Ατομική Διπλωματική Εργασία

ΕΙΣΑΓΩΓΗ ΤΩΝ ΕΝΝΟΙΩΝ ΔΟΜΗΣ ΚΑΙ ΣΥΝΘΗΚΗΣ ΣΕ ΣΗΜΑΣΙΟΛΟΓΙΚΟ ΠΡΟΤΥΠΟ ΜΕΛΕΤΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Γεώργιος Τερτίτσνι

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2016

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΙΣΑΓΩΓΗ ΤΩΝ ΕΝΝΟΙΩΝ ΔΟΜΗΣ ΚΑΙ ΣΥΝΘΗΚΗΣ ΣΕ ΣΗΜΑΣΙΟΛΟΓΙΚΟ ΠΡΟΤΥΠΟ ΜΕΛΕΤΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Γεώργιος Τερτίτσνι

Επιβλέπουσα Καθηγήτρια
Άννα Φιλίππου

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

Μάιος 2016

Ευχαριστίες

Καταρχάς θα ήθελα να εκφράσω τις ολόψυχες ευχαριστίες μου προς την καθηγήτρια κα. Άννα Φιλίππου, επιβλέπουσα καθηγήτρια της διπλωματικής αυτής εργασίας για την εμπιστοσύνη που μου έδειξε ως προς τη διεκπεραίωση της αλλά και για την τεράστια ευκαιρία που μου έδωσε να ασχοληθώ με ένα τόσο ενδιαφέρον και χρήσιμο θέμα. Θα ήθελα επίσης να την ευχαριστήσω για την άριστη συνεργασία, την κατανόηση, την υπομονή, τον πολύτιμο χρόνο που αφιέρωνε συνεχώς για εμένα αλλά κυρίως για τις συμβουλές της οι οποίες με βοήθησαν όχι μόνο στην ολοκλήρωση της εργασίας αυτής αλλά και καθόλι τη διάρκεια του προπτυχιακού κύκλου σπουδών μου.

Παράλληλα, εφόσον η παρούσα εργασία αποτελεί την ολοκλήρωση του κύκλου σπουδών μου ως προπτυχιακός φοιτητής θα ήθελα να ευχαριστήσω τα σημαντικότερα άτομα της ζωής μου, τους γονείς μου, Ιβάν και Αντρούλλα για την τεράστια αγάπη τους, την οικονομική, ψυχολογική στήριξη τους η οποία αποτελούσε πάντοτε την κινητήρια δύναμη για μένα να συνεχίζω. Τα όσα μου έχουν προσφέρει είναι αμέτρητα και χωρίς τη δική τους συμβολή όλα αυτά τα χρόνια τίποτα δεν θα ήταν εφικτό. Είμαι πραγματικά ευγνώμων για όσα έχω πάρει από αυτούς και ως ελάχιστη έκφραση ενός τεράστιου ευχαριστώ τους αφιερώνω εξ' ολοκλήρου την παρούσα εργασία.

Τέλος, δεν θα μπορούσα να μην εκφράσω παράλληλα ένα μεγάλο ευχαριστώ στο άτομο το οποίο αποτελούσε για μένα πάντοτε πρότυπο ζωής, την αδελφή μου Κατερίνα, η οποία στάθηκε δίπλα μου όλα αυτά τα χρόνια και με βοηθούσε πάντοτε σε ότι ήθελα. Νιώθω πραγματικά περήφανος και ευλογημένος που σε όλες τις δύσκολες στιγμές της ζωής μου είχα δίπλα μου την αδελφή μου. Είναι το άτομο του οποίου η ακαδημαϊκή πορεία και εξέλιξη αποτελούσε πάντοτε για μένα φωτεινό παράδειγμα καθώς μέσα από αυτή, μου δίδαξε πως στα δύσκολα ποτέ δεν τα παρατάμε και πώς η ανέλιξη για τον άνθρωπο δεν έχει όρια.

Περίληψη

Η ικανοποίηση του αισθήματος της ιδιωτικότητας αποτελούσε πάντοτε σημαντική παράμετρο ως προς την ικανοποίηση του αισθήματος ελευθερίας των ατόμων. Η ραγδαία ανάπτυξη της τεχνολογίας που χαρακτηρίζει την σημερινή εποχή και η όλο ένα και μεγαλύτερη χρήση ευαίσθητων προσωπικών πληροφοριών από διάφορα συστήματα εγείρει νέα ζητήματα όσον αφορά την ιδιωτικότητα. Η χρήση των πληροφοριών αυτών ποικίλει από συστήματα τα οποία υλοποιούνται διαδικτυακά για ιστοσελίδες, συστήματα ελέγχου κυβερνητικών υπηρεσιών αλλά και εφαρμογές κινητών συσκευών οι οποίες λαμβάνουν πρόσβαση σε συγκεκριμένες πληροφορίες της συσκευής. Όλα τα παραπάνω συστήματα συνοδεύονται από πολιτικές ιδιωτικότητας που καθορίζουν το σύνολο των ενεργειών που εφαρμόζουν πάνω στις ευαίσθητες πληροφορίες που συλλέγουν και επεξεργάζονται. Στην απουσία ωστόσο εργαλείων ελέγχου ικανοποίησης των πολιτικών αυτών από τα διάφορα συστήματα δημιουργείτε ένα κλίμα δυσπιστίας από τους ανθρώπους και το αίσθημα εμπιστοσύνης προς αυτά χάνεται.

Στηριζόμενοι στην ανάγκη θεώρησης τέτοιων εργαλείων ελέγχου η παρούσα διπλωματική εργασία εκμεταλλευόμενη εργαλεία που προσφέρει η Επιστήμη της Πληροφορικής και συγκεκριμένα οι Τυπικές Μέθοδοι έρχεται να προτείνει ένα τυπικό πλαίσιο ελέγχου πολιτικών ιδιωτικότητας από συστήματα με τη χρήση τύπων. Συγκεκριμένα η παρούσα διπλωματική εργασία επεκτείνει ένα υφιστάμενο πλαίσιο ελέγχου πολιτικών ιδιωτικότητας με την ενσωμάτωση της έννοιας της συνθήκης όσον αφορά την τυπική διατύπωση των πολιτικών ιδιωτικότητας αλλά και συμπεριφορά συστημάτων, τη δυνατότητα καταγραφής πολιτικών σε επίπεδο δομών πληροφοριών ενώ επεκτείνεται και το σύνολο των τυπικών δικαιωμάτων που μπορούν να διατυπωθούν δια μέσου μιας πολιτικής. Το προτεινόμενο πλαίσιο ελέγχου περιλαμβάνει ένα τυπικό ορισμό για την διατύπωση πολιτικών ιδιωτικότητας με την χρήση τύπων, ένα προτεινόμενο λογισμό για την μοντελοποίηση συστημάτων ο οποίος συνοδεύεται από ένα σύστημα τύπων και αποδείξεις μέσω των οποίων καθορίζεται η ικανοποίηση πολιτικών ιδιωτικότητας από τα συστήματα των οποίων η λειτουργία έχει μοντελοποιηθεί. Το προτεινόμενο πλαίσιο ελέγχου βρίσκει εφαρμογή σε διάφορα παραδείγματα χρήσης από περιπτώσεις που προκύπτουν μέσα από σενάρια της πραγματικής ζωής που αφορούν πολιτικές ιδιωτικότητας και συστήματα που εργάζονται βάσει αυτών.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

1.1 Κίνητρο Διπλωματικής Εργασίας

Η όρος ιδιωτικότητα είναι ένας όρος ο οποίος δύσκολα μπορεί να οριστεί καθότι για αυτόν υπάρχουν διάφοροι φιλοσοφικοί νομικοί κοινωνικοί και τεχνολογικοί ορισμοί ενώ αρκετές φορές η απάντηση ως προς το τι είναι η ιδιωτικότητα εξαρτάται και καθορίζεται από το άτομο το οποίο αφορά η ερώτηση. Ο καθηγητής του πανεπιστημίου Columbia Alan F.Westin, Columbia ο οποίος ασχολήθηκε με την έννοια της ιδιωτικότητας από το 1967 ορίζει αυτήν ως εξής [15]: *"Ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων ή των οργανισμών να καθορίσουν για τους εαυτούς τους πότε, πώς, και σε ποιο βαθμό οι πληροφορίες σχετικά με αυτούς κοινοποιούνται στους άλλους".*

Η Επιστήμη της Πληροφορικής διαδραματίζει τεράστιο ρόλο και είναι άρρηκτα συνδεδεμένη με την έννοια της ιδιωτικότητας. Από τη μια, η ραγδαία τεχνολογική εξέλιξη λόγω της σημαντικής έκρηξης που παρατηρείται ως προς τη χρήση του διαδικτύου, η μηχανογράφηση ευαίσθητων προσωπικών πληροφοριών όπως για παράδειγμα στοιχεία που αφορούν ασθένειες, η χρήση των κοινωνικών δικτύων, αλλά και η χρήση των προσωπικών μας ηλεκτρονικών φορητών συσκευών σε καθημερινή βάση με διάφορες εφαρμογές που λαμβάνουν πρόσβαση στις προσωπικές μας πληροφορίες εγείρουν σημαντικά ζητήματα ως προς την προστασία των ευαίσθητων αυτών πληροφοριών αλλά και την ικανοποίηση του αισθήματος της ιδιωτικότητας. Ταυτόχρονα, η Επιστήμη της Πληροφορικής προσφέρει σημαντικά εργαλεία που μπορούν να χρησιμοποιηθούν για την αντιμετώπισή των κινδύνων που πηγάζουν από τη

χρήση των πληροφοριών αυτών και την προστασία της ιδιωτικότητας των ατόμων. Ένα από τα σημαντικότερα εργαλεία όπως αναφέρεται και σχετικά στο [14] είναι οι Τυπικές Μέθοδοι. Με τον όρο *Τυπικές Μέθοδοι* αναφερόμαστε σε εφαρμοσμένα μαθηματικά τα οποία μπορούν να χρησιμοποιηθούν για τη μοντελοποίηση και ανάλυση υπολογιστικών συστημάτων. Όσον αφορά την έννοια της ιδιωτικότητας τα διάφορα τυπικά μοντέλα που έχουν εφαρμοστεί και εξετάζουν την έννοια αυτή, όπως αναφέρεται και στο [14] ποικίλουν από Θεωρίες Παιγνίων μέχρι και θεωρίες Αλγεβρών Διεργασιών. Αυτά μπορούν να χρησιμοποιηθούν για να προσομοιώσουν τη συμπεριφορά ενός συστήματος να συλλάβουν απαιτήσεις που ορίζει μια πολιτική ιδιωτικότητας προσφέροντας τη δυνατότητα ελέγχου ικανοποίησης πολιτικών από συστήματα με μαθηματική ακρίβεια και υπόβαθρο.

1.2 Βασική Ιδέα Διπλωματικής Εργασίας

Η βασική ιδέα για την εκπόνηση της παρούσας διπλωματικής εργασίας συνιστάται από την παραπάνω ανάγκη ελέγχου της ικανοποίησης πολιτικών ιδιωτικότητας από διάφορα συστήματα τα οποία πρέπει να σέβονται τις απαιτήσεις ιδιωτικότητας των χρηστών αλλά και τις πολιτικές ιδιωτικότητας πάνω στις οποίες ορίζουν την λειτουργία τους. Για το λόγο αυτό η παρούσα διπλωματική εργασία στηριζόμενη σε προτεινόμενες μεθοδολογίες για έλεγχο πολιτικών ιδιωτικότητας που προτείνονται στα [4,5] δίνει ένα καινούριο επεκτάμενο τυπικό πλαίσιο για έλεγχο πολιτικών ιδιωτικότητας.

1.3 Σκοπός Διπλωματικής Εργασίας

Σκοπός της διπλωματικής αυτής εργασίας είναι να ληφθούν υπόψιν σημαντικές παράμετροι αναφορικά με την τυπική διατύπωση των διαφόρων πολιτικών ιδιωτικότητας και να ενσωματωθούν στα πλαίσια μιας υφιστάμενης μεθοδολογίας ελέγχου. Για το λόγο αυτό μετά και από σχετική έρευνα διαφόρων πολιτικών σκοπός της παρούσας εργασίας τέθηκε η ενσωμάτωση των αφαιρετικών εννοιών δομής και συνθήκης στα πλαίσια ενός σημασιολογικού προτύπου για τη μελέτη της ιδιωτικότητας.

Συγκεκριμένα ο σκοπός της εργασίας αυτής αναφέρεται στην ενσωμάτωση των παραπάνω εννοιών τόσο ως προς τη τυπική διατύπωση των διαφόρων πολιτικών ιδιωτικότητας όσο και στη συμπεριφορά των διαφόρων συστημάτων καθότι θεωρούνται έννοιες που εμφανίζονται αρκετά συχνά σε διάφορα συστήματα και πολιτικές. Η

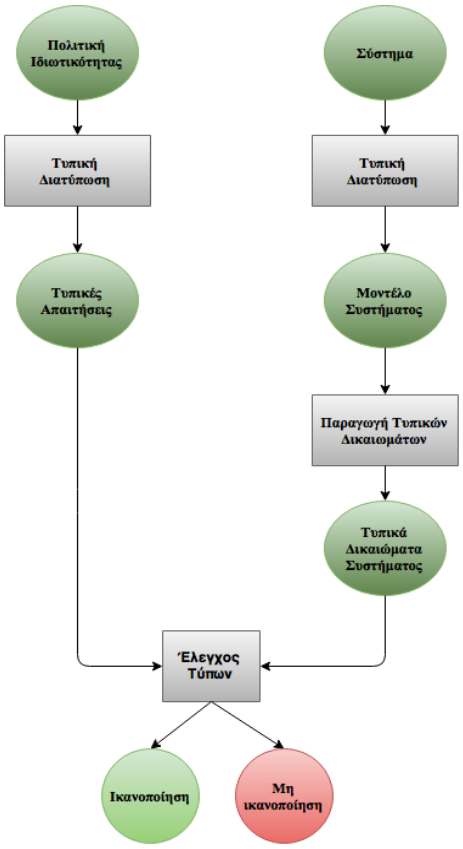
αφαιρετική έννοια της συνθήκης είναι άρρηκτα συνδεδεμένη με την καταγραφή πολιτικών ιδιωτικότητας καθότι αυτή συναντάται σε σχετικές νομοθεσίες ιδιωτικότητας όπως το $COPPA$ [2] και ταυτόχρονα θεωρείται ως μια από τις βασικές παραμέτρους διατύπωσης πολιτικών ιδιωτικότητας όπως σχετικά αναφέρεται και στο [6] το οποίο προσδιορίζει τις βασικές παραμέτρους που πρέπει να λαμβάνονται υπόψιν για την τυπική διατύπωση πολιτικών ιδιωτικότητας. Οι συνθήκες διατυπώνονται ούτως ώστε να περιορίζουν τα επιτρεπτά δικαιώματα που είναι δυνατό να εκτελούνται σε διάφορα δεδομένα στη βάση συγκεκριμένων καταστάσεων που πρέπει να ικανοποιούνται. Το ίδιο ισχύει και με τα διάφορα συστήματα τα οποία πολλές φορές αναπροσαρμόζουν τη συμπεριφορά τους βάσει συγκεκριμένων καταστάσεων που συναντώνται στα πλαίσια του περιβάλλοντος λειτουργίας τους.

Η δεύτερη έννοια την οποία τέθηκε ο στόχος να ενσωματώσουμε στα πλαίσια της παρούσας εργασίας αφορά την έννοια αναφορικά με τις δομές δεδομένων. Οι δομές δεδομένων είναι μια έννοια που συναντάται αρκετά συχνά σε πολλά συστήματα και πολιτικές, καθότι είναι δυνατό να διατυπώνονται ξεχωριστά δικαιώματα για τα διάφορα πεδία μιας δομής και τα οποία πρέπει τα αντίστοιχα συστήματα να λαμβάνουν υπόψιν τους κατά τη λειτουργίας τους. Με τη ενσωμάτωση της έννοιας της δομής δίνεται η δυνατότητα καταγραφής διαφορετικών δικαιωμάτων που προκύπτουν μέσα από το διαχωρισμό των πεδίων της δομής κάτι που ενισχύει σημαντικά το πλαίσιο ελέγχου πολιτικών.

1.4 Μεθοδολογία Διπλωματικής Εργασίας

Η μεθοδολογία που ακολουθήθηκε στα πλαίσια της παρούσας εργασίας είναι η ακόλουθη. Αρχικά, έγινε μια εκτενής μελέτη και έρευνα σε διάφορα ερευνητικά άρθρα τα οποία αφορούσαν τις Τυπικές Μέθοδους και την Ιδιωτικότητα με σκοπό την πλήρη κατανόηση και εξασφάλιση της κατάλληλης γνώσης για το πως έχουν προκύψει τα διάφορα σημασιολογικά πρότυπα μελέτης αυτής. Με την ολοκλήρωση των παραπάνω μελετήθηκαν διάφορες πολιτικές ιδιωτικότητας διαδικτυακά αλλά και διάφορες πολιτικές που προκύπτουν μέσα από νομοθεσίες ούτως ώστε να εντοπιστούν οι σημαντικότερες αφαιρετικές έννοιες αναφορικά με τη διατύπωση τους. Ακολούθως τέθηκε ο στόχος οι σημαντικότερες από αυτές να ενσωματωθούν από την παρούσα

εργασία σε ένα υφιστάμενο πλαίσιο ελέγχου που συναντάται στα [4,5]. Οι έννοιες που ενσωματώνονται μετά και από τη σχετική μελέτη προηγουμένως είναι οι έννοιες δομής και συνθήκης. Όσον αφορά το τυπικό πλαίσιο ελέγχου πολιτικών ιδιωτικότητας από διάφορα συστήματα, αυτό δίνεται σχηματικά μέσα από το Σχήμα 1.1.



Σχήμα 1.1: Τυπικό πλαίσιο ελέγχου πολιτικών ιδιωτικότητας

Συγκεκριμένα ο τυπικός έλεγχος ικανοποίησης πολιτικών ιδιωτικότητας από τα διάφορα συστήματα γίνεται ως εξής. Δεδομένης μιας πολιτικής ιδιωτικότητας και ενός συστήματος, η αρχή γίνεται με την τυπική διατύπωση της πολιτικής ιδιωτικότητας ούτως ώστε να συλληφθούν τυπικά οι διάφορες απαιτήσεις που ορίζονται από αυτή πάνω σε ένα σύνολο τύπων. Για το σκοπό αυτό το πρώτο σημείο το οποίο επεκτείνεται από την παρούσα εργασία αφορά τον τρόπο με τον οποίο γίνεται η τυπική διατύπωση των πολιτικών ιδιωτικότητας ενσωματώνοντας της έννοιες που αναφέραμε και παραπάνω δομής και συνθήκης αλλά και την ενίσχυση των τυπικών δικαιωμάτων μέσα από κατηγοριοποίηση τύπων και τη χρήση δομών. Όσον αφορά τώρα το σύστημα το οποίο θα ελεγχθεί ως προς το κατά πόσο αυτό ικανοποιεί την αντίστοιχη πολιτική ιδιωτικότητας, η συμπεριφορά αυτού πρέπει να μοντελοποιηθεί μέσω μιας άλγεβρας

διεργασιών η οποία θα συλλαμβάνει τη συμπεριφορά του. Επειδή ωστόσο τα διάφορα μοντέλα ενός συστήματος συλλαμβάνουν αποκλειστικά και μόνο τη συμπεριφορά του, θεωρείται απαραίτητη η διατύπωση ενός συστήματος παραγωγής των τυπικών δικαιωμάτων που ασκούνται από το σύστημα πάνω σε ένα σύνολο τύπων για να είναι δυνατός ο έλεγχος μέσω ελέγχου τύπων του κατά πόσο αυτό ικανοποιεί την πολιτική ιδιωτικότητας. Για το σκοπό αυτό, διατυπώθηκε ο λογισμός της άλγεβρας διεργασιών CP calculus η οποία συλλαμβάνει τις επεκτάσεις αναφορικά με τις συνθήκες και τη δυνατότητα χρήσης δομών δεδομένων. Ταυτόχρονα για σκοπούς παραγωγής των τυπικών δικαιωμάτων που ασκούνται από ένα σύστημα διατυπώθηκε ένα σύστημα παραγωγής τύπων το οποίο συνοδεύει το λογισμό της CP calculus. Η ολοκλήρωση της επέκτασης αναφορικά με την εισαγωγή των εννοιών δομής και συνθήκης, επιτεύχθηκε μέσα από τη διατύπωση ενός συνόλου αποδείξεων οι οποίες εξασφάλισαν την ορθότητα και ασφάλεια του προτεινόμενου πλαισίου ελέγχου, ενώ μέσα από ένα σύνολο ορισμών δόθηκε η έννοια της ικανοποίησης ή όχι μιας πολιτικής ιδιωτικότητας από ένα σύστημα με τη χρήση ελέγχου τύπων.

1.5 Δομή Διπλωματικής Εργασίας

Η δομή της εργασίας βάσει και των όσων περιγράψαμε παραπάνω έχει ως ακολούθως: Συγκεκριμένα στο Κεφάλαιο 2 γίνεται αναφορά στο υπόβαθρο και προηγούμενη εργασία πάνω στην οποία έχει στηριχθεί η παρούσα εργασία. Ακολούθως στο Κεφάλαιο 3 δίνεται η περιγραφή των πολιτικών ιδιωτικότητας και ο τυπικός ορισμός τους ενώ στο Κεφάλαιο 4 διατυπώνεται ο προτεινόμενος λογισμός μοντελοποίησης συστημάτων της CP calculus. Στο Κεφάλαιο 5 ορίζεται ένα σύστημα τύπων το οποίο συνοδεύει το λογισμό της CP calculus. Στο Κεφάλαιο 6 δίνονται όλες οι απαραίτητες αποδείξεις αναφορικά με το προτεινόμενο πλαίσιο ελέγχου ενώ με την ολοκλήρωση των αποδείξεων στο Κεφάλαιο 7 το προτεινόμενο πλαίσιο ελέγχου βρίσκει εφαρμογή σε περιπτώσεις χρήσης της πραγματικής ζωής. Στο Κεφάλαιο 8 παρουσιάζονται τα συμπεράσματα και ενδεχόμενες μελλοντικές εργασίες που προκύπτουν από την παρούσα διπλωματική εργασία.

Κεφάλαιο 2

Προηγούμενη Εργασία

2.1 Τυπικές Μέθοδοι και Ιδιωτικότητα

Όπως αναφέραμε και στο εισαγωγικό κεφάλαιο, οι Τυπικές Μέθοδοι μπορούν να χρησιμοποιηθούν ως ένα από τα εργαλεία που προσφέρει η Επιστήμη της Πληροφορικής για τον έλεγχο πολιτικών ιδιωτικότητας. Τα διάφορα μοντέλα που προκύπτουν για την εξέταση της ιδιωτικότητας όπως αναφέρεται και στο [14] ποικίλουν από Θεωρίες Παιγνίων μέχρι και θεωρίες αλγεβρών διεργασιών. Στα υποκεφάλαια που ακολουθούν θα αναφερθούμε σε διάφορες άλγεβρες διεργασιών και εκδοχές τους που έχουν προταθεί για τη μελέτη της ιδιωτικότητας.

2.2 Άλγεβρες Διεργασιών

Μια σημαντική κατηγορία των Τυπικών Μέθοδων είναι αυτή των αλγεβρών διεργασιών. Οι άλγεβρες διεργασιών προσφέρουν μια προσέγγιση αναφορικά με τη διατύπωση

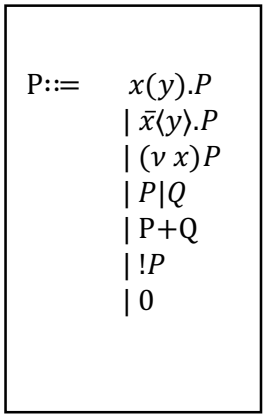
προδιαγραφών και επαλήθευση συστημάτων που δίνει έμφαση στις ενέργειες που εκτελούνται από ένα σύστημα, επιτρέποντας την επικοινωνία και το συγχρονισμό μεταξύ διεργασιών που το αποτελούν ενώ επικεντρώνονται στην εξέταση των αλληλεπιδράσεων ενός συστήματος με το περιβάλλον του. Τα διάφορα συστήματα σε μια άλγεβρα διεργασιών μοντελοποιούνται ως σύνθεση διαφόρων υποσυστημάτων των οποίων η συμπεριφορά μοντελοποιείται ως μια διεργασία. Σημαντική συνεισφορά τους είναι το γεγονός ότι επιτρέπουν την εξαγωγή συμπερασμάτων για πολύπλοκα συστήματα από ιδιότητες των επιμέρους συνιστωσών τους για αυτό και χρησιμοποιούνται σε ενθυλακωμένα συστήματα στα οποία η συμπεριφορά των συστημάτων προκύπτει μέσα από τις επιμέρους συνιστώσες που το αποτελούν. Μια άλγεβρα διεργασιών περιλαμβάνει μια γλώσσα προδιαγραφής για τη μοντελοποίηση συστημάτων, μια αυστηρά διατυπωμένη σημασιολογία για το σύνολο των ενεργειών που είναι δυνατό να πραγματοποιηθούν σε ένα περιβάλλον και ένα σύνολο από έννοιες εκλέπτυνσης συμπεριφοράς οι οποίες επιτρέπουν την εξαγωγή συμπερασμάτων του κατά πόσο δύο συστήματα είναι τα ίδια ή κατά πόσο το ένα σύστημα υλοποιεί το άλλο.

2.3 Ο Λογισμός της π-calculus

Μια από τις σημαντικότερες άλγεβρες διεργασιών και η οποία έχει συνεισφέρει σημαντικά ως προς την μελέτη της ιδιωτικότητας είναι ο λογισμός της π-caluclus ο οποίος προτάθηκε από τους Robin Milner, Joachin Parrow και David Walker, στο [9] το 1992. Ο λογισμός της π-calculus χρησιμοποιεί δύο βασικές κατηγορίες οντοτήτων αναφορικά με τη μοντελοποίηση συστημάτων. Συγκεκριμένα στηρίζεται σε ένα σύνολο διεργασιών οι οποίες μοντελοποιούν τις συνιστώσες ενός συστήματος και σε ένα σύνολο από ονόματα τα οποία χρησιμοποιούνται για τις ονομασίες των καναλιών επικοινωνίας μεταξύ διεργασιών και των αντικειμένων επικοινωνίας. Το χαρακτηριστικό εκείνο το οποίο καθιστά την π-calculus ξεχωριστή είναι η δυνατότητα χρήσης καναλιών ως αντικείμενα της επικοινωνίας ανάμεσα σε διεργασίες. Έτσι πέραν των αντικειμένων τα κανάλια επικοινωνίας ανάμεσα στις διεργασίες μπορούν να στέλνουν και κανάλια τα οποία να δίνουν πρόσβαση σε αντικείμενα πληροφορίας.

