πρότυπα αλλά μόνο αυτό της μη-παρατηρησιμότητας (Πίνακας 6.4). Σε όποια άλλη περίπτωση ισχύει ότι και στην περίπτωση της ανωνυμίας-ψευδωνυμίας.

Μετά την εκτέλεση της συγκεκριμένης συνάρτησης τα αποτελέσματα των προτύπων ιδιωτικότητας που θα εφαρμοστούν στη διεργασία που υλοποιεί τον τελικό στόχο, που δέχτηκε ως παράμετρο εισόδου η συνάρτηση, βρίσκονται στις τέσσερις αυτές μεταβλητές.

iv) Διαδικασία Assign_pp(Pk,id,an,unlink,unob)

Σκοπός της διαδικασίας αυτής είναι να εφαρμόσει σε μια διεργασία, που υλοποιεί τελικούς στόχους επηρεασμένους από απαιτήσεις ιδιωτικότητας, τα πρότυπα ιδιωτικότητας που εντοπίστηκαν από τη συνάρτηση Locate_pp(). Πιο συγκεκριμένα, η διαδικασία αυτή δέχεται ως είσοδο το όνομα μιας διεργασίας και τις τιμές των τεσσάρων μεταβλητών που εξήγαγε η συνάρτηση Locate_pp() και εφαρμόζει τα αντίστοιχα πρότυπα ιδιωτικότητας στην αντίστοιχη διεργασία.

Είναι προφανές ότι η διαδικασία Assign_pp() εκτελείται μετά την ολοκλήρωση της συνάρτησης Locate_pp() μιας και πρέπει να γνωρίζει τις τιμές για τις τέσσερις μεταβλητές ώστε να μπορέσει να εφαρμόσει τα σωστά πρότυπα ιδιωτικότητας στην αντίστοιχη διεργασία. Ο αλγόριθμος της διαδικασίας παρουσιάζεται παρακάτω.

Assign_pp(P_k,id,an,unlink,unob)

Init (Pk)

Pk(id)=1

Pk(5)=an

Pk(6)=unlink

Pk(7)=unob

Η Assign_pp φροντίζει να θέσει τις σωστές τιμές στις επτά μεταβλητές προτύπων ιδιωτικότητας στη διεργασία που αναφέρεται ως πρώτο όρισμα στην ίδια τη διαδικασία. Έτσι με το πέρας αυτής της διαδικασίας έχουν καθοριστεί τα πρότυπα ιδιωτικότητας που θα εφαρμοστούν στη κάθε διεργασία.

Ο τρόπος λειτουργίας της διαδικασίας είναι απλός. Στην αρχή αρχικοποιούνται όλες οι τιμές των μεταβλητών προτύπων ιδιωτικότητας με τη χρήση της διαδικασίας Init(). Στη συνέχεια η μεταβλητή που βρίσκεται στη θέση που δηλώνει η τιμή της μεταβλητής id παίρνει τη τιμή 1. Όπως αναφέρθηκε πριν η μεταβλητή αυτή μπορεί να λάβει μία τιμή από το 0 έως το 4. Αν δεν υπάρχει καμία μεταβλητή ιδιωτικότητας από τις πρώτες τέσσερις που να έχει τη τιμή 1 τότε η id θα ισούται με 0. Όταν φτάσει στη διαδικασία Assign_pp θα πάει να ανατεθεί η τιμή 1 στη μεταβλητή που βρίσκεται στη θέση 0 η οποία φυσικά και δεν υπάρχει. Αν όμως υπάρχουν μία ή περισσότερες μεταβλητές ιδιωτικότητας, από τις πρώτες τέσσερις, που είχαν τιμή 1 τότε η id θα περιέχει τη θέση της τελευταίας που είχε τη τιμή αυτή. Το Pk(id)=1 σημαίνει ότι η διαδικασία θα πάει και θα αναθέσει ως τιμή της μεταβλητής προτύπου ιδιωτικότητας που βρίσκεται στη θέση id τη τιμή 1.

Ομοίως και για τις υπόλοιπες μεταβλητές. Οι μεταβλητές an, unlink και unob περιέχουν τις τιμές 1 ή 0 ανάλογα με το αν θα εφαρμοστεί το αντίστοιχο πρότυπο ιδιωτικότητας ή όχι. Έτσι και οι μεταβλητές προτύπου ιδιωτικότητας θα λάβουν τις τιμές των μεταβλητών αυτών.

Ολοκληρώνοντας και αυτό το βήμα, έχουν αναγνωρίστει οι διεργασίες που υλοποιούν τους τελικούς στόχους που επηρεάζονται από στόχους ιδιωτικότητας καθώς επίσης έχουν εφαρμοστεί τα αντίστοιχα πρότυπα ιδιωτικότητας.

6.4. Βήμα 4ο – Επιλογή των τεχνολογιών που υποστηρίζουν την υλοποίηση των προαναφερθέντων προτύπων ιδιωτικότητας

Στο τελευταίο βήμα, προτείνεται μια σειρά από τεχνολογίες και αρχιτεκτονικές για την υλοποίηση των προτύπων ιδιωτικότητας που εφαρμόστηκαν στις αντίστοιχες διεργασίες ιδιωτικότητας στο προηγούμενο βήμα.

Για να εκφραστεί φορμαλιστικά η διαδικασία της επιλογής τεχνολογιών και αρχιτεκτονικών απαιτείται η ένταξη όλων αυτών σε ένα σύνολο τεχνολογιών όπως ορίζεται παρακάτω.

Ορισμός 6: Κάθε τεχνολογία IT_i ανήκει σε ένα σύνολο τεχνολογιών, το σύνολο IT:

$$IT = \{IT_1, IT_2, IT_3, \ldots\ldots\ldots, IT_{\mu-1}, IT_{\mu}\}$$

Για να μπορέσει να γίνει η αντιστοιχία μεταξύ των προτύπων ιδιωτικότητας και των τεχνολογιών που τα υλοποιούν ανατίθενται σε κάθε τεχνολογία επτά τιμές που δηλώνουν ποια πρότυπα μπορεί να υλοποιήσει η κάθε μια από αυτές.

Συγκεκριμένα, σε κάθε τεχνολογία ανατίθενται επτά τιμές οι οποίες δηλώνουν ποια πρότυπα ιδιωτικότητας υλοποιεί η κάθε μία βάση του Πίνακα 5.1. Για παράδειγμα, η αρχιτεκτονική Tor υλοποιεί τα

πρότυπα της ανωνυμίας-ψευδωνυμίας, της μη-συνδεσιμότητας και της μη-παρατηρησιμότητας. Από τη στιγμή που για κάθε πρότυπο ανατίθεται η τιμή 0 ή 1 ανάλογα με το αν υλοποιείται η όχι και από τη στιγμή επίσης που η σειρά των προτύπων παραμένει η ίδια όπως και προηγουμένως, η ανάθεση των επτά τιμών στη τεχνολογία Tor θα ήταν η εξής: (0,0,0,0,1,1,1) σημαίνοντας ότι η συγκεκριμένη τεχνολογία δεν υλοποιεί πρότυπα ιδιωτικότητας των διεργασιών της αυθεντικοποίησης, εξουσιοδότησης, αναγνώρισης και προστασίας δεδομένων ενώ αντίθετα υλοποιεί πρότυπα ιδιωτικότητας της ανωνυμίας-ψευδωνυμίας, μη-συνδεσιμότητας και μη-παρατηρησιμότητας. Για κάθε τεχνολογία λοιπόν ισχύει:

$$IT_i = \{auth,author,ident,dat\_prot,anon\_pseud,unlinkab,unobserv\},$$

$$auth,author,ident,dat\_prot,anon\_pseud,unlinkab,unobserv \in \{0,1\}$$

Οι επτά μεταβλητές λαμβάνουν αντίστοιχα την τιμή 0 ή 1 ανάλογα με το αν η συγκεκριμένη τεχνολογία υλοποιεί το συγκεκριμένο πρότυπο ή όχι. Στην ουσία οι μεταβλητές αντιπροσωπεύουν τα πρότυπα ιδιωτικότητας.

Τα πρότυπα ιδιωτικότητας που έχουν εφαρμοστεί σε κάθε διεργασία από το προηγούμενο βήμα ελέγχονται και προτείνονται μια σειρά από τεχνολογίες που τα υλοποιούν. Για το σκοπό αυτό προτείνεται η συνάρτηση Locate_ITs(P). Συγκεκριμένα, η συνάρτηση αυτή λαμβάνει σαν είσοδο τις τιμές των μεταβλητών προτύπων ιδιωτικότητας των διεργασιών του συστήματος και επιστρέφει τα ονόματα των τεχνολογιών που μπορούν να υλοποιήσουν τα πρότυπα ιδιωτικότητας για κάθε διεργασία. Σε πρώτη φάση η συνάρτηση προτείνει τις τεχνολογίες που ικανοποιούν ακριβώς τα πρότυπα ιδιωτικότητας της κάθε διεργασίας. Π.χ αν μια διεργασία έχει τις εξής επτά τιμές (0,1,0,0,1,0,1) τότε η συνάρτηση θα επιστρέψει τα ονόματα των τεχνολογιών που υλοποιούν και τα τρία

αυτά πρότυπα, δηλαδή όσα έχουν ακριβώς τις ίδιες τιμές όπως αυτές της διεργασίας. Έπειτα προτείνονται οι τεχνολογίες που υλοποιούν έστω και ένα από τα πρότυπα ιδιωτικότητας που εφαρμόζονται στη κάθε διεργασία. Ο αλγόριθμος της συνάρτησης παρουσιάζεται παρακάτω:

```
Locate_ITs(P)
For i=1 to K
      positions=0
      for c=1 to N
           temp[c]=0
      end for
      for j=1 to N
          count=0
          for l=1 to 7
              if P[ i,l] =T_P[ j,l] then
                        count=count+1
              end if
           if count=7 then
              positions=positions+1
              temp[positions]=j
           end if
           end for
      end for
      write ('Technologies for Process P',i)
      write ('Primary Suggestions')
      if positions=0 then
              write (' No Primary Suggestions')
      else
              for m=1 to positions
                        write (Names_T[temp[m]])
              end for
      end if
      write ('Secondary Suggestions')
```

```
    for j=1 to N
        for l=1 to 7
            if (P[ i,l] = 1) and (T_P[ j,l]=1) then
                flag=0
                for m=1 to positions
                    if temp[m]=j then
                        flag=1
                    end if
                end for
                if flag=0 then
                    write (Names_T[ j ])
                    positions:=positions+1
                    temp[positions]:=j
                end if
            end if
        end for
    end for
end for
```

Ο πίνακας P είναι ένας πίνακας δύο διαστάσεων με K γραμμές και 7 στήλες, όπου K είναι το σύνολο των διεργασιών και 7 το σύνολο των απαιτήσεων. Παρομοίως ο πίνακα T_P είναι ένας πίνακας N γραμμών και 7 στηλών, όπου N είναι το σύνολο των τεχνολογιών, δηλαδή το σύνολο IT.

Πρέπει να επισημανθεί ότι δεν επιλέγεται η βέλτιστη από τις προτεινόμενες τεχνολογίες. Αυτό γίνεται από τον υπεύθυνο υλοποίησης του συστήματος ή τον ίδιο τον προγραμματιστή διότι αυτοί πρέπει να συνυπολογίσουν και άλλους παράγοντες όπως κόστος, πολυπλοκότητα κ.λπ. Η PriS καθοδηγεί τον υπεύθυνο υλοποίησης προτείνοντας έναν αριθμό τεχνολογιών που μπορούν να υλοποιήσουν τα πρότυπα ιδιωτικότητας που έχουν αναγνωρισθεί στα προηγούμενα βήματα και που αντιστοιχούν στις απαιτήσεις του προς ανάπτυξη συστήματος.

6.5. Συμπεράσματα

Στο κεφάλαιο αυτό αναπτύχθηκε το φορμαλιστικό μοντέλο της PriS βάσει του εννοιολογικού της μοντέλου που περιγράφηκε στο πέμπτο κεφάλαιο. Με τη σαφή απεικόνιση των εννοιών και των βασικών σταδίων της μεθοδολογίας υποστηρίζεται η δυνατότητα δημιουργίας ενός εργαλείου που να υποστηρίζει τις ενέργειές της.

Στο επόμενο κεφάλαιο περιγράφεται η εφαρμογή της μεθοδολογίας σε ένα σύστημα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου.

7. Εφαρμογή της μεθοδολογίας PriS σε σύστημα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου

Οι ενότητες που ακολουθούν περιγράφουν την εφαρμογή της μεθοδολογίας PriS σε ένα σύστημα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου (Aegean, University of the 2003). Πρόκειται για ένα πιλοτικό σύστημα το οποίο αναπτύχθηκε στα πλαίσια ενός Ευρωπαϊκού προγράμματος από το Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων του Πανεπιστημίου Αιγαίου σε συνεργασία με το Πανεπιστήμιο του Regensburg, την εταιρεία Cryptomathic, την εταιρεία Quality and Reliability και το Οικονομικό Πανεπιστήμιο Αθηνών.