2.3.1 Σύνταξη

Η γλώσσα μοντελοποίησης διεργασιών της π-calculus με το αντίστοιχο σύνολο τελεστών δίνεται στο παρακάτω σχήμα:



Σχήμα 2.1: Σύνταξη της άλγεβρας διεργασιών π – calculus

Περιγραφή σύνταξης της π-calculus

Ο συμβολισμός P, Q αναφέρεται σε διεργασίες και τα x, y σε ονόματα.

Ο τελεστής $x(y).P$, αποτελεί τη λεγόμενη "Θύρα εισόδου" και καθορίζει ότι μια διεργασία η οποία ορίζεται βάσει του παραπάνω εφόσον λάβει σαν είσοδο από το κανάλι x την πληροφορία y, τότε συνεχίζει τη λειτουργία της με τη συμπεριφορά η οποία ορίζεται μέσα από τη διεργασία P. Το αντίστοιχο κανάλι y περιορίζεται στα όρια της διεργασίας P και αποτελεί τη θέση τοποθέτησης του ονόματος που θα πάρει ως είσοδο η διεργασία P.

Ο τελεστής $\bar{x}\langle y\rangle.P$, αποτελεί τη λεγόμενη "Θύρα εξόδου" και καθορίζει ότι μια διεργασία η οποία ορίζεται βάσει του παραπάνω μπορεί να εξάγει μέσω του καναλιού x το όνομα y, και να συνεχίσει τη συμπεριφορά της όπως αυτή ορίζεται μέσα από τη διεργασία P.

Ο τελεστής $(\nu\ x)P$, αφορά τη δημιουργία ενός νέου ονόματος στα πλαίσια της διεργασίας P. Το όνομα αυτό είναι γνωστό μόνο στα πλαίσια αυτής.

Ο τελεστής $P|Q$ συλλαμβάνει τη δυνατότητα παράλληλης εκτέλεσης διεργασιών. Βάσει αυτού οι δύο διεργασίες P και Q μπορούν να εκτελούνται παράλληλα και να συντονίζονται σε κοινά τους κανάλια ή να εκτελούν ανεξάρτητες ενέργειες μεταξύ τους. Στις περιπτώσεις όπου οι διεργασίες συντονίζονται μεταξύ τους χρησιμοποιούν ενέργειες

οι οποίες είναι συμπληρωματικές μεταξύ τους, δηλαδή ενέργειες εξόδου και εισόδου σε κοινό κανάλι.

Ο τελεστής $P + Q$ ορίζεται ως ο τελεστής επιλογής και επιτρέπει σε μια διεργασία τη δυνατότητα συνέχισης της εκτέλεσης της βάσει συμπεριφοράς που ορίζεται είτε από τη διεργασία P είτε από τη διεργασία Q.

Η διεργασία ! P παρουσιάζει τη δυνατότητα μιας διεργασίας να δημιουργεί άπειρα αντίγραφα του εαυτού της η οποία μπορεί να αποδοθεί και μέσα από την παρακάτω ισοδυναμία η οποία περιγράφει την παράλληλη εκτέλεση πολλών ίδιων διεργασιών ! P ≡ ! P|P.

Τέλος ο συμβολισμός 0 αναφέρεται στην τερματική διεργασία, τη διεργασία η οποία έχει ολοκληρώσει την εκτέλεση της.

Στο [9] οι συγγραφείς ορίζουν δύο σύνολα αναφορικά με τα ονόματα που εμφανίζονται στο λογισμό. Συγκεκριμένα ορίζουν το σύνολο των ελεύθερων ονομάτων χρησιμοποιώντας το συμβολισμό $fn(P)$, εννοώντας το σύνολο των ελεύθερων εμφανίσεων ονομάτων εντός μιας διεργασίας P. Αντίστοιχα ορίζεται και το σύνολο των δεσμευμένων εμφανίσεων ονομάτων εντός μιας διεργασίας P, ακολουθώντας το συμβολισμό $bn(P)$. Αναφορικά με τους κανόνες της σύνταξης της γλώσσας και των προηγουμένων συναρτήσεων προκύπτουν τα ακόλουθα:

- Ο τελεστής εισόδου $x(y).P$ προσθέτει στο σύνολο των ελεύθερων εμφανίσεων ονομάτων της διεργασίας P το όνομα x και στο σύνολο των δεσμευμένων εμφανίσεων ονομάτων για αυτή το όνομα y. Έτσι $fn(P) = fn(P) \cup \{x\}$ και $bn(P) = bn(P) \cup \{y\}$
- Ο τελεστής εξόδου $\bar{x}\langle y\rangle.P$ προσθέτει στο σύνολο των ελεύθερων εμφανίσεων της διεργασίας και τα δύο ονόματα ενώ στο σύνολο των δεσμευμένων εμφανίσεων ονομάτων για για αυτή τίποτα. Έτσι $fn(P) = fn(P) \cup \{x, y\}$
- Ο τελεστής δέσμευσης ονόματος $(\nu\, x)P$ προσθέτει στο σύνολο των δεσμευμένων εμφανίσεων ονομάτων της διεργασίας P το όνομα x. Έτσι $bn(P) = bn(P) \cup \{x\}$

- Ο τελεστής παράλληλης εκτέλεσης διεργασιών $P|Q$ ορίζει ως το σύνολο ελεύθερων και δεσμευμένων ονομάτων την ένωση των αντίστοιχων συνόλων για τις διεργασίες P και Q. Έτσι $fn(P) = fn(P) \cup fn(Q)$ και $bn(P) = bn(P) \cup bn(Q)$

2.3.2 Σημασιολογία

Η σημασιολογική ερμηνεία της π-calculus δίνεται μέσα από ένα σύνολο κανόνων, τους λεγόμενους κανόνες Μείωσης. Οι σχετικοί κανόνες ορίζουν τους τρόπους με τους οποίους μπορεί να μετεξελιχθεί μια διεργασία σε μια άλλη με την εκτέλεση μόνο ενός βήματος από τα παραπάνω. Συμβολικά η δυνατότητα εκτέλεσης ενός βήματος από μια διεργασία P και η συνέχιση της συμπεριφοράς της ως μια διεργασία Q δίνεται από το $P \rightarrow Q$ ενώ η σχέση $\rightarrow$ περιλαμβάνει τους κανόνες που μπορούν να εξαχθούν από τους ακόλουθους κανόνες:

$$Comm : (x(y).P) + R \mid \bar{x}\langle z\rangle.Q|M) \rightarrow P\{^{z}/_{y}\}|Q$$

$$PAR: \frac{P \rightarrow P'}{P|Q \rightarrow P'|Q}$$

$$RES: \frac{P \rightarrow Q}{(\nu\, x)P \rightarrow (\nu\, x)Q}$$

$$STRUCT: \frac{P \equiv Q \; P \rightarrow P' \; P' \equiv Q'}{Q \rightarrow Q'}$$

Πριν προχωρήσουμε στη περιγραφή των παραπάνω κανόνων να τονίσουμε ότι οι κανόνες αυτοί έχουν τη μορφή κλάσματος όπου στον αριθμητή εμφανίζονται οι απαραίτητες συνθήκες οι οποίες πρέπει να ισχύουν ούτως ώστε να είναι δυνατή η εξαγωγή του συμπεράσματος που βρίσκεται στον παρονομαστή.

Περιγραφή των κανόνων Μείωσης

Ο πρώτος κανόνας του ($Comm$) ορίζει τη δυνατότητα συγχρονισμού δύο διεργασιών που εκτελούνται παράλληλα μέσω του καναλιού x, με την προϋπόθεση ότι οι δύο ενέργειες είναι συμπληρωματικές, δηλαδή αν μια διεργασία εκτελεί ενέργεια εισόδου σε ένα κανάλι και η άλλη διεργασία έξοδο στο συγκεκριμένο κανάλι εγγράφοντας το όνομα z, τότε το αποτέλεσμα της εκτέλεσης στην παραπάνω μετάβαση είναι πέρα από το συγχρονισμό εντός του καναλιού για τις δύο διεργασίες η αντικατάσταση του σχετικού ονόματος y από το z.

Ο δεύτερος κανόνας του (PAR) ορίζει ότι αν μια διεργασία P μπορεί να μεταβεί με την εκτέλεση ενός βήματος σε μια διεργασία P' τότε η παράλληλη σύνθεση της με μια διεργασία Q και την εκτέλεση μιας ενέργειας θα οδηγήσει στην κατάσταση $P'|Q$.

Ο τρίτος κανόνας του (RES) ορίζει ότι αν μια διεργασία P μπορεί να μεταβεί σε μια διεργασία Q τότε η δέσμευση ενός ονόματος στα πλαίσια της P διατηρείται και στη διεργασία Q.

Ο τέταρτος κανόνας του $(STRUCT)$ ορίζει ότι αν δύο διεργασίες P, Q είναι δομικά ισοδύναμες τότε εάν η P εκτελώντας ένα βήμα μπορεί να βρεθεί στην κατάσταση P' και η P' είναι ισοδύναμη με την Q' τότε και η Q μπορεί εκτελώντας μια μετάβαση να βρεθεί στη διεργασία Q'.

Η σχέση δομικής ισοδυναμίας εμφανίζεται στο Σχήμα 2.2. Οι συμβολισμοί P, Q, R αναφέρονται σε διεργασίες

$P \equiv P$	$!P \equiv P \mid !P$
$P \equiv Q \Rightarrow Q \equiv P$	$P \equiv Q \Rightarrow !P \equiv !Q$
$P \equiv Q, Q \equiv R \Rightarrow P \equiv R$	$(\nu\, x)0 \equiv 0$
$P \mid 0 \equiv P$	$(\nu\, x)P \equiv P$ όπου $x \notin fn(P)$
$P \mid Q \equiv Q \mid P$	$(\nu\, x)(\nu\, y)P \equiv (\nu\, y)(\nu\, x)P$
$P \mid (Q \mid R) \equiv (P \mid Q) \mid R$	$P \equiv Q \Rightarrow (\nu\, x)P \equiv (\nu\, x)Q$
$P \equiv Q \Rightarrow P \mid R \equiv Q \mid R$	$(\nu\, x)(P \mid Q) \equiv P \mid (\nu\, x)Q$ αν $x \notin fn(P)$

Σχήμα 2.2: Οι κανόνες δομικής ισοδυναμίας της π-calculus

2.4 Ο Λογισμός της π-calculus with groups

Στηριζόμενοι στην π-calculus της οποίας ο ορισμός δόθηκε παραπάνω οι συγγραφείς στο [1], ήρθαν να προτείνουν μια επέκταση της προσθέτοντας την έννοια της ομάδας (group). Με την προσθήκη της έννοιας αναφορικά με τις ομάδες κατάφεραν να περιορίσουν τα κανάλια και τις πληροφορίες εντός συγκεκριμένων οντοτήτων των ομάδων επιδιώκοντας την παρεμπόδιση αποκάλυψης τους σε τρίτα μη εξουσιοδοτημένα άτομα τα οποία δεν ανήκουν εντός της ομάδας. Η παραπάνω συμβολή αναφορικά με την εξέταση της ιδιωτικότητας θεωρείται άκρως σημαντική σε συστήματα διαχείρισης προσωπικών πληροφοριών, καθώς αρκετές φορές τα στοιχεία δεν πρέπει και ούτε είναι επιθυμητό να

αποκαλύπτονται εκτός του συστήματος. Επιπρόσθετα του συνόλου των ομάδων, εισάγουν και την έννοια του τύπου ο οποίος συσχετίζει τα ονόματα του λογισμού της π-calculus. Συγκεκριμένα, ο κάθε τύπος καταγράφει για το κάθε κανάλι την ομάδα στην οποία ανήκει και τον τύπο των αντικειμένων που μεταφέρονται μέσω των καναλιών. Ο τυπικός ορισμός ενός τύπου όπως δίνεται και στο [1] εμφανίζεται στο Σχήμα 2.3.

Types:

$T ::=$	channel type
$G[T_1, \ldots, T_n]$	polyadic channel in group G

Σχήμα 2.3: Ο ορισμός του τύπου στην π-calculus with groups

2.4.1 Σύνταξη

Η γλώσσα μοντελοποίησης της π-calculus with groups με το αντίστοιχο σύνολο των τελεστών δίνεται στο παρακάτω σχήμα:

Expressions and processes:

x, y, p, q	names, variables
$P, Q, R ::=$	process
$x(y_1{:}T_1, \ldots, y_k{:}T_k).P$	channel input
$\bar{x}\langle y_1, \ldots, y_k\rangle$	channel output
$(\nu G)P$	group creation
$(\nu x{:}T)P$	restriction
$P \mid Q$	composition
$!P$	replication
$\mathbf{0}$	inactivity

Σχήμα 2.4: Σύνταξη της άλγεβρας διεργασιών π – calculus with groups

Περιγραφή σύνταξης της π-calculus with groups

Οι συμβολισμοί x, y, p, q αναφέρονται σε ονόματα και μεταβλητές αντίστοιχα ενώ οι συμβολισμοί P, Q, R σε διεργασίες. Με την εισαγωγή της έννοιας της ομάδας, ορίζονται δύο επιπρόσθετες συναρτήσεις οι οποίες δίνουν με τη σειρά τους το σύνολο των ελεύθερων εμφανίσεων ομάδων σε διεργασίες και τύπους, συμβολικά $fg(P)$ και $fg(T)$ αντίστοιχα.

Ο τελεστής εισόδου σε κανάλι $x(y_1{:}T_1, \ldots\ldots, y_k{:}T_k).P$ ορίζεται αντίστοιχα με τον τελεστή εισόδου της π-calculus δίνοντας ωστόσο τη δυνατότητα πολλαπλής μεταφοράς ονομάτων εντός των καναλιών ενώ όπως αναφέραμε και παραπάνω το κάθε όνομα πλέον

συσχετίζεται με ένα συγκεκριμένο τύπο. Το σύνολο των ονομάτων με τους τύπους τους αντίστοιχα και στην π-calculus δεσμεύονται εντός της διεργασίας P. Το x αντίστοιχα θεωρείται ελεύθερο.

Ο τελεστής εξόδου σε κανάλι $\bar{x}\langle y_1, \dots, y_k \rangle . P$ ορίζεται αντίστοιχα του τελεστή εξόδου στη π-calculus δίνοντας ωστόσο τη δυνατότητα πολλαπλής μεταφοράς ονομάτων εντός των καναλιών. Τόσο το x όσο και όλα τα y_i θεωρούνται ελεύθερα στα πλαίσια της διεργασίας P.

Ο τελεστής δημιουργίας ομάδας στα πλαίσια μια διεργασίας που δίνεται από το $(\nu\ G)P$ δεσμεύει την ομάδα G στα πλαίσια της διεργασίας P.

Ο τελεστής δέσμευσης μιας ονομασίας στα πλαίσια μια διεργασίας P, ορίζεται αντίστοιχα με την π–calculus με τη διαφορά ότι το όνομα ανατίθεται σε ένα τύπο. Προφανώς και το όνομα περιορίζεται στα πλαίσια της διεργασίας P.

Τέλος οι τελεστές παράλληλης εκτέλεσης διεργασιών, αναδρομικότητας και τερματικής διεργασίας ορίζονται αντίστοιχα του λογισμού της π-calculus.

2.4.2 Σημασιολογία

Όσον αφορά τη σημασιολογία ισχύουν τα αντίστοιχα που ίσχυαν και στην περίπτωση της π-calculus με την προσθήκη του παρακάτω κανόνα ω προς το σύνολο των κανόνων Μείωσης.

$$(GRES)\ \frac{P \to Q}{(\nu\ G)P \to (\nu\ G)Q}$$

ο οποίος δηλώνει ότι αν μια διεργασία P μπορεί να μεταβεί με την εκτέλεση ενός βήματος σε μια διεργασία Q τότε ο περιορισμός μιας ομάδας στα πλαίσια της P μεταφέρεται με την εκτέλεση της διεργασίας και στην διεργασία Q.

Οι κανόνες ισοδυναμίας επεκτείνονται με την εισαγωγή του συνόλου των παρακάτω κανόνων ισοδυναμίας:

$P \equiv Q \Rightarrow (\nu G)Q \equiv (\nu G)P$
$(\nu G_1)(\nu G_2)P \equiv (\nu G_2)(\nu G_1)P$
$(\nu G)(\nu x{:}T)P \equiv (\nu G)P$ *όπου* $G \notin fg(T)$
$(\nu G)(P \mid Q) \equiv P \mid (\nu G)Q$ *όπου* $G \notin fg(P)$

Σχήμα 2.5: Οι επιπρόσθετοι κανόνες δομικής ισοδυναμίας της π-calculus with groups

2.5 Χρήση της π-calculus with groups για μελέτη της Ιδιωτικότητας

Στηριζόμενοι στο λογισμό της π-calculus with groups οι συγγραφείς στο [4] προτείνουν ένα τυπικό πλαίσιο για τη μελέτη της ιδιωτικότητας και συγκεκριμένα προτείνουν ένα πρότυπο για τον έλεγχο πολιτικών ιδιωτικότητας. Πέραν της π-calculus with groups το προτεινόμενο πλαίσιο συνοδεύεται και από ένα τυπικό σύστημα που χρησιμοποιείται για την καταγραφή απαιτήσεων ιδιωτικότητας σχετικά με πολιτικές οι οποίες αφορούν την επεξεργασία συλλογή και αποκάλυψη ευαίσθητων προσωπικών πληροφοριών. Η καταγραφή αυτή γίνεται με τη χρήση τυπικών δικαιωμάτων. Ο λογισμός ενισχύθηκε με ένα σύστημα τύπων για την καταγραφή των ασκούμενων δικαιωμάτων από τις διάφορες το οποίο έδωσε την δυνατότητα μέσω στατικού ελέγχου τύπων να εξακριβωθεί κατά πόσο ένα σύστημα το οποίο έχει μοντελοποιηθεί στην π-calculus with groups με μερικές επεκτάσεις τις οποίες θα δούμε παρακάτω ικανοποιεί ή όχι μια πολιτική ιδιωτικότητας.

2.5.1 Τυπική διατύπωση πολιτικών ιδιωτικότητας

Η τυπική καταγραφή μιας πολιτικής ιδιωτικότητας που προτείνεται δίνεται από το παρακάτω και αναθέτει ένα σύνολο δικαιωμάτων σε οντότητες συγκεκριμένων κατηγοριών για ένα σύνολο βασικών τύπων οι οποίοι εργάζονται κάτω από συγκεκριμένους σκοπούς [4]. Ο συμβολισμός G αναφέρεται στην έννοια της ομάδας, $\tilde{u}$ σε μια πλειάδα από σκοπούς και το t αναφέρεται σε βασικούς τύπους για το σύνολο των ονομάτων.

Ο τυπικός ορισμός των πολιτικών ιδιωτικότητας δίνεται από το ακόλουθο σχήμα.

$$\begin{array}{lrcl} \text{(Permissions)} & \mathsf{Perm} & ::= & \mathsf{read} \mid \mathsf{write} \mid \mathsf{access} \mid \mathsf{disclose}\, G \\ \text{(Hierarchies)} & H & ::= & \varepsilon \mid G : \tilde{u}[H_j]_{j \in J} \\ \text{(Policies)} & \mathscr{P} & ::= & \mathrm{t} \gg \langle H, \pi \rangle \mid \mathscr{P}; \mathscr{P} \end{array}$$

Σχήμα 2.6: Σύνταξη της τυπικής διατύπωσης πολιτικών

Η συνάρτηση π χρησιμοποιείται για την ανάθεση δικαιωμάτων σε οντότητες συγκεκριμένων κατηγοριών κάτω από κάποιο σκοπό ενώ μια πολιτική καταγράφει τα δικαιώματα όπως αυτά εμφανίζονται στο σύνολο ($Permissions$) που μπορούν να εφαρμόζονται από τις οντότητες βάσει μιας πολιτικής. Τα δικαιώματα καταγράφουν τις επιτρεπτές ενέργειες που είναι δυνατό μια οντότητα του συστήματος να εκτελέσει οποτεδήποτε για ένα συγκεκριμένο σκοπό.

2.5.2 Περιγραφή προτεινόμενου λογισμού

Ο προτεινόμενος λογισμός για τη μοντελοποίηση συστημάτων στο προτεινόμενο πλαίσιο ελέγχου πολιτικών ιδιωτικότητας όπως περιγράψαμε και παραπάνω στηρίζεται στη π-calculus with groups, επεκτείνοντας τη σε διάφορα σημεία ενώ ενσωματώνεται και η εκτέλεση διεργασιών υπό συγκεκριμένο σκοπό. Συγκεκριμένα στο προτεινόμενο λογισμό χρησιμοποιούνται δύο βασικές οντότητες το σύνολο των ονομάτων $\mathcal{N}$ το οποίο αποτελείται από στοιχεία της μορφής a, b, x, y και το σύνολο ομάδων $\mathcal{G}$ αντίστοιχα της π-calculus with groups. Κάθε όνομα ανατίθεται σε ένα τύπο, ωστόσο ο τύπος πλέον μπορεί να είναι είτε ένας βασικός τύπος πληροφορίας ο οποίας να αναφέρεται σε συγκεκριμένα δεδομένα του συστήματος ή να είναι κανάλι το οποίο μεταφέρει βάσει ομάδας ένα τύπο. Ως εκ τούτου ο ορισμός του τύπου δίνεται από την ακόλουθη σχέση $T ::= t \mid G[T]$. Με την προσθήκη του τύπου ο λογισμός ορίζεται σε δύο επίπεδα στο επίπεδο του συστήματος και στο επίπεδο των διεργασιών. Σχηματικά η σύνταξη του λογισμού δίνεται από το ακόλουθο:

$$
\begin{array}{lcl}
P & ::= & x(y{:}T).P \;\mid\; \bar{x}\langle z\rangle.P \;\mid\; (\nu\, a{:}T)P \;\mid\; P_1 \mid P_2 \;\mid\; !P \;\mid\; \mathbf{0} \\
S & ::= & (\nu\, G)P\langle u\rangle \;\mid\; (\nu\, G)S \;\mid\; (\nu\, a{:}T)S \;\mid\; S_1 \mid S_2 \;\mid\; \mathbf{0}
\end{array}
$$

Σχήμα 2.7: Σύνταξη προτεινόμενου λογισμού

Όσον αφορά το επίπεδο των διεργασιών οι κανόνες λειτουργούν αντίστοιχα αυτών του λογισμού της π-calculus with groups. Όσον αφορά το επίπεδο του συστήματος επιτρέπεται η δέσμευση διεργασίας που εργάζεται υπό συγκεκριμένο σκοπό στα πλαίσια μιας ομάδας με τον τελεστή $(\nu G)P\langle u\rangle$, ο περιορισμός μιας ομάδας στα πλαίσια ενός συστήματος μέσω του $(\nu\, G)S$, η δέσμευση ονόματος στα πλαίσια ενός συστήματος, η παράλληλη εκτέλεση συστημάτων και ο τερματισμός ενός συστήματος. Η συμπεριφορά των τριών τελευταίων τελεστών είναι η αντίστοιχη της συμπεριφοράς για το επίπεδο των διεργασιών.

Τον ορισμό του λογισμού ακολουθεί ο ορισμός ενός συστήματος μεταβάσεων με ετικέτες το οποίο συλλαμβάνει αντίστοιχα τους κανόνες Μείωσης του λογισμού. Η ετικέτα τ αναφέρεται στην εσωτερική ενέργεια όπου οι ετικέτες $x(y)$ και $\bar{x}\langle y\rangle$ αναφέρονται στις ενέργειες εισόδου και εξόδου αντίστοιχα ενώ οι ετικέτα $(\nu y)\bar{x}\langle y\rangle$ περιορίζει την έξοδο της ενέργειας εξόδου. Οι ετικέτες είναι οι ακόλουθες:

$$\ell \ ::= \ \tau \ \mid \ x(y) \ \mid \ \bar{x}\langle y\rangle \ \mid \ (\nu\, y)\bar{x}\langle y\rangle$$

Σχήμα 2.8: Οι ετικέτες του συνόλου του συστήματος μεταβάσεων

Η σχέση $dual(l, l')$ αν και μόνο αν $\{l, l'\} = \{x(y), \bar{x}\langle y\rangle\}$ ή $\{l, l'\} = \{x(y), (\nu\, y)\bar{x}\langle y\rangle\}$ συλλαμβάνει τις περιπτώσεις όπου δύο ετικέτες - μεταβάσεις μπορούν να συγχρονιστούν. Έτσι το προτεινόμενο σύστημα μεταβάσεων με ετικέτες δίνεται από το παρακάτω Σχήμα 2.9. Χρησιμοποιείται ο μέτα συμβολισμός F όπου $F ::= P|S$.

$$x(y:T).P \xrightarrow{x(z)} P\{z/y\}\ (\mathsf{In}) \qquad \bar{x}\langle z\rangle.P \xrightarrow{\bar{x}\langle z\rangle} P\ (\mathsf{Out})$$

$$\frac{F_1 \xrightarrow{\ell} F_1' \quad \mathtt{bn}(\ell)\cap \mathtt{fn}(F_2)=\emptyset}{F_1 \mid F_2 \xrightarrow{\ell} F_1' \mid F_2}\ (\mathsf{ParL}) \qquad \frac{F_2 \xrightarrow{\ell} F_2' \quad \mathtt{bn}(\ell)\cap \mathtt{fn}(F_1)=\emptyset}{F_1 \mid F_2 \xrightarrow{\ell} F_1 \mid F_2'}\ (\mathsf{ParR})$$

$$\frac{F \xrightarrow{\ell} F' \quad x \notin \mathtt{fn}(\ell)}{(\nu\, x:T)F \xrightarrow{\ell} (\nu\, x:T)F'}\ (\mathsf{ResN}) \qquad \frac{F \xrightarrow{\bar{x}\langle y\rangle} F'}{(\nu\, y:T)F \xrightarrow{(\nu\, y)\bar{x}\langle y\rangle} F'}\ (\mathsf{Scope})$$

$$\frac{S \xrightarrow{\ell} S'}{(\nu\ G)S \xrightarrow{\ell} (\nu\ G)S'}\ (\mathsf{ResGS}) \qquad \frac{P \xrightarrow{\ell} P'}{(\nu\ G)P\langle u\rangle \xrightarrow{\ell} (\nu\ G)P'\langle u\rangle}\ (\mathsf{ResGP})$$

$$\frac{P \xrightarrow{\ell} P'}{!P \xrightarrow{\ell} P' \mid !P}\ (\mathsf{Repl}) \qquad \frac{F_1 \xrightarrow{\ell_1} F_1' \quad F_2 \xrightarrow{\ell_2} F_2' \quad \mathsf{dual}(\ell_1,\ell_2)}{F_1 \mid F_2 \xrightarrow{\tau} (\nu\ \mathtt{bn}(\ell_1)\cup\mathtt{bn}(\ell_2))(F_1' \mid F_2')}\ (\mathsf{Com})$$

$$\frac{F \equiv_\alpha F'' \quad F'' \xrightarrow{\ell} F'}{F \xrightarrow{\ell} F'}\ (\mathsf{Alpha})$$