7.1. Περιγραφή του συστήματος ψηφοφορίας μέσω Διαδικτύου

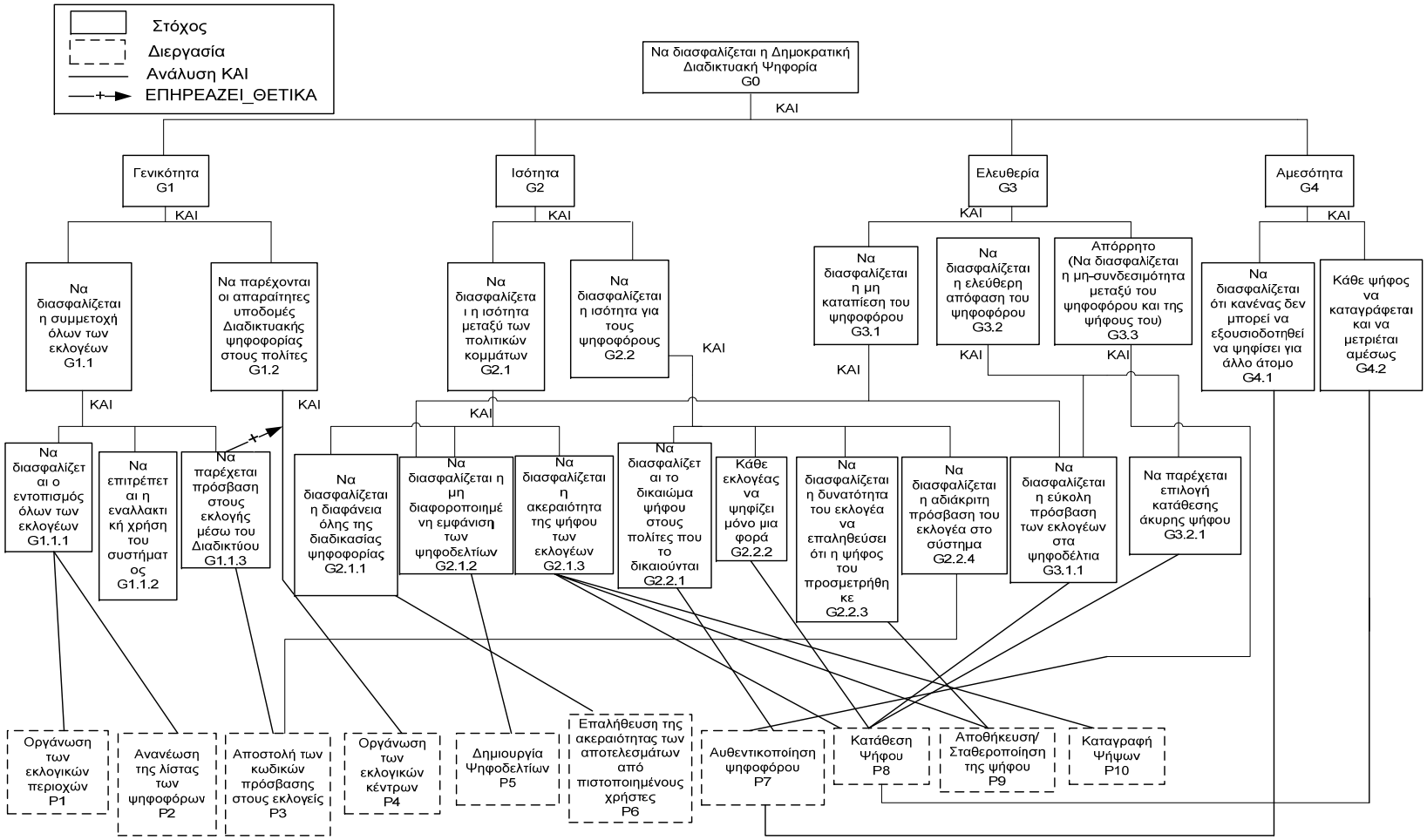
Ο βασικός σκοπός του συστήματος ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου είναι η παροχή του δικαιώματος κατάθεσης ψήφου στους πολίτες-εκλογείς μέσω του Διαδικτύου, συμβάλλοντας στην απλοποίηση της ακολουθηθείσας διαδικασίας ψηφοφορίας με φυσική παρουσία, με αποτέλεσμα να μπορεί δυνητικά να αυξηθεί η συμμετοχή των πολιτών στην ψηφοφορία αφού όλη η διαδικασία διευκολύνεται γι' αυτούς.

Το Διαδικτυακό αυτό σύστημα ηλεκτρονικής ψηφοφορίας περιγράφεται από τέσσερις βασικές αρχές οι οποίες διαμορφώνουν και τους τέσσερις πρωταρχικούς στόχους του: α) Γενικότητα (Generality), β)

Ισότητα (Equality), γ) Ελευθερία (Freedom) και δ) Αμεσότητα (Directness) (Aegean, University of the 2003).

Συγκεκριμένα, η αρχή της γενικότητας αναφέρεται στο δικαίωμα ψήφου που αποκτούν όλοι οι πολίτες μόλις συμπληρώσουν το δέκατο όγδοο έτος της ζωής τους. Η ισότητα αναφέρεται στο γεγονός ότι αφενός μεν τα πολιτικά κόμματα που συμμετέχουν στη διαδικασία των εκλογών και αφετέρου δε οι πολίτες-εκλογείς έχουν ίσα δικαιώματα πριν, κατά τη διάρκεια και μετά την ολοκλήρωση των εκλογών και της ψηφοφορίας, ενώ κανένας τρίτος, είτε σύστημα ή οποιοσδήποτε άλλος δεν έχουν δικαίωμα να το αλλάξουν αυτό. Η ελευθερία αναφέρεται στο γεγονός ότι η όλη διαδικασία των εκλογών και της ψηφοφορίας διεξάγεται χωρίς βία, πίεση, εξαναγκασμό και παρεμβάσεις ή άλλου είδους επηρεασμούς από τους πολιτικούς, την πολιτεία ή οποιοδήποτε άλλο άτομο ή οντότητα. Η αμεσότητα αναφέρεται στο γεγονός ότι δεν υπάρχουν ενδιάμεσοι που να παρεμβαίνουν στη διαδικασία της ψηφοφορίας και ότι κάθε ψήφος καταγράφεται και προσμετράται αμέσως.

Με βάση τους τέσσερις αυτούς στόχους του Διαδικτυακού συστήματος ψηφοφορίας, κατασκευάστηκε το μοντέλο των στόχων και των διεργασιών που υλοποιούν τους τελικούς στόχους του συστήματος (βλέπε Σχήμα 7.1). Στο τελευταίο επίπεδο του μοντέλου τα σχήματα με διακεκομμένα πλαίσια απεικονίζουν τις διεργασίες του συστήματος που υλοποιούν τους τελικούς στόχους. Το μοντέλο του Σχήματος 7.1 αποτελεί τη βάση πάνω στην οποία θα εφαρμοστούν οι τέσσερις ενέργειές της PriS όπως περιγράφηκε στο κεφάλαιο 5 και αναλύεται ακολούθως.



Σχήμα 7.1. Το μοντέλο Στόχων-Διεργασιών του συστήματος ψηφοφορίας μέσω Διαδικτύου

7.2. Εφαρμογή της PriS

7.2.1. Εύρεση των απαιτήσεων-στόχων ιδιωτικότητας

Με βάση τις ανάγκες των ενδιαφερομένων μερών (ψηφοφόροι, κόμματα κτλ) καταγράφηκαν οι δύο στόχοι ιδιωτικότητας που πρέπει να ικανοποιηθούν στο συγκεκριμένο σύστημα: η μη-συνδεσιμότητα και η μη-παρατηρησιμότητα.

Επιπλέον των δύο αυτών στόχων εντοπίζονται και δύο ακόμη στόχοι ιδιωτικότητας που προϋπάρχουν στο μοντέλο στόχων του οργανισμού αυτός της αυθεντικοποίησης, που υλοποιείται από τη διεργασία P7 «Αυθεντικοποίηση Ψηφοφόρου» καθώς και ο στόχος της εξουσιοδότησης όπως υλοποιείται από τη διεργασία P6 «Επαλήθευση της ακεραιότητας των αποτελεσμάτων από πιστοποιημένους χρήστες».

Δεδομένου ότι γνωρίζουμε ήδη ποιες διεργασίες επηρεάζονται από τους στόχους ιδιωτικότητας της αυθεντικοποίησης και εξουσιοδότησης στο επόμενο βήμα εξετάζουμε ποιες διεργασίες επηρεάζονται από τους δύο νέους στόχους μη-παρατηρησιμότητας και μη-συνδεσιμότητας.

7.2.2. Ανάλυση της επίδρασης των απαιτήσεων-στόχων της ιδιωτικότητας στις διεργασίες

Το επόμενο βήμα είναι η ανάλυση της επίδρασής τους στους στόχους και τις διεργασίες του συστήματος. Συγκεκριμένα εντοπίζονται οι στόχοι, οι υπό-στόχοι και οι διεργασίες που επηρεάζονται με την εισαγωγή των στόχων ιδιωτικότητας στο σύστημα. Οι στόχοι μαζί με τους αντίστοιχους υπό-στόχους που επηρεάζονται εμφανίζονται στον Πίνακα 7.1. Στη συνέχεια αναλύεται ο τρόπος με τον οποίο επηρεάζεται κάθε στόχος.

Συγκεκριμένα, για κάθε στόχο του οργανισμού που επηρεάζεται, οι νέες απαιτήσεις-στόχοι της ιδιωτικότητας υλοποιούνται είτε με την αλλαγή/βελτίωση του κάθε στόχου του οργανισμού, είτε με την εισαγωγή νέων στόχων. Για παράδειγμα, ο στόχος G1.1 «Να διασφαλίζεται η συμμετοχή όλων των εκλογέων» και ο αντίστοιχος υπό-στόχος G1.1.3 «Να παρέχεται πρόσβαση στους εκλογείς μέσω του Διαδικτύου» επηρεάζονται από την απαίτηση-στόχο ιδιωτικότητας της μη-συνδεσιμότητας.

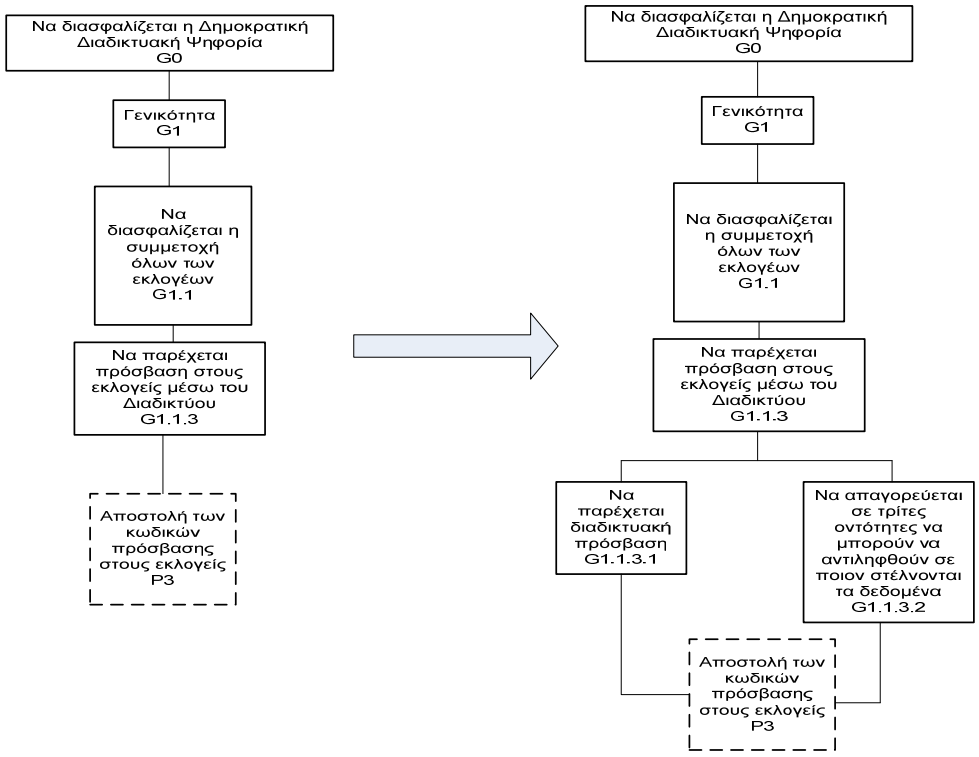
Πίνακας 7.1. Στόχοι και υπό-στόχοι που επηρεάζονται

Στόχοι Ιδιωτικότητας	**Στόχοι που επηρεάζονται**
Να διασφαλίζεται η μη-συνδεσιμότητα	G1.1) Να διασφαλίζεται η συμμετοχή όλων των εκλογέων G1.1.3) Να παρέχεται πρόσβαση στους εκλογείς μέσω Διαδικτύου G2.1) Να διασφαλίζεται η ισότητα μεταξύ των πολιτικών κομμάτων G2.1.3) Να διασφαλίζεται η ακεραιότητα της ψήφου των εκλογέων G2.2) Να διασφαλίζεται η ισότητα για τους ψηφοφόρους G2.2.1) Να διασφαλίζεται το δικαίωμα ψήφου στους πολίτες που το δικαιούνται
Να διασφαλίζεται η μη-παρατηρησιμότητα	G2.1) Να διασφαλίζεται η ισότητα μεταξύ των πολιτικών κομμάτων G2.1.1) Να διασφαλίζεται η διαφάνεια όλης της διαδικασίας ψηφοφορίας

Για να υλοποιηθεί ο στόχος αυτός απαιτείται να δημιουργηθούν δύο νέοι υπό-στόχοι, ο G1.1.3.1 «Να παρέχεται διαδικτυακή πρόσβαση» και ο G1.1.3.2 «Να απαγορεύεται σε τρίτες οντότητες να μπορούν να