Σχήμα 2.9: Το σύστημα μεταβάσεων με ετικέτες

2.5.3 Σύστημα Τύπων

Η διατύπωση ενός συστήματος στον προτεινόμενο λογισμό δίνει τη συμπεριφορά του. Ωστόσο απαιτείται και ένα σύστημα τύπων με το οποίο να είναι δυνατή η καταγραφή των ασκούμενων δικαιωμάτων από τις οντότητες του πάνω στο σύνολο των βασικών τύπων. Για το σκοπό αυτό ορίζονται τρεις βασικές οντότητες οι οποίες συμβολικά δίνονται από τα Γ, Δ, Θ. Στο σύνολο Γ καταγράφονται τα ονόματα και οι ομάδες που έχουν ήδη καταγραφεί στο σύστημα. Η διεπαφή Δ καταγράφει το σύνολο των δικαιωμάτων που ασκούνται σε βασικούς τύπους ενώ η ολοκληρωμένη εφαρμογή του συστήματος των τύπων παράγει τη διεπαφή Θ η οποία καταγράφει για κάθε κομμάτι του

συστήματος τα ασκούμενα δικαιώματα κάτω από συγκεκριμένο σκοπό. Ανάλογα της ενέργειας για την παραγωγή της διεπαφή Δ ορίζονται οι συναρτήσεις του Σχήματος 2.10 με το Δ_T^r να αναφέρεται σε δικαιώματα που προκύπτουν από ενέργειες εισόδου και το Δ_T^w να αναφέρεται σε δικαιώματα που προκύπτουν από ενέργειες εξόδου. Ο τυπικός ορισμός των κανόνων παραγωγής του συστήματος των τύπων δίνεται στο Σχήμα 2.11.

$$\Delta_T^r = \begin{cases} \mathrm{t} : \mathrm{read} & \text{if } T = \mathrm{t} \\ \mathrm{t} : \mathrm{access} & \text{if } T = G[\mathrm{t}] \\ \emptyset & \text{otherwise} \end{cases} \qquad \Delta_T^w = \begin{cases} \mathrm{t} : \mathrm{write} & \text{if } T = \mathrm{t} \\ \mathrm{t} : \mathrm{disclose}\ G & \text{if } T = G[\mathrm{t}] \\ \emptyset & \text{otherwise} \end{cases}$$

Σχήμα 2.10: Διεπαφές παραγωγής δικαιωμάτων

$$\text{(Name)}\ \frac{\mathtt{fg}(T) \subseteq \Gamma}{\Gamma \cdot x : T \vdash x \triangleright T} \qquad \text{(Nil)}\ \ \Gamma \vdash \mathbf{0} \triangleright \emptyset$$

$$\text{(In)}\ \frac{\Gamma \cdot y : T \vdash P \triangleright \Delta \quad \Gamma \vdash x \triangleright G[T]}{\Gamma \vdash x(y:T).P \triangleright \Delta \uplus \Delta_T^r} \qquad \text{(Out)}\ \frac{\Gamma \vdash P \triangleright \Delta \quad \Gamma \vdash x \triangleright G[T] \quad \Gamma \vdash y \triangleright T}{\Gamma \vdash \overline{x}\langle y \rangle.P \triangleright \Delta \uplus \Delta_T^w}$$

$$\text{(ParP)}\ \frac{\Gamma \vdash P_1 \triangleright \Delta_1 \qquad \Gamma \vdash P_2 \triangleright \Delta_2}{\Gamma \vdash P_1 \mid P_2 \triangleright \Delta_1 \uplus \Delta_2} \qquad \text{(ParS)}\ \frac{\Gamma \vdash S_1 \triangleright \Theta_1 \qquad \Gamma \vdash S_2 \triangleright \Theta_2}{\Gamma \vdash S_1 \mid S_2 \triangleright \Theta_1 ; \Theta_2}$$

$$\text{(ResNP)}\ \frac{\Gamma \cdot x : T \vdash P \triangleright \Delta}{\Gamma \vdash (\nu\, x : T) P \triangleright \Delta} \qquad \text{(ResNS)}\ \frac{\Gamma \cdot x : T \vdash S \triangleright \Theta}{\Gamma \vdash (\nu\, x : T) S \triangleright \Theta}$$

$$\text{(ResGP)}\ \frac{\Gamma \cdot G \vdash P \triangleright \Delta}{\Gamma \vdash (\nu\, G) P\langle u \rangle \triangleright G[u] \oplus \Delta} \qquad \text{(ResGS)}\ \frac{\Gamma \cdot G \vdash S \triangleright \Theta}{\Gamma \vdash (\nu\, G) S \triangleright G \oplus \Theta}$$

$$\text{(Rep)}\ \frac{\Gamma \vdash P \triangleright \Delta}{\Gamma \vdash !P \triangleright \Delta^!}$$

Σχήμα 2.11: Κανόνες Συστήματος των Τύπων

2.5.4 Ικανοποίηση πολιτικών ιδιωτικότητας

Με την ολοκλήρωση και την εφαρμογή του συστήματος των τύπων δίνεται και ο τρόπος με τον οποίο μπορεί να γίνει ο έλεγχος ικανοποίησης μιας πολιτικής ιδιωτικότητας. Συγκεκριμένα ορίζεται ότι μια πολιτική ιδιωτικότητας γίνεται σεβαστή από ένα σύστημα το οποίο εργάζεται βάση αυτής εάν το σύνολο των ασκούμενων δικαιωμάτων από τις οντότητες αυτού είναι υποσύνολο όλων των δυνατών που επιτρέπονται από την πολιτική μέσω της ιεραρχίας που εμφανίζεται. Η ικανοποίηση μιας πολιτικής ιδιωτικότητας $\mathcal{P}$ από μια παραχθείσα διεπαφή δικαιωμάτων Θ δίνεται από το ακόλουθο.

$$\frac{\langle H, \pi \rangle \Vdash \langle H^{\downarrow}, \tilde{p} \rangle \qquad \mathscr{P} \Vdash \Theta}{\mathrm{t} \gg \langle H, \pi \rangle ; \mathscr{P} \Vdash \mathrm{t} \gg \langle H^{\downarrow}, \tilde{p} \rangle ; \Theta} \qquad \mathscr{P} \Vdash \emptyset$$

Σχήμα 2.12: Ορισμός ικανοποίησης μιας πολιτικής ιδιωτικότητας

2.6 Συμπεράσματα

Η έννοια της ιδιωτικότητας έχει απασχολήσει την ερευνητική κοινότητα της Επιστήμης της Πληροφορικής ενώ οι Τυπικές Μέθοδοι όπως παρουσιάζεται και παραπάνω βρίσκουν εφαρμογή αναφορικά με την ανάγκη ελέγχου πολιτικών ιδιωτικότητας από συστήματα. Τέτοια πλαίσια ελέγχου εμφανίζονται στα [4,5] τα οποία επιτρέπουν τον έλεγχο ικανοποίησης πολιτικών ιδιωτικότητας από υποψήφιά συστήματα. Στηριζόμενοι στα όσα αναφέρθηκαν και παραπάνω αλλά και με κίνητρο την ενίσχυση του πλαισίου ελέγχου πολιτικών ιδιωτικότητας ούτως ώστε να μπορεί να συλλάβει επιπρόσθετες έννοιες που προκύπτουν μέσα από την ανάλυση των πολιτικών ιδιωτικότητας, προτείνεται η ανάπτυξη ενός τυπικού πλαισίου για τη μελέτη της ιδιωτικότητας το οποίο επεκτείνει το ήδη υπάρχον από το [4] ενσωματώνοντας την έννοια της συνθήκης τόσο σε επίπεδο πολιτικής όσο και σε επίπεδο λογισμού, τη δυνατότητα χρήσης δομών δεδομένων πληροφορίας, όταν αυτά χρησιμοποιούνται και τη δυνατότητα ταυτοποίησης οντοτήτων μιας δομής από επιμέρους στοιχεία που καταγράφονται για αυτή. Η ισχύς της προτεινόμενης μεθοδολογίας εμφανίζεται και μέσα από την εφαρμογή της σε παραδείγματα που προκύπτουν από μελέτη διαφόρων σεναρίων της πραγματικής ζωής και τα οποία εμφανίζονται στο προτελευταίο κεφάλαιο της παρούσας εργασίας.

Κεφάλαιο 3
Πολιτικές Ιδιωτικότητας

3.1 Περιγραφή

Μια πολιτική ιδιωτικότητας ορίζει μια συλλογή από κανόνες οι οποίοι καθορίζουν τις επιτρεπτές ενέργειες που είναι σε θέση να εκτελέσει οποιοδήποτε οντότητα ενός συστήματος πάνω σε ένα σύνολο ευαίσθητων προσωπικών δεδομένων. Οι ενέργειες αυτές κατηγοριοποιούνται σε ενέργειες που αφορούν τη συλλογή, επεξεργασία και αποκάλυψη τους σε άλλους. Ταυτόχρονα, μια πολιτική ιδιωτικότητας διασφαλίζει ότι τα ευαίσθητα προσωπικά δεδομένα προστατεύονται τόσο από εξωτερικές επιθέσεις και τρίτες μη εξουσιοδοτημένες οντότητες, όπως επίσης ότι τυγχάνουν του δέοντος σεβασμού κατά την εσωτερική διαχείριση τους από τις οντότητες εντός των διαφόρων συστημάτων. Οι διάφορες πολιτικές ιδιωτικότητας δύναται να εκφράζονται είτε στη φυσική γλώσσα είτε μέσω συγκεκριμένων τυπικών γλωσσών οι οποίες μπορούν να συλλάβουν πιο αυστηρά τις διάφορες έννοιες ιδιωτικότητας. Μερικά παραδείγματα τυπικών γλωσσών για τη διατύπωση πολιτικών ιδιωτικότητας όπως αυτά εμφανίζονται και στο [6] είναι οι Platform for Privacy Preferences (P3P), Enterprise Privacy Authorization Language (EPAL), eXtensible Access Control Markup Language (XACML) και άλλες. Μια πολιτική ιδιωτικότητας για την τυπική περιγραφή της πρέπει να περιλαμβάνει τις παρακάτω έξι συνιστώσες όπως σχετικά εντοπίζεται και στο [6]:

1. Διαχειριστές Δεδομένων (Data Users)

   Οι διαχειριστές των δεδομένων είναι τα άτομα τα οποία λαμβάνουν πρόσβαση και τα οποία μπορούν να εκτελέσουν διάφορες ενέργειες σε ευαίσθητα προσωπικά δεδομένα τα οποία αφορούν άλλα άτομα και για τα οποία έχουν

καταγραφεί σημαντικές πληροφορίες. Ο καθορισμός των οντοτήτων αυτό σε μια πολιτική ιδιωτικότητας θεωρείται ζωτικής σημασίας.

2. Ενέργειες (Actions)

   Οι ενέργειες αναφέρονται στις διάφορες διαδικασίες και λειτουργίες που μπορούν να εκτελέσουν οι διαχειριστές του συστήματος στο σύνολο των προσωπικών δεδομένων. Στη διατύπωση της πολιτικής συχνά οι ενέργειες αυτές αναφέρονται και ως τα δικαιώματα που δύναται να έχουν σε ένα σύνολο δεδομένων.

3. Κατηγορίες Δεδομένων (Data Categories)

   Οι κατηγορίες χρησιμοποιούνται για την περιγραφή του τύπου των δεδομένων και των διαφόρων κατηγοριών. Η περιγραφή αυτή γίνεται σε υψηλό επίπεδο και συχνά αποφεύγονται περιττές λεπτομέρειες.

4. Σκοποί (Purposes)

   Η κατηγορία των σκοπών χρησιμοποιείται για να περιγράψει το λόγο για τον οποίο ένα οποιοδήποτε σύστημα ή οντότητα χειρίζεται ευαίσθητα προσωπικά δεδομένα.

5. Συνθήκες (Conditions)

   Οι συνθήκες χρησιμοποιούνται για να περιγράψουν τις καταστάσεις που πρέπει να ισχύουν ώστε να είναι δυνατή η εκτέλεση μιας οποιασδήποτε ενέργειας από το διαχειριστή των δεδομένων. Η πιο συνήθης συνθήκη που συναντάται σε πολιτικές ιδιωτικότητας είναι η παροχή άδειας από το άτομο το οποίο αφορούν τα ευαίσθητα δεδομένα πριν αυτά τύχουν επεξεργασίας.

6. Υποχρεώσεις (Obligations)

   Οι υποχρεώσεις καθορίζουν τις ενέργειες που πρέπει να εκτελεστούν με την ολοκλήρωση μιας συγκεκριμένες ενέργειας.

3.2 Βασικές Έννοιες και Τυπικός Ορισμός

Στο παρόν υποκεφάλαιο καθορίζονται οι βασικές έννοιες που απαιτούνται για την τυπική διατύπωση των πολιτικών ιδιωτικότητας και στη συνέχεια δίνεται ο τυπικός ορισμός τους. Η παρούσα εργασία επεκτείνει το υφιστάμενο τυπικό πλαίσιο διατύπωσης πολιτικών ιδιωτικότητας ενισχύοντας το μέσω της δυνατότητας ανάθεσης δικαιωμάτων υπό την ικανοποίηση συγκεκριμένων συνθηκών, περιορίζοντας ουσιαστικά τα δικαιώματα που ανατίθενται σε ομάδες βάσει των συνθηκών που πρέπει να

ικανοποιούνται. Επιπρόσθετα, εισάγεται η έννοια της δομής πληροφοριών η οποία επιτρέπει τη δυνατότητα καταγραφής πολιτικών ιδιωτικότητας πάνω σε μια δομή από πληροφορίες και εσωτερική διαφοροποίηση των δικαιωμάτων για το σύνολο των βασικών τύπων του πεδίου της. Τέλος βάση σχετικής κατηγοριοποίησης που ορίζεται στα πλαίσια της τυπικής διατύπωσης των βασικών τύπων για πεδία μιας δομής, το σύνολο των τυπικών δικαιωμάτων ενισχύεται με το δικαίωμα ταυτοποίησης. Η δομή του παρόντος υποκεφαλαίου έχει ως εξής, στο Υποκεφάλαιο 3.2.1 παρουσιάζονται οι βασικές έννοιες που απαιτούνται για την τυπική διατύπωση των πολιτικών ιδιωτικότητας και στη συνέχεια στο Υποκεφάλαιο 3.2.2 παρουσιάζεται και τυπικά ο ορισμός μιας πολιτικής ιδιωτικότητας.

3.2.1 Βασικές Έννοιες

Το υφιστάμενο πλαίσιο τυπικής διατύπωσης πολιτικών ιδιωτικότητας συλλαμβάνει τις συνιστώσες κάτω από τις οποίες πρέπει να διατυπωθεί μια πολιτική ιδιωτικότητας επεκτείνοντας το υφιστάμενο με την ενσωμάτωση της έννοιας των συνθηκών και τον δομών πληροφοριών. Συγκεκριμένα για την τυπική διατύπωση μιας πολιτικής ιδιωτικότητας θεωρούμε την ύπαρξη ενός συνόλου $\mathcal{G}$ το οποίο αποτελείται από στοιχεία της μορφής $G_1, \dots, G_n$ και το οποίο ορίζεται ως το σύνολο των ομάδων. Αυτό χρησιμοποιείται για να δώσει το σύνολο των διαχειριστών των δεδομένων μιας πολιτικής ορίζοντας και τις σχετικές ομάδες στις οποίες ανήκουν. Ταυτόχρονα θεωρούμε την ύπαρξη ενός συνόλου $\mathcal{U}$ με στοιχεία της μορφής $u_1, u_2, \dots, u_n$ και το οποίο ορίζεται ως το σύνολο των σκοπών μιας πολιτικής. Όσον αφορά το σύνολο των ενεργειών που μπορούν να εφαρμοστούν σε ευαίσθητα προσωπικά δεδομένα θεωρούμε την ύπαρξη ενός συνόλου δικαιωμάτων $Perm$ και των οποίων η τυπική περιγραφή δίνεται παρακάτω.

Για το σύνολο των ευαίσθητων προσωπικών δεδομένων που αποθηκεύονται σε ένα σύστημα ορίζουμε ένα σύνολο από βασικούς τύπους με στοιχεία της μορφής t. Ένας βασικός τύπος μπορεί να αποτελεί ευαίσθητη πληροφορία η οποία ανήκει σε ένα σύνολο βασικών τύπων T ή να αποτελεί μια δομή t_S η οποία συνδυάζει ένα σύνολο από πεδία και αντίστοιχους βασικούς τύπους. Έτσι ένας βασικός τύπος μπορεί να έχει την παρακάτω μορφή : t και $t_S = \{field_1 : t_S.t_1, \dots, field_k : t_S.t_k\}$. Ο βασικός τύπος για ένα πεδίο της δομής έχει την εξής μορφή $t_S.t_i$ αφού συνοδεύεται από τον βασικό τύπο της δομής στην οποία αναφέρεται. Να τονίσουμε ότι για κάθε διαφορετική οντότητα μιας

δομής την οποία αφορά η σχετική δομή ορίζεται ένα σύνολο από βασικούς τύπους δομής και εσωτερικών πεδίων και το οποίο αναπαριστά την ευαίσθητη πληροφορία που αφορά τη συγκεκριμένη οντότητα ενώ όταν υπάρχουν χαρακτηριστικά δομής τα οποία μπορούν να πάρουν πολλές τιμές ορίζουμε για αυτές ξεχωριστούς βασικούς τύπους και ανάλογα πεδία. Στα παρακάτω παραδείγματα δίνουμε αφαιρετικά την περιγραφή μιας δομής με τις αντίστοιχες ονομασίες βασικών τύπων για πεδία της. Θεωρούμε ότι το πρώτο γράμμα κάθε βασικού τύπου είναι κεφαλαίο ενώ ο βασικός τύπος δομής δίνεται με όλα τα γράμματα κεφαλαία. Ας πάρουμε για παράδειγμα μια πολιτική ενός νοσοκομείου στο οποίο οι πληροφορίες των ασθενών αποθηκεύονται υπό την μορφή δομής η οποία αποτελείται από τα πεδία, ονόματος, επιθέτου, πόλης και χώρας. Βασιζόμενοι στα παραπάνω πρέπει να ορίσουμε το βασικό τύπο της δομής t_S και ο οποίος δίνεται από το $PDATA$ ενώ για κάθε πεδίο εντός της δομής ορίζουμε τους βασικούς τύπους $Name, Surname, Town$ και $Country$. Ως αποτέλεσμα το σύνολο των βασικών τύπων είναι $PDATA, PDATA.Name, PDATA.Surname, PDATA.Town$ και $PDATA.Country$ ενώ και τυπικά ο βασικός τύπος της δομή με τους αντίστοιχους βασικούς τύπους εσωτερικά πεδία αυτής για ένα ασθενή δίνεται από το παρακάτω.

$$PDATA = \{$$
$$name: PDATA\ .Name,$$
$$surname: PDATA.Surname,$$
$$town: PDATA.Town,$$
$$country: PDATA.Country\}$$

Το σύνολο των ευαίσθητων προσωπικών δεδομένων όπως περιγράφεται και στο [7] κατηγοριοποιείται σε δεδομένα τα οποία μπορούν να χρησιμοποιηθούν για την κατευθείαν και μοναδική ταυτοποίηση οντοτήτων με δεδομένα όπως ο αριθμός κοινωνικών ασφαλίσεων (SSN), αλλά και σε μια άλλη κατηγορία δεδομένων τα οποία από μόνα τους δεν να δώσουν έμμεση ή άμεση ταυτοποίηση. Η παραπάνω κατηγοριοποίηση συναντάται και σε διάφορες διαδικτυακές πολιτικές [11,12], όταν αυτές αναφέρονται σε διαδικασίες συνάθροισης και διαχωρίζουν ότι τα συστήματα τους για τους σκοπούς αυτούς δεν χρησιμοποιούν ποτέ δεδομένα που είναι δυνατό να ταυτοποιήσουν τον οποιοδήποτε μοναδικά. Ως εκ τούτου για την ενίσχυση του πλαισίου διατύπωσης μιας πολιτικής ορίζουμε την ύπαρξη δύο κατηγοριών για τους βασικούς τύπους πεδίων δομής, οι οποίες διαχωρίζονται από τη δυνατότητα χρήσης τιμής του

συγκεκριμένου πεδίου για την ταυτοποίηση μιας οντότητας της δομής. Για το σύνολο των βασικών τύπων πεδίου δομής που μπορούν να ταυτοποιήσουν οποιαδήποτε οντότητα δομής ορίζουμε την κατηγορία τύπων T^p και για το σύνολο των βασικών τύπων πεδίων δομής που δεν δίνουν άμεση ή έμμεση ταυτοποίηση ορίζουμε την κατηγορία τύπων T^N.

Με βάση το παράδειγμα που δόθηκε προηγουμένως για την δομή των πληροφοριών ενός ασθενή νοσοκομείου και υποθέτοντας ότι τα επίθετα στο συγκεκριμένο παράδειγμα είναι μοναδικά και προσδιοριστικά του κάθε ατόμου το σύνολο T^p είναι ίσο με $T^p = \{PDATA.Surname\}$, ενώ το αντίστοιχο σύνολο για τους βασικούς τύπος πεδίων μη ταυτοποίησης είναι ίσο με $T^N = \{PDATA.Name, PDATA.Town, PDATA.Country\}$.

Για τον καθορισμό του συνόλου των συνθηκών ορίζουμε την ύπαρξη ενός συνόλου από συνθήκες οι οποίες δίνονται μέσα από το σύνολο $Cond$ με στοιχεία της μορφής $cond_1, cond_2, \dots, cond_n$ και τις επιμέρους συνθήκες να προκύπτουν ως εξής. Θεωρούμε την ύπαρξη ενός συνόλου συγκριτικών τελεστών έστω op οι οποίοι προκύπτουν ανάλογα του βασικού τύπου, δύο συναρτήσεις op_1 και op_2 οι οποίες αναφέρονται σε συνήθεις μοναδιαίες και δυαδικές αριθμητικές πράξεις που μπορούν να εφαρμοστούν ανάλογα του βασικού τύπου σε τιμές αυτού. Με το c αναφερόμαστε σε οποιαδήποτε σταθερά τιμή μπορεί να έχει κάποιος βασικός τύπος με το v σε μεταβλητή τιμή του βασικού τύπου και με $field$, στο πεδίο ενός βασικού τύπου όταν αυτός αναφέρεται στο βασικό τύπο πεδίου μιας δομής. Βάσει και των παραπάνω το σύνολο των συνθηκών προκύπτει ως ακολούθως:

$$cond ::= true \mid \neg cond \mid cond_1 \vee cond_2 \mid w\ op\ w$$
$$w ::= field \mid v \mid c \mid op_1(w_1) \mid op_2(w_1, w_2)$$

Θεωρούμε ότι μια συνθήκη μπορεί να είναι το λογικό $true$, το οποίο ορίζει την μη ύπαρξη οποιασδήποτε συνθήκης, η άρνηση, η διάζευξη επιμέρους συνθηκών και η δυνατότητα χρήσης τελεστών σύγκρισης μέσω του συνόλου op για τιμές του βασικού τύπου. Οι τιμές αυτές μπορεί να είναι μια οποιαδήποτε σταθερά (c) ή μεταβλητή τιμή (v) ενός βασικού τύπου το πεδίο του όταν αυτός αναφέρεται σε βασικό τύπο πεδίου δομής $(field)$ ή το αποτέλεσμα των συναρτήσεων που περιγράφονται και παραπάνω op_1, op_2.

3.2.2 Τυπικός Ορισμός

Τυπικά μια πολιτική ιδιωτικότητας δίνεται από το παρακάτω:

$$(Permissions)\ Perm ::= read \mid write \mid access \mid disclose\ G \mid identify$$

$$(Field\ Types\ Permissions)\ FP ::= \varepsilon \mid t_s.t{:}\,\tilde{p}_f; FP$$

$$(Hierarchies)\ H ::= \varepsilon \mid G{:}\,\{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j\in J}$$

$$(Policies)\ \mathcal{P} ::= t \gg \langle H, u\rangle \mid \mathcal{P}\ ; \mathcal{P}$$

Κάθε πολιτική ορίζει ένα σύνολο δικαιωμάτων ιδιωτικότητας ($Perm$) που αποτελούν τις ενέργειες που είναι δυνατό να εκτελεστούν σε ένα ευαίσθητη προσωπική πληροφορία. Οι πιθανές αυτές ενέργειες είναι ανάγνωση, μέσω του δικαιώματος $read$ και αντίστοιχα εγγραφή μέσω του δικαιώματος $write$. Όσον αφορά τη δυνατότητα πρόσβασης στη συγκεκριμένη πληροφορία ορίζεται το δικαίωμα $access$ ενώ το δικαίωμα αποκάλυψης της σε μια ομάδα G ορίζεται μέσω του δικαιώματος $disclose\ G$. Το ειδικό δικαίωμα $identify$ αφορά βασικούς τύπους δομής. Αυτό επιτρέπει την ταυτοποίηση μιας οντότητας την οποία αφορά η συγκεκριμένη δομή και προκύπτει όταν για τουλάχιστον ένα βασικό τύπο πεδίου της δομής υπάρχει το δικαίωμα ανάγνωσης ή εγγραφής και ο συγκεκριμένος τύπος ανήκει στην κατηγορία των T^p.

Ακολούθως στοιχεία της μορφής $FP ::= \varepsilon \mid t_s.t{:}\,\tilde{p}_f; FP$ ορίζονται ως δικαιώματα τύπων για πεδία και ανατίθενται σε κάθε βασικό τύπο πεδίου δομής όταν η διατυπωμένη ιεραρχία δικαιωμάτων αφορά βασικό τύπο δομής. Τα δικαιώματα που παραχωρούνται για κάθε τύπο διατυπώνονται μέσα από την πλειάδα δικαιωμάτων $\tilde{p}_f$.