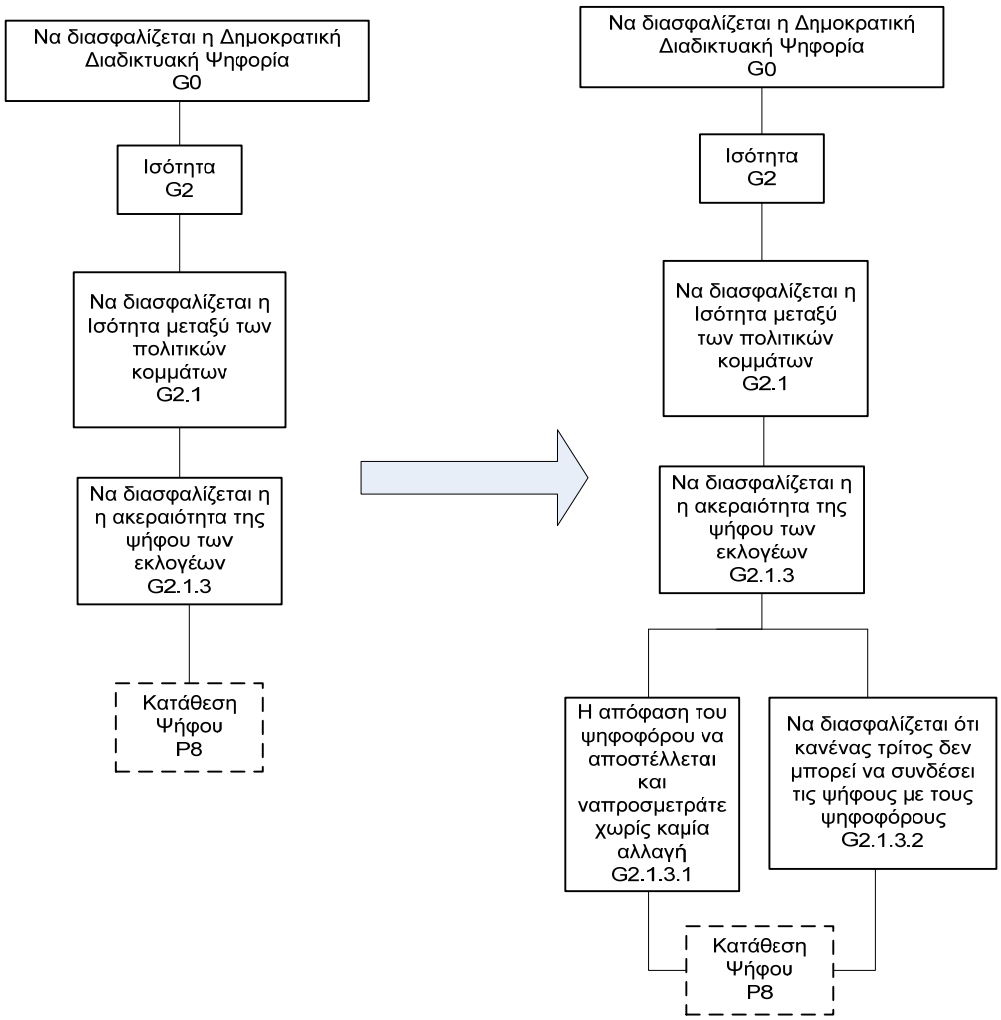
αντιληφθούν σε ποιον αποστέλλονται τα δεδομένα». Πιο συγκεκριμένα, το σύστημα ψηφοφορίας μέσω Διαδικτύου είναι υπεύθυνο να παρέχει στους εκλογείς ένα όνομα χρήστη και έναν κωδικό πρόσβασης πριν την έναρξη των εκλογών.

Σύμφωνα με τις απαιτήσεις του οργανισμού η επικοινωνία μεταξύ του συστήματος και των εκλογέων πρέπει να γίνει με τρόπο μη-συνδέσιμο, δηλαδή κάθε κακόβουλη τρίτη οντότητα να μη μπορεί να αποκαλύψει σε ποιον στέλνονται τα δεδομένα αυτά ακόμη και αν καταφέρει να αποκαλύψει μέρος της πληροφορίας που αποστέλλεται, επιτυγχάνοντας έτσι τη προστασία των προσωπικών δεδομένων του εκλογέα τα οποία αν υποκλέπτονταν θα οδηγούσαν στην αναγνώριση της ταυτότητάς του. Η δομή του αρχικού στόχου-υπό-στόχου καθώς και η νέα δομή του, συμπεριλαμβανομένης και της μη-συνδεσιμότητας, παρουσιάζονται στο Σχήμα 7.2.



Σχήμα 7.2. Αλλάζοντας τον υπό-στόχο G1.1.3 «Να παρέχεται πρόσβαση στους εκλογείς μέσω Διαδικτύου»

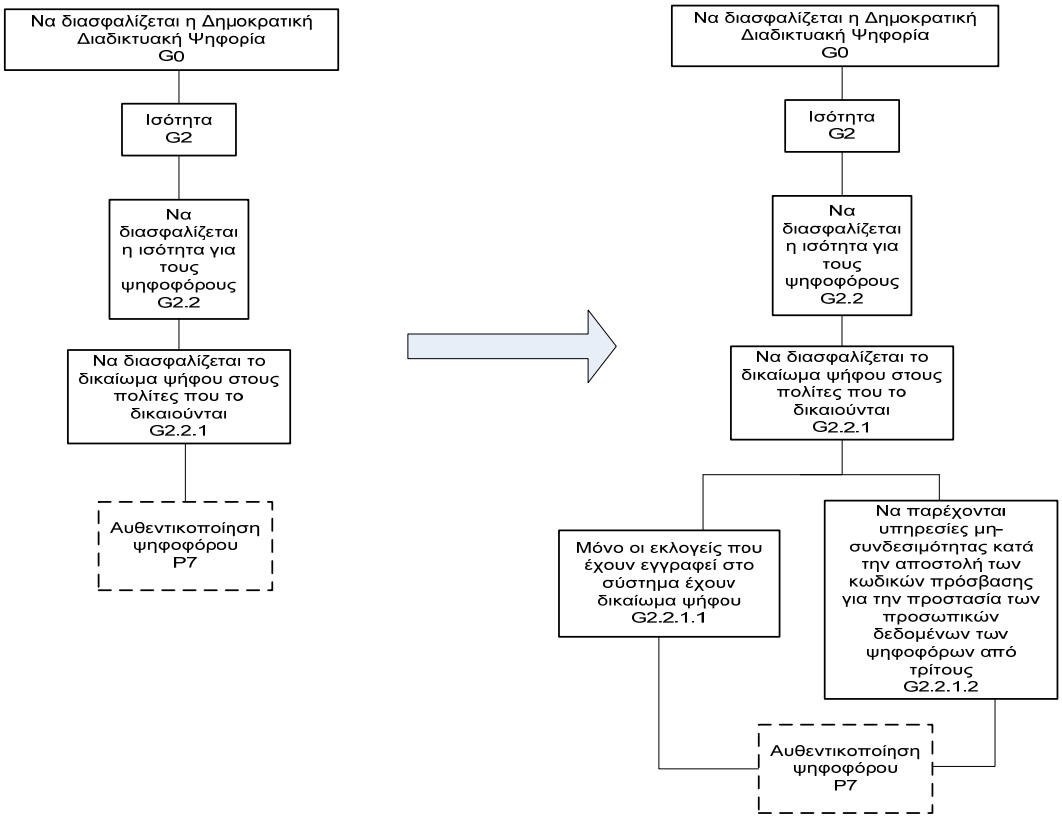
Ο στόχος της μη-συνδεσιμότητας έχει αντίκτυπο επίσης και στον υπό-στόχο G2.1.3 «Να διασφαλίζεται η ακεραιότητας της ψήφου των εκλογέων». Στη συγκεκριμένη περίπτωση, η μη-συνδεσιμότητα είναι απαραίτητη για την προστασία της ιδιωτικότητας των εκλογέων γιατί κατά τη διαδικασία της κατάθεσης της ψήφου δεν θα πρέπει καμία τρίτη οντότητα να μπορεί να συνδέσει την ψήφο με το ψηφοφόρο, αφενός μεν για να μην αποκαλύψει τα προσωπικά στοιχεία αυτού και αφετέρου για να μην αποκαλύψει τις πολιτικές του πεποιθήσεις. Για να προστατευθεί η ιδιωτικότητα του χρήστη δύο νέοι υπό-στόχοι εισάγονται όπως φαίνεται στην Σχήμα 7.3.



Σχήμα 7.3. Αλλάζοντας τον υπό-στόχο

G2.1.3 «Να διασφαλίζεται η ακεραιότητα της ψήφου των εκλογέων»

Ο υπό-στόχος G2.2.1 «Να διασφαλίζεται το δικαίωμα ψήφου στους πολίτες που το δικαιούνται» χρειάζεται επίσης επαναπροσδιορισμό από τη στιγμή που κατά το σχετικό έλεγχο του δικαιώματος ψήφου των χρηστών του συστήματος επιβάλλεται η προστασία της ιδιωτικότητάς τους. Δηλαδή, κατά τη διάρκεια της αυθεντικοποίησης ενός εκλογέα στο σύστημα, δε θα πρέπει οι κακόβουλες τρίτες οντότητες να μπορούν να «κλέψουν» καμία μορφή πληροφορίας που θα μπορέσει να οδηγήσει εκ των υστέρων στην αναγνώριση των εκλογέων και στα προσωπικά τους δεδομένα. Για το σκοπό αυτό, το σύστημα πρέπει να παρέχει υπηρεσίες που προστατεύουν τη μη-συνδεσιμότητα του χρήστη κατά τη διάρκεια της αυθεντικοποίησής του. Παράλληλα, η αυθεντικοποίηση καθαυτή αποτελεί στόχο ιδιωτικότητας του συστήματος (βλ. παράγραφο 7.2.1).



Σχήμα 7.4. Αλλάζοντας τον υπό-στόχο G 2.2.1 «Να διασφαλιστεί το δικαίωμα ψήφου στους πολίτες που το δικαιούνται»

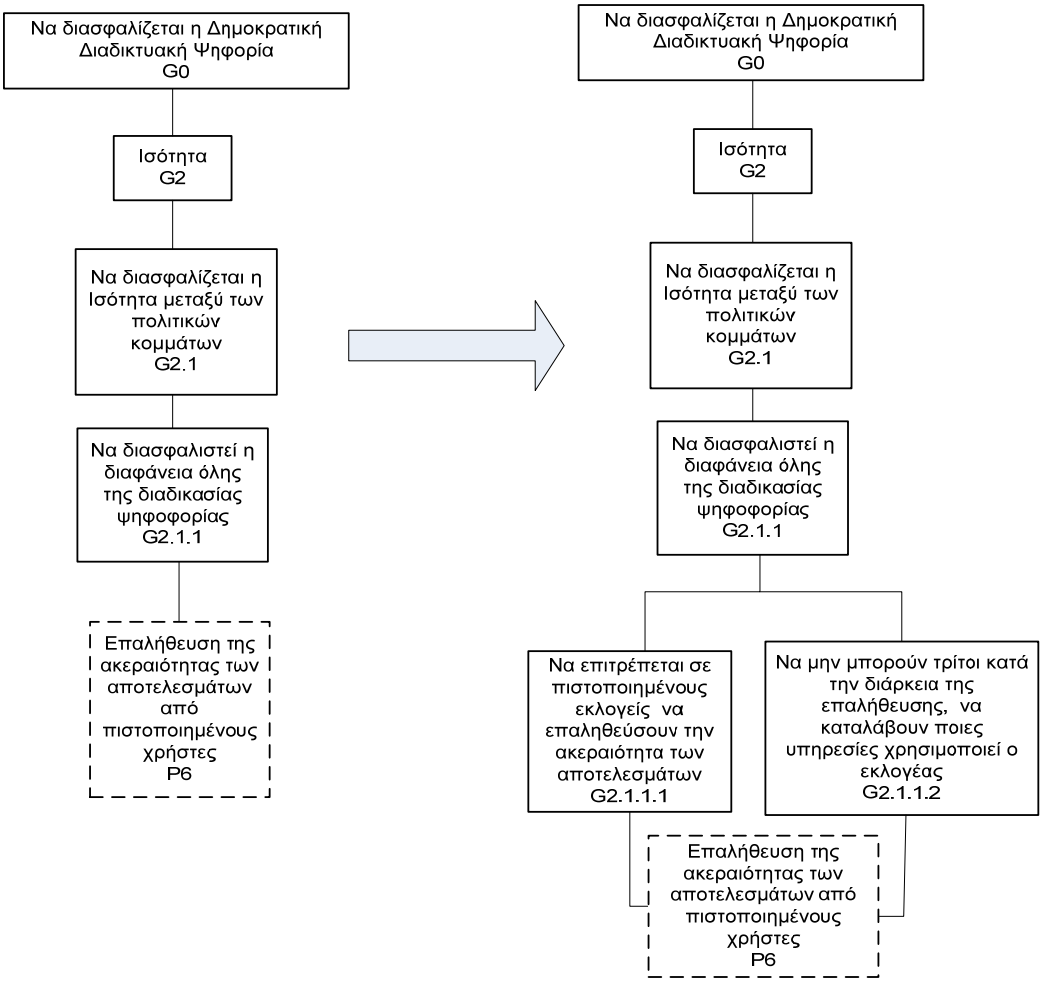
Επομένως ο στόχος G2.2.1 «Να διασφαλιστεί το δικαίωμα ψήφου στους πολίτες που το δικαιούνται» μετατρέπεται όπως φαίνεται στο Σχήμα 7.4. Ο στόχος G2.2.1.1 υλοποιεί το στόχο της αυθεντικοποίησης, ενώ ο G2.2.1.2 το στόχο της μη-συνδεσιμότητας.

Επιπλέον, για να ικανοποιηθεί ο στόχος της μη-παρατηρησιμότητας των εκλογέων, πρέπει να επαναπροσδιοριστεί ο υπό-στόχος G2.1.1 «Να διασφαλιστεί η διαφάνεια όλης της διαδικασίας ψηφοφορίας».