Τα στοιχεία της μορφής $\mathrm{H_i} = \mathrm{G}{:}\,\{(cond, \tilde{p}, \widetilde{FP})\}[\mathrm{H_j}]_{\mathrm{j}\in\mathrm{J}}$, ορίζονται ως ιεραρχίες δικαιωμάτων και συλλαμβάνουν την ιεραρχία των ομάδων για την παροχή δικαιωμάτων σε κάθε βασικό τύπο. Πέραν των ομάδων η συγκεκριμένη ιεραρχία συλλαμβάνει τις δυνατές συνθήκες κάτω από τις οποίες ανατίθενται τα δικαιώματα ως προς τους βασικούς τύπους. Στις περιπτώσεις όπου η ιεραρχία αυτή αφορά τύπο δομής τότε συλλαμβάνει πέραν των δικαιωμάτων για τον βασικό τύπο της δομής τα δικαιώματα για κάθε βασικό τύπο πεδίου της μέσω της πλειάδας $\widetilde{FP}$. Η ανάθεση για κάθε βασικό τύπο πεδίου της δομής γίνεται με τη διατύπωση των δικαιωμάτων που το αφορούν ενώ η συνθήκη παραμένει η ίδια με του βασικού τύπου της δομής. Συνεπώς έστω μια ιεραρχία

δικαιωμάτων $\mathrm{H_i}$ της εξής μορφής $\mathrm{H_i} = \mathrm{G}\colon\{(cond, \tilde{p}, \widetilde{FP})\}[\mathrm{H_j}]_{\mathrm{j}\in\mathrm{J}}$, το συγκεκριμένο ορίζει ότι για την ομάδα G, παραχωρείται το σύνολο των δικαιωμάτων $\tilde{p}$ υπό την ικανοποίηση της συνθήκης $cond$. Εάν η ιεραρχία δικαιωμάτων αναφέρεται σε βασικό τύπο δομής τότε η πλειάδα $\widetilde{FP}$ συλλαμβάνει τα δικαιώματα για κάθε βασικό τύπο πεδίου εσωτερικά αυτής. Τα δικαιώματα που παραχωρούνται μέσω του $\widetilde{FP}$, στους βασικούς τύπους των πεδίων παραχωρούνται αντίστοιχα υπό την ικανοποίηση της συνθήκης $cond$. Παράλληλα, λόγω της ιεραρχίας η οποία προκύπτει μέσα από τη χρήση των ομάδων, είναι σημαντικό να τονιστεί ότι οποιαδήποτε οντότητα μιας ομάδας G βρίσκεται σε χαμηλότερο επίπεδο ιεραρχίας από μια άλλη ομάδα G', κληρονομεί τα δικαιώματα αυτής της υπερομάδας. Πιο συγκεκριμένα, έστω η ακόλουθη ιεραρχία δικαιωμάτων H η οποία έχει την ακόλουθη μορφή όπως σχετικά εμφανίζεται και παρακάτω $G\colon\{(cond, \tilde{p}, \widetilde{FP})\}[H_1, \dots, H_m]$, αυτό δηλώνει τη δυνατότητα σε οντότητές μιας ομάδας $\mathrm{G_i}$ όπου $\mathrm{G_i}$ ανήκει σε μια εκ των $\mathrm{H_1}, \dots, \mathrm{H_m}$ να κληρονομεί τα δικαιώματα $\tilde{p}$ υπό την συνθήκη $cond$ από την ομάδα G για τον βασικό τύπο στον οποίο αναφέρεται αλλά και το σύνολο όλων των δικαιωμάτων που ορίζονται μέσα από το $\widetilde{FP}$ για κάθε βασικό τύπο πεδίου. Μια οντότητα δυνατό να ανήκει σε περισσότερες από μια ομάδες.

Όσον αφορά τη διατύπωση της πολιτικής, η εκάστοτε ιεραρχία δικαιωμάτων αφορά ένα συγκεκριμένο σκοπό ο οποίος με τη σειρά του ορίζεται μέσα από το u και το αποτέλεσμα του συνδυασμού ιεραρχίας και σκοπού ανατίθεται σε ένα βασικό τύπο. Ο βασικός τύπος δύναται να αναφέρεται σε βασικό τύπο πληροφορίας ανεξάρτητος δομής ή στο βασικό τύπο μιας δομής.

Ορίζουμε τη βοηθητική συνάρτηση $\mathrm{groups(H)}$ της οποίας σκοπός είναι η ομαδοποίηση του σύνολού των ομάδων εντός μιας ιεραρχίας δικαιωμάτων.

$$\mathrm{groups(H)} = \begin{cases} \{\mathrm{G}\} \cup \left(\mathrm{U_{j\in J} groups(H_j)}\right) & \text{εάν } H = \mathrm{G}\colon\{(cond, \tilde{p}, \widetilde{FP})\}[\mathrm{H_j}]_{\mathrm{j}\in\mathrm{J}} \\ \emptyset & \text{εάν } H = \varepsilon \end{cases}$$

Λέμε ότι μια πολιτική $\mathcal{P} = t_1 \gg \langle H_1, u_1\rangle, \dots, t_n \gg \langle H_n, u_n\rangle$ είναι καλά ορισμένη και γραφούμε $\mathcal{P}\colon\diamond$ άν ικανοποιούνται τα ακόλουθα:

1. Τα t_i και κάθε $t_s.t$ εσωτερικά κάθε ιεραρχίας δικαιωμάτων H είναι διαφορετικά μεταξύ τους.

2. Εάν το $\mathrm{H} = \mathrm{G}\colon \{(cond, \tilde{p}, \widetilde{FP})\}[\mathrm{H_j}]_{\mathrm{j}\in\mathrm{J}}$ συναντάται σε κάποιο $\mathrm{H_i}$ τότε η ομάδα $\mathrm{G} \notin \mathrm{groups}(\mathrm{H_j}), \forall_{\mathrm{j}\in\mathrm{J}}$ αφού η ιεραρχία των ομάδων δεν είναι κυκλική.
3. Το δικαίωμα $identify$ εμφανίζεται μόνο σε ένα σύνολο $\tilde{p}$ όταν η ιεραρχία αφορά βασικό τύπο δομής.

Ορίζουμε τις εξής συντομεύσεις αναφορικά με τη διατύπωση μιας ιεραρχίας δικαιωμάτων, ισχύει ότι όταν ο τύπος μιας ιεραρχίας είναι βασικός τύπος ανεξάρτητος δομής τότε οι τριάδες $(cond, \tilde{\mathrm{p}}, \emptyset)$ συντομεύονται σε δυάδες της μορφής $(cond, \tilde{p})$, αφού το σύνολο $\widetilde{FP} = \emptyset$.

Συντομεύουμε σε:

- $G\colon \{(cond, \tilde{p})\}[\mathrm{H_j}]_{\mathrm{j}\in\mathrm{J}}$ όταν $\mathrm{H} = \mathrm{G}\colon \{(cond, \tilde{\mathrm{p}}, \emptyset)\}[\mathrm{H_j}]_{\mathrm{j}\in\mathrm{J}}$
- $G\colon \{(cond, \tilde{p})\}$ όταν $H = G\colon \{(cond, \tilde{p}, \emptyset)\}[\varepsilon]$
- $G\colon \{(cond, \tilde{p}, \widetilde{FP})\}$ όταν $H = G\colon \{(cond, \tilde{p}, \widetilde{FP})\}[\varepsilon]$
- $G\colon$ όταν $H = \mathrm{G}\colon \{(cond, \emptyset, \emptyset)\}[\varepsilon]$ και $cond$ να μην ορίζεται.

3.3 Παράδειγμα

Εφαρμογή της τυπικής διατύπωσης πολιτικών ιδιωτικότητας που προτείνεται παραπάνω για ένα σενάριο πολιτικής νοσοκομειακού συστήματος του οποίου η περιγραφή ακολουθεί παρακάτω.

Έστω, ένα σύστημα νοσοκομείου το οποίο χειρίζεται πληροφορίες αναφορικά με τους ασθενείς του. Εντός του νοσοκομείου υπάρχουν δύο ομάδες οι οποίες χειρίζονται ευαίσθητα προσωπικά δεδομένα ορίζοντας και τη σχετική ιεραρχία των ομάδων στο σύστημα. Υπάρχει η ομάδα των ιατρών του νοσοκομείου $(Doctor)$ και η ομάδα των νοσοκόμων $(Nurse)$. Θεωρώντας την ονομασία του συστήματος ως $Hospital$ η ιεραρχία των ομάδων είναι η ακόλουθη: $Hospital[Doctor, Nurse]$.

Σκοπός της λειτουργίας των ομάδων αυτών είναι η παροχή διάγνωσης στους ασθενείς συνεπώς ορίζουμε το σκοπό $diagnosis_h$. Οι πληροφορίες για ένα ασθενή που αποθηκεύονται στο σύστημα του νοσοκομείου και ορίζουν τη δομή των πληροφοριών του είναι το όνομα, το φύλο, η ηλικία και η διάγνωση του. Έτσι ορίζουμε τον βασικό

τύπο $PDATA$ για το βασικό τύπο της δομής είναι οι εσωτερικοί τύποι πεδίων είναι οι ακόλουθοι: $PDATA.Name$ που αναφέρεται στο όνομα του ασθενή, $PDATA.Sex$ που αναφέρεται στο φύλο του, $PATA.Age$ που αναφέρεται στην ηλικία του και τέλος το $PDATA.Diagnosis$ που αναφέρεται στην ασθένεια με την οποία έχει διαγνωσθεί. Για τους παραπάνω τύπους πεδίων θεωρούμε ότι το όνομα είναι δυνατό να ταυτοποιήσει ένα ασθενή μοναδικά, σε αντίθεση με τους υπόλοιπους τύπους πεδίων που δεν μπορούν. Συνεπώς το για το σύνολο T^p ισχύει ότι $T^p = \{PDATA.Name\}$ ενώ για το σύνολο T^N έχουμε ότι $T^N = \{PDATA.Sex, PDATA.Age, PDATA.Diagnosis\}$.

Ο βασικός τύπος δομής με τα αντίστοιχα πεδία και σύνολο βασικών τύπων πεδίων ενός ασθενή είναι ο ακόλουθος.

$$PDATA = \{$$
$$name: PDATA.Name,$$
$$sex: PDATA.Sex,$$
$$age: PDATA.Age,$$
$$diagnosis: PDATA.Diagnosis\}$$

Η πολιτική του συστήματος ορίζει τα εξής:

1. Στο βασικό τύπο της δομής δεδομένων αλλά και όλων των πεδίων εσωτερικά της δομής του ασθενή δικαιούται να λάβουν πρόσβαση και οι δύο ομάδες. Τα δικαιώματα ως προς τη διαχείριση των βασικών τύπων για τα πεδία της δομής διαχωρίζονται και διαφέρουν ως ακολούθως όπως φαίνεται από τα σημεία (2) και (3) της πολιτικής πιο κάτω.
2. Για τους σκοπούς της διάγνωσης του ασθενή η ομάδα των Νοσοκόμων δικαιούται να εγγράψει το όνομα, φύλο και ηλικία του ασθενή, όταν αυτός προσέλθει στο νοσοκομείο χωρίς την ικανοποίηση οποιασδήποτε συνθήκης. Η δυνατότητα εγγραφής του ευαίσθητου τύπου πεδίου που αφορά το όνομα το οποίο ανήκει στην κατηγορία των T^p, επιτρέπει την ταυτοποίηση της οντότητας την οποία καταγράφει στο σύστημα συνεπώς της παραχωρείται και το δικαίωμα ταυτοποίησης ως προς τη δομή των πληροφοριών του ασθενή.
3. Με την εγγραφή τους στο σύστημα η ομάδα Ιατρός δικαιούται να διαβάσει χωρίς να ικανοποιεί οποιαδήποτε συνθήκη την ηλικία και το φύλο του ασθενή. Εάν το

πεδίο ηλικίας του ασθενή έχει τιμή μεγαλύτερη η ίση των 18 οπόταν και η συνθήκη της πολιτικής η οποία ορίζεται ως

$$cond: age \geq 18$$

ικανοποιείται, μπορεί να προχωρήσει σε διάγνωση του καταχωρώντας την στο σύστημα και διαβάζοντας το όνομα του με το οποίο μπορεί να τον ταυτοποιήσει. Λόγω χρήσης της δομής για τις πληροφορίες του ασθενή είναι απαραίτητος ο ορισμός της ιεραρχίας δικαιωμάτων ως προς το βασικό τύπο του $PDATA$ και ο προσδιορισμός επιμέρους δικαιωμάτων για τους τύπους των πεδίων της δομής. Η ιεραρχία H διατυπώνεται και αφορά το σκοπό της διάγνωσης στο περιβάλλον του νοσοκομείου ενώ βάσει της πολιτικής παραπάνω περιέχει τα ακόλουθα:

$$H = Hospital: [$$

$$Nurse: \left(true, \{access, identify\}, \langle \begin{matrix} PDATA.Name: \{access, write\}; \\ PDATA.Sex: \{access, write\}; \\ PDATA.Age: \{access, write\}; \\ PDATA.Diagnosis: \{access\}; \end{matrix} \rangle \right),$$

$$Doctor: \{ \left(true, \{access\}, \langle \begin{matrix} PDATA.Name: \{access\}; \\ PDATA.Sex: \{access, read\}; \\ PDATA.Age: \{access, read\}; \\ PDATA.Diagnosis: \{access\}; \end{matrix} \rangle \right),$$

$$\left(age \geq 18, \{identify\}, \langle \begin{matrix} PDATA.Name: \{read\}; \\ PDATA.Diagnosis: \{write\}; \end{matrix} \rangle \right) \}]$$

Ως εκ τούτου η πολιτική διατυπώνεται και τυπικά ως ακολούθως:

$$\mathcal{P} = PDATA \gg \langle H, diagnosis_h \rangle$$

Κεφάλαιο 4

Ο Λογισμός της CP calculus

4.1 Περιγραφή

Το παρόν κεφάλαιο δίνει την περιγραφή του προτεινόμενου λογισμού της εργασίας και συγκεκριμένα του λογισμού της CP (Conditional Polyadic π-calculus) calculus. Ο προτεινόμενος λογισμός αποτελεί επέκταση του λογισμού για τη μοντελοποίηση συστημάτων που εμφανίζεται στο [4] με την ενσωμάτωση της υπό συνθήκης εκτέλεσης διεργασιών και τη δυνατότητα μεταφοράς πλειάδων μέσω των καναλιών. Για το σκοπό αυτό λήφθηκαν υπόψιν και οι σχετικές επεκτάσεις που προτείνονται στο [8] το οποίο έδωσε την επέκταση της monadic π-calculus σε polyadic π-calculus. Ο προτεινόμενος λογισμός χρησιμοποιείται για την μοντελοποίηση και καταγραφή της συμπεριφοράς συστημάτων τα οποία λειτουργούν στα πλαίσια των διαφόρων πολιτικών ιδιωτικότητας.

4.2 Ορισμός της CP calculus

Το παρόν υποκεφάλαιο ορίζει τις βασικές έννοιες του προτεινόμενου λογισμού της CP calculus στο Υποκεφάλαιο 4.2.1 ενώ του ορισμού των βασικών εννοιών ακολουθεί στο Υποκεφάλαιο 4.2.2 η διατύπωση της σύνταξης του λογισμού σε επίπεδο συστήματος και διεργασιών.

4.2.1 Βασικές Έννοιες

Ισχύουν από προηγουμένως τα σύνολα των ομάδων $\mathcal{G}$ και σκοπών $\mathcal{U}$ ενώ θεωρούμε την ύπαρξη ενός συνόλου ονομάτων N το οποίο αποτελείται από στοιχεία της μορφής a, b, x, y ή οποιαδήποτε συμβολοσειρά η οποία αντιπροσωπεύει το δεδομένο ή κανάλι στο οποίο θα αναφέρεται. Επίσης υποθέτουμε την ύπαρξη ενός συνόλου από βασικούς τύπους έστω D. Κάθε όνομα από το σύνολο N, ανατίθεται είτε σε ένα βασικό τύπο αντιπροσωπεύοντας ένα στοιχείο πληροφορίας του συγκεκριμένου τύπου, είτε σε ένα τύπο καναλιού ο οποίος έχει την ακόλουθη μορφή $\mathrm{G}[\tilde{\mathrm{T}}]$ και το οποίο συλλαμβάνει την ύπαρξη ενός καναλιού στα πλαίσια της ομάδας G που δύναται να μεταφέρει ένα σύνολο από τιμές οι οποίες έχουν τύπο T. Το κάθε όνομα ανατίθεται σε ακριβώς ένα τύπο.

Για την υποστήριξη της υπό συνθήκης εκτέλεσης διεργασιών ορίζουμε ένα σύνολο από εκφράσεις (e) το οποίο προκύπτει αντίστοιχα του συνόλου των συνθηκών από το κεφάλαιο των πολιτικών ιδιωτικότητας προηγουμένως.

Θεωρούμε ότι το $\tilde{\mathrm{T}}$ αναφέρεται σε μια πλειάδα με ονόματα τα οποία ανατίθενται σε αντίστοιχους τύπους. Συνεπώς το σύνολο των τύπων για κάθε όνομα δίνεται από την παρακάτω BNF:

$$\mathrm{T} ::= \mathrm{t} \mid \mathrm{G}[\tilde{\mathrm{T}}], \tilde{\mathrm{T}} = \mathrm{T}_1, \dots, \mathrm{T}_\mathrm{n} \text{ και } \mathrm{n} \in \mathbb{N}$$

4.2.2 Σύνταξη

Ακολουθεί η σύνταξη του λογισμού της CP calculus για τη μοντελοποίηση συστημάτων η οποία διατυπώνεται σε επίπεδο διεργασιών και συστήματος όπως αυτά εμφανίζονται στο Σχήμα 4.1

$P ::= x(\tilde{y}_T).P'$	$S ::= (\nu\ G)\ P\langle u\rangle$
$\mid \bar{x}\langle\tilde{y}\rangle.P'$	$\mid (\nu\ G)\ S'$
$\mid (\nu\ \tilde{x}_T)P'$	$\mid (\nu\ \tilde{x}_T)\ S'$
$\mid P_1 \mid P_2$	$\mid S_1 \mid S_2$
$\mid !\ P$	$\mid 0$
$\mid if\ e\ then\ P\ else\ Q$	
$\mid 0$	

$\text{Όπου: } \tilde{y}_T = y_1{:}T_1, \dots, y_n{:}T_n, \tilde{y} = y_1, \dots, y_n \text{ και } \tilde{x}_T = x_1{:}T_1, \dots, x_n{:}T_n \text{ με } n \in \mathbb{N}$

Σχήμα 4.1: Λογισμός της CP calculus σε επίπεδο διεργασιών και συστήματος

Περιγραφή τελεστών της CP calculus

Οι συμβολισμοί P, P', Q αναφέρονται σε διεργασίες και S, S' σε συστήματα.

Ο τελεστής $x(\tilde{y}_T)P'$ αποτελεί τη "θύρα εισόδου πολλαπλών πληροφοριών" και καθορίζει ότι μια διεργασία μπορεί να αναγνώσει όλες τις πληροφορίες που μεταφέρονται μέσω του διανύσματος ονομάτων και τα οποία έχουν ανατεθεί σε συγκεκριμένους βασικούς τύπους $\tilde{y}_T$και ακολούθως να συνεχίσει τη λειτουργία της σύμφωνα με τη συμπεριφορά που ορίζει η διεργασία P'. Τα ονόματα $y_1 \dots y_n$, που μεταφέρονται μέσω του καναλιού x περιορίζονται στα όρια της διεργασίας P' και αποτελούν θέσεις που μπορούν να τοποθετηθούν τα ονόματα που θα μεταφερθούν κατά την ενέργεια εισόδου.

Ο τελεστής $\tilde{x}\langle\tilde{y}\rangle.P$ αποτελεί τη "θύρα εξόδου πολλαπλών πληροφοριών" για την διεργασία που την περιλαμβάνει. Με την εκτέλεση της παραπάνω ενέργειας η διεργασία μπορεί να εξάγει μέσω του καναλιού x όλα τα ονόματα του διανύσματος ονομάτων $\tilde{y} = y_1 \dots y_n$ και στη συνέχεια να συνεχίσει τη λειτουργία με τη συμπεριφορά η οποία ορίζεται μέσα από τη διεργασία P'.

Ο τελεστής $(\nu\ \tilde{x}_T)P'$ αναφέρεται στη δημιουργία ενός συνόλου νέων ονομάτων με την αντίστοιχη ανάθεση τους σε ένα βασικό τύπο στα πλαίσια της διεργασίας P', τα ονόματα αυτά είναι γνωστά μόνο στα πλαίσια της διεργασίας από την οποία δεσμεύονται.

Ο τελεστής $\mathrm{P}_1|\mathrm{P}_2$ αναφέρεται στον τελεστή του ταυτοχρονισμού ο οποίος επιτρέπει την παράλληλη εκτέλεση των διεργασιών $\mathrm{P}_1|\mathrm{P}_2$.

Ο τελεστής !P αναφέρεται στον τελεστή αναδρομικότητας επιτρέποντας σε μια διεργασία να δημιουργεί πολλαπλά αντίγραφα του εαυτού της.

Ο τελεστής $if\ e\ then\ P\ else\ Q$, αποτελεί την υποσυνθήκη εκτέλεση μιας διεργασίας. Συγκεκριμένα ορίζει ότι βάσει της τιμής που έχει η έκφραση e, η συμπεριφορά της διεργασίας διαφοροποιείται. Ως εκ τούτου, αν η τιμή της έκφρασης e αποτιμάται σε $true$, τότε η διεργασία συνεχίζει τη συμπεριφορά της όπως αυτή ορίζεται μέσα από τη διεργασία P διαφορετικά αν η τιμή της έκφρασης e αποτιμάται σε $false$ η διεργασία ορίζει τη συμπεριφορά της μέσα από τη διεργασία Q.

Ο τελεστής 0 αναφέρεται στον τελεστή της τερματικής διεργασίας.

Ο τελεστής $(\nu\ G)P\langle u\rangle$, καταγράφει την ύπαρξη στο σύστημα μιας διεργασίας της οποίας ο σκοπός λειτουργίας της είναι το u ενώ ανήκει στην ομάδα από τον τελεστή κατασκευής ομάδας G. Με το συσχετισμό του σκοπού και της διεργασίας P προσπαθούμε να συλλάβουμε το σκοπό για τον οποίο η εκάστοτε διεργασία εκτελείται.

Ο τελεστής $(\nu\ G)S$, καταγράφει την ύπαρξη ενός συστήματος το οποίο ανήκει στην ομάδα G. Με το συσχετισμό μιας διεργασίας ή ενός συστήματος με ομάδες συλλαμβάνουμε τα μέλη των ομάδων ενός συστήματος.

Οι επόμενοι τρείς τελεστές, περιορισμού ονομάτων στα πλαίσια ενός συστήματος $(\nu\ \tilde{x}_T)\ S'$, παράλληλης εκτέλεσης συστημάτων $S_1|S_2$ και τερματισμού 0, έχουν παρόμοια συμπεριφορά με αυτή ως προς το επίπεδο των διεργασιών.

Οι ονομασίες των διεργασιών πρέπει να είναι μοναδικές, ενώ εάν μια οντότητα ενός συστήματος ανήκει σε δύο διαφορετικές ομάδες με αντίστοιχη ιεραρχία, καταγράφουμε τη συμπεριφορά της για κάθε ομάδα ξεχωριστά.

4.3 Σύστημα μεταβάσεων με ετικέτες

Με τη διατύπωση της σύνταξης του προτεινόμενου λογισμού της CP calculus, είμαστε σε θέση να ορίσουμε το σχετικό σύστημα μεταβάσεων με ετικέτες. Το σύστημα μεταβάσεων δίνει τη σημασιολογική ερμηνεία του λογισμού και προσδιορίζει το σύνολο των επιτρεπτών ενεργειών που μπορούν να εκτελεστούν από μια διεργασία ή σύστημα οδηγώντας σε μια καινούρια κατάσταση. Η παρούσα ενότητα διαχωρίζεται σε δύο υποκεφάλαια. Στο πρώτο υποκεφάλαιο παρατίθεται το σύνολο των βοηθητικών συναρτήσεων για τις ελεύθερες και δεσμευμένες εμφανίσεις ονομάτων και ομάδων οι οποίες χρησιμοποιούνται για το δεύτερο υποκεφάλαιο στο οποίο δίνεται το σύνολο των κανόνων του συστήματος μεταβάσεων με ετικέτες.

4.3.1 Βοηθητικές Συναρτήσεις

Ορίζουμε, τις συναρτήσεις $fn(P), bn(P), fn(S), bn(S)$ οι οποίες συλλαμβάνουν το σύνολο των ελευθέρων και δεσμευμένων ονομάτων σε επίπεδο διεργασιών αλλά και

συστήματος για τον προτεινόμενο λογισμό.

Ισχύει ότι:

$$\tilde{y}_T = y_1{:}T_1, \dots, y_n{:}T_n, \tilde{y} = y_1, \dots, y_n \text{ και } \tilde{x}_T = x_1{:}T_1, \dots, x_n{:}T_n \text{ με } n \in \mathbb{N}$$

Συγκεκριμένα ορίζουμε τις παρακάτω συναρτήσεις:

$$fn(P) = \begin{cases} \{x\} \cup fn(P') & \text{εάν } P = x(\tilde{y}_T).P' \\ \{x\} \cup \{y_1 \dots y_n\} \cup fn(P') & \text{εάν } P = \bar{x}\langle\tilde{y}\rangle.P' \\ fn(P') - \{x_1 \dots x_n\} & \text{εάν } P = (\nu\tilde{x}_T)P' \\ fn(P_1) \cup fn(P_2) & \text{εάν } P = \mathrm{P}_1|\mathrm{P}_2 \\ fn(P) & \text{εάν } P = !\,\mathrm{P} \\ \emptyset & \text{εάν } P = 0 \end{cases}$$

$$bn(P) = \begin{cases} \{y_1 \dots y_n\} \cup bn(P') & \text{εάν } P = x(\tilde{y}_T).P' \\ bn(P') & \text{εάν } P = \bar{x}\langle\tilde{y}\rangle.P' \\ \{x_1 \dots x_n\} \cup bn(P') & \text{εάν } P = (\nu\tilde{x}_T)P' \\ bn(P_1) \cup bn(P_2) & \text{εάν } P = \mathrm{P}_1|\mathrm{P}_2 \\ bn(P) & \text{εάν } P = !\,\mathrm{P} \\ \emptyset & \text{εάν } P = 0 \end{cases}$$

$$fn(S) = \begin{cases} fn(P) & \text{εάν } S = (\nu G)\mathrm{P}\langle u\rangle \\ fn(S') & \text{εάν } S = (\nu G)\mathrm{S}' \\ fn(S') - \{x_1 \dots x_n\} & \text{εάν } S = (\nu\tilde{x}_T)\mathrm{S}' \\ fn(S_1) \cup fn(S_2) & \text{εάν } S = S_1|\,S_2 \\ \emptyset & \text{εάν } S = 0 \end{cases}$$

$$bn(S) = \begin{cases} bn(P) & \text{εάν } S = (\nu G)\mathrm{P}\langle u\rangle \\ bn(S') & \text{εάν } S = (\nu G)\mathrm{S}' \\ \{x_1 \dots x_n\} \cup bn(S') & \text{εάν } S = (\nu\tilde{x}_T)\mathrm{S}' \\ bn(S_1) \cup bn(S_2) & \text{εάν } S = S_1|\,S_2 \\ \emptyset & \text{εάν } S = 0 \end{cases}$$

Επιπρόσθετα ορίζουμε το συναρτήσεις για το σύνολο των ελεύθερων ομάδων εντός διεργασιών, συστήματος και τύπων οι οποίες δίνονται μέσα από τα $fg(P), fg(S), fg(T)$ αντίστοιχα.

$$fg(P) = \begin{cases} \cup_{i\in I} fg(T_i) \cup fg(P') & \text{εάν } P = x(\tilde{y}_T).P', \text{όπου } \tilde{y}_T = \langle y_i : T_i \rangle_{i\in I} \\ fg(P') & \text{εάν } P = \bar{x}\langle\tilde{y}\rangle.P' \\ \cup_{i\in I} fg(T_i) \cup fg(P') & \text{εάν } P = (\nu\tilde{x}_T)P', \text{όπου } \tilde{x}_T = \langle x_i : T_i \rangle_{i\in I} \\ fg(P_1) \cup fg(P_2) & \text{εάν } P = \mathrm{P}_1|\mathrm{P}_2 \\ fg(P) & \text{εάν } P = !\,\mathrm{P} \\ \emptyset & \text{εάν } P = 0 \end{cases}$$

$$fg(S) = \begin{cases} fg(P) - \{G\} & \text{εάν } S = (\nu G)\mathrm{P}\langle u\rangle \\ fg(S') - \{G\} & \text{εάν } S = (\nu G)\mathrm{S}' \\ fg(S') \cup_{i\in I} fg(T_i) & \text{εάν } S = (\nu\,\tilde{x}_T)\mathrm{S}', \text{όπου } \tilde{x}_T = \langle x_i : T_i \rangle_{i\in I} \\ fg(S_1) \cup fg(S_2) & \text{εάν } S = S_1|\,S_2 \\ \emptyset & \text{εάν } S = 0 \end{cases}$$

$$fg(T) = \begin{cases} \emptyset & \text{εάν } T = t \\ \{G\} \cup fg(T_i) & \text{εάν } T = G[\tilde{\mathrm{T}}] \end{cases}$$

Οι ελεύθερες εμφανίσεις των ομάδων λαμβάνουν χώρα εντός των τύπων T ενός συστήματος ή διεργασίας.