Για την υλοποίηση του στόχου αυτού θα πρέπει οι πιστοποιημένοι εκλογείς να έχουν το δικαίωμα της επαλήθευσης της ακεραιότητας των αποτελεσμάτων μετά το πέρας των εκλογών. Στην περίπτωση αυτή πρέπει να εξασφαλίζεται ότι δεν υπάρχει η δυνατότητα σε τρίτους να γνωρίζουν ότι κάποιος χρησιμοποιεί τη συγκεκριμένη υπηρεσία ούτε για ποιών πολιτικών κομμάτων τα αποτελέσματα δείχνει ενδιαφέρον, αφού κάτι τέτοιο αν γινόταν αντιληπτό θα μπορούσε να ερμηνευτεί ως έκφραση πολιτικών ενδιαφερόντων ή πολιτικών πεποιθήσεων. Η μη-παρατηρησιμότητα παρέχει αυτή τη δυνατότητα αφού όταν υλοποιηθεί, οι όποιοι τρίτοι δεν μπορούν να αντιληφθούν ποια υπηρεσία χρησιμοποιείται από ποιον/ποια ακόμη και αν αντιληφθούν ότι συγκεκριμένοι χρήστες βρίσκονται στο σύστημα. Επιπλέον, όπως αναφέρθηκε στη παράγραφο 7.2.1, για να εξασφαλιστεί ότι μόνο πιστοποιημένοι χρήστες επαληθεύουν τα αποτελέσματα, θα πρέπει να υπάρχει δυνατότητα εξουσιοδότησης των χρηστών.

Με βάση τα παραπάνω, ο στόχος G2.1.1 «Να διασφαλιστεί η διαφάνεια όλης της διαδικασίας ψηφοφορίας» τροποποιείται όπως φαίνεται στο σχήμα 7.5.

Με βάση το παραπάνω τροποποιημένο μοντέλο στόχων οι διεργασίες που επηρεάζονται είναι οι P3, P6, P7, P8 όπως φαίνεται και στον πίνακα 7.2.



Σχήμα 7.5. Αλλάζοντας τον υπό-στόχο G2.1.1 «Να διασφαλιστεί η διαφάνεια όλης της διαδικασίας ψηφοφορίας»

Πίνακας 7.2. Διεργασίες που υλοποιούν τους τελικούς στόχους που επηρεάζονται

Στόχοι που επηρεάζονται από τους στόχους ιδιωτικότητας	**Διεργασίες που τους υλοποιούν**
G1.1.3.2) Να απαγορεύεται σε τρίτες οντότητες να μπορούν να αντιληφθούν σε ποιόν στέλνονται τα δεδομένα	P3) Αποστολή των κωδικών πρόσβασης στους εκλογείς
G2.1.3.2) Να διασφαλίζεται ότι κανένας τρίτος δεν μπορεί να συνδέσει τις ψήφους με τους ψηφοφόρους	P8) Κατάθεση Ψήφου
G2.2.1.1) Μόνο οι εκλογείς που έχουν εγγραφεί στο σύστημα έχουν δικαίωμα ψήφου	P7) Αυθεντικοποίηση ψηφοφόρου
G2.2.1.2) Να παρέχονται υπηρεσίες μη-συνδεσιμότητας κατά την αποστολή των κωδικών πρόσβασης για την προστασία των προσωπικών δεδομένων των ψηφοφόρων από τρίτους	P7) Αυθεντικοποίηση ψηφοφόρου
G2.1.1.1) Να επιτρέπεται σε πιστοποιημένους εκλογείς να επαληθεύσουν την ακεραιότητα των αποτελεσμάτων	P6) Επαλήθευση της ακεραιότητας των αποτελεσμάτων από πιστοποιημένους χρήστες
G2.1.1.2) Να μην μπορούν τρίτοι, κατά τη διάρκεια της επαλήθευσης, να καταλάβουν ποιες υπηρεσίες χρησιμοποιεί ο εκλογέας	P6) Επαλήθευση της ακεραιότητας των αποτελεσμάτων από πιστοποιημένους χρήστες

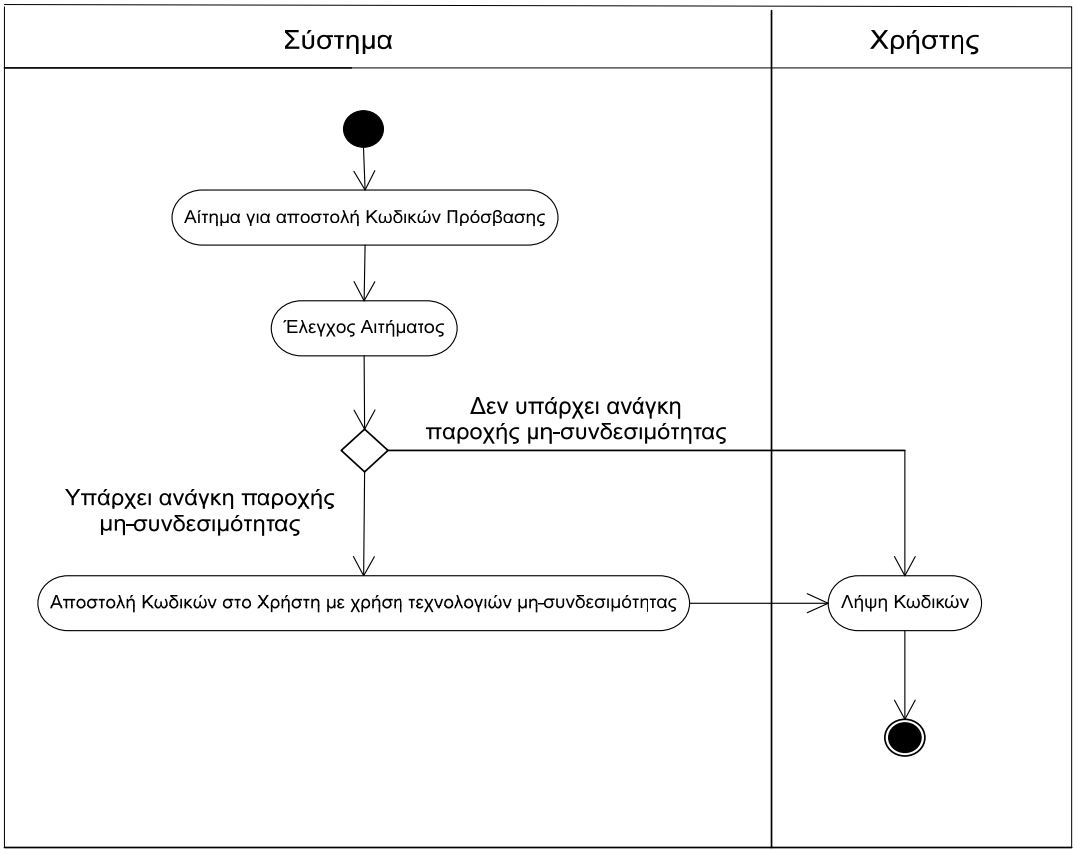
7.2.3. Διαμόρφωση των διεργασιών ιδιωτικότητας με τη χρήση προτύπων ιδιωτικότητας

Το επόμενο βήμα είναι η εφαρμογή των προτύπων ιδιωτικότητας, στις διεργασίες που αναγνωρίστηκε ότι επηρεάζονται από τους στόχους ιδιωτικότητας (Πίνακας 7.2).

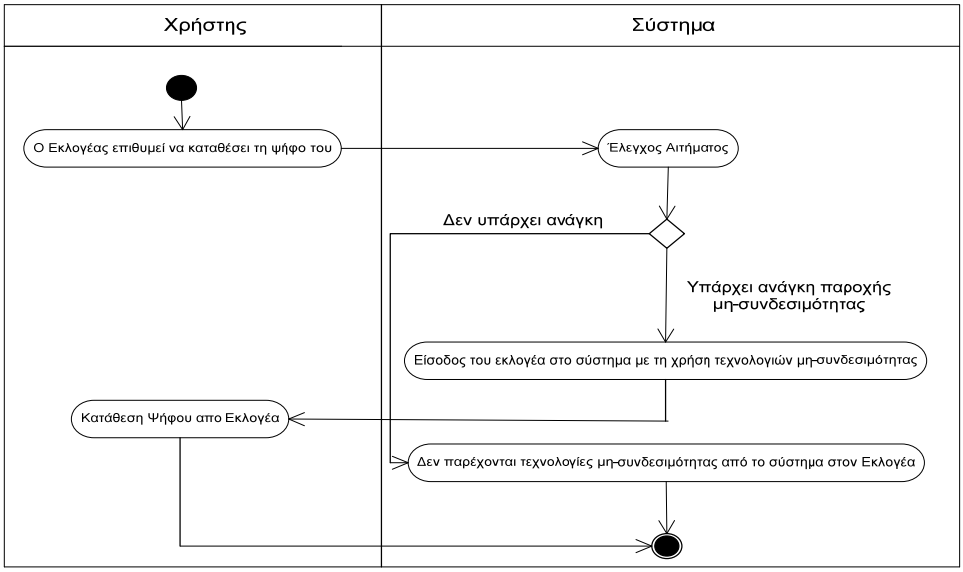
Η πρώτη διεργασία που επηρεάζεται είναι η P3 «Αποστολή των κωδικών πρόσβασης στους εκλογείς». Η απαίτηση ιδιωτικότητας που επειρεάζει αυτή τη διεργασία είναι η μη-συνδεσιμότητα. Από την στιγμή που δεν υπάρχει άλλος τελικός στόχος με διαφορετική απαίτηση ιδιωτικότητας που να υλοποιείται από την ίδια διεργασία, εφαρμόζεται σε αυτή το πρότυπο ιδιωτικότητας της μη-συνδεσιμότητας. Το αποτέλεσμα παρουσιάζεται στο Σχήμα 7.6.

Σύμφωνα με το σχήμα 7.6, για να μπορέσει να επιτευχθεί η αποστολή των κωδικών στους εκλογείς, θα πρέπει σε κάθε αποστολή, πρώτα να υλοποιείται μια επικοινωνία που θα χρησιμοποιεί τεχνολογίες προστασίας της μη-συνδεσιμότητας μεταξύ των εκλογέων και του συστήματος.

Η επόμενη διεργασία που επηρεάζεται είναι η P8 «Κατάθεση ψήφου» από τους εκλογείς. Και στη περίπτωση αυτή εφαρμόζεται το πρότυπο ιδιωτικότητας της μη-συνδεσιμότητας. Το αποτέλεσμα παρουσιάζεται στο Σχήμα 7.7.



Σχήμα 7.6. Εφαρμογή του προτύπου ιδιωτικότητας της μη-συνδεσιμότητας στη διεργασία P3 «Αποστολή των κωδικών πρόσβασης στους εκλογείς»



Σχήμα 7.7. Εφαρμογή του προτύπου ιδιωτικότητας της μη-συνδεσιμότητας στη διεργασία P8 «Κατάθεση Ψήφου»

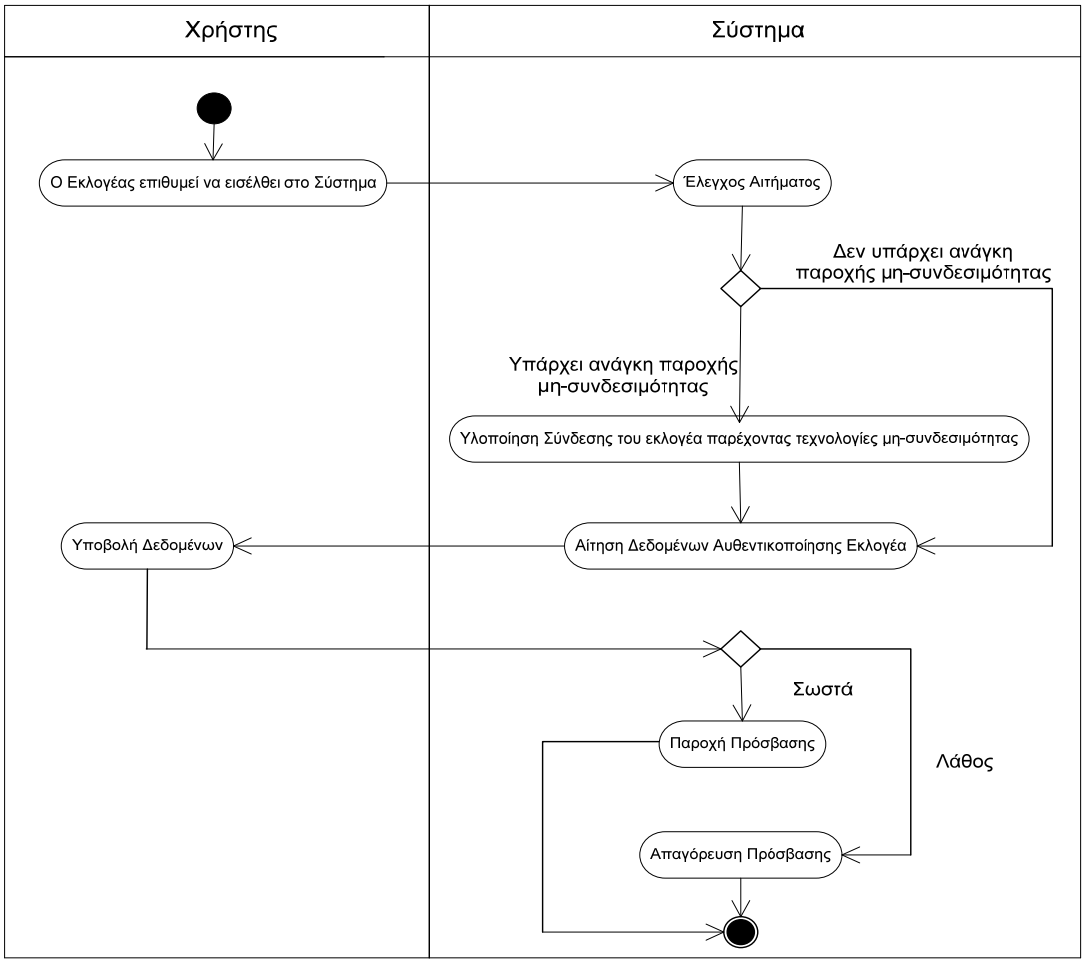
Όπως φαίνεται στο παραπάνω σχήμα 7.7, όταν ο εκλογέας εισέρχεται στο σύστημα ζητείται από αυτόν να δηλώσει τι ενέργειες θέλει να κάνει. Όταν ο εκλογέας ζητήσει να καταθέσει την ψήφο του, τότε το σύστημα υλοποιεί μία επικοινωνία μεταξύ τους παρέχοντας υπηρεσίες μη-συνδεσιμότητας ώστε κανένας τρίτος να μην μπορέσει να συνδέσει το χρήστη με την ψήφο που καταθέτει.