4.3.2 Ορισμός

Ορίζουμε το ακόλουθο σύνολο ετικετών που αντιπροσωπεύουν τις δυνατές ενέργειες του λογισμού:

$$l ::= \tau|\, x(\tilde{y}_T)|\bar{x}\langle\tilde{y}\rangle|(\nu\,\tilde{y}_T)\bar{x}\langle\tilde{y}\rangle$$

Η ετικέτα τ, αναφέρεται στην εσωτερική ενέργεια όπου το $x(\tilde{y}_T)$ αποτελεί ενέργεια εισόδου και το $\bar{x}\langle\tilde{y}\rangle$ αποτελεί την ενέργεια εξόδου ενώ οι πλειάδες που μεταφέρονται μεταξύ τους είναι ισοπληθείς.

Η ετικέτα $(\nu\,\tilde{y}_T)\bar{x}\langle\tilde{y}\rangle$ ορίζεται ως η ενέργεια περιορισμού της εξόδου και πιο συγκεκριμένα περιορίζεται το σύνολο των αντικειμένων που εμπεριέχονται στην πλειάδα $\tilde{y}$ στην έξοδο της από το κανάλι x. Οι συναρτήσεις $fn(l)$ και $bn(l)$, επιστρέφουν το σύνολο των ελεύθερων και δεσμευμένων ονομάτων του l, εκατέρωθεν.

Ισχύει ότι $\tilde{y}_T = y_1 : T_1, \dots, y_n : T_n, \tilde{y} = y_1, \dots, y_n$ *και* $\tilde{x}_T = x_1 : T_1, \dots, x_n : T_n$ με $n \in \mathbb{N}$

$$fn(l) = \begin{cases} x & \text{εάν } l = x(\tilde{y}_T) \\ \{x\} \cup \{y_1, \dots, y_n\} & \text{εάν } l = \bar{x}\langle\tilde{y}\rangle \\ x & \text{εάν } l = (\nu\,\tilde{y}_T)\bar{x}\langle\tilde{y}\rangle \end{cases}$$

$$bn(l) = \begin{cases} x & \text{εάν } l = x(\tilde{y}_T) \\ \emptyset & \text{εάν } l = x\langle\tilde{y}\rangle \\ x & \text{εάν } l = (\nu\ \tilde{y}_T)\bar{x}\langle\tilde{y}\rangle \end{cases}$$

Επιπρόσθετα ορίζουμε τη δυαδική σχέση $dual(l, l')$ η οποία συσχετίζει δυαδικές ενέργειες ως ακολούθως:

$dual(l, l')$ αν και μόνο αν $(l, l') \in \{(\ x(\tilde{y}_T), \bar{x}\langle\tilde{y}\rangle), (x(\tilde{y}_T), (\nu\ \tilde{y}_T)\bar{x}\langle\tilde{y}\rangle)\}$

Παρακάτω παρουσιάζουμε το σύστημα μεταβάσεων με ετικέτες σε παρένθεση η ονομασία του εκάστοτε κανόνα. Χρησιμοποιούμε το μέτα συμβολισμό F όπου F ::= P |S.

$\mathrm{x}(\tilde{\mathrm{y}}_\mathrm{T}).\,\mathrm{P} \xrightarrow{\mathrm{x}(\tilde{\mathrm{z}})} \mathrm{P}\{^{z_i}/_{y_i}\}_{\forall_{i=1..n}}$ (In)

$\bar{x}\langle\tilde{\mathrm{z}}\rangle.\,\mathrm{P} \xrightarrow{\bar{\mathrm{x}}(\tilde{\mathrm{z}})} \mathrm{P}$ (Out)

$$\frac{F_1 \xrightarrow{l} F_1'\ \ bn(l) \cap fn(F_2) = \emptyset}{F_1|F_2 \xrightarrow{l} F_1'|F_2}\ (ParL) \qquad \frac{F_2 \xrightarrow{l} F_2'\ \ bn(l) \cap fn(F_1) = \emptyset}{F_1|F_2 \xrightarrow{l} F_1\ |F_2'}\ (ParR)$$

$$\frac{F \xrightarrow{l} F'\ \ x_1 \ldots x_n\ \notin fn(l)}{(\nu\ \tilde{x}_T)F \xrightarrow{l} (\nu\ \tilde{x}_T)F'}(ResN) \qquad \frac{F \xrightarrow{\bar{x}\langle\tilde{y}\rangle} F'}{(\nu\ \tilde{y}_T)F \xrightarrow{(\nu\ \tilde{y}_T)\bar{x}\langle\tilde{y}\rangle} F'}(Scope)$$

$$\frac{S \xrightarrow{l} S'}{(\nu G)S \xrightarrow{l} (\nu G)S'}(ResGS) \qquad \frac{P \xrightarrow{l} P'}{(\nu\ G)P\langle u\rangle \xrightarrow{l} (\nu\ G)P'\langle u\rangle}\ (ResGP)$$

$$\frac{P \xrightarrow{l} P'}{!\,P \xrightarrow{l} P'|!\,P}(Repl) \qquad \frac{F_1 \xrightarrow{l_1} F_1'\ F_2 \xrightarrow{l_2} F_2'\ \ dual(l_1, l_2)}{F_1|F_2 \xrightarrow{\tau} (\nu\ bn(l_1) \cup bn(l_2))\ F_1'\ |F_2'}(Com)$$

$$\frac{P \xrightarrow{l} P'\ \ [\![e]\!] = true}{if\ e\ then\ P\ else\ Q \xrightarrow{l} P'}(True) \qquad \frac{Q \xrightarrow{l} Q'\ \ [\![e]\!] = false}{if\ e\ then\ P\ else\ Q \xrightarrow{l} Q'}(False)$$

$$\frac{F \equiv_a F''\ \ F'' \xrightarrow{l} F'}{F \xrightarrow{l} F'}(Alpha)$$

Σχήμα 4.2: Το σύστημα μεταβάσεων με ετικέτες του λογισμού της CP calculus

Περιγραφή κανόνων του συστήματος μεταβάσεων με ετικέτες

Ο κανόνας (In) ορίζει ότι αν μια διεργασία είναι σε θέση να λάβει ως είσοδο μια πλειάδα ονομάτων με συγκεκριμένο τύπο, $\tilde{y}_T$ και λάβει ως είσοδο της μια πλειάδα $\tilde{z}$ τότε μπορεί να συνεχίσει τη λειτουργία της με τη συμπεριφορά που ορίζει η διεργασία P αντικαθιστώντας κάθε όνομα του συνόλου $\tilde{y}_T$ με το αντίστοιχο στην είσοδο του $\tilde{z}$. Τα δύο σύνολα πρέπει να περιλαμβάνουν τον ίδιο αριθμό ονομάτων και να τα ονόματα σε

κάθε θέση να είναι του ανάλογου τύπου.

Ο κανόνας (Out) ορίζει ότι αν μια διεργασία είναι σε θέση να εγγράψει σε ένα κανάλι μια πλειάδα ονομάτων $\tilde{z}$ τότε με την εγγραφή τους μπορεί να συνεχίσει τη λειτουργία της με τη συμπεριφορά όπως αυτή ορίζεται μέσα από τη διεργασία P.

Ο κανόνας ($ParL$) ορίζει ότι αν μια διεργασία η σύστημα F_1 με την εκτέλεση μιας ενέργειας l μεταβαίνει σε μια νέα διεργασία η σύστημα F_1' τότε όταν εκτελείται παράλληλα με μια αντίστοιχη διεργασία ή σύστημα F_2 μπορεί να εκτελέσει την ενέργεια l και να συνεχίσει τη συμπεριφορά της βάση του F_1' αν δεν δεσμεύεται κανένα ελεύθερο όνομα της F_2 μέσω της ενέργειας l.

Ο κανόνας ($ParR$) ορίζει ότι αν μια διεργασία η σύστημα F_2 με την εκτέλεση μιας ενέργειας l μεταβαίνει σε μια νέα διεργασία η σύστημα F_2' τότε όταν εκτελείται παράλληλα με μια αντίστοιχη διεργασία ή σύστημα F_1 μπορεί να εκτελέσει την ενέργεια l και να συνεχίσει τη συμπεριφορά της βάση του F_2' αν δεν δεσμεύεται κανένα ελεύθερο όνομα της F_1 μέσω της ενέργειας l.

Ο κανόνας ($ResN$) ορίζει ότι αν μια διεργασία η σύστημα F με την εκτέλεση μιας ενέργειας l οδηγείτε σε μια νέα διεργασία η σύστημα F' τότε μπορεί να δεσμεύσει ένα σύνολο ονομάτων με τον αντίστοιχο τύπο τους και να εκτελέσει την ενέργεια l αν κανένα όνομα δεν εμφανίζεται σε αυτά των ελεύθερων ονομάτων της l.

Ο κανόνας ($Scope$) ορίζει ότι αν μια διεργασία ή σύστημα με την εκτέλεση μιας ενέργειας εξόδου σε ένα σύνολο ονομάτων $\tilde{y}$, οδηγείτε σε μια νέα διεργασία η σύστημα F' τότε είναι δυνατό να δεσμεύσει το σύνολο αυτό στην αρχή της F και να προχωρήσει με τα νέα δεσμευμένα ονόματα στη διεργασία F'.

Ο κανόνας ($ResGS$) ορίζει ότι αν ένα σύστημα S με την εκτέλεση μιας ενέργειας l οδηγείτε σε ένα νέο σύστημα S' τότε η δέσμευση μιας ομάδας στα πλαίσια του συστήματος S μεταφέρεται με την εκτέλεση της l και στο S'.

Ο κανόνας ($ResGP$) ορίζει ότι αν μια διεργασία P με την εκτέλεση μιας ενέργειας l

οδηγείτε σε μια νέα διεργασία P' τότε η δέσμευση μιας ομάδας στα πλαίσια της διεργασίας P μεταφέρεται με την εκτέλεση της l και στη P'.

Ο κανόνας $(Repl)$ ορίζει ότι αν μια διεργασία με την εκτέλεση μιας ενέργειας l οδηγείτε σε μια νέα διεργασία P' τότε η εκτέλεση της ίδιας ενέργειας στον τελεστή $!P$ οδηγεί στο $P'|!P$.

Ο κανόνας (Com) ορίζει ότι αν μια διεργασία ή σύστημα F_1 με την εκτέλεση μιας ενέργειας l_1 οδηγείτε σε μια νέα διεργασία ή σύστημα F_1' και αντίστοιχα μια διεργασία ή σύστημα F_2 με την εκτέλεση μιας ενέργειας l_2 οδηγείτε σε μια νέα διεργασία ή σύστημα F_2' τότε αν οι δύο αυτές ενέργειες (l_1, l_2) ικανοποιούν τη σχέση $dual(l_1, l_2)$ τότε η παράλληλη εκτέλεση των $F_1|F_2$ οδηγεί μέσω της ενέργειας συγχρονισμού στα $F_1'|F_2'$ με τη δέσμευση όλων των ονομάτων που ήταν δεσμευμένα στα πλαίσια των ενεργειών l_1, l_2.

Η συνάρτηση $[\![e]\!]$, επιστρέφει την τιμή της έκφρασης e, η οποία μπορεί να αποτιμάται στις λογικές τιμές $true$ και $false$. Μέσω της τιμής αυτής μπορούμε να προσδιορίσουμε πιο κομμάτι της διεργασίας θα εκτελεστεί όταν μια διεργασία ορίζεται μέσα από τον τελεστή της υπό συνθήκης εκτέλεσης.

Ο κανόνας $(True)$ ορίζει ότι αν μια διεργασία P με την εκτέλεση μιας ενέργειας l οδηγείτε σε μια νέα διεργασία P' και η έκφραση e αποτιμάται σε $true$ τότε η υπό συνθήκη εκτέλεση μέσω του $if\ e\ then\ P\ else\ Q$ θα οδηγήσει με την εκτέλεση της ενέργειας l στη συνέχιση της συμπεριφοράς της όπως αυτή ορίζεται από τη P'.

Ο κανόνας $(False)$ ορίζει ότι αν μια διεργασία Q με την εκτέλεση μιας ενέργειας l οδηγείτε σε μια νέα διεργασία Q' και η έκφραση e αποτιμάται σε $false$ τότε η υπό συνθήκη εκτέλεση μέσω $if\ e\ then\ P\ else\ Q$ θα οδηγήσει με την εκτέλεση της ενέργειας l τη συνέχιση της συμπεριφοράς της όπως αυτή ορίζεται από τη Q'.

Το $\equiv_a$, αναφέρεται στη σχετική ισοδυναμία $a-equivalence$ και ο σχετικός κανόνας $(Alpha)$, αναφέρει ότι όταν δύο διεργασίες ή συστήματα είναι ισοδύναμα ως προς την σχέση ισοδυναμίας $a-equivalence$ τότε η εκτέλεση μιας ενέργειας l από ένα ισοδύναμο σύστημα ή διεργασία είναι δυνατή και από το άλλο και η νέα κατάσταση που

προκύπτει είναι η ίδια.

4.4 Παράδειγμα

Εφαρμόζουμε τον προτεινόμενο λογισμό της CP calculus για τη μοντελοποίηση ενός συστήματος στα πλαίσια της πολιτικής που αναφέρθηκε παραπάνω και αφορά το σύστημα του νοσοκομείου. Η μοντελοποίηση γίνεται με την χρήση του προτεινόμενου λογισμού της CP calculus. Ισχύει η ιεραρχία και οι ομάδες $Hospital, Nurse, Doctor$. Η συμπεριφορά του συστήματος ορίζεται ως ακολούθως. Οποτεδήποτε ένας ασθενής επισκέπτεται το νοσοκομείο καταχωρούνται για αυτόν τα δεδομένα του ονόματος, ηλικίας και φύλου του από το νοσοκόμο στα πεδία της εγγραφής στα οποία λαμβάνει προηγουμένως πρόσβαση. Όταν ο ιατρός αναλάβει τη διάγνωση του ασθενή λαμβάνει πρόσβαση στη δομή των πληροφοριών του και αφού διαβάσει και ελέγξει την ηλικία του προχωρεί με την καταγραφή της διάγνωσης του η οποία γίνεται εφόσον αυτός είναι ενήλικας δηλαδή η τιμή ως προς τον βασικό τύπο πεδίου της ηλικίας είναι μεγαλύτερη του 18. Σε περίπτωση που το άτομο είναι ενήλικο ο ιατρός προχωρεί στην διάγνωση του διαβάζοντας για την ταυτοποίηση του, το όνομα του.

Ισχύει το ακόλουθο σύνολο βασικών τύπων δομής και των αντίστοιχων πεδίων αυτής.
$PDATA, PDATA.Name, PDATA.Sex, PDATA.Age, PDATA.Diagnosis$

Μοντελοποίηση παραδείγματος συστήματος με τη χρήση του λογισμού της CP calculus

$$System = (\nu Hospital)((\nu\ Nurse)N\langle diagnosis_h\rangle \mid (\nu\ Doctor)D\langle diagnosis_h\rangle)$$

$$N = pdataCh\big(x{:}\,T_{Name}, y{:}\,T_{Sex}, z{:}\,T_{Age}, w{:}\,T_{diagnosis}\big).\ \big(\nu\ d_{name}{:}\,PDATA.Name, d_{sex}{:}\,PDATA.Sex, d_{age}{:}\,PDATA.Age\big).\ \bar{x}\langle d_{name}\rangle.\bar{y}\langle d_{sex}\rangle.\bar{z}\langle d_{age}\rangle.0$$

$$D = pdataChD\big(xd{:}\,T_{Name}, yd{:}\,T_{Sex}, zd{:}\,T_{Age}, wd{:}\,T_{diagnosis}\big).\ zd(age{:}\,PDATA.Age).if\,(age \geq 18)\ then\ xd\big(name_p{:}\,PDATA.Name\big).\ \big(\nu\ d_{diagnosis}{:}\,PDATA.Diagnosis\big).\overline{wd}\,\langle d_{diagnosis}\rangle.0$$

Συγκεκριμένα γράφουμε τα παρακάτω:

$$T_{PDATA} = Hospital\left[T_{Name}, T_{Sex}, T_{Age}, T_{diagnosis}\right]$$

$$T_{Name} = Hospital\,[PDATA.Name]$$

$$T_{Sex} = Hospital\,[PDATA.Sex]$$

$$T_{Age} = Hospital\,[PDATA.Age]$$

$$T_{diagnosis} = Hospital\,[PDATA.Diagnosis]$$

Κεφάλαιο 5

Το Σύστημα Τύπων του λογισμού της CP calculus

5.1 Περιγραφή

Στο κεφάλαιο αυτό θα ορίσουμε ένα σύστημα τύπων για τον προτεινόμενο λογισμό της CP calculus. Το σύστημα αυτό θα ελέγχει ότι όλες οι οντότητες ικανοποιούν τους τύπους και χρησιμοποιούν τον καθένα σύμφωνα με τον ορισμό του. Ταυτόχρονα, θα γίνεται υπολογισμός μιας διεπαφής για κάθε βασικό τύπο του συστήματος ο οποίος θα καταγράφει τα ασκούμενα δικαιώματα από κάθε ομάδα στο σύστημα και η οποία θα χρησιμοποιηθεί στο τέλος για σκοπούς ελέγχου της ικανοποίησης μιας πολιτικής ιδιωτικότητας. Το βασικότερο συστατικό αναφορικά με το προτεινόμενο σύστημα τύπων ορίζεται ως το περιβάλλον Γ το οποίο συλλαμβάνει το σύνολο των ομάδων και τύπων που έχουν τα διάφορα ονόματα του λογισμού. Με την εφαρμογή του ελέγχου τύπων στο λογισμό και τις διάφορες ενέργειες που εμφανίζονται σε αυτό προκύπτουν δύο επιπρόσθετες έννοιες το περιβάλλον Δ και η διεπαφή Θ. Συγκεκριμένα το περιβάλλον Δ αφορά τα δικαιώματα και τη συνθήκη κάτω από την οποία ασκούνται αυτά πάνω σε ένα βασικό τύπο του συστήματος ενώ η διεπαφή Θ έρχεται να ολοκληρώσει την τυπική διατύπωση των ασκούμενων δικαιωμάτων για κάθε ένα από τους βασικούς τύπους αναθέτοντας τα σε μια ιεραρχία ομάδων η οποία συνοδεύεται από τον εκάστοτε σκοπό και συνθήκη. Παρακάτω εμφανίζεται ο ορισμός και οι κανόνες παραγωγής των βασικών στοιχείων που περιεγράφηκαν παραπάνω:

$$\Gamma ::= \emptyset \mid \Gamma \cdot x{:}\,T \quad \mid \quad \Gamma \cdot G$$
$$\Delta ::= \emptyset \mid t{:}\,(\tilde{p}, cond).\,\Delta$$
$$\Theta ::= \emptyset \mid t \gg \langle H^{\downarrow}, \tilde{p} \rangle; \Theta$$

Ισχύει ότι $\mathrm{H}^{\downarrow} ::= \mathrm{G}[\mathrm{H}^{\downarrow}] \mid G[u, cond]$

Σχήμα 5.1: Βασικά συστατικά Συστήματος Τύπων

Το $H^{\downarrow}$ συλλαμβάνει ιεραρχίες στις οποίες οι ομάδες διατυπώνονται γραμμικά. Θα αναφερόμαστε με το συμβολισμό $H^{\downarrow}$ ως μια διεπαφή ιεραρχίας. Το πεδίο τιμών του περιβάλλοντος $\Gamma, dom(\Gamma)$, περιλαμβάνει όλα τα ονόματα και ομάδες οι οποίες έχουν δηλωθεί και ανήκουν στο περιβάλλον αυτό. Το Περιβάλλον Δ, έχει την ακόλουθη μορφή $t_1 : (\tilde{p}_1, cond_1). , \ldots , t_n : (\tilde{p}_n, cond_n)$. Αυτό συσχετίζει τα δικαιώματα $\tilde{p}_i \subseteq Perm$ και την εκάστοτε συνθήκη $cond_i$ πάνω στο βασικό τύπο t_i. Με το συσχετισμό ενός τύπου με το αντίστοιχο δικαίωμα ως προς τις πολιτικές ιδιωτικότητας $read$ και $write$ εννοούμε ότι είναι δυνατή η ανάγνωση, εγγραφή αντίστοιχα ευαίσθητης πληροφορίας που αφορά το βασικό τύπο πληροφορίας t και η οποία μεταφέρεται μέσω καναλιών της μορφής $\mathrm{G}[\widetilde{\mathrm{T}}]$ για οποιαδήποτε ομάδα G. Τα δικαιώματα $access$ και $disclose\, G$ όταν αυτά συσχετίζονται με ένα τύπο t, αναφέρονται στη δυνατότητα παραλαβής και προώθησης αντίστοιχα ενός καναλιού με τύπο $\mathrm{G}\left[\mathrm{G}'[\widetilde{\mathrm{T}}]\right]$ για οποιαδήποτε ομάδα G. Έτσι, τα δικαιώματα $read$ και $write$ συσχετίζονται άμεσα με την επεξεργασία και διαχείριση ευαίσθητων πληροφοριών ενώ τα δικαιώματα $access$ και $disclose\ G$, συσχετίζονται με τη διαχείριση καναλιών τα οποία περιλαμβάνουν ευαίσθητες πληροφορίες βασικών τύπων. Το δικαίωμα του $identify$ όταν αυτό συσχετίζεται με ένα βασικό τύπο δομής δηλώνει την ανάγνωση ή εγγραφή πληροφορίας ενός βασικού τύπου πεδίου δομής ο οποίος ανήκει στην κατηγορία των T^p. Τέλος, η διεπαφή Θ συσχετίζει τους βασικούς τύπους με ένα σύνολο από δικαιώματα και μια γραμμική ιεραρχία από ομάδες οι οποίες αναφέρονται στο σύνολο των σκοπών και συνθηκών. Μια γραμμική ιεραρχία έχει την ακόλουθη μορφή: $\langle G_1[G_2[\ldots G_n[u, cond]]]\rangle$. Διαισθητικά, το ακόλουθο $t \gg \langle G_1\left[G_2\left[\ldots G_n[u, cond]\right]\right]\tilde{p}, \rangle$, συλλαμβάνει το γεγονός της ύπαρξης στο σύστημα μιας οντότητας η οποία ανήκει στις ομάδες $G_1, \ldots, G_n$ εργάζεται κάτω από το σκοπό u και ικανοποιώντας τη συνθήκη $cond$ εφαρμόζει τα δικαιώματα $\tilde{p}$ πάνω σε πληροφορίες του βασικού τύπου t.

Παρακάτω καθορίζουμε τρεις βασικούς κανόνες διατύπωσης των τύπων. Συγκεκριμένα έχουμε τους εξής κανόνες $\Gamma \vdash \mathrm{x} \rhd \mathrm{T}, \Gamma \vdash \mathrm{P} \rhd \Delta$ και $\Gamma \vdash \mathrm{S} \rhd \Theta$. Ο κανόνας $\Gamma \vdash \mathrm{x} \rhd \mathrm{T}$ δηλώνει πώς κατά την τυπική διατύπωση του περιβάλλοντος Γ, το όνομα x έχει τύπο T. Ο κανόνας $\Gamma \vdash P \rhd \Delta$ εκφράζει το γεγονός ότι η διεργασία P είναι καλά ορισμένη κάτω από το συγκεκριμένο περιβάλλον Γ και παράγει το περιβάλλον Δ. Στο συγκεκριμένο κανόνα, το Γ καταγράφει τους τύπους των ονομάτων της διεργασίας P και το Δ

καταγράφει τα δικαιώματα τα οποία εκτελούνται πάνω στα ονόματα που ανήκουν στο P για κάθε ένα από τους βασικούς τύπους. Τέλος, ο κανόνας $\Gamma \vdash S \rhd \Theta$ ορίζει ότι το σύστημα S είναι καλά ορισμένο στο περιβάλλον Γ και παράγει τη διεπαφή Θ η οποία καταγράφει τους συμμετέχοντες στις ομάδες όλων των συστατικών του S και τα δικαιώματα τα οποία αυτοί ασκούν πάνω σε βασικούς τύπους υπό τον ανάλογο σκοπό και συνθήκη.

5.2 Κανόνες και Αξιώματα

Παρακάτω, ορίζουμε το σύνολο των κανόνων με τους οποίος δίνεται το σύστημα των τύπων για την υποστήριξη του λογισμού της CP calculus.

$$(Name)\frac{fg(t) \subseteq \Gamma}{\Gamma \cdot x : T \ \vdash x \rhd \mathrm{T}} \qquad (\mathrm{In})\ \frac{\Gamma \cdot\ y_1 : T_1 \ldots y_N : T_N\ \vdash \mathrm{P} \rhd \Delta\ \Gamma \vdash x \rhd \mathrm{G}[\tilde{\mathrm{T}}]}{\Gamma \vdash x\big(y_1 : T_1 \ldots y_N : T_n\big).\, P \rhd \Delta \uplus \Delta^{r}_{T_{i,i=1..n}}}$$

$$(Nil)\ \Gamma \vdash 0 \rhd \emptyset, true \qquad (\mathrm{Out})\ \frac{\Gamma \vdash \mathrm{P} \rhd \Delta\ \Gamma \vdash x \rhd \mathrm{G}[\tilde{\mathrm{T}}] \Gamma \vdash y_1 \rhd T_1 \ldots y_N \rhd T_N}{\Gamma \vdash \bar{x}\langle y_1, \ldots y_N \rangle.\, \mathrm{P} \rhd \Delta \uplus \Delta^{W}_{T_{i,i=1..n}}}$$

$$(ParP)\frac{\Gamma \vdash P_1 \rhd \Delta_1\ \Gamma \vdash P_2 \rhd \Delta_2}{\Gamma \vdash P_1 | P_2 \rhd\ \Delta_1 \uplus \Delta_2} \qquad (ParS)\frac{\Gamma \vdash S_1 \rhd \Theta_1\ \Gamma \vdash S_2 \rhd \Theta_2}{\Gamma \vdash S_1 | S_2 \rhd\ \Theta_1\ ;\Theta_2}$$

$$(ResNP)\frac{\Gamma \cdot x_1 : T_1 \ldots x_N : T_N \vdash \mathrm{P} \rhd \Delta}{\Gamma \vdash (\nu\, \tilde{x}_T) P \rhd\ \Delta} \qquad (ResNS)\frac{\Gamma \cdot x_1 : T_1 \ldots x_N : T_N \vdash S \rhd \Theta}{\Gamma \vdash (\nu\, \tilde{x}_T) S \rhd\ \Theta}$$

$$(ResGP)\frac{\Gamma \cdot\ G\ \vdash \mathrm{P} \rhd \Delta}{\Gamma \vdash (\nu\ G) P\langle u \rangle \rhd \mathrm{G[u]} \oplus \Delta} \qquad (ResGS)\frac{\Gamma \cdot\ G\ \vdash \mathrm{S} \rhd \Theta}{\Gamma \vdash (\nu\ G) S \rhd \mathrm{G} \oplus \Theta}$$

$$(If)\frac{\Gamma \vdash P \rhd \Delta_1\ \Gamma \vdash \mathrm{Q} \rhd \Delta_2}{\Gamma \vdash if\ e\ then\ P\ else\ Q \rhd \Delta_1 \ominus e\ , \Delta_2\ \ominus \neg e} \qquad (Repl)\frac{\Gamma\ \vdash \mathrm{P} \rhd \Delta}{\Gamma \vdash !\, P \rhd \Delta^{!}}$$

Σχήμα 5.2: Το σύνολο των κανόνων του συστήματος των τύπων

Γράφουμε τα παρακάτω:

$$\Delta^{r}_{T} = \begin{cases} t : (\{read\}, true) & \text{εάν } T = t\ , t = t_s.t \text{ και } t_s.t \in T^n \\ t : (\{read\}, true).\, t_s : (\{identify\}, true) & \text{εάν } T = t\ , t = t_s.t \text{ και } t_s.t \in T^P \\ t : (\{read\}, true) & \text{εάν } T = t, \\ t : (\{access\}, true) & \text{εάν } T = G[\tilde{T}] \\ \emptyset & \text{διαφορετικά} \end{cases}$$

$$\Delta_T^w = \begin{cases} t\colon (\{write\}, true) & \text{εάν } T = t\,, t = t_s.t \text{ και } t_s.t \in T^n \\ t\colon (\{write\}, true).\, t_s\colon (\{identify\}, true) & \text{εάν } T = t\,, t = t_s.t \text{ και } t_s.t \in T^P \\ t\colon (\{write\}, true) & \text{εάν } T = t \\ t\colon (\{disclose\ G\}, true) & \text{εάν } T = G[\tilde{T}] \\ \emptyset & \text{διαφορετικά} \end{cases}$$

Ο τελεστής $\oplus$ ορίζεται ως εξής:

$$G[u] \oplus \left(t_1\colon (\tilde{p}_1, cond_1) \ldots t_n\colon (\tilde{p}_n, cond_n)\right) = t_1 \gg \langle G[u, cond_1], \tilde{p}_1\rangle; \ldots; t_n \gg \langle G[u, cond_n], \tilde{p}_n\rangle$$

$$G \oplus \left(t_1 \gg \langle H_1^{\downarrow}, \tilde{p}_1\rangle; \ldots t_m \gg \langle H_m^{\downarrow}, \tilde{p}_m\rangle;\right) = t_1 \gg \langle G\left[H_1^{\downarrow}\right], \tilde{p}_1\rangle; \ldots t_m \gg \langle G[H_m^{\downarrow}], \tilde{p}_m\rangle;$$

Συγκεκριμένα όταν ο τελεστής $\oplus$ εφαρμόζεται σε ένα περιβάλλον Δ με μια ομάδα G η οποία λειτουργεί για τον σκοπό u, παράγει τη διεπαφή Θ η οποία για κάθε τύπο του περιβάλλοντος Δ συλλαμβάνει την ομάδα G, το σκοπό u, και τη συνθήκη όπως αυτή προκύπτει από το ήδη παραγόμενο περιβάλλον Δ για την οποία ασκούνται τα επιμέρους δικαιώματα και αυτά έχουν προκύψει με την εφαρμογή του συστήματος των τύπων και περιλαμβάνονται και αυτά στο Δ. Στη δεύτερη περίπτωση όταν ο τελεστής $\oplus$ εφαρμόζεται σε μια ομάδα G με τη διεπαφή Θ διαθέσιμη, αυτό έχει ως αποτέλεσμα την επισύναψη της ομάδας G σε όλες τις διεπαφές ιεραρχίας του Θ. Η νέα ομάδα που ενσωματώνεται θεωρούμε ότι είναι πιο ψηλά στην ιεραρχία και είναι πρώτη από όλες τις υπόλοιπες που ανήκουν στην ιεραρχία του Θ.

Ορίζουμε τη σχέση $\uplus$ ως εξής:

$$\Delta_1 \uplus \Delta_2 = \begin{cases} t\colon (\tilde{p}_1 \cup \tilde{p}_2, cond_1)\,, t : (\tilde{p}_1, cond_1) \in \Delta_1, t : (\tilde{p}_2, cond_2) \in \Delta_2 \text{ και } cond_1 = cond_2 \\ t : (\tilde{p}_1, cond_1).\, t\colon (\tilde{p}_2, cond_2), t\colon (\tilde{p}_1, cond_1) \in \Delta_1, t : (\tilde{p}_2, cond_2) \in \Delta_2 \text{ και } cond_1 \neq cond_2 \\ t_1 : (\tilde{p}_1, cond_1).\, t_2\colon (\tilde{p}_2, cond_2), t_1\colon (\tilde{p}_1, cond_1) \in \Delta_1, t_2 : (\tilde{p}_2, cond_2) \in \Delta_2 \end{cases}$$

Η παραπάνω σχέση χρησιμοποιείται για να ενώσει δύο περιβάλλοντα Δ_1 και Δ_2, τα οποία έχουν προκύψει από την εφαρμογή του συστήματος των τύπων. Χωρίζουμε την σχέση αυτή σε τρεις περιπτώσεις. Οι πρώτες δύο αφορούν τον ίδιο βασικό τύπο και η τρίτη περίπτωση αφορά βασικούς τύπους οι οποίοι δεν είναι ίδιοι μεταξύ τους. Συγκεκριμένα ορίζουμε ότι εάν ένας βασικός τύπος ανήκει και στα δύο περιβάλλοντα υπό την ίδια συνθήκη τότε τα ασκούμενα δικαιώματα προς τον τύπο αυτό ενώνονται σε ένα ενιαίο σύνολο ενώ η συνθήκη διατηρείται στο καινούριο σύνολο. Η δεύτερη περίπτωση όπου ένας βασικός τύπος εμφανίζεται και στα δύο περιβάλλοντα αλλά με διαφορετική

συνθήκη τότε η χρήση τους σε ένα ενιαίο πλαίσιο διατηρεί την εκάστοτε συνθήκη και ασκούμενα δικαιώματα χωρίς την οποιαδήποτε μεταβολή. Η τρίτη περίπτωση όπου οι δύο βασικοί τύποι είναι ανεξάρτητοι μεταξύ τους δεν οδηγούν σε οποιαδήποτε μεταβολή ως προς το νέο περιβάλλον που θα προκύψει απλά θα ανήκουν σε ένα ενιαίο περιβάλλον ακολουθούμενος ο ένας από τον άλλο.

Ορίζουμε τον τελεστή $\ominus$, ο οποίος με τη σειρά του ενσωματώνει στο περιβάλλον Δ, τη συνθήκη για την οποία έχουν ασκηθεί τα δικαιώματα επεκτείνοντας το πεδίο των συνθηκών. Έστω το παρακάτω περιβάλλον $\Delta = \mathrm{t}_1 : (\tilde{p}_1, cond_1). \ldots . \mathrm{t}_\mathrm{n} : (\tilde{p}_n, cond_n)$ και μια έκφραση e. Η διεπαφή Δ επεκτείνεται στο πεδίο των συνθήκων για κάθε τύπο με την νέα συνθήκη η οποία αποτελεί την τομή της υπάρχουσας συνθήκης $cond_i$ με την έκφραση e. Συγκεκριμένα έστω $\Delta = t_1 : (\tilde{p}_1, cond_1). \ldots . t_n : (\tilde{p}_n, cond_n)$ και η έκφραση e. Ισχύει ότι το $cond_1 \wedge e$ είναι μια συνθήκη στην οποία ικανοποιούνται και το $cond_1$ και η έκφραση e. Ισχύει τετριμμένα $true \wedge e = e$

$$\Delta \ominus e = t_1 : (\tilde{p}_1, cond_1 \wedge e). \ldots . t_n : (\tilde{p}_n, cond_n \wedge e)$$

Περιγραφή κανόνων - αξιωμάτων του συστήματος των τύπων

Κανόνας (Name): Χρησιμοποιείται για τα ονόματα των τύπων κατά τη διατύπωση του ονόματος απαιτούμε ότι όλες οι ομάδες ονομάτων των τύπων εμφανίζονται στο σχετικό περιβάλλον που ορίζουμε Γ.

Αξίωμα (Nil): Δηλώνει ότι η τερματική διεργασία 0 θα μπορούσε να διατυπωθεί για τη διατύπωση οποιουδήποτε περιβάλλοντος τύπων και να αναφερθεί στο κενό περιβάλλον Δ στο οποίο συμπεριλαμβάνεται το κενό σύνολο δικαιωμάτων ενώ δεν ικανοποιείται καμιά συνθήκη και ως εκ τούτου συνθήκη $true$.

Κανόνας (In): Χρησιμοποιείται για να εισάγει το περιβάλλον που παράγεται από μια διεργασία με την εκτέλεση μιας ενέργειας εισόδου. Συγκεκριμένα, εάν ένα περιβάλλον Γ επεκτείνεται με το σύνολο των τύπων $y_1 : T_1 \ldots y_N : T_N$ με $n \in \mathbb{N}$, παράγοντας το περιβάλλον Δ ως το περιβάλλον που προκύπτει από μια διεργασία P, τότε μπορούμε να συμπεράνουμε ότι η διεργασία με την ενέργεια εισόδου $x(y_1 : T_1 \ldots y_N : T_n).P$ επεκτείνει το περιβάλλον Δ για κάθε τύπο που περιέχεται εντός του καναλιού x, επεκτείνοντας τα δικαιώματα για αυτούς σύμφωνα με τους κανόνες που ορίζονται από τη σχέση $\Delta_\mathrm{T}^\mathrm{r}$.

Συγκεκριμένα για κάθε τύπο $\mathrm{T_{i\,1\le i\le n}}$ με την εφαρμογή του $\Delta_{\mathrm{T}}^{\mathrm{r}}$ ισχύει ένα από τα ακόλουθα:

i. Εάν το $\mathrm{T_i}$ είναι κάποιος βασικός τύπος πεδίου δομής ο οποίος ανήκει στην κατηγορία των T^n τότε το περιβάλλον Δ επεκτείνεται με το t: $(\{read\}, true)$ από τη στιγμή που η διεργασία διαβάζει ένα αντικείμενο τύπου t το οποίο δεν μπορεί να χρησιμοποιηθεί για την ταυτοποίηση οντότητας της δομής.
ii. Εάν το $\mathrm{T_i}$ είναι κάποιος βασικός τύπος πεδίου δομής ο οποίος ανήκει στην κατηγορία των T^P τότε το περιβάλλον Δ επεκτείνεται με το t: $(\{read\}, true)$ ως προς το συγκεκριμένο τύπο και ταυτόχρονα ο τύπος της δομής επεκτείνεται με το δικαίωμα $identify\ t_s$: $(\{identify\}, true)$ αφού μόλις διαβάστηκε ένας τύπος πεδίου ο οποίος μπορεί να χρησιμοποιηθεί για την ταυτοποίηση οντότητας της δομής.
iii. Εάν το $\mathrm{T_i}$ είναι κάποιος βασικός τύπος t, όχι πεδίου t τότε το περιβάλλον Δ επεκτείνεται με το t: $(\{read\}, true)$.
iv. Εάν το $\mathrm{T_i} = \mathrm{G}[\mathrm{G}'[\widetilde{\mathrm{T}}]]$ και κάποιος βασικός τύπος $\mathrm{t} \in \widetilde{\mathrm{T}}$ τότε το περιβάλλον Δ επεκτείνεται μέσω του t: $(\{access\}, true)$
v. Το περιβάλλον Δ παραμένει ως έχει χωρίς καμιά αλλαγή σε όλες τις υπόλοιπες περιπτώσεις.

Σε όλες τις περιπτώσεις όπου το περιβάλλον επεκτείνεται με δικαιώματα αυτό γίνεται με την ικανοποίηση της συνθήκης $true$ ως προς το πεδίο των συνθηκών του εκάστοτε περιβάλλοντος. Η διαδικασία όπως είπαμε και πιο πάνω επαναλαμβάνεται για κάθε τύπο εντός του καναλιού x αναπροσαρμόζοντας το σύνολο των δικαιωμάτων για αυτούς και εφαρμόζοντας τη σχετική σχέση ⊎.

Κανόνας (Out): Παρόμοια με τον κανόνα (In) ο κανόνας του Out προσπαθεί με τη σειρά του να ενσωματώσει στη διατύπωση των τύπων τις διεργασίες οι οποίες προκύπτουν μέσα από ενέργειες εξόδου. Συγκεκριμένα, εάν στη διατύπωση του Γ μέχρι τώρα έχει παραχθεί το περιβάλλον Δ για τη διεργασία P, τότε η διεργασία αυτή με τη συμπερίληψη της ενέργειας εξόδου μέσω του καναλιού x, και συνόλου ονομάτων $y_1, \dots y_N$ $(\bar{x}\langle y_1, \dots y_N\rangle.\mathrm{P})$, επεκτείνεται βάσει του Δ_{T}^{w} για κάθε τύπο των ονομάτων $y_1, \dots y_N$. Συγκεκριμένα για κάθε τύπο $\mathrm{T_{i\,1\le i\le n}}$ με την εφαρμογή του $\Delta_{\mathrm{T}}^{\mathrm{w}}$ ισχύει ένα από τα ακόλουθα:

i. Εάν το T_i είναι κάποιος βασικός τύπος πεδίου δομής ο οποίος ανήκει στην κατηγορία των T^n τότε το περιβάλλον Δ επεκτείνεται με το t: $(\{write\}, true)$ από τη στιγμή που η διεργασία εγγράφει ένα αντικείμενο τύπου t το οποίο δεν μπορεί να χρησιμοποιηθεί για την ταυτοποίηση οντότητας της δομής.

ii. Εάν το T_i είναι κάποιος βασικός τύπος πεδίου δομής ο οποίος ανήκει στην κατηγορία των T^P τότε το περιβάλλον Δ επεκτείνεται με το t: $(\{write\}, true)$ ως προς το συγκεκριμένο τύπο και ταυτόχρονα ο τύπος της δομής επεκτείνεται με το δικαίωμα $identify$ οπόταν t_s: $(\{identify\}, true)$ αφού η διεργασία εγγράφει ένα αντικείμενο τύπου t το οποίο μπορεί να χρησιμοποιηθεί για την ταυτοποίηση μιας οντότητας της συγκεκριμένης δομής t_s.

iii. Εάν το T_i είναι κάποιος βασικός τύπος t, όχι πεδίου, τότε το περιβάλλον Δ επεκτείνεται με το t: $\{write\}, true$.

iv. Εάν το $T_i = G[G'[\tilde{T}]]$ και κάποιος βασικός τύπος $t \in \tilde{T}$ τότε το περιβάλλον Δ επεκτείνεται μέσω του t: $(\{disclose\ G\}, true)$ από τη στιγμή που η διεργασία αποκαλύπτει ένα κανάλι το οποίο περιλαμβάνει προσωπικά δεδομένα αυτού του τύπου μέσω καναλιού που ανήκει στην ομάδα G.

v. Το περιβάλλον Δ παραμένει ως έχει χωρίς καμιά αλλαγή σε όλες τις υπόλοιπες περιπτώσεις.

Σε όλες τις περιπτώσεις όπου το περιβάλλον επεκτείνεται με δικαιώματα αυτό γίνεται με την ικανοποίηση της συνθήκης $true$ ως προς το πεδίο των συνθηκών του εκάστοτε περιβάλλοντος. Η διαδικασία όπως είπαμε και πιο πάνω επαναλαμβάνεται για κάθε τύπο εντός του καναλιού x αναπροσαρμόζοντας το σύνολο των δικαιωμάτων για αυτούς εφαρμόζοντας τη σχετική σχέση ⊎.

Κανόνας (ParP): Ο κανόνας με τον οποίο δίνεται η παράλληλη λειτουργία δύο διεργασιών χρησιμοποιεί τον τελεστή ⊎ ο οποίος με τη σειρά του ενσωματώνει τα περιβάλλοντα Δ που έχουν παράξει οι δύο διεργασίες P_1 και P_2 σε ένα ενιαίο περιβάλλον το οποίο αποτελεί αποτέλεσμα της εφαρμογής του δυαδικού τελεστή σχέσης ⊎.

Κανόνας (ParS): Ο κανόνας με τον οποίο δίνεται η παράλληλη λειτουργία δύο συστημάτων χρησιμοποιείται για να συνενώσει τις δύο διεπαφές των συστημάτων που ορίζονται από δύο συστήματα το S_1 και S_2.

Κανόνας (ResNP): Ο κανόνας για τον περιορισμό ονομάτων στα πλαίσια μιας διεργασίας καθορίζει ότι εάν η διεργασία P με τη διατύπωση της ως προς το σύστημα των τύπων του περιβάλλοντος $\Gamma \cdot x_1 : T_1 \dots x_N : T_N$ παράγει το περιβάλλον Δ τότε το $(\nu\, \tilde{x}_T)P$ διατυπώνεται και αυτό στο περιβάλλον Γ, χωρίς να αλλάζει το περιβάλλον Δ.

Κανόνας (ResNS): Ο κανόνας για τον περιορισμό ονομάτων στα πλαίσια ενός συστήματος ορίζεται αντίστοιχα με τον κανόνα του $ResNP$, με τη μοναδική διαφορά ότι το σύνολο των ονομάτων περιορίζεται στο επίπεδο συστήματος, χωρίς να αλλάζει αυτή τη φορά η διεπαφή Θ.

Οι παρακάτω δύο κανόνες χρησιμοποιούνται για σκοπούς δημιουργίας των ομάδων.
Κανόνας (ResGP): Με τον παρόν κανόνα, μια διεργασία δεσμεύεται στα πλαίσια μιας ομάδας. Συγκεκριμένα έχουμε ότι, εάν η διεργασία P έχει παράξει το περιβάλλον Δ, τότε το σύστημα με την προσθήκη του κανόνα $(\nu\, G)P\langle u\rangle$ παράγει τη διεπαφή Θ η οποία ενσωματώνει το $G[u] \oplus \Delta$, με τη συμπεριφορά του τελεστή $\oplus$ να είναι αυτή που ορίζεται παραπάνω.

Κανόνας (ResGS): Αντίστοιχα με παραπάνω, ο κανόνας του $ResGP$, δεσμεύει ένα σύστημα στα πλαίσια μια ομάδας και πιο συγκεκριμένα έχουμε ότι εάν το S παράγει τη τυπική διεπαφή Θ τότε η διεργασία $(\nu G)S$ παράγει τη διεπαφή που προκύπτει ως αποτέλεσμα του $G \oplus \Theta$ με τη συμπεριφορά του τελεστή $\oplus$ να είναι αυτή που ορίζεται παραπάνω.

Κανόνας (If): Ο συγκεκριμένος κανόνας του συστήματος των τύπων προκύπτει από την υπό συνθήκη εκτέλεση μιας διεργασίας και συγκεκριμένα ορίζεται ότι αν μια διεργασία P παράγει το περιβάλλον Δ_1, όπου P η συμπεριφορά της διεργασίας στην περίπτωση που η τιμή της έκφρασης e είναι $true$ και Δ_2 το περιβάλλον που προκύπτει μέσα από την διεργασία Q και P η συμπεριφορά της διεργασίας στην περίπτωση που η τιμή της έκφρασης e είναι $false$. Τότε τα εκάστοτε Δ_1 και Δ_2 επεκτείνονται το μεν Δ_1 με $\Delta_1 \ominus$

e και το Δ_2 επεκτείνεται με $\Delta_2 \ominus \neg e$, και την συμπεριφορά του τελεστή $\ominus$, να είναι αυτή που ορίζεται παραπάνω.

Αξίωμα(Rep): Το αξίωμα αυτό χρησιμοποιείται για τις αναδρομικές διεργασίες και συγκεκριμένα διεργασίες που περιλαμβάνουν το ! P, καθορίζοντας ότι εάν το P παράγει τη διεπαφή Δ τότε και το ! P παράγει την ίδια διεπαφή Δ επαναληπτικά.

5.3 Παράδειγμα

Θα εφαρμόσουμε το προτεινόμενο σύστημα τύπων για το λογισμό της CP calculus ούτως ώστε να δούμε και σε εφαρμογή το σύνολο των παραπάνω αξιωμάτων και κανόνων.

Συγκεκριμένα θα εφαρμόσουμε έλεγχο τύπων για το μοντέλο του συστήματος του νοσοκομείου στο αντίστοιχο παράδειγμα του κεφαλαίου του λογισμού της CP calculus.

Η μοντελοποίηση του συστήματος στο λογισμό της CP calculus προηγουμένως ήταν η ακόλουθη:

$$System = (\nu Hospital)((\nu\ Nurse)N\langle diagnosis_h\rangle \mid (\nu\ Doctor)D\langle diagnosis_h\rangle)$$

$$N = pdataCh\big(x{:}\,T_{Name}, y{:}\,T_{Sex}, z{:}\,T_{Age}, w{:}\,T_{diagnosis}\big).\ \big(\nu\ d_{name}{:}\,PDATA.Name, d_{sex}{:}\,PDATA.Sex, d_{age}{:}\,PDATA.Age\big).\ \bar{x}\langle d_{name}\rangle.\bar{y}\langle d_{sex}\rangle.\bar{z}\langle d_{age}\rangle.0$$

$$D = pdataChD\big(xd{:}\,T_{Name}, yd{:}\,T_{Sex}, zd{:}\,T_{Age}, wd{:}\,T_{diagnosis}\big).\ zd(age{:}\,PDATA.Age).if\,(age \geq 18)\ then\ xd\big(name_p{:}\,PDATA.Name\big).\ \big(\nu\ d_{diagnosis}{:}\,PDATA.Diagnosis\big).\overline{wd}\,\langle d_{diagnosis}\rangle.0$$

Ισχύει η ύπαρξη των παρακάτω βασικών τύπων:

$PDATA, PDATA.Name, PDATA.Sex, PDATA.Age, PDATA.Diagnosis$

Τα σύνολα κατηγοριών βασικών τύπων πεδίων της δομής του $PDATA$ είναι:

$T^p = \{PDATA.Name\}$

$T^N = \{PDATA.Sex, PDATA.Age, PDATA.Diagnosis\}$

Συγκεκριμένα γράφουμε τα παρακάτω:

$T_{PDATA} = Hospital\left[T_{Name}, T_{Sex}, T_{Age}, T_{diagnois}\right]$

$T_{Name} = Hospital[PDATA.Name]$

$T_{Sex} = Hospital[PDATA.Sex]$

$T_{Age} = Hospital[PDATA.Age]$

$T_{Diagnosis} = Hospital[PDATA.Diagnosis]$

Για την εκτέλεση του ελέγχου τύπων θεωρείται το περιβάλλον Γ το οποίο ισούται με:

$\Gamma = pdataCh: T_{PDATA} \cdot x: T_{Name} \cdot y: T_{Sex}, z: T_{Age} \cdot w: T_{diagnosis} \cdot$

$d_{name}: PDATA.Name \cdot d_{sex}: PDATA.Sex \cdot d_{age}: PDATA.Age \cdot$

$pdataChD: T_{PDATA} \cdot xd: T_{Name} \cdot yd: T_{Sex} \cdot zd: T_{Age} \cdot wd: T_{diagnosis} \cdot$

$age: PDATA.Age \cdot name_p: PDATA.Name \cdot d_{diagnosis}: PDATA.Diagnosis$

Ξεκινούμε με τη διεργασία N για το νοσοκόμο

$N = pdataCh\big(x: T_{Name}, y: T_{Sex}, z: T_{Age}, w: T_{diagnosis}\big).$

$\big(\nu\ d_{name}: PDATA.Name, d_{sex}: PDATA.Sex, d_{age}: PDATA.Age\big).$

$\bar{x}\langle d_{name}\rangle.\, \bar{y}\langle d_{sex}\rangle.\, \bar{z}\langle d_{age}\rangle.\, 0$

και παίρνουμε τα παρακάτω:

$\Gamma \vdash 0 \rhd \emptyset, true$

$(κανόνας\ Nil)$

$\Gamma \vdash \bar{z}\langle d_{age}\rangle.\, 0 \rhd PDATA.Age: (\{write\}, true)$

$(κανόνας\ Out)$

$\Gamma \vdash \bar{y}\langle d_{sex}\rangle.\, \bar{z}\langle d_{age}\rangle.\, 0 \rhd$

$PDATA.Age: (\{write\}, true).$

$PDATA.Sex: (\{write\}, true).$

$(κανόνας\ Out)$

$\Gamma \vdash \bar{x}\langle d_{name}\rangle.\, \bar{y}\langle d_{sex}\rangle.\, \bar{z}\langle d_{age}\rangle.\, 0 \rhd$

$PDATA.Age: (\{write\}, true).$

$PDATA.Sex: (\{write\}, true).$

$PDATA.Name: (\{write\}, true).$

$PDATA: (\{identify\}, true)$

$(κανόνας\ Out)$

$\Gamma \vdash \big(\nu\ d_{name}, : PDATA.Name, d_{sex}: PDATA.Sex, d_{age}: PDATA.Age\big)$

$\bar{x}\langle d_{name}\rangle.\, \bar{y}\langle d_{sex}\rangle.\, \bar{z}\langle d_{age}\rangle.\, 0 \rhd$

$PDATA.Age: (\{write\}, true).$

$PDATA.Sex: (\{write\}, true).$

$PDATA.Name: (\{write\}, true).$

$PDATA: (\{identify\}, true)$

$(κανόνας\ ResNP)$

$\Gamma \vdash pdataCh\big(x: T_{Name}, y: T_{Sex}, z: T_{Age}, w: T_{diagnosis}\big).$

$\big(\nu\ d_{name}, : PDATA.Name, d_{sex}: PDATA.Sex, d_{age}: PDATA.Age\big)$

$\bar{x}\langle d_{name}\rangle.\, \bar{y}\langle d_{sex}\rangle.\, \bar{z}\langle d_{age}\rangle.\, 0 \rhd$

$PDATA.Age: (\{access, write\}, true).$

$PDATA.Sex: (\{access, write\}, true).$

$PDATA.Name: (\{access, write\}, true).$

$PDATA.Diagnosis: (\{access\}, true).$

$PDATA: (\{identify\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash (\nu\ Nurse)N\langle diagnosis_h\rangle \rhd$

$PDATA.Age \gg \langle Nurse[diagnosis_h, true], \{access, write\}\rangle;$

$PDATA.Sex \gg \langle Nurse[diagnosis_h, true], \{access, write\}\rangle;$

$PDATA.Name \gg \langle Nurse[diagnosis_h, true], \{access, write\}\rangle;$

$PDATA.Diagnosis \gg \langle Nurse[diagnosis_h, true], \{access\}\rangle;$

$PDATA \gg \langle Nurse[diagnosis_h, true], \{identify\}\rangle;$

$(κανόνας\ ResGP)$

Συνεχίζουμε με τη διεργασία D για το γιατρό

$D = pdataChD\big(xd: T_{Name}, yd: T_{Sex}, zd: T_{Age}, wd: T_{diagnosis}\big).$

$zd(age: PDATA.Age).\, if\,(age \geq 18)\ then\ xd\big(name_p: PDATA.Name\big).$

$\big(\nu\ d_{diagnosis}: PDATA.Diagnosis\big).\, \overline{wd}\,\langle d_{diagnosis}\rangle.\, 0$

όπου:

$\Gamma \vdash 0 \rhd \emptyset, true$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Nil)$

$\Gamma \vdash \overline{wd}\,\langle d_{diagnosis}\rangle.\,0 \rhd PDATA.Diagnosis: (\{write\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash \big(\nu\ d_{diagnosis}: PDATA.Diagnosis\big).\overline{wd}\,\langle d_{diagnosis}\rangle.\,0 \rhd$
$PDATA.Diagnosis: (\{write\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP)$

$\Gamma \vdash xd\big(name_p: PDATA.Name\big).\big(\nu\ d_{diagnosis}: PDATA.Diagnosis\big).$
$\overline{wd}\,\langle d_{diagnosis}\rangle.\,0 \rhd$
$PDATA.Diagnosis: (\{write\}, true).$
$PDATA.Name: (\{read\}, true).$
$PDATA: (\{identify\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash if\,(age \geq 18)\ then\ xd\big(name_p: PDATA.Name\big).$
$\big(\nu\ d_{diagnosis}: PDATA.Diagnosis\big).\overline{wd}\,\langle d_{diagnosis}\rangle.\,0 \rhd$
$PDATA.Diagnosis: (\{write\}, age \geq 18).$
$PDATA.Name: (\{read\}, age \geq 18).$
$PDATA: (\{identify\}, age \geq 18)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ If)$

$\Gamma \vdash zd(age: PDATA.Age).\,if\,(age \geq 18)\ then$
$xd\big(name_p: PDATA.Name\big).\big(\nu\ d_{diagnosis}: PDATA.Diagnosis\big).$
$\overline{wd}\,\langle d_{diagnosis}\rangle.\,0 \rhd$
$PDATA.Diagnosis: (\{write\}, age \geq 18).$
$PDATA.Name: (\{read\}, age \geq 18).$
$PDATA: (\{identify\}, age \geq 18).$
$PDATA.Age: (\{read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash pdataChD\big(xd: T_{Name}, yd: T_{Sex}, zd: T_{Age}, wd: T_{diagnosis}\big).$
$zd(age: PDATA.Age).\,if\,(age \geq 18)\ then$
$xd\big(name_p: PDATA.Name\big).\big(\nu\ d_{diagnosis}: PDATA.Diagnosis\big).$
$\overline{wd}\,\langle d_{diagnosis}\rangle.\,0 \rhd$

$PDATA.Diagnosis$: $(\{write\}, age \geq 18)$.