Η διεργασία P7 «Αυθεντικοποίηση ψηφοφόρου» επηρεάζεται επίσης από το στόχο της μη-συνδεσιμότητας μιας και πρέπει να προφυλαχτεί η ιδιωτικότητα του ψηφοφόρου ακόμη και στην περίπτωση που κάποιος τρίτος καταφέρει να υποκλέψει μέρος ή τα πλήρη δεδομένα αυθεντικοποίησης του χρήστη. Σκοπός της μη-συνδεσιμότητας, στην προκειμένη περίπτωση, είναι ότι ακόμη και σε περίπτωση κλοπής των δεδομένων αυθεντικοποίησης, η τρίτη κακόβουλη οντότητα δεν θα μπορεί να τα συνδέσει με τον ψηφοφόρο με αποτέλεσμα να μην κινδυνεύσουν τα προσωπικά δεδομένα του.

Στη συγκεκριμένη διεργασία, όμως, δεν εφαρμόζεται μόνο το πρότυπο ιδιωτικότητας της μη-συνδεσιμότητας, αλλά και αυτό τις αυθεντικοποίησης. Σε αυτές τις περιπτώσεις τα πρότυπα ιδιωτικότητας εφαρμόζονται συνδυαστικά ώστε να υλοποιηθούν οι απαραίτητες ενέργειες όλων των αντίστοιχων προτύπων ιδιωτικότητας. Έτσι στην προκειμένη περίπτωση, στη διεργασία P7 «Αυθεντικοποίηση ψηφοφόρου» εφαρμόζεται ο συνδυασμός των προτύπων της μη-συνδεσιμότητας και της αυθεντικοποίησης. Το αποτέλεσμα της εφαρμογής του συνδυασμού των δύο προτύπων εμφανίζεται στο Σχήμα 7.8.

Η τελευταία διεργασία που επηρεάζεται είναι αυτή της επαλήθευσης της ακεραιότητας των αποτελεσμάτων. Κατά τη διάρκεια της επαλήθευσης, δεν θα πρέπει κανένας τρίτος να έχει τη δυνατότητα να παρατηρήσει για ποια δεδομένα - αποτελέσματα ενδιαφέρεται ο κάθε ψηφοφόρος μιας και αυτό θα μπορούσε να οδηγήσει σε παραβίαση της

ιδιωτικότητάς του. Έτσι, το πρότυπο ιδιωτικότητας για τη μη-παρατηρησιμότητα εφαρμόζεται στη διεργασία P6 «Επαλήθευση της ακεραιότητας των αποτελεσμάτων».

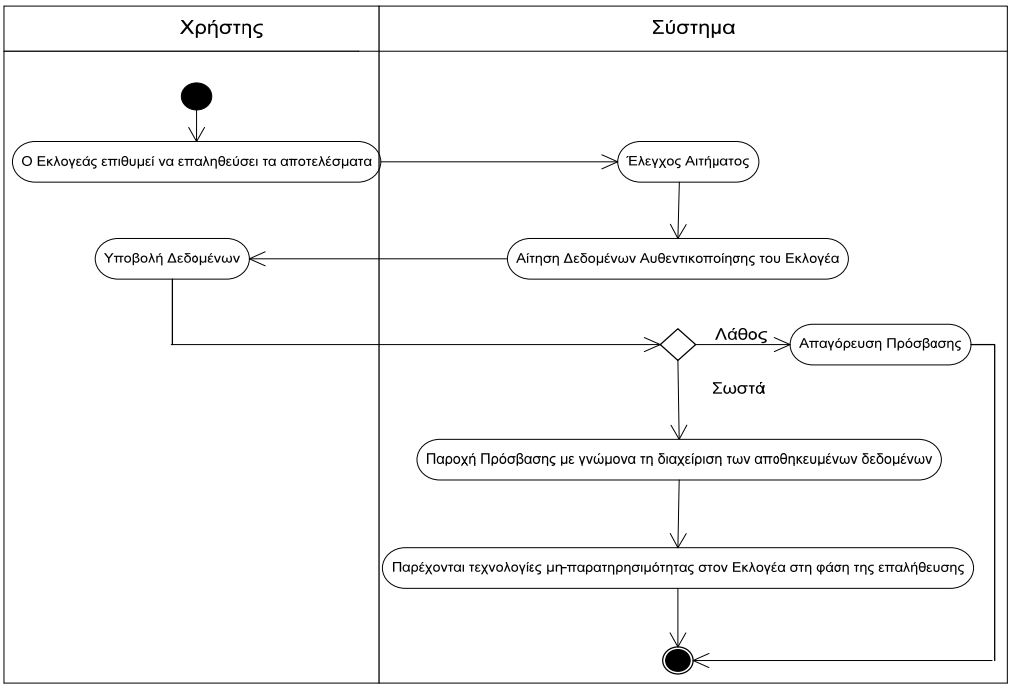


Σχήμα 7.8. Εφαρμογή των προτύπων ιδιωτικότητας της μη-συνδεσιμότητας και της αυθεντικοποίησης στη διεργασία P7 «Αυθεντικοποίηση Ψηφοφόρου»

Επιπλέον του προτύπου ιδιωτικότητας της μη-παρατηρησιμότητας, χρειάζεται να εφαρμοστεί και το πρότυπο της εξουσιοδότησης. Όπως και στην προηγούμενη περίπτωση, η PriS συνδυάζει τα δύο πρότυπα ιδιωτικότητας με αποτέλεσμα τη δημιουργία ενός κοινού προτύπου που θα καλύπτει τις ενέργειες και των δύο.

Το αποτέλεσμα της εφαρμογής του συνδυασμού των δύο προτύπων εμφανίζεται στο Σχήμα 7.9.

Συγκεκριμένα, ο ψηφοφόρος ζητά από το σύστημα να επαληθεύσει τα αποτελέσματα των εκλογών. Το σύστημα ελέγχει το αίτημά του και ενεργοποιεί τη διεργασία της εξουσιοδότησης για να κατοχυρώσει στο χρήστη τα ανάλογα δικαιώματα. Για να γίνει η κατοχύρωση των δικαιωμάτων ενεργοποιείται η διεργασία της αυθεντικοποίησης που ζητά από το χρήστη τα στοιχεία ταυτοποίησης του. Αν αυτά είναι σωστά ο χρήστης εξουσιοδοτείται και μέσω μιας σύνδεσης κατά την οποία παρέχονται υπηρεσίες μη-παρατηρησιμότητας επαληθεύει τα αποτελέσματα που θέλει γνωρίζοντας ότι η ιδιωτικότητά του προστατεύεται από δυνητικές ενέργειες κακόβουλων τρίτων οντοτήτων.



Σχήμα 7.9. Εφαρμογή των προτύπων ιδιωτικότητας της μη-παρατηρησιμότητας και της εξουσιοδότησης στη διεργασία P6 «Επαλήθευση της ακεραιότητας των αποτελεσμάτων»

7.2.4. Εύρεση των τεχνολογιών που υποστηρίζουν την υλοποίηση των παραπάνω προτύπων ιδιωτικότητας

Σε τελική αυτή φάση ο υπεύθυνος υλοποίησης του συστήματος θα πρέπει να επιλέξει την κατάλληλη τεχνολογία(-ες) για να υλοποιήσει τις διεργασίες του συστήματος που επηρεάζονται από τους στόχους ιδιωτικότητας δηλαδή τους στόχους της μη-συνδεσιμότητας, της μη-παρατηρησιμότητας, της αυθεντικοποίησης και της εξουσιοδότησης.

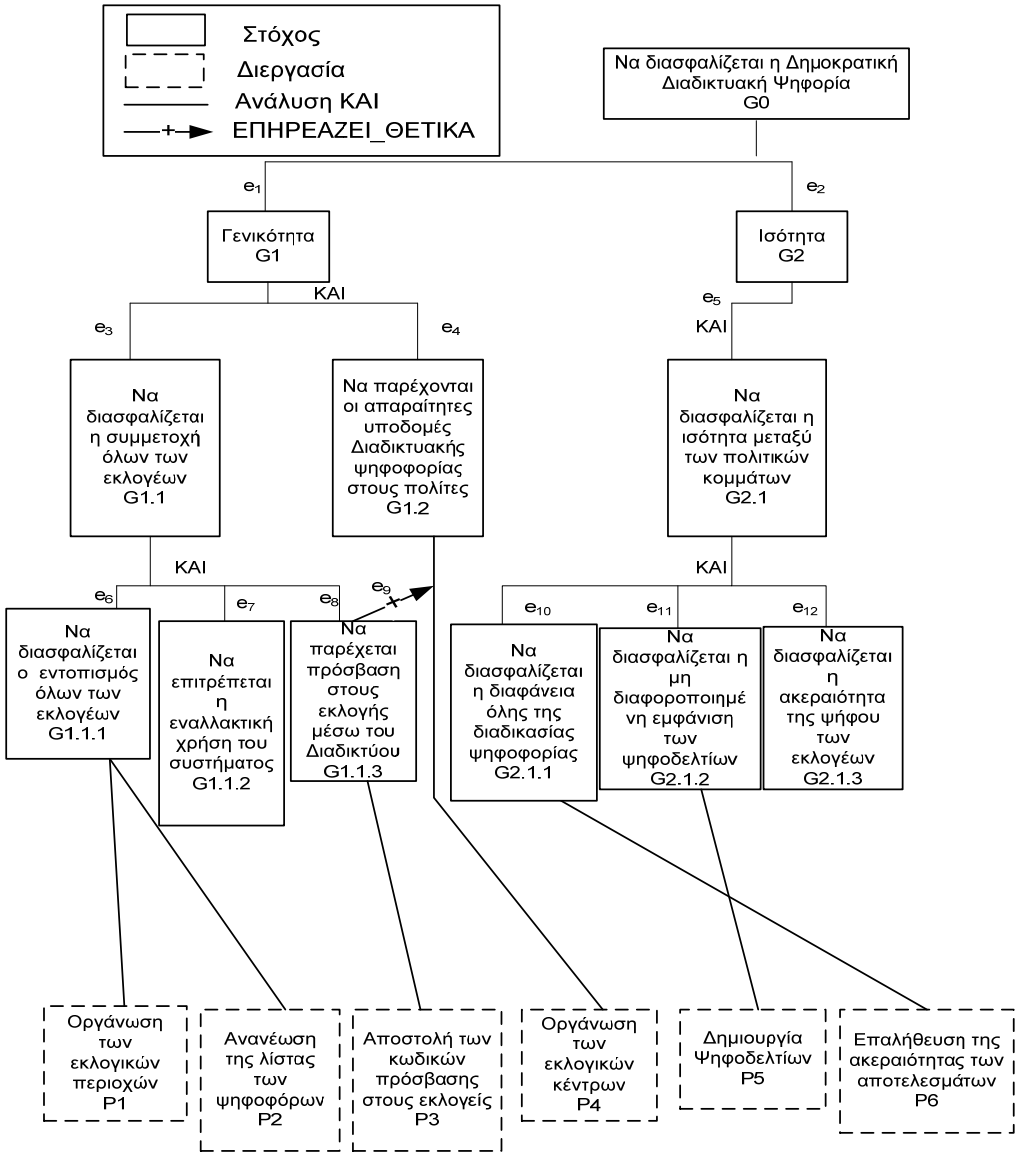
Ο Πίνακας 5.1 συγκεντρώνει όλες τις τεχνολογίες που υλοποιούν τις παραπάνω ενέργειες ιδιωτικότητας (σημειώνονται με «Χ» στον Πίνακα 5.1 οι τεχνολογίες που υλοποιούν κάθε πρότυπο ιδιωτικότητας») βάσει αυτού προτείνονται οι τεχνολογίες που υλοποιούν όλες τις παραπάνω ενέργειες. Αν δεν υπάρχουν αυτές προτείνονται οι τεχνολογίες που καλύπτουν τις περισσότερες από αυτές κ.λπ. Στο συγκεκριμένο σύστημα η αρχιτεκτονική Tor καλύπτει την υλοποίηση της μη-συνδεσιμότητας και της μη-παρατηρησιμότητας. Άρα θα προταθεί ως μια πιθανή λύση η Tor για την υλοποίηση των δύο αυτών προτύπων και μετά θα προταθούν και τεχνολογίες που υλοποιούν την εξουσιοδότηση και την αυθεντικοποίηση.

Ο υπεύθυνος υλοποίησης του συστήματος έχει την τελική ευθύνη για την επιλογή των τεχνολογιών που θα χρησιμοποιηθούν μιας και η επιλογή αυτών εξαρτάται και από άλλους παράγοντες όπως κόστος, πολυπλοκότητα υλοποίησης κ.λπ. τα οποία γνωρίζει εκείνος και συνεισφέρουν για τη λήψη της τελικής του απόφασης.

7.3. Εφαρμογή του φορμαλιστικού μοντέλου της PriS

Στην ενότητα αυτή παρουσιάζεται η εφαρμογή του φορμαλιστικού μοντέλου της PriS. Η εφαρμογή του φορμαλιστικού μοντέλου πραγματοποιείται σε ένα μέρος του συστήματος ψηφοφορίας μέσω

Διαδικτύου και όχι σε ολόκληρο το μοντέλο που περιγράφηκε προηγουμένως. Πιο συγκεκριμένα περιγράφεται η εφαρμογή του φορμαλιστικού μοντέλου στα πρώτα δύο τμήματα της ιεραρχίας που αφορούν την υλοποίηση των στόχων της γενικότητας και της ισότητας. Με τον ίδιο τρόπο, όπως περιγράφεται παρακάτω, το μοντέλο εφαρμόζεται και στα αλλά τρία τμήματα της ιεραρχίας. Η υλοποίηση των στόχων της ισότητας και της γενικότητας φαίνεται στο σχήμα 7.10.



Σχήμα 7.10. Μέρος του μοντέλου Στόχων-Διεργασιών του συστήματος ψηφοφορίας μέσω Διαδικτύου

Παρακάτω περιγράφονται φορμαλιστικά οι τέσσερις ενέργειες της PriS αναφορικά με το μοντέλο στόχων-διεργασιών του Σχήματος 7.10 με σκοπό να γίνει μία πλήρης περιγραφή της όλης διαδικασίας, από τον ορισμό της ιεραρχίας των στόχων μέχρι την εύρεση των τεχνολογιών υλοποίησης των παραμέτρων ιδιωτικότητας, με φορμαλιστικό τρόπο.

7.3.1. Εύρεση των στόχων ιδιωτικότητας

Το πρώτο βήμα είναι ο ορισμός του συνόλου των στόχων και των συσχετίσεων τους, το σύνολο V. Στη συγκεκριμένη περίπτωση, το σύνολο V αποτελείται από όλους τους στόχους, σύνολο G και από όλες τις συσχετίσεις τους, σύνολο E, όπως φαίνονται στο Σχήμα 7.10.

$$V = (G,E)$$

$$V = (\{G_0,G_1,G_{1.1},G_{1.2},G_{1.1.1},G_{1.1.2},G_{1.1.3},G_2,G_{2.1},G_{2.1.1},G_{2.1.2},G_{2.1.3}\},$$
$$\{e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8,e_9,e_{10},e_{11},e_{12}\})$$

Έπειτα ακολουθεί ο ορισμός των σχέσεων και ο αντίστοιχος τύπος τους μεταξύ των στόχων του συνόλου G. Με βάση το μοντέλο του Σχήματος 4.10 ορίζονται τα ακόλουθα:

$$e_1=(G_0,G_1,2)$$
$$e_2=(G_0,G_2,2)$$
$$e_3=(G_1,G_{1.1},2)$$
$$e_4=(G_1,G_{1.2},2)$$
$$e_5=(G_2,G_{2.1},2)$$
$$e_6=(G_{1.1},G_{1.1.1},2)$$
$$e_7=(G_{1.1},G_{1.1.2},2)$$
$$e_8=(G_{1.1},G_{1.1.3},2)$$
$$e_9=(G_{1.1.3},G_{1.2},3)$$

$$e_{10}=(G_{2.1},G_{2.1.1},2)$$
$$e_{11}=(G_{2.1},G_{2.1.2},2)$$
$$e_{12}=(G_{2.1},G_{2.1.3},2)$$

Έπειτα ορίζονται για κάθε στόχο ιδιωτικότητας του συστήματος οι απαιτήσεις ιδιωτικότητας που τον επηρεάζουν. Με τη χρήση της διαδικασίας Assign_pv() ορίζόνται οι τιμές των μεταβλητών ιδιωτικότητας των στόχων στους οποίους έχουν αντίκτυπο οι στόχοι ιδιωτικότητας του συστήματος. Οι ορισμοί παρουσιάζονται παρακάτω.

$$\text{Assign\_pv}(G_{1.1}) = (0,0,0,0,0,1,0)$$

$$\text{Assign\_pv}(G_{1.1.3}) = (0,0,0,0,0,1,0)$$

$$\text{Assign\_pv}(G_{2.1}) = (0,1,0,0,0,1,1)$$

$$\text{Assign\_pv}(G_{2.1.1}) = (0,1,0,0,0,0,1)$$

$$\text{Assign\_pv}(G_{2.1.3}) = (0,0,0,0,0,1,0)$$

Όπως προαναφέρθηκε, όταν μια απαίτηση ιδιωτικότητας επηρεάζει ένα μη-τελικό στόχο, επηρεάζονται και όλοι οι στόχοι_παιδιά του. Στο συγκεκριμένο παράδειγμα ο στόχος $G_{2.1}$ επηρεάζεται από το στόχο της μη-συνδεσιμότητας, της εξουσιοδότησης και της μη-παρατηρησιμότητας. Οι απαιτήσεις αυτές κληρονομούνται και στους στόχους $G_{2.1.1}$ και $G_{2.1.3}$ μιας και είναι παιδιά του στόχου $G_{2.1}$. Παρόλα αυτά, κατά την ανάλυση των στόχων διαπιστώθηκε ότι στο στόχο $G_{2.1}$ υλοποιούνται οι απαίτησεις της μη-συνδεσιμότητας και της εξουσιοδότησης ενώ στο στόχο $G_{2.1.3}$ μόνο αυτή της μη-παρατηρησιμότητας. Για το λόγο αυτό στις δηλώσεις που προηγήθηκαν ο στόχος $G_{2.1}$ περιορίζεται από τους στόχους της μη-συνδεσιμότητας, της εξουσιοδότησης και της μη-παρατηρησιμότητας ενώ τα παιδιά αυτού μόνο με τους στόχους που προαναφέρθηκαν. Με τη

χρήση της διαδικασίας Assign_pv(), επιτρέπεται η παρέμβαση στον ορισμό των τιμών των μεταβλητών ιδιωτικότητας σε περιπτώσεις όπως και αυτή του συγκεκριμένου συστήματος που περιγράφεται.

Μετά τον ορισμό των απαιτήσεων ιδιωτικότητας στους αντίστοιχους στόχους ιδιωτικότητας ακολουθεί η εισαγωγή νέων στόχων ή/και η βελτίωση των στόχων του οργανισμού με σκοπό την προσαρμογή του μοντέλου στην κάλυψη των νέων απαιτήσεων του οργανισμού. Στο συγκεκριμένο σύστημα και με βάση το Σχήμα 7.2 οι νέοι στόχοι που εισήχθησαν στο μοντέλο στόχων είναι οι στόχοι $G_{1.1.3.1}$ και $G_{1.1.3.2}$, $G_{2.1.1.1}$ και $G_{2.1.1.2}$. Μετά την εισαγωγή των νέων στόχων τα σύνολο G και E επαναπροσδιορίζονται ως εξής:

$$G = \{G_0,G_1,G_{1.1},G_{1.2},G_{1.1.1},G_{1.1.2},G_{1.1.3},G_{1.1.3.1},G_{1.1.3.2},G_2,G_{2.1},G_{2.1.1}, G_{2.1.1.1}, G_{2.1.1.2}, G_{2.1.2},G_{2.1.3}\} \text{ και}$$

$$E = \{e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8,e_9,e_{10},e_{11},e_{12},e_{13},e_{14},e_{15},e_{16}\}$$

Για τους νέους στόχους επαναλαμβάνεται η διαδικασία καθορισμού των μεταβλητών ιδιωτικότητας που υποδεικνύει τις απαιτήσεις ιδιωτικότητας που τους περιορίζουν. Επίσης ορίζονται οι συσχετίσεις μεταξύ του στόχο $G_{1.1.3}$ και των στόχων $G_{1.1.3.1}$ και $G_{1.1.3.2}$ μέσω των e_{13} και e_{14} και οι συσχετίσεις του στόχου $G_{2.1.1}$ με τους στόχους $G_{2.1.1.1}$ και $G_{2.1.1.2}$ μέσω των e_{15} και e_{16}.

$$e_{13}=(G_{1.1.3},G_{1.1.3.1},2)$$

$$e_{14}=(G_{1.1.3},G_{1.1.3.2},2)$$

$$e_{15}=(G_{2.1.1},G_{2.1.1.1},2)$$

$$e_{16}=(G_{2.1.1},G_{2.1.1.2},2)$$

$$\text{Assign\_pv}(G_{1.1.3.2}) = (0,0,0,0,0,1,0)$$

$$\text{Assign\_pv}(G_{2.1.1.1}) = (0,1,0,0,0,0,0)$$

$$\text{Assign\_pv}(G_{2.1.1.2}) = (0,0,0,0,0,0,1)$$

Έτσι με το τρόπο αυτό ορίστηκε η τροποποιημένη ιεραρχία των στόχων του οργανισμού και επισημάνθηκαν οι απαιτήσεις ιδιωτικότητας που επηρεάζουν κάθε στόχο στην ιεραρχία.

Ο πίνακας γειτνίασης του νέου μοντέλου στόχων συμπεριλαμβανομένων των νέων στόχων που εισήχθησαν φαίνεται στο πίνακα 7.3.

Πίνακας 7.3. Πίνακας Γειτνίασης του ιεραρχικού μοντέλου στόχων

	G_0	G_1	$G_{1.1}$	$G_{1.2}$	$G_{1.1.1}$	$G_{1.1.2}$	$G_{1.1.3}$	$G_{1.1.3.1}$	$G_{1.1.3.2}$	G_2	$G_{2.1}$	$G_{2.1.1}$	$G_{2.1.2}$	$G_{2.1.3}$
G_0	0	2	0	0	0	0	0	0	0	2	0	0	0	0
G_1	0	0	2	2	0	0	0	0	0	0	0	0	0	0
$G_{1.1}$	0	0	0	0	2	2	2	0	0	0	0	0	0	0
$G_{1.2}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{1.1.1}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{1.1.2}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{1.1.3}$	0	0	0	3	0	0	0	2	2	0	0	0	0	0
$G_{1.1.3.1}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{1.1.3.2}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G_2	0	0	0	0	0	0	0	0	0	0	2	0	0	0
$G_{2.1}$	0	0	0	0	0	0	0	0	0	0	0	2	2	2
$G_{2.1.1}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{2.1.1.1}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{2.1.1.2}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{2.1.2}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$G_{2.1.3}$	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Στο επόμενο βήμα του φορμαλιστικού μοντέλου ορίζονται οι διεργασίες που υλοποιούν τους σχετικούς με την ιδιωτικότητα στόχους καθώς και τα πρότυπα ιδιωτικότητας που εφαρμόζονται στις διεργασίες αυτές.

7.3.2. Ανάλυση της επίδρασης των στόχων ιδιωτικότητας στις διεργασίες

Πρώτα ορίζεται το σύνολο P που περιλαμβάνει όλες τις διεργασίες που υλοποιούν τους τελικούς στόχους του οργανισμού με βάση και το μοντέλο του Σχήματος 7.10. Ο ορισμός του συνόλου P είναι ο ακόλουθος:

$$P = \{P_1, P_2, P_3, P_4, P_5, P_6\}$$

Στη συνέχεια για κάθε τελικό στόχο ορίζεται ποιες διεργασίες τον υλοποιούν. Με τη χρήση της διαδικασίας Match_G_P() ορίζονται για τους τελικούς στόχους οι αντίστοιχες διεργασίες.

$$\text{Match\_G\_P}(G_{1.1.1}) = (P_1, P_2)$$

$$\text{Match\_G\_P}(G_{1.1.3.1}) = (P_2)$$

$$\text{Match\_G\_P}(G_{1.1.3.2}) = (P_2)$$

$$\text{Match\_G\_P}(G_{1.2}) = (P_4)$$

$$\text{Match\_G\_P}(G_{2.1.1}) = (P_6)$$

$$\text{Match\_G\_P}(G_{2.1.2}) = (P_5)$$

Μετά τους παραπάνω ορισμούς, κάθε τελικός στόχος έχει συνδεθεί με τις αντίστοιχες διεργασίες που τον υλοποιούν. Έτσι ο στόχος $G_{1.1.1}$ επηρεάζει τη διεργασία P1 και P2, ο στόχος $G_{1.1.3.1}$ τη διεργασία P2, κ.ο.κ.

Στο επόμενο βήμα εφαρμόζονται τα πρότυπα ιδιωτικότητας ανάλογα με τους στόχους ιδιωτικότητας που υλοποιεί κάθε τελικός στόχος και οι οποίοι επηρεάζουν την εκάστοτε διεργασία που τους υλοποιεί.

7.3.3. Διαμόρφωση των διεργασιών ιδιωτικότητας με τη χρήση προτύπων ιδιωτικότητας

Σε αυτό το στάδιο γίνεται ο εντοπισμός των προτύπων ιδιωτικότητας που θα εφαρμοστούν στις αντίστοιχες διεργασίες. Στη συγκεκριμένη περίπτωση, οι διεργασίες που είναι σχετικές με την υλοποίηση των στόχων ιδιωτικότητας είναι η P_3 και η P_6. Η P_3 υλοποιεί τον στόχο $G_{1.1.3.2}$ και η διεργασία P_6 υλοποιεί τους τελικούς στόχους $G_{2.1.1.1}$ και $G_{2.1.1.2}$.

Για το σκοπό αυτό εφαρμόζεται η Locate_pp() για τους δύο παραπάνω στόχους ώστε να εντοπισθούν τα πρότυπα που θα εφαρμοστούν στις αντίστοιχες διεργασίες.

Το αποτέλεσμα είναι:

$$\text{Id}=0,\ \text{an}=0,\ \text{unlink}=1,\ \text{unob}=0, \text{ for the goal } G_{1.1.3.2}$$

$$\text{Id}=0,\ \text{an}=0,\ \text{unlink}=0,\ \text{unob}=1, \text{ for the goal } G' \ (G_{2.1.1.1} \vee G_{2.1.1.2})$$

Κατόπιν εφαρμόζεται η διαδικασία Assign_pp() στις αντίστοιχες διεργασίες P_3 και P_6 ώστε οι μεταβλητές προτύπων ιδιωτικότητας να λάβουν τις ανάλογες τιμές, δηλώνοντας έτσι ποια πρότυπα θα εφαρμοστούν στη κάθε διεργασία. Οι παρακάτω τιμές θα ανατεθούν στις διεργασίες αυτές δηλώνοντας ότι στη μεν διεργασία P_3 θα εφαρμοστεί το πρότυπο της μη-συνδεσιμότητας, στη δε διεργασία P_6 αυτά της εξουσιοδότησης και της μη-παρατηρησιμότητας.