$PDATA.Name$: $(\{read\}, age \geq 18)$.

$PDATA$: $(\{identify\}, age \geq 18)$.

$PDATA.Age$: $(\{access, read\}, true)$.

$PDATA.Name$: $(\{access\}, true)$.

$PDATA.Sex$: $(\{access\}, true)$.

$PDATA.Diagnosis$: $(\{access\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash (\nu\ Doctor)D\langle diagnosis_h \rangle \rhd$

$PDATA.Diagnosis \gg \langle Doctor[diagnosis_h, age \geq 18], \{write\}\rangle$;

$PDATA.Name \gg \langle Doctor[diagnosis_h, age \geq 18], \{read\}\rangle$;

$PDATA \gg \langle Doctor[diagnosis_h, age \geq 18], \{identify\}\rangle$;

$PDATA.Age \gg \langle Doctor[diagnosis_h, true], \{access, read\}\rangle$;

$PDATA.Name \gg \langle Doctor[diagnosis_h, true], \{access\}\rangle$;

$PDATA.Sex \gg \langle Doctor[diagnosis_h, true], \{access\}\rangle$;

$PDATA.Diagnosis \gg \langle Doctor[diagnosis_h, true], \{access\}\rangle$;

$(κανόνας\ ResGP)$

Συνδυάζοντας τα παραπάνω έχουμε:

$\Gamma \vdash (\ (\nu\ Nurse)N\langle diagnosis_h \rangle$

$|(\nu\ Doctor)D\langle diagnosis_h \rangle) \rhd$

$PDATA.Age \gg \langle Nurse[diagnosis_h, true], \{access, write\}\rangle$;

$PDATA.Sex \gg \langle Nurse[diagnosis_h, true], \{access, write\}\rangle$;

$PDATA.Name \gg \langle Nurse[diagnosis_h, true], \{access, write\}\rangle$;

$PDATA.Diagnosis \gg \langle Nurse[diagnosis_h, true], \{access\}\rangle$;

$PDATA \gg \langle Nurse[diagnosis_h, true], \{identify\}\rangle$;

$PDATA.Diagnosis \gg \langle Doctor[diagnosis_h, age \geq 18], \{write\}\rangle$;

$PDATA.Name \gg \langle Doctor[diagnosis_h, age \geq 18], \{read\}\rangle$;

$PDATA \gg \langle Doctor[diagnosis_h, age \geq 18], \{identify\}\rangle$;

$PDATA.Age \gg \langle Doctor[diagnosis_h, true], \{access, read\}\rangle$;

$PDATA.Name \gg \langle Doctor[diagnosis_h, true], \{access\}\rangle$;

$PDATA.Sex \gg \langle Doctor[diagnosis_h, true], \{access\}\rangle$;

$PDATA.Diagnosis \gg \langle Doctor[diagnosis_h, true], \{access\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ParS)$

Τέλος από το σύστημα σε συντομία (S) παίρνουμε:

$\Gamma \vdash S = (\nu\ Hospital)(\ (\nu\ Nurse)N\langle diagnosis_h\rangle$

$|(\nu\ Doctor)D\langle diagnosis_h\rangle) \rhd$

$PDATA.Age \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Sex \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Name \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access\}\rangle;$

$PDATA \gg \langle Hospital[Nurse[diagnosis_h, true]], \{identify\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{write\}\rangle;$

$PDATA.Name \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{read\}\rangle;$

$PDATA \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{identify\}\rangle;$

$PDATA.Age \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access, read\}\rangle;$

$PDATA.Name \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

$PDATA.Sex \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResGS)$

Κεφάλαιο 6

Αποδείξεις Ασφάλειας και Ορθότητας

6.1 Ορθότητα και Ασφάλεια

Στο παρόν κεφάλαιο καταγράφεται το σύνολο των ορισμών, λημμάτων, θεωρημάτων και σχετικών αποδείξεων μέσω των οποίων εξασφαλίζεται ότι το προτεινόμενο πλαίσιο ελέγχου πολιτικών ιδιωτικότητας με τη χρήση τύπων χαρακτηρίζεται από ασφάλεια και αξιοπιστία.

Λήμμα 1: Αντικατάστασης (Substitution)
Εάν $\Gamma \cdot x : T \vdash P \rhd \Delta$ τότε $\Gamma \cdot y : T \vdash \{y/x\} \rhd \Delta$
Η απόδειξη προκύπτει με επαγωγή στο σύνολο των κανόνων σύνταξης διεργασιών.

Αρχίζουμε με τον καθορισμό μιας έννοιας η οποία συλλαμβάνει μια διάταξη στις διεπαφές των δικαιωμάτων που προκύπτουν από την εφαρμογή του συστήματος των τύπων. Συγκεκριμένα, ο σχεσιακός τελεστής $\preccurlyeq$ συλλαμβάνει τις αλλαγές που λαμβάνουν χώρα στη διεπαφή του περιβάλλοντος που διατυπώνεται όταν μια διεργασία εκτελέσει μια ενέργεια. Μπορούμε διαισθητικά να αντιληφθούμε το συγκεκριμένο ως εξής. Όταν εκτελείται μια ενέργεια τα ονόματα διατηρούν ή χάνουν κάποιες από τις δυνατότητες που ορίζονται για αυτές από τη διεπαφή τους η οποία προκύπτει μέσα από την τυπική διατύπωση τους. Ουδέποτε ουσιαστικά δεν πρόκυτε μια διεργασία να εκτελέσει μια ενέργεια και να λάβει περισσότερα δικαιώματα από αυτά τα οποία έχουν προκύψει από τον έλεγχο των τύπων.

Ορισμός 1: $(\Theta_1 \preccurlyeq \Theta_2)$

1. $\tilde{p}_1 \preccurlyeq \tilde{p}_2$ εάν ισχύει ότι το $\tilde{p}_1 \sqsubseteq \tilde{p}_2$.

2. $\Delta_1 \preccurlyeq \Delta_2$ εάν για κάθε t, για το οποίο ισχύει ότι $\mathrm{t} : \tilde{\mathrm{p}}_1 \in \Delta_1$, έχουμε ότι $\mathrm{t} : \tilde{\mathrm{p}}_2 \in \Delta_2$, και ταυτόχρονα ισχύει ότι $\tilde{\mathrm{p}}_1 \preccurlyeq \tilde{\mathrm{p}}_2$
3. $\Theta_1 \preccurlyeq \Theta_2$ εάν ισχύουν τα παρακάτω:
   i. $dom(\Theta_1) = do(\Theta_2)$, και
   ii. για κάθε t, για το οποίο $t \gg \langle H, \tilde{p}_1 \rangle \in \Theta_1$ έχουμε ότι $t \gg \langle H, \tilde{p}_2 \rangle \in \Theta_2$ και $\tilde{\mathrm{p}}_1 \preccurlyeq \tilde{\mathrm{p}}_2$.

Η συνάρτηση $dom(\Theta)$, επιστρέφει το σύνολο των βασικών τύπων της διεπαφής Θ.

Ορισμός 2: Η συνάρτηση $Conds(G)$

Ορίζουμε τη βοηθητική συνάρτηση $Conds(G)$ της οποίας σκοπός είναι η ομαδοποίηση του συνόλου των συνθηκών που εμφανίζονται σε κάθε τριάδα της μορφής $(cond, \tilde{p}, \widetilde{FP})$ και η οποία αναφέρεται σε μια ομάδα G στην διατύπωση μιας ιεραρχίας πολιτικής H όπου $H = G{:}\{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j\in J}$.

$$Conds(G) = \{cond_k | \ \forall_{k\in K}(cond_k, \tilde{p}_k, \widetilde{FP}_k) \text{ του } G{:}\{(cond, \tilde{p}, \widetilde{FP})\}\}$$

Ορισμός 3: Η σχέση $\rightarrow_{cond}$

Ορίζουμε την σχέση $\rightarrow_{cond}$ όπου $cond_x \rightarrow_{cond} cond_y$, με $cond_x, cond_y \in Conds$ εάν οι δύο συνθήκες δεν είναι ξένες μεταξύ τους και η συνθήκη $cond_x$ θεωρείται σημασιολογικά πιο περιοριστική ή ισοδύναμη μιας συνθήκης $cond_y$ οπόταν τα οποιαδήποτε δικαιώματα ανατίθενται ως προς τη συνθήκη $cond_y$ στην διατύπωση της πολιτικής είναι εφικτά και διαμέσου της συνθήκης $cond_x$. Ισχύει τετριμμένα ότι $cond_x \rightarrow_{cond} cond_x$. Όταν οι συνθήκες διατυπώνονται ως προς την ικανοποίηση τους ισχύει ότι:

- $cond_x \rightarrow_{cond} true$
- $cond_x \rightarrow_{cond} cond_x \vee cond_y$

Ορισμός 4

1. Έστω η ακόλουθη ιεραρχία πολιτικής $H = G{:}\{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j\in J}$ η οποία συνοδεύεται από το σκοπό u_H. Θεωρούμε την ύπαρξη ενός συνόλου $\widetilde{HP}$ το οποίο αποτελεί την ένωση δύο υποσυνόλων από διεπαφές ιεραρχίες και ασκούμενα δικαιώματα $\widetilde{HP} = \widetilde{HP}_t \cup \widetilde{HP}_f$ με το σύνολο $\widetilde{HP}_t$ να περιλαμβάνει δυάδες της μορφής $(H_i^{\downarrow}, \tilde{p}_i)$ οι οποίες προέκυψαν από την εφαρμογή του συστήματος των τύπων και αφορούν ένα βασικό τύπο δομής ή βασικό τύπο ανεξαρτήτου δομής

και το σύνολο $\widetilde{HP}_f$ να περιλαμβάνει δυάδες που έχουν ίδια μορφή όπως και αυτές του συνόλου $\widetilde{HP}_t$ αλλά αφορούν βασικούς τύπους πεδίων μιας δομής. Όταν ο τύπος είναι ανεξάρτητος δομής τότε το σύνολο $\widetilde{HP}_f = \emptyset$ και το σύνολο $\widetilde{HP}$ αποτελείται αποκλειστικά και μόνο από το σύνολο των διεπαφών ιεραρχίες και δικαιώματα του βασικού τύπου δηλαδή το σύνολο $\widetilde{HP}_t$.

Γράφουμε $\langle H, u_H \rangle \Vdash \widetilde{HP}$ εάν

a. Για κάθε διεπαφή ιεραρχίας $\mathrm{H}_{\mathrm{i}}^{\downarrow} = \mathrm{G}_1\left[\mathrm{G}_2[\ldots \mathrm{G}_n[u_i, cond_i]]\right]$ του συνόλου $\widetilde{HP}_t$ και αντίστοιχο σύνολο ασκούμενων δικαιωμάτων $\tilde{p}_i$ ισχύει ότι $\tilde{p}_i \subseteq perms_H(G_1, \ldots, G_n, u_i, cond_i)$ με $\tilde{G} = \langle G_1, \ldots, G_n \rangle$

$$perms_H(\tilde{G}, u_i, cond_i) = \begin{cases} \bigcup_{\forall k} \tilde{p}_k \bigcup \left(\bigcup_{j \in J} perms_H(\tilde{G} - G, u_i, cond_i) \right) \text{ (i)} \\ \bigcup_{j \in J} perms_H(\tilde{G} - G) \text{ (ii)} \\ \emptyset \text{ (iii)} \\ \bot \text{ (iv)} \end{cases}$$

(i) Εάν $H = G\colon \{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j \in J}, u_i = u_H, \forall k\ cond_k \in Conds(G)$ τέτοιο ώστε $cond_i \rightarrow_{cond} cond_k, G \in \tilde{G}$

(ii) Εάν $H = G\colon \{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j \in J}, u_i \neq u_H$ ή $\nexists\ cond_k \in Conds(G)$ τέτοιο ώστε $cond_i \rightarrow_{cond} cond_k, G \in \tilde{G}$

(iii) Εάν $H = \varepsilon$

(iv) Εάν $H = G\colon \{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j \in J}, G \notin \tilde{G}, \tilde{G} \neq \varepsilon$

b. Χωρίζουμε το σύνολο του $\widetilde{HP}_f$ σε υποσύνολα που περιέχουν διεπαφές ιεραρχίες και ασκούμενα δικαιώματα που αφορούν κάθε βασικό τύπο πεδίου μιας δομής $t_s.t$, και προκύπτουν σύνολα της μορφής $\widetilde{HP}_{f_l}$ για κάθε βασικό τύπο $t_s.t_{l,l \in L}$ ενός βασικού τύπου t_s. Πρέπει επίσης να ισχύει ότι: Για κάθε διεπαφή ιεραρχίας $H_{l,i}^{\downarrow} = \mathrm{G}_1[\mathrm{G}_2[\ldots \mathrm{G}_n[u_{l,i}, cond_{l,i}]]]$ κάθε συνόλου $\widetilde{HP}_{f_l}$ για βασικό τύπο πεδίου δομής $t_s.t_{l,l \in L}$ και ασκούμενα δικαιώματα $\tilde{p}_{l,i}$, ισχύει ότι $\tilde{p}_{l,i} \subseteq perms_{HFP_l}(G_1, \ldots, G_n, u_{l,i}, cond_{l,i})$ με $\tilde{G} = \langle G_1, \ldots, G_n \rangle$

$$perms_{HFP_l}(\tilde{G}, u_{l,i}, cond_{l,i}) = \begin{cases} \bigcup_{\forall k} \tilde{p}_{f_{k,l}} \bigcup \left(\bigcup_{j \in J} perms_{HFP}(\tilde{G} - G, u_{l,i}, cond_{l,i}) \right) \text{ (i)} \\ \bigcup_{j \in J} perms_{HFP}(\tilde{G} - G) \text{ (ii)} \\ \emptyset \text{ (iii)} \\ \perp \text{ (iv)} \end{cases}$$

(i) Εάν $H = G: \{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j \in J}, u_{l,i} = u_H, \forall k \; cond_k \in Conds(G)$

τέτοιο ώστε $cond_{l,i} \rightarrow_{cond} cond_k, G \in \tilde{G}, t_s.t_l : \tilde{p}_{f_{k,l}} \in \widetilde{FP}_k, G \in \tilde{G}$

(ii) Εάν $H = G: \{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j \in J}, u_i \neq u_H$ ή $\nexists \; cond_k \in Conds(G)$

τέτοιο ώστε $cond_i \rightarrow_{cond} cond_k \,, t_s.t_l : \tilde{p}_{f_{k,l}} \in \widetilde{FP}_k, G \in \tilde{G}$

(iii) Εάν $H = \varepsilon$

(iv) Εάν $H = G: \{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j \in J}, G \notin \tilde{G}, \tilde{G} \neq \varepsilon$

Σημείωση: Το σημείο b. ικανοποιείται τετριμμένα όταν $\widetilde{HP}_f = \emptyset$.

2. Έστω μια πολιτική ιδιωτικότητας η οποία συμβολικά δίνεται μέσα από το $\mathcal{P}$ και μια διεπαφή τύπων Θ. Η διεπαφή Θ ικανοποιεί την πολιτική $\mathcal{P}$, γράφοντας $\mathcal{P} \Vdash \Theta$, αν:

$$\frac{\langle H, u_H \rangle \Vdash \widetilde{HP} \qquad \mathcal{P} \Vdash \Theta}{t \gg \langle H, u_H \rangle; P \Vdash t \gg \langle H_i^{\downarrow}, \tilde{p}_l \rangle; \wedge \, t_s.t_l \gg \langle H_{l,i}^{\downarrow}, \tilde{p}_{l.i} \rangle; \Theta} \qquad \mathcal{P} \Vdash \emptyset$$

$$\forall_{i \in I} \left(H_i^{\downarrow}, \tilde{p}_l \right) \in \widetilde{HP}_t \wedge \forall_{l \in L} \forall_{i \in I} (H_{l,i}^{\downarrow}, \tilde{p}_{l.i}) \in \widetilde{HP}_f, \widetilde{HP} = \widetilde{HP}_t \cup \widetilde{HP}_f$$

Σύμφωνα με το παραπάνω, ισχύουν τα ακόλουθα αναφορικά με τις συνθήκες ικανοποίησης μιας πολιτικής. $\langle H, u_H \rangle \Vdash \widetilde{HP}$ με το σύνολο $\widetilde{HP}$ να αναφέρεται στο σύνολο των διεπαφών ιεραρχίας που έχουν προκύψει από την εφαρμογή του συστήματος των τύπων για ένα βασικό τύπο t και αντίστοιχα σύνολα από ασκούμενα δικαιώματα που αφορούν τον ίδιο το βασικό τύπο αλλά και βασικούς τύπους πεδίων του όταν αυτός αναφέρεται σε βασικό τύπο δομής. Για κάθε βασικό τύπο και αντίστοιχη διεπαφή από το σύνολο του $\widetilde{HP}_t$, που αφορά το βασικό τύπο υπολογίζουμε το σύνολο των δικαιωμάτων που επιτρέπονται μέσω της πολιτικής για όλες τις ομάδες της διεπαφής. Ο υπολογισμός γίνεται στο σημείο a. με τη χρήση της συνάρτησης $perms_H(G_1, \dots, G_n, u_i, cond_i)$. Όσον αφορά το σημείο b. μετά τον υπολογισμό αντίστοιχων συνόλων από διεπαφές και δικαιώματα για κάθε βασικό τύπο πεδίου μιας δομής όταν αυτά υπάρχουν γίνεται ο υπολογισμός του συνόλου των επιτρεπτών δικαιωμάτων για κάθε βασικό τύπο πεδίου

μιας δομής και διεπαφή ιεραρχίας με τη χρήση μιας παρόμοιας συνάρτησης της $perms_{HFP_l}(G_1, \dots, G_n, u_{l,i}, cond_{l,i})$. Επιθυμούμε όπως για σκοπούς ικανοποίησης της πολιτικής κάθε φορά τα ασκούμενα δικαιώματα είναι υποσύνολο αυτών που επιτρέπονται από την πολιτική ιδιωτικότητας και προκύπτουν από τον υπολογισμό των παραπάνω συναρτήσεων. Σε μια τέτοια περίπτωση όταν τα σημεία a. και b. Ικανοποιούνται, η ιεραρχία της πολιτικής με την ανάθεση του σκοπού ικανοποιείται από τις διεπαφές ιεραρχίας και τα αντίστοιχα σύνολα διεπαφών ιεραρχίας με ασκούμενα δικαιώματα οπόταν η ανάθεση της ιεραρχίας της πολιτικής και του σκοπού ως προς τον βασικό τύπο ικανοποιείται από μια διεπαφή η οποία περιλαμβάνει την ανάθεση όλων των διεπαφών και δικαιωμάτων του συνόλου $\widetilde{HP}$ τόσο για βασικό τύπο όσο και κάθε εσωτερικού πεδίου του.

Η σχέση ικανοποίησης προκύπτει άμεσα από τα παραπάνω επαναλαμβάνοντας την διαδικασία για κάθε βασικό τύπο και αντίστοιχη παραγόμενη διεπαφή. Ο υπολογισμός των δικαιωμάτων και στις δύο περιπτώσεις συναρτήσεων συνοδεύεται από τον έλεγχο του κατά πόσο οι ομάδες της διεπαφής ιεραρχίας είναι συμβατές με αυτές της πολιτικής. Οι συναρτήσεις δεν ορίζονται αν σε οποιοδήποτε σημείο της ιεραρχίας των δικαιωμάτων της πολιτικής η ομάδα για την οποία παραχωρούνται τα δικαιώματα δεν εμφανίζεται στο σύνολο των ομάδων της ιεραρχίας της διεπαφής. Ως προς τον υπολογισμό των επιμέρους δικαιωμάτων αυτός προκύπτει ως εξής. Όταν η ομάδα της ιεραρχίας της πολιτικής για την οποία γίνεται ο έλεγχος ανήκει στο σύνολο των ομάδων της διεπαφής και η συνθήκη της διεπαφής υπό εξέταση συνεπάγεται μια συνθήκη της ιεραρχίας ικανοποιώντας τη σχέση $\rightarrow_{cond}$ τότε ανατίθενται μέσω της συνάρτησης υπολογισμού τα αντίστοιχα δικαιώματα. Αυτό γίνεται και στις δύο περιπτώσεις συναρτήσεων και τα δικαιώματα ανατίθενται για κάθε συνθήκη που ικανοποιεί την σχέση $\rightarrow_{cond}$. Στην περίπτωση όπου η συνεπαγωγή δεν ορίζεται για καμιά συνθήκη της πολιτικής ή ο σκοπός της διεπαφής δεν είναι ο ίδιος με αυτό της ιεραρχίας ο υπολογισμός συνεχίζεται για την επόμενη ομάδα της διεπαφής.

Έτσι στο σημείο 2 του παρόντος ορισμού καταγράφουμε την ικανοποίηση μιας πολιτικής ιδιωτικότητας $\mathcal{P}$ από μια παραγόμενη διεπαφή Θ ενός συστήματος ορίζοντας ότι $\mathcal{P} \Vdash \Theta$, εάν για κάθε βασικό τύπο της πολιτικής και ανάθεση του ως προς τον σκοπό u_H και ιεραρχία δικαιωμάτων Η αυτός ικανοποιείται από μια παραγόμενη διεπαφή που

περιλαμβάνει τις διεπαφές ιεραρχίας που αφορούν τον ίδιο το βασικό τύπο αλλά και κάθε βασικό τύπο πεδίου ο οποίος συναντάται εντός της ιεραρχίας Η.

Από το παραπάνω ορισμό και τον τελεστή $\preccurlyeq$ προκύπτει άμεσα το Αποτέλεσμα 1.

Αποτέλεσμα 1

Εάν $\mathcal{P} \Vdash \Theta_1$ και $\Theta_2 \preccurlyeq \Theta_1$ τότε $\mathcal{P} \Vdash \Theta_2$.

Ορισμός 5: Η συνάρτηση $\pi(cond, G, T)$

Ορίζουμε τη βοηθητική συνάρτηση $\pi(cond, G, T)$ της οποίας σκοπός είναι η ομαδοποίηση των επιτρεπτών δικαιωμάτων που ορίζονται για μια συνθήκη $cond$ και ομάδα G στα πλαίσια μιας ιεραρχίας πολιτικής $H = G: \{(cond, \tilde{p}, \widetilde{FP})\}[H_j]_{j \in J}$ και αφορούν ένα βασικό τύπο διαχωρίζοντας περιπτώσεις βασικών τύπων πεδίων και ανεξάρτητων δομής ή δομής. Χρησιμοποιούμε από τον Ορισμό 3 τη σχέση $\rightarrow_{cond}$ και από τον Ορισμό 2 τη συνάρτηση $Conds(G)$ ενώ η συνάρτηση $\pi(cond, G, t)$ ορίζεται ως εξής. Δεδομένης μιας ιεραρχίας πολιτικής $H = G: \{(cond_k, \tilde{p}_k, \widetilde{FP}_k)\}[H_j]_{j \in J}$

$$\pi(cond, G, T) = \begin{cases} \bigcup_{\forall k} \tilde{p}_k,\ cond \rightarrow_{cond} cond_k \ και\ cond_k \in Conds(G), T = t \text{ ή } t_s \\ \bigcup_{\forall k} \tilde{p}_f,\ cond \rightarrow_{cond} cond_k \ και\ cond_k \in Conds(G), T = t_s.t, t_s.t : \tilde{p}_f \in \widetilde{FP}_k \end{cases}$$

Η βοηθητική συνάρτηση $\pi(cond, G, T)$ ορίζεται και λειτουργά βάσει δύο περιπτώσεων. Από την μια καταφέρνει να ομαδοποιήσει δικαιώματα που αφορούν ένα βασικό τύπο δομής ή ανεξάρτητου δομής και τα οποία προκύπτουν μέσω του συνόλου δικαιωμάτων $\tilde{p}_k$. Η συλλογή των δικαιωμάτων αυτών γίνεται για κάθε δυνατή συνθήκη και αντίστοιχο σύνολο δικαιωμάτων η οποία ικανοποιεί την σχέση $\rightarrow_{cond}$. Η δεύτερη περίπτωση ομαδοποίησης συνθηκών προκύπτει ως προς κάποιο βασικό τύπο πεδίου δομής οπόταν τα δικαιώματα που ομαδοποιούνται ανήκουν στο σύνολο του $\tilde{p}_f$.