$P_3 = (0,0,0,0,0,1,0)$

$P_6 = (0,1,0,0,0,0,1)$

7.3.4. Εύρεση των τεχνολογιών που υποστηρίζουν την υλοποίηση των προαναφερθέντων προτύπων ιδιωτικότητας

Στο τελευταίο βήμα εντοπίζονται και προτείνονται με τη χρήση της συνάρτησης Locate_ITs(P), μια σειρά από τεχνολογίες υλοποίησης απαιτήσεων ιδιωτικότητας για το συγκεκριμένο σύστημα, με βάση τα πρότυπα ιδιωτικότητας που αναγνωρίσθηκαν στο προηγούμενο βήμα και πρέπει να υλοποιηθούν.

Στη συγκεκριμένη περίπτωση η PriS αναζητά και προτείνει τις τεχνολογίες εκείνες που υλοποιούν τα πρότυπα της εξουσιοδότησης, της μη-συνδεσιμότητας και της μη-παρατηρησιμότητας. Για τη διεργασία P_3 προτείνει όλες τις τεχνολογίες που υλοποιούν το πρότυπο της μη-συνδεσιμότητας, ενώ για την P_6 αυτές της εξουσιοδότησης και της μη-παρατηρησιμότητας. Συγκεκριμένα, τα αποτελέσματα θα είναι τα ακόλουθα:

Για τη διεργασία P3:

Primary Suggestions:

- Surrogate Keys

Secondary Suggestions:

- Trusted Third Parties
- Onion Routing
- Mix-Nets
- Hordes
- Gap
- Tor
- CRM Personalisation

- Application Data Management
- Spyware Detection and Removal
- Browser Cleaning Tools
- Activity Tracer Erasers
- Hard Disk Data Eraser

Για τη διεργασία P6:

Primary Suggestions:

None

Secondary Suggestions:

- Identity Management
- Biometrics
- Smart Cards
- Permission Management
- Notification and Audit Tools
- Hordes
- Gap
- Tor
- Spyware Detection and Removal
- Browser Cleaning Tools
- Activity Tracer Erasers
- Hard Disk Data Eraser
- Encrypting Email
- Encrypting Transactions
- Encrypting Documents

Όπως αναφέρθηκε και προηγουμένως, ο υπεύθυνος υλοποίησης του συστήματος είναι εκείνος που έχει ως τελική αρμοδιότητα να επιλέξει ποια τεχνολογία είναι επαρκής και ποια τελικά θα υιοθετηθεί και θα

εφαρμοστεί. Ο ρόλος της PriS είναι καθοδηγητικός, προτείνοντας μια σειρά από τεχνολογίες σχετικές με το περιεχόμενο και τις απαιτήσεις του συστήματος. Εκείνος θα αποφασίσει με γνώμονα και άλλους παράγοντες όπως το κόστος, την πολυπλοκότητα υλοποίησης του συστήματος, κ.λπ.

7.4. Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκε η εφαρμογή της μεθοδολογίας PriS σε ένα σύστημα ηλεκτρονικής ψηφοφορίας μέσω του Διαδικτύου. Εφαρμόζοντας τη μεθοδολογία στη μελέτη περίπτωσης διαπιστώθηκε ότι είναι υλοποιήσιμη. Εφαρμόστηκαν όλα τα στάδια πάνω σε πραγματικά δεδομένα και αποδείχθηκε ότι με τη χρήση της μεθοδολογίας μπόρεσαν να ενσωματωθούν οι απαιτήσεις ιδιωτικότητας στο υπόλοιπο σύστημα. Επίσης προτάθηκαν επιτυχώς τεχνολογίες ενίσχυσης της ιδιωτικότητας που να υλοποιούν τις συγκεκριμένες απαιτήσεις καθοδηγώντας με ορθό τρόπο τον υπεύθυνο υλοποίησης του συστήματος.

Ωστόσο διαπιστώθηκε επίσης ότι η μεθοδολογία είναι σε μερικά στάδια πολύ επαναληπτική. Συγκεκριμένα οι δηλώσεις με τη χρήση της Assign_pv καθυστερούν την όλη διαδικασία μιας και για κάθε στόχο πρέπει να δηλωθούν ξεχωριστά οι στόχοι ιδιωτικότητας που τον επηρεάζουν. Επίσης καθυστέρηση παρατηρείται στην εύρεση των τεχνολογιών ιδιωτικότητας με τη χρήση της συνάρτησης Locate_ITs(P). Συγκεκριμένα όταν αυξάνεται ο αριθμός των διεργασιών αυξάνεται κατά πολύ και ο χρόνος εύρεσης των κατάλληλων τεχνολογιών. Είναι βέβαιο ότι η δημιουργία και χρήση ενός εργαλείου θα αύξανε κατά πολύ την ταχύτητά της μεθοδολογίας μειώνοντας τον αριθμό των επαναλήψεων.

8. Επίλογος

Η ιδιωτικότητα είναι διεθνώς αναγνωρισμένη ως ανθρώπινο δικαίωμα το οποίο πρέπει να προστατεύεται από τις κοινωνίες που συμμετέχουν και δραστηριοποιούνται οι άνθρωποι. Μια από τις κοινωνίες αυτές είναι και η κοινωνία της πληροφορίας η οποία χρησιμοποιεί ως δίαυλο επικοινωνίας το Διαδίκτυο και τις υπηρεσίες του.

Καθημερινά, όλο και περισσότεροι χρήστες χρησιμοποιούν το Διαδίκτυο αφού οι υπηρεσίες που προσφέρει διευκολύνουν κατά πολύ το τρόπο και τη ποιότητα ζωής τους. Η ραγδαία αύξηση των χρηστών, τα τελευταία χρόνια, οδήγησε τους παρόχους υπηρεσιών να αυξήσουν τους ρυθμούς παραγωγής προϊόντων και υπηρεσιών με σκοπό αφενός μεν την καλύτερη εξυπηρέτηση των χρηστών αφετέρου δε την καθιέρωσή τους στην πώληση συγκεκριμένων προϊόντων και υπηρεσιών και την καταξίωση τους με στόχο το κέρδος.

Η γρήγορη αυτή εξέλιξη, σε συνδυασμό με την ολοένα και αυξανόμενη τάση των χρηστών στη χρήση των υπηρεσιών, που παρέχονται από το Διαδίκτυο, οδήγησε στη δημιουργία επισφαλών πληροφοριακών συστημάτων και εφαρμογών καθώς και επισφαλών διαύλων επικοινωνίας μεταξύ των εφαρμογών αυτών και των χρηστών.

Παράλληλα όσο περισσότεροι χρήστες χρησιμοποιούν το Διαδίκτυο, τόσο περισσότερα προσωπικά δεδομένα μεταφέρονται καθημερινά μέσα από επισφαλή δίκτυα και επεξεργάζονται από εφαρμογές και συστήματα χωρίς να λαμβάνονται τα απαραίτητα μέτρα προστασίας των δεδομένων αυτών. Η προστασία της ιδιωτικότητας των χρηστών είναι ένα ζήτημα άκρως σημαντικό το οποίο, ακόμη και σήμερα,

δεν αντιμετωπίζεται ολοκληρωμένα, και αυτό αποτέλεσε το κίνητρο της συγκεκριμένης εργασίας.

8.1. Στόχοι και Αποτελέσματα της Παρούσας Έρευνας

Ανάλυση της τρέχουσας πρακτικής στο χώρο της τεχνολογίας απαιτήσεων ασφαλείας (security requirements engineering) οδήγησε στη διαπίστωση ότι οι περισσότερες μεθοδολογίες επικεντρώνονται είτε στον εντοπισμό των απαιτήσεων ιδιωτικότητας είτε στο καθορισμό των τεχνικών υλοποίησης. Δηλαδή, δεν γίνεται σαφής σύνδεση μεταξύ απαιτήσεων και τεχνολογικών λύσεων με αποτέλεσμα να μην είναι σαφές που και ποιες τεχνολογίες πρέπει να εφαρμοστούν κάθε φορά ώστε το υπό-κατασκευή σύστημα να προστατεύει την ιδιωτικότητα των χρηστών.

Με στόχο την κάλυψη αυτού του κενού προτάθηκε μια μεθοδολογία η οποία αναγνωρίζει ποιες είναι οι βασικές απαιτήσεις ιδιωτικότητας που πρέπει να υλοποιηθούν σε ένα πληροφοριακό σύστημα και με ποια μέθοδο αυτές θα αντιμετωπιστούν κατά τη σχεδίαση του συστήματος.

Συγκεκριμένα, η προτεινόμενη μεθοδολογία ορίζει ένα σύνολο στόχων ιδιωτικότητας οι οποίοι επιλεκτικά εφαρμόζονται στους στόχους του οργανισμού. Στη συνέχεια, εξετάζεται η επίδραση των στόχων ιδιωτικότητας στις διεργασίες του οργανισμού με την εφαρμογή προτύπων ιδιωτικότητας σε κάθε διεργασία ξεχωριστά, βάσει των συγκεκριμένων απαιτήσεων ιδιωτικότητας. Τέλος, εντοπίζονται και προτείνονται μια σειρά από τεχνολογίες ενίσχυσης της ιδιωτικότητας. Η επιλογή γίνεται για κάθε διεργασία ξεχωριστά βάσει των προτύπων ιδιωτικότητας που έχουν εφαρμοστεί σε αυτή.

Βασικό πλεονέκτημα της προτεινόμενης μεθοδολογίας είναι η αντιμετώπιση της ιδιωτικότητας ως ξεχωριστό κριτήριο στη φάση της σχεδίασης και όχι στη φάση της υλοποίησης, συνδέοντας έτσι τις απαιτήσεις ιδιωτικότητας του οργανισμού με αντίστοιχες τεχνολογικές λύσεις βασισμένες στις συγκεκριμένες απαιτήσεις και στο συγκεκριμένο τρόπο λειτουργίας του οργανισμού.

Επίσης, μέσω της προτεινόμενης μεθοδολογίας ορίζονται επιμέρους στόχοι ιδιωτικότητας οδηγώντας έτσι σε ένα λεπτομερή προσδιορισμό και σε μια σαφή ανάλυση των ζητημάτων ιδιωτικότητας στο υπό-ανάπτυξη σύστημα. Αυτό είναι απαραίτητο δεδομένου ότι η επίδραση της ιδιωτικότητας είναι αρκετά σύνθετη και δεν μπορεί να αντιμετωπισθεί σαν μία και μόνο απαίτηση.

Ένα άλλο πλεονέκτημα της προτεινόμενης μεθοδολογίας είναι ότι ορίζει συγκεκριμένα πρότυπα διεργασιών και τα συσχετίζει με τις απαιτήσεις ιδιωτικότητας με σκοπό την ανάδειξη της επίδρασης των στόχων ιδιωτικότητας στις διεργασίες του οργανισμού. Συγκεκριμένα, για κάθε απαίτηση ορίζεται και το αντίστοιχο πρότυπο το οποίο εφαρμόζεται σε κάθε διεργασία που υλοποιεί έναν ή περισσότερους στόχους ιδιωτικότητας αναλύοντας έτσι την επίδραση των στόχων σε αυτές.

Τέλος, με τη χρήση των προτύπων, προτείνονται μια σειρά από τεχνολογίες και προϊόντα ενίσχυσης της ιδιωτικότητας για την υλοποίηση της κάθε διεργασίας ξεχωριστά (ανάλογα με τα πρότυπα ιδιωτικότητας που εφαρμόζονται σε αυτή). Έτσι αφενός μεν προτείνονται συγκεκριμένες τεχνολογικές λύσεις ανά διεργασία και όχι συνολικά, αφετέρου δε οι τεχνολογικές λύσεις αυτές στηρίζονται στην ανάλυση των στόχων του εκάστοτε οργανισμού και στις αντίστοιχες διεργασίες που τους υλοποιούν, καλύπτοντας έτσι το κενό μεταξύ των διεργασιών και των τεχνολογικών λύσεων που πρέπει να εφαρμοστούν.

8.2. Επόμενα Βήματα

Με βάση τα όσα αναφέρθηκαν στα προηγούμενα κεφάλαια προκύπτουν μια σειρά από ερευνητικά ζητήματα που αποτελούν και τα επόμενα βήματα της παρούσας έρευνας.

Βασική ανάγκη για την υποστήριξη της λειτουργίας της προτεινόμενης μεθοδολογίας είναι η ανάπτυξη ενός εργαλείου το οποίο θα μπορεί να αναγνωρίζει αυτόματα την επίδραση των στόχων ιδιωτικότητας στο μοντέλο στόχων-διεργασιών βασιζόμενο στη φορμαλιστική απεικόνιση της μεθοδολογίας. Επίσης, το εργαλείο θα παρέχει στους υπεύθυνους υλοποίησης του συστήματος μια περιγραφή της κάθε τεχνολογίας ενίσχυσης της ιδιωτικότητας καθώς και μια μορφή καθοδήγησης για το τρόπο εφαρμογής της τεχνολογίας που θα επιλέξουν να εφαρμόσουν επιτυγχάνοντας παράλληλα την ευκολότερη και αποτελεσματικότερη χρήση της μεθοδολογίας.

Ο δεύτερος βασικός άξονας της μελλοντικής έρευνας είναι η μελέτη κατηγοριοποίησης των τεχνολογιών ενίσχυσης ιδιωτικότητας με τη χρήση ασαφούς λογικής. Συγκεκριμένα, θα εξεταστεί η δημιουργία ομάδων τεχνολογιών για την υλοποίηση του κάθε προτύπου. Στην παρούσα φάση η PriS ακολουθεί τη δυαδική λογική (0 ή 1) για να εκφράσει το αν μία τεχνολογία υλοποιεί ή δεν υλοποιεί ένα πρότυπο ιδιωτικότητας. Η μελλοντική έρευνα στηρίζεται στην προσαρμογή αυτής της λογικής, καταργώντας το απόλυτο 0 και 1 και προσαρμόζοντας τη μεθοδολογία με τέτοιο τρόπο ώστε οι τεχνολογίες να έχουν συγκεκριμένο βαθμό συμμετοχής στην υλοποίηση συγκεκριμένων προτύπων και όχι απόλυτο. Πιο αναλυτικά, κατηγοριοποιώντας τις τεχνολογίες σε ομάδες κάθε τεχνολογία θα έχει ένα βαθμό συμμετοχής στην ομάδα ο οποίος θα δηλώνει αν και σε τι βαθμό μπορεί να υλοποιήσει το συγκεκριμένο

πρότυπο βελτιώνοντας έτσι το τρόπο επιλογής των τεχνολογιών μιας και αντί της λογικής του 0 και 1 (υλοποιεί - δεν υλοποιεί) θα υπάρχουν βαθμοί συμμετοχής της κάθε τεχνολογίας στην υλοποίηση του κάθε προτύπου. Με το τρόπο αυτό θα επιτυγχάνεται ένας δυναμικότερος τρόπος επιλογής των τεχνολογιών αφού πολλές φορές οι τεχνολογίες δεν μπορούν να υλοποιήσουν με την ίδια αποτελεσματικότητα απαιτήσεις για τις οποίες είναι σχεδιασμένες μιας και βασίζονται σε τρίτους παράγοντες όπως το περιβάλλον εφαρμογής, τα συνεργαζόμενα λογισμικά κτλ.

Τέλος, στη λογική του προηγούμενου άξονα, απαιτείται έρευνα για την αναζήτηση κατάλληλων κριτηρίων αξιολόγησης των τεχνολογιών ενίσχυσης της ιδιωτικότητας που θα βοηθούν τον υπεύθυνο υλοποίησης του συστήματος στην επιλογή της κατάλληλης τεχνολογίας. Με τη χρήση κριτηρίων αξιολόγησης για κάθε τεχνολογία θα γίνεται ευκολότερα αντιληπτός ο τρόπος λειτουργίας της, τα πεδία εφαρμογής της, τα πλεονεκτήματα και τα μειονεκτήματά της σε σχέση με άλλες τεχνολογίες που υλοποιούν ίδια πρότυπα ιδιωτικότητας. Λαμβάνοντας υπόψη τα κριτήρια αυτά, ο υπεύθυνος υλοποίησης, θα αποκτά μια σαφέστερη εικόνα για την κάθε τεχνολογία ώστε να επιλέξει ευκολότερα, γρηγορότερα και αποτελεσματικότερα τη/τις βέλτιστη/τες τεχνολογία/ες για το υπό-ανάπτυξη σύστημα.

Βιβλιογραφία

Aegean, University of the (2003). E-Vote:An Internet-based electronic voting system. University of the Aegean, Project Deliverable D 7.6, IST Programme 2000#29518, 21/11/2003, Samos.

Antón, A. (1996). Goal-based requirements analysis. ICRE'96. Colorado Springs, Colorado, USA, IEEE 136-144.

Antón, A. and J. Earp (2000). Strategies for developing policies and requirements for secure electronic commerce systems. 1st Workshop on security and privacy in e-commerce. Acm.

Bellotti, V. and A. Sellen (1993). Design for privacy in ubiquitous computing environments. Proceedings of the third european conference on computer supported cooperative work (ECSCW 93). G. In Michelis, Simone, C., Schmidt, K. 93-108.

Bennett, K. and C. Grothoff (2003). GAP-practical anonymous networking. Proceedings of Privacy Enhancing Technologies workshop (PET 2003), Dresden, Germany, Springer-Verlag **LNCS 2670**, 26-28 March 2003.

Boyan, J. (1997). "The Anonymizer:Protecting user privacy on the web." Computer-Mediated Communication Magazine **4**(9).

Business, Week (1998). "A Little Net Privacy, Please." Available at: www.businessweek.com **last accessed: 17/12/2007**.

Cannon, J.C. (2004). Privacy, What developers and IT professionals should know, Addison-Wesley.

Chaum, D. (1981). "Untraceable electronic mail, return addresses, and digital pseudonyms." Communications of the ACM **24**(2): 84-88.

Chaum, D. (1985). "Security without identification: Transactions systems to make Big Brother obsolete." Communications of the ACM **28**(10): 1030-1044.

Chaum, D. (1988). "The Dining cryptographers problem:Unconditional sender and recipient untraceability." Journal of Cryptology **1**(1): 65-75.

Chung, L. (1993). Dealing with security requirements during the development of information systems. The 5th international conference of advanced information systems engineering, CAiSE'93, Paris, France, Springer Verlag **LNCS 685**, pp: 234-251

Chung, L., B. Nixon, E. Yu. and J. Mylopoulos (2000). Non-Functional requirements in software engineering, Kluwer Academic Publishers.

Dardenne, A. and A. van Lamsweerde (1996). Formal refinement patterns for goal-driven requierements elaboration. 4th ACM SIGSOFT International Symposium on the Foundations of Software Engineering pp: 179-190

Dardenne, A., A. van Lamsweerde and S. Fickas (1993). "Goal-directed requirements acquisition." Science of computer programming **20**: 3-50.

Dingledine, R., N. Mathewson and P. Syverson (2004). Tor: The second generator onion router. Proceedings of the 13th USENIX Security Symposium, San Diego, California, USA pp: 303-320 13-19 August 2004.

EU, Directive. (1995). Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data.

Fischer-Hubner, S. (2001). IT-security and privacy-Design and use of privacy enhancing security mechanisms. 5th International Conference on Applications of Natural Language to Information Systems, Versailles, France, Lecture Notes in Computer Science **1958**, pp: 35-106 June 2000.

Goldschlang, D., P. Syverson and M. Reed (1999). "Onion Routing for anonymous and private Internet connections." Communications of the ACM **42**(2): 39-41.

Gritzalis, S. (2004). "Enhancing Web privacy and anonymity in the digital era." Information Management and Security Group **12**(3): 255-288.

Group, META (2005). Privacy Enhancing Technologies. Report v1.1.

He, Q. and A. Antón (2003). A framework for modeling privacy requirements in role engineering. International workshop on requirements engineering for software quality (REFSQ). Klagenfurt/Verden, Austria.

Hong, J., J. Ng, S. Lederer and J. Landey (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. Symposium on Designing Interactive Systems archive - Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques. Acm-Press. Cambridge, MA, USA 91-100.

J.Holvast (1993). Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?, Elsevier Science Publishers B.V. (North-Holland) **IFIP-WG9.2 340 References Conference**.

Jensen, C., J. Tullio, C. Potts and E. Mynatt (2005). STRAP: A Structured Analysis Framework for Privacy. GVU Technical Report, Georgia Institute of Technology, GIT-GVU-05-02.

Kalloniatis, C., E. Kavakli and S. Gritzalis (2004). Security requirements engineering for e-Government Applications. DEXA EGOV'04 Conference. Springer-Verlag, LNCS. **3183** 66-71.

Kalloniatis, C., E. Kavakli and S. Gritzalis (2005a). Dealing with Privacy Issues during the System Design Process. 5th IEEE International Symposium on Signal Processing and Information Technology, Athens pp: 546-551 18-21 December.

Kalloniatis, C., E. Kavakli and S. Gritzalis (2005b). PriS Methodology: Incorporating Privacy Requirements into the System Design Process. Symposium on Requirements Engineering for Information Security, 13th IEEE International Requirements Engineering Conference, Paris, IEEE 29 August - 2 September.

Kalloniatis, C., E. Kavakli and S. Gritzalis (2007). Using privacy process patterns for incorporating privacy requirements into the system design process. Workshop on secure software engineering (SecSe 2007) in conjuction with the international conference on availability, reliability and security (ARES 2007), Vienna, Austria 10-13 April.

Kavakli, E. (2004). Modeling organizational goals:Analysis of current methods. Proceedings of the 2004 ACM symposium on applied computing. Acm. Nicosia, CY 1339-1343.

Kavakli, E., S. Gritzalis and C. Kalloniatis (2007). "Protecting Privacy in System Design: The Electronic Voting Case." Transforming Government: People, Process and Policy **1**(4): 307-332.

Kavakli, E., C. Kalloniatis and S. Gritzalis (2005). Addressing Privacy:Matching user requirements with implementation techniques. 7th Hellenic European Conference on Computer Mathematics and its Applications (HERCMA 2005), Athens 22-24 September.

Kavakli, E., C. Kalloniatis, P. Loucopoulos and S. Gritzalis (2006). "Incorporating privacy requirements into the system design process:The PriS conceptual framework." Internet Research Journal **16**(2): 140-158.

Koorn, R., H. van Gils, J. Hart, P. Overbeek and R. Tellegen (2004). Privacy Enhancing Technologies-White paper for decision makers. Ministry of the Interior and Kingdom Relations, the Netherlands.

Letier, E. and A. van Lamsweerde (2002a). Agent-based tactics for goal-oriented requirements elaboration. 24th International Conference on Software Engineering (ICSE'02) pp: 83-93

Letier, E. and A. van Lamsweerde (2002b). Deriving operational software specifications from system goals. 10th ACM SIGSOFT International Symposium on the Foundations of Software Engineering pp: 119-128

Liu, L., E. Yu. and J. Mylopoulos (2002). Analyzing security requirements as relationships among strategic actors. SREIS'02. Raleigh, North Carolina.

Liu, L., E. Yu. and J. Mylopoulos (2003). Security and privacy requirements analysis within a social setting. IEEE,11th international requirements engineering conference (RE'03). Monterey Bay, California, USA.

Loucopoulos, P. (2000). From information modelling to enterprise modelling. Information systems engineering: State of the art and research themes pp: 67-78

Loucopoulos, P. and E. Kavakli (1997). Enterprise knowledge management and conceptual modelling. Current Issues and Future Directions, Selected Papers from the Symposium on Conceptual Modeling, (ER'97), P. P. Chen et al. (ed), Lecture Notes in Computer Science **1565**, pp: 123-143 Springer 1999.

Moffett, D. and B. Nuseibeh (2003). A framework for security requirements engineering. Department of computer science, University of York, YCS 368.

Mouratidis., H., P. Giorgini and G. Manson (2003a). Integrating security and systems engineering: Towards the modelling of secure information systems. LNCS 2681. Springer-Verlag. Berlin Heidelberg 63-78.

Mouratidis., H., P. Giorgini and G. Manson (2003b). An ontology for modelling security:The tropos project. Proceedings of the KES 2003 invited session ontology and multi-agent systems design (OMASD'03)-Lecture Notes in Artificial Intelligence 2773. V. Palade, R. Howlett and L Jain. United Kingdom, University of Oxford, Springer-Verlag 1387-1394.

Perini, P., P. Bresciani, P. Giorgini, F. Giunchiglia and J. Mylopoulos (2001). Towards an agent-oriented approach to software engineering, Modena-Italy

Pfitzmann, A. (1990). Diensteintegrierende, Kommunikationsmnetze mit teilnehmeruberprufbaren Datenschutz. Informatik-Fachberichte 234. Springer-Verlag. Berlin Heidelberg New York.

Pfitzmann, A. and M Hansen (2007). Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonumity and Identity Management-A Consolidated Proposal for Terminology v.029. TU Dresden
ULD Kiel, 31 July 2007, Dresden.

Pfitzmann, A. and M. Waidner (1987). "Networks without user observability." Computer and Security **6**(2): 158-166.

Pfitzmann, B., M. Waidner and A. Pfitzmann (1990). Rechsicherheit trotz Anonymitat in offenen digitalen Systemen. Datenschutz und Datensicherheit (DuD), No 6 (Part 1) pp. 243-253, No 7 (Part 2) pp. 305-315.

PricewaterhouseCoopers (2001). "Privacy:a weak link in the cyber-chain." E-Business Leadres Series, PricewaterhouseCoopers, New York.

Privacy International, Electronic Privacy Information Center (1999). Privacy and Human Rights - An International Survey of Privacy Laws and Developments.

R.Rosenberg (1992). The Social Impact of Computers, Academic Press.

Reed, M., P. Syverson and D. Goldschlang (1998). "Anonymous connections and Onion Routing." IEEE Journal on Selected Areas in Communications **16**(4): 482-494.

Reiter, M. and A. Rubin (1998). "Crowds:Anonymity for Web transactions." ACM Transactions of Information and System Security **1**(1): 66-92.

Reiter, M. and A. Rubin (1999). "Anonymous Web Transactions with Crowds." Communications of the ACM **42**(2): 32-38.

Shields, C. and B. Levine (2000). A protocol for anonymous communication over the Internet. In:Samarati, P.-Jajodia, S.(eds):Proceedings of the 7th ACM Conference on computer and communications security. New York, NY, ACM-Press 33-42.

van Lamsweerde, A. and E. Letier (2000). "Handling obstacles in goal-oriented requirements engineering." IEEE Trans. Soft. Eng. **26**: 978-1005.

van Lamsweerde, A., Darimont R. and E. Letier (1998). "Managing conflicts in Goal-driven requirements engineering." IEEE Trans. Soft. Eng. **24**(11): 908-925.

van Lamsweerde, A., Darimont R. and Massonet P. (1995). Goal-directed elaboration of requirements for a meeting scheduler: Problems and lessons learnt. 2nd IEEE International Symposium on Requirements Engineering pp: 194-203

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

Welfare, US Department of Health Education and (1973). Code of Fair Information practises (The).

Westin, A. (1967). Privacy and Freedom, The Bodley Head Ltd.

Yu., E. (1993). Modeling organisations for information systems requirements engineering. 1st IEEE International Symposium on Requirements Engineering pp: 34-41

Yu., E. (1997). Towards Modelling and reasoning support for early phase requirements engineering. 3rd IEEE International Symposium on Requirements Engineering pp: 226-235

Yu., E. and Cysneiros L. (2002). Designing for privacy and other competing requirements. 2nd Symposium on Requirements Engineering for Information Security (SREIS'02)

Yu., E. and Cysneiros L. (2003). Designing for Privacy in a Multi-Agent World. Trust, Reputation and Security:Theories and Pactice, Springer Verlag **LNCS 2631**, pp: 209-223