Ορισμός 6: Ικανοποίηση μιας πολιτικής ιδιωτικότητας (Policy Satisfaction)

Έστω $\mathcal{P} : \diamond$. Λέμε ότι το σύστημα S ικανοποιεί την πολιτική ιδιωτικότητας $\mathcal{P}$ και γράφουμε $\mathcal{P} \vdash S$, εάν $\Gamma \vdash S \rhd \Theta$ για κάποιο περιβάλλον Γ και διεπαφή Θ για την οποία ισχύει $\mathcal{P} \Vdash \Theta$.

Προχωρούμε με τον καθορισμό της έννοιας μιας εσφαλμένης διεργασίας η οποία διασαφηνίζει την έννοια της ικανοποίησης των πολιτικών ιδιωτικότητας από υποψήφια συστήματα και διεργασίες αυτών.

Ορισμός 7: Εσφαλμένη Διεργασία (Error Process)
Έστω η πολιτική $\mathcal{P}$, το περιβάλλον Γ και το παρακάτω σύστημα S.

$$S \equiv (\nu\ G_1)(\nu\ x_1 \colon \mathrm{T}_1)(\ldots((\nu\ G_n)(\nu\ x_n \colon \mathrm{T}_n)P\langle u\rangle \mid Q\langle u'\rangle \mid S_n) \ldots \mid S_1)$$

Το σύστημα S, είναι μια εσφαλμένη διεργασία ως προς την πολιτική ιδιωτικότητας $\mathcal{P}$ και το περιβάλλον Γ, εάν υπάρχει κάποιος βασικός τύπος $\mathcal{P} = t \gg \langle H, u\rangle\ ; \mathcal{P}'$ ή βασικός τύπος πεδίου $t_s.t$ εντός της ιεραρχίας δικαιωμάτων H για τον οποίο συμβαίνει τουλάχιστον ένα από τα ακόλουθα. Ισχύει ότι $\tilde{G} = \langle G_1, \ldots, G_n\rangle$. Για τους κανόνες 1 έως 5 θεωρούμε ότι ο σκοπός ιεραρχίας είναι ίδιος με το σκοπό λειτουργίας της P.

1. Δικαίωμα $read$ - Ισχύει ένα από τα παρακάτω
   - $read \notin \bigcup_{G\in\tilde{G}}\ \pi(true, G, T)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], y \colon T \in \tilde{y}_T$, όπου $T \in \{t, t_s.t\}$ και $P = x(\tilde{y}_T).P'$ ή

   - $read \notin \bigcup_{G\in\tilde{G}}\ \pi(cond, G, T)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], y \colon T \in \tilde{y}_T$, όπου $T \in \{t, t_s.t\}, cond = e, [\![e]\!] = true$
     και $P = if\,(e)\ then\ x(\tilde{y}_T).P'$ ή

   - $read \notin \bigcup_{G\in\tilde{G}} \pi(\neg cond, G, T)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], y \colon T \in \tilde{y}_T$, όπου $T \in \{t, t_s.t\}, cond = e, [\![e]\!] = false$
     και $P = if\,(e)\ then\ Q\ else\ x(\tilde{y}_T).P'$

2. Δικαίωμα $write$ – Ισχύει ένα από τα παρακάτω
   - $write \notin \bigcup_{G\in\tilde{G}}\ \pi(true, G, T)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], y \colon T$ όπου $T \in \{t, t_s.t\}, y \in \tilde{y}$, και $P = \bar{x}\langle\tilde{y}\rangle.P'$ ή

   - $write \notin \bigcup_{G\in\tilde{G}}\ \pi(cond, G, T)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], y \colon T$ όπου $T \in \{t, t_s.t\}, y \in \tilde{y}$,

$cond = e, [\![e]\!] = true$ και $P = if(e)\ then\ \bar{x}\langle\tilde{y}\rangle.P'$ ή

- $write \notin \bigcup_{G\in\tilde{G}} \pi(\neg cond, G, T)$ και $\exists x, y$ τέτοια ώστε
  $\Gamma \vdash x \rhd G[\tilde{T}], y{:}\,T$, όπου $T \in \{t, t_s.t\}, y \in \tilde{y}$,
  $cond = e, [\![e]\!] = false$ και $P = if(e)\ then\ Q\ else\ \bar{x}\langle\tilde{y}\rangle.P'$

3. Δικαίωμα $access$ – Ισχύει ένα από τα παρακάτω
   - $access \notin \bigcup_{G\in\tilde{G}} \pi(true, G, T)$ και $\exists x$ τέτοιο ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], \mathrm{T} \in \widetilde{\mathrm{T}}$, όπου $T \in \{t, t_s.t\}, x{:}\,\mathrm{G}\left[\widetilde{\mathrm{T}}\right] \in \tilde{x}_T$
     και $P = y(\tilde{x}_T).P'$ ή

   - $access \notin \bigcup_{G\in\tilde{G}} \pi(cond, G, T)$ και $\exists x$ τέτοιο ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], \mathrm{T} \in \widetilde{\mathrm{T}}$, όπου $T \in \{t, t_s.t\}, x{:}\,\mathrm{G}\left[\widetilde{\mathrm{T}}\right] \in \tilde{x}_T$,
     $cond = e, [\![e]\!] = true$ και $P = if(e)\ then\ y(\tilde{x}_T).P'$ ή

   - $access \notin \bigcup_{G\in\tilde{G}} \pi(\neg cond, G, T)$ και $\exists x$ τέτοιο ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], \mathrm{T} \in \widetilde{\mathrm{T}}$, όπου $T \in \{t, t_s.t\}, x{:}\,\mathrm{G}\left[\widetilde{\mathrm{T}}\right] \in \tilde{x}_T$,
     $cond = e, [\![e]\!] = false$ και $P = if(e)\ then\ Q\ else\ y(\tilde{x}_T).P'$

4. Δικαίωμα $disclose\ G'$ – Ισχύει ένα από τα παρακάτω
   - $disclose\ G' \notin \bigcup_{G\in\tilde{G}} \pi(true, G, T)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], \Gamma \vdash y \rhd \mathrm{G}'\left[\mathrm{G}\left[\widetilde{\mathrm{T}}\right]\right], \mathrm{T} \in \widetilde{\mathrm{T}}$, όπου $T \in \{t, t_s.t\}$,
     $x \in \tilde{x}$ και $P = \bar{y}\langle\tilde{x}\rangle.P'$ ή

   - $disclose\ G' \notin \bigcup_{G\in\tilde{G}} \pi(cond, G, t)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], \Gamma \vdash y \rhd \mathrm{G}'\left[\mathrm{G}\left[\widetilde{\mathrm{T}}\right]\right], \mathrm{T} \in \widetilde{\mathrm{T}}$, όπου $T \in \{t, t_s.t\}$,
     $x \in \tilde{x}\ , cond = e, [\![e]\!] = true$ και $P = if(e)\ then\ \bar{y}\langle\tilde{x}\rangle.P'$ ή

   - $disclose\ G' \notin \bigcup_{G\in\tilde{G}} \pi(\neg cond, G, t)$ και $\exists x, y$ τέτοια ώστε
     $\Gamma \vdash x \rhd G[\tilde{T}], \Gamma \vdash y \rhd \mathrm{G}'\left[\mathrm{G}\left[\widetilde{\mathrm{T}}\right]\right], \mathrm{T} \in \widetilde{\mathrm{T}}$, όπου $T \in \{t, t_s.t\}$,
     $x \in \tilde{x}\ , cond = e, [\![e]\!] = false$ και $P = if(e)\ then\ Q\ else\ \bar{y}\langle\tilde{x}\rangle.P'$

5. Δικαίωμα $identify$ – Ισχύει ένα από τα παρακάτω
   - $identify \notin \bigcup_{G \in \tilde{G}} \pi(true, G, t_s)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t \in \tilde{y}_T, t_s.t \in T^p$ και $P = x(\tilde{y}_T).P'$ ή
   - $identify \notin \bigcup_{G \in \tilde{G}} \pi(cond, G, t_s)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t \in \tilde{y}_T, t_s.t \in T^p, cond = e, [\![e]\!] = true$ και $P = if(e)\ then\ x(\tilde{y}_T).P'$ ή
   - $identify \notin \bigcup_{G \in \tilde{G}} \pi(\neg cond, G, t_s)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t \in \tilde{y}_T, t_s.t \in T^p, cond = e, [\![e]\!] = false$ και $P = if(e)\ then\ Q\ else\ x(\tilde{y}_T).P'$ ή
   - $identify \notin \bigcup_{G \in \tilde{G}} \pi(true, G, t_s)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t, y \in \tilde{y}, t_s.t \in T^p$ και $P = \bar{x}\langle\tilde{y}\rangle.P'$ ή
   - $identify \notin \bigcup_{G \in \tilde{G}} \pi(cond, G, t_s)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t, y \in \tilde{y}, t_s.t \in T^p, cond = e, [\![e]\!] = true$ και $P = if(e)\ then\ \bar{x}\langle\tilde{y}\rangle.P'$ ή
   - $identify \notin \bigcup_{G \in \tilde{G}} \pi(\neg cond, G, t_s)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t, y \in \tilde{y}, t_s.t \in T^p, cond = e, [\![e]\!] = false$ και $P = if(e)\ then\ Q\ else\ \bar{x}\langle\tilde{y}\rangle.P'$

6. Εάν ο σκοπός u σύμφωνα με τον οποίο ορίζεται μια διεργασία P είναι διαφορετικός από αυτό της ιεραρχίας της πολιτικής τότε η διεργασία αυτή αποτελεί εσφαλμένη διεργασία εάν εφαρμόζει οποιοδήποτε ενέργεια πάνω σε οποιοδήποτε τύπο υπό οποιαδήποτε συνθήκη.

Ο διαχωρισμός των κανόνων είναι ο εξής. Οι κανόνες (1-5) ελέγχουν συστήματα στα οποία ο σκοπός λειτουργίας των διεργασιών είναι συμβατός με αυτό της ιεραρχίας της πολιτικής οπόταν προκύπτει λανθασμένη συμπεριφορά εντός των διεργασιών λόγω των συνθηκών. Ο κανόνας 6 αφορά περιπτώσεις όπου ο σκοπός των διεργασιών είναι

διαφορετικός από αυτό ο οποίος ορίζεται από την ιεραρχία της πολιτικής, έτσι προκύπτει εσφαλμένη διεργασία μέσω του σκοπού λειτουργίας μιας διεργασίας. Οι κανόνες (1) και (2) εσφαλμένης διεργασίας αφορούν τα δικαιώματα ανάγνωσης και εγγραφής ενός βασικού τύπου αντίστοιχα και αφορούν ενέργειες που εφαρμόζονται κατευθείαν σε κάποιο βασικό τύπο ο οποίος μεταφέρεται μέσω κάποιου ονόματος στις πλειάδες εγγραφής και ανάγνωσης καταγράφοντας το γεγονός ότι εάν μια διεργασία συγκεκριμένης ομάδας δεν εξασφαλίζει το δικαίωμα ανάγνωσης ή εγγραφής ενός βασικού τύπου T είτε αυτός αναφέρεται σε βασικό τύπο t είτε σε βασικό τύπο πεδίου δομής $t_s.t$, σε οποιοδήποτε σημείο της ιεραρχίας της για οποιαδήποτε εκ των τριών περιπτώσεων συνθηκών δηλαδή χωρίς συνθήκη $(true)$, στην ικανοποίηση μιας συνθήκης $(cond)$ και στην μη ικανοποίηση μιας συνθήκης $(\neg cond)$ τότε αναμένετε να μην εμφανίζει την ενέργεια εισόδου και εξόδου αντίστοιχα όταν εργάζεται υπό τον σκοπό της πολιτικής. Όταν η συνθήκη αναφέρεται στην συνθήκη $true$ τότε δεν αναμένουμε να εμφανιστεί η ενέργεια εισόδου και εξόδου αντίστοιχα, σε οποιοδήποτε σημείο της διεργασίας και χωρίς τη χρήση του τελεστή if. Στις περιπτώσεις ικανοποίησης μιας συνθήκης όταν γίνεται ο υπολογισμός των δυνατών δικαιωμάτων που επιτρέπονται στην κάθε περίπτωση συνθήκης, μια διεργασία αναμένετε να μην εμφανίσει τελεστή εισόδου και εξόδου ο οποίος με την ικανοποίησης της έκφρασης που αφορά την συνθήκη της πολιτικής να εκτελεί τις ενέργειες εισόδου και εξόδου στο κομμάτι της υπό ικανοποίησης εκτέλεσης διεργασιών όταν χρησιμοποιείται ο τελεστής if. Το ίδιο με το παραπάνω εφαρμόζεται και στις περιπτώσεις όπου υπολογίζονται τα δικαιώματα για τη μη ικανοποίηση οποιασδήποτε συνθήκης και οι ενέργειες εμφανίζονται στο κομμάτι της μη ικανοποίησης μιας συνθήκης του τελεστή if.

Οι κανόνες (3) και (4) εσφαλμένης διεργασίες προκύπτουν παρόμοια με τα παραπάνω και αφορούν τα δικαιώματα πρόσβασης και αποκάλυψης με την διαφορά ότι ελέγχουν ενέργειες όπου γίνεται εγγραφή και ανάγνωση καναλιών τα οποία εσωτερικά περιέχουν κάποιο όνομα που αναφέρεται σε βασικό τύπο. Ο κανόνας (5) αφορά το δικαίωμα της ταυτοποίησης το οποίο προκύπτει αποκλειστικά και μόνο για ένα βασικό τύπο δομής και ορίζει ότι η ενέργεια εισόδου ή εξόδου ενός βασικού τύπου πεδίου δομής που ανήκει στην κατηγορία των T^p σε οποιαδήποτε περίπτωση συνθήκης και αντίστοιχη συμπεριφορά δεν πρέπει να εμφανίζεται εάν το δικαίωμα αυτό δεν εντοπίζεται στην σχετική ιεραρχία δικαιωμάτων βάση συνθήκης για το βασικό τύπο της δομής. Ο κανόνας

(6) έρχεται να ολοκληρώσει την διατύπωση των κανόνων εσφαλμένης διεργασίας και αναφέρεται στις περιπτώσεις όπου ο σκοπός για τον οποίο ορίζεται η συμπεριφορά μιας διεργασίας είναι διαφορετικός από αυτόν στον οποίο ορίζεται η ιεραρχία των δικαιωμάτων για κάποιος βασικούς τύπους τότε δεν αναμένεται να εμφανίσει την οποιαδήποτε συμπεριφορά η οποία να επιτρέπει ενέργειες σε βασικούς τύπους που ανήκουν στην ιεραρχία Η.

Λήμμα 2: Ασφάλεια Τύπων (Type Safety)

Έστω ένα σύστημα S το οποίο είναι μια εσφαλμένη διεργασία σε σχέση με μια καλά ορισμένη πολιτική ιδιωτικότητας $\mathcal{P}$ και ενός περιβάλλοντος Γ. Εάν το $\Gamma \vdash S \rhd \Theta$ προφανώς $\mathcal{P} \Vdash \Theta$.

Απόδειξη:

Από τον ορισμό μιας εσφαλμένης διεργασίας

$$S \equiv (\nu\ G_1)(\nu\ x_1 \colon \mathrm{T}_1)(\ldots.((\nu\ G_n)(\nu\ x_n \colon \mathrm{T}_n)P\langle u\rangle \mid Q\langle u'\rangle \mid S_n) \ldots \mid S_1)$$

Το σύστημα S, είναι μια εσφαλμένη διεργασία ως προς την πολιτική ιδιωτικότητας $\mathcal{P}$ και το περιβάλλον Γ, εάν υπάρχει κάποιος βασικός τύπος $\mathcal{P} = t \gg \langle H, u\rangle\ ; \mathcal{P}'$ ή βασικός τύπος πεδίου $t_s.t$ εντός της ιεραρχίας δικαιωμάτων H, ισχύει ότι $\tilde{G} = \langle G_1, \ldots, G_n\rangle$, για τον οποίο μπορεί να συμβαίνει ένας από τους έξι κανόνες. Οι πρώτοι πέντε αφορούν ενέργειες και δικαιώματα που προκύπτουν βάση συνθήκης και εσωτερικά χωρίζονται σε έξι πιθανές περιπτώσεις ενώ ο τελευταίος κανόνας αναφέρεται στο σκοπό εκτέλεσης μιας διεργασίας. Αποδεικνύουμε τη περίπτωση του δικαιώματος $read$ ενώ οι υπόλοιπες περιπτώσεις δικαιωμάτων και κανόνες (2)(3)(4) μέχρι και το κανόνα (5) ταυτοποίησης είναι οι ίδιες. Αποδεικνύουμε τους κανόνες (5) και (6) εσφαλμένης διεργασίας ξεχωριστά.

1. Έστω ότι $read \notin \bigcup_{G \in \tilde{G}} \pi(true, G, T)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y \colon T \in \tilde{y}_T, T = t$ και $P = x(\tilde{y}_T).P'$. Για να είμαστε σε θέση να έχουμε ένα περιβάλλον Δ για τη διεργασία P θα πρέπει στο τελευταίο βήμα να χρησιμοποιήσαμε το κανόνα του συστήματος των τύπων (In) για να μπορέσουμε να συμπεράνουμε ότι για κάποιο τύπο $t\ \Gamma \vdash P = x(\tilde{y}_T).P' \rhd \Delta \uplus \{t \colon (\{read\}, true)\}$. Με μια σειρά εφαρμογή των κανόνων $(ParP), (ParS)$ και $(ResGP), (ResGS)$ θα είχαμε κατασκευάσει μια διεπαφή δικαιωμάτων Θ για το σύστημα S το οποίο θα δώσει για το

τύπο t, $\Gamma \vdash S \rhd \Theta'; t \gg \langle G_1[\dots G_n[u, true], \{read \cup \tilde{p}\}\rangle$ και ένα σύνολο δικαιωμάτων $\tilde{p}$. Ωστόσο κάτι τέτοιο θα έδινε μια διεπαφή η οποία δεν συμβαδίζει με την ιεραρχία και σκοπό της πολιτικής οπόταν $\langle H, u_H\rangle \nVdash \widetilde{HP}$ και έτσι $P \nVdash \Theta$. Η περίπτωση αναφορικά με ένα βασικό τύπο πεδίου $t_s.t, T = t_s.t$, το δικαίωμα $read$ και συνθήκη $true$ προκύπτει με τον ίδιο τρόπο ομαδοποιώντας επιτρεπτά δικαιώματα βάση του τύπου του πεδίου.

Έστω ότι $read \notin \bigcup_{G\in\tilde{G}} \pi(cond, G, T)\ cond = e, [\![e]\!] = true$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y{:}\, T \in \tilde{y}_T,\ T = t$ και $P = if(e)\ then\ x(\tilde{y}_T).P'$. Για να είμαστε σε θέση να έχουμε ένα περιβάλλον Δ για τη διεργασία P θα πρέπει κατά την ανάγνωση του στο κανάλι x να χρησιμοποιήσαμε το κανόνα του συστήματος των τύπων (In) για να μπορέσουμε να συμπεράνουμε ότι για το τύπο $t, \Gamma \vdash P = x(\tilde{y}_T).P' \rhd \Delta \uplus \{t{:}\, (\{read\}, true)\}$ και τέλος να εφαρμόσουμε το κανόνα του συστήματος των τύπων (If) ο οποίος για το βασικό τύπο $t, \Gamma \vdash P = if(e)\ then\ x(\tilde{y}_T).P' \rhd\ t{:}\, (\{read\}, true \wedge e)$. Με μια σειρά εφαρμογή των κανόνων $(ParP), (ParS)$ και $(ResGP), (ResGS)$ θα είχαμε κατασκευάσει μια διεπαφή δικαιωμάτων Θ για το σύστημα S το οποίο θα δώσει $\Gamma \vdash S \rhd \Theta'; t \gg \langle G_1[\dots G_n[u, cond], \{read \cup \tilde{p}\}\rangle$ όπου $cond = e \wedge true = e$ για ένα σύνολο δικαιωμάτων $\tilde{p}$. Ωστόσο κάτι τέτοιο θα έδινε μια διεπαφή η οποία δεν συμβαδίζει με την ιεραρχία και σκοπό της πολιτικής οπόταν $\langle H, u_H\rangle \nVdash \widetilde{HP}$ και έτσι $P \nVdash \Theta$. Η περίπτωση αναφορικά με ένα βασικό τύπο πεδίου $t_s.t, T = t_s.t$, το δικαίωμα $read$ και οποιαδήποτε συνθήκη ικανοποίησης $cond$ προκύπτει με τον ίδιο τρόπο ομαδοποιώντας επιτρεπτά δικαιώματα βάση του τύπου του πεδίου.

Έστω ότι $read \notin \bigcup_{G\in\tilde{G}} \pi(\neg cond, G, T)\ cond = e, [\![e]\!] = false$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y{:}\, T \in \tilde{y}_T, T = t$, και η διεργασία P ορίζεται ως $P = if(e)\ then\ Q\ else\ x(\tilde{y}_T).P'$. Για να είμαστε σε θέση να έχουμε ένα περιβάλλον Δ για τη διεργασία P θα πρέπει κατά την ανάγνωση του στο κανάλι x να χρησιμοποιήσαμε το κανόνα του συστήματος των τύπων (In) για να μπορέσουμε να συμπεράνουμε ότι $, \Gamma \vdash P = x(\tilde{y}_T).P' \rhd \Delta \uplus \{t{:}\, (\{read\}, true)\}$ και στο τέλος να εφαρμόσουμε το κανόνα του

συστήματος των τύπων (If) ο οποίος για βασικό τύπο $t, \Gamma \vdash P = if(e)\ then\ Q\ else\ x(\tilde{y}_T).P' \rhd t: (\{read\}, true \wedge \neg e)$. Με μια σειρά εφαρμογής των κανόνων $(ParP), (ParS)$ και $(ResGP), (ResGS)$ θα είχαμε κατασκευάσει μια διεπαφή δικαιωμάτων Θ για το σύστημα S το οποίο θα δώσει $\Gamma \vdash S \rhd \Theta'; t \gg \langle G_1[\dots G_n[u, \neg cond], \{read \cup \tilde{p}\}\rangle$, όπου $cond = \neg e \wedge true = \neg e$ για ένα σύνολο δικαιωμάτων $\tilde{p}$. Ωστόσο κάτι τέτοιο θα έδινε μια διεπαφή η οποία δεν συμβαδίζει με την ιεραρχία και σκοπό της πολιτικής οπόταν $\langle H, u_H\rangle \nVdash \widetilde{HP}$ και έτσι $P \nVdash \Theta$. Η περίπτωση αναφορικά με ένα βασικό τύπο πεδίου $t_s.t, T = t_s.t$, το δικαίωμα $read$ και συνθήκη $\neg cond$ προκύπτει με τον ίδιο τρόπο ομαδοποιώντας επιτρεπτά δικαιώματα βάση του τύπου του πεδίου.

2. Οι περιπτώσεις για τους κανόνες (2)(3)(4) προκύπτουν με παρόμοιο τρόπο όπως και η περίπτωση 1.
3. Η περίπτωση του κανόνα (5) εσφαλμένης διεργασίας.

   Έστω ότι $identify \notin \bigcup_{G \in \tilde{G}} \pi(true, G, t_s)$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t \in \tilde{y}_T, t_s.t \in T^p$ και $P = x(\tilde{y}_T).P'$. Για να είμαστε σε θέση να έχουμε ένα περιβάλλον Δ για τη διεργασία P θα πρέπει στο τελευταίο βήμα να χρησιμοποιήσαμε το κανόνα του συστήματος των τύπων (In) για να μπορέσουμε να συμπεράνουμε ότι για κάποιο τύπο δομής t_s *και* $t_s.t\ \Gamma \vdash P = x(\tilde{y}_T).P' \rhd \Delta \uplus \{t_s.t: (read, true).t_s: (identify, true)\}$. Με μια σειρά εφαρμογή των κανόνων $(ParP), (ParS)$ και $(ResGP), (ResGS)$ θα είχαμε κατασκευάσει μια διεπαφή δικαιωμάτων Θ για το σύστημα S το οποίο θα δώσει για το τύπο t_s, $\Gamma \vdash S \rhd \Theta'; t_s \gg \langle G_1[\dots G_n[u, true], \{identify \cup \tilde{p}\}\rangle$ για ένα σύνολο δικαιωμάτων $\tilde{p}$. Ωστόσο κάτι τέτοιο θα έδινε μια διεπαφή η οποία δεν συμβαδίζει με την ιεραρχία και σκοπό της πολιτικής οπόταν $\langle H, u_H\rangle \nVdash \widetilde{HP}$ και έτσι P $\nVdash$ Θ. Παρόμοια προκύπτει και η περίπτωση από το δικαίωμα εγγραφής του βασικού τύπου πεδίου δομής της κατηγορίας T^p και χρήση του κανόνα από το σύστημα των τύπων (Out).

   Έστω ότι $identify \notin \bigcup_{G \in \tilde{G}} \pi(cond, G, t_s)\ cond = e, [\![e]\!] = true$ και $\exists x, y$ τα οποία $\Gamma \vdash x \rhd G[\tilde{T}], y: t_s.t \in \tilde{y}_T, t_s.t \in T^p, P = if(e)\ then\ x(\tilde{y}_T).P'$. Για να είμαστε σε θέση να έχουμε ένα περιβάλλον Δ για τη διεργασία P θα

πρέπει να χρησιμοποιήσαμε το κανόνα του συστήματος των τύπων (In) για να μπορέσουμε να συμπεράνουμε ότι για το βασικό τύπο δομής t_s και τον αντίστοιχο τύπο πεδίου $t_s.t$ το παρακάτω για το Γ $\Gamma \vdash P = x(\tilde{y}_T).P' \rhd \Delta \uplus \{t_s.t\colon(\{read\}, true).t_s\colon(\{identify\}, true)\}$ και τέλος με την εφαρμογή του κανόνα από το σύστημα των τύπων (If) για το βασικό τύπο της δομής t_s προκύπτει $\Gamma \vdash P = if(e)\ then\ x(\tilde{y}_T).P' \rhd t_s\colon(\{identify\}, true \wedge e)$. Με μια σειρά εφαρμογής των κανόνων $(ParP), (ParS)$ και $(ResGP), (ResGS)$ θα είχαμε κατασκευάσει μια διεπαφή δικαιωμάτων Θ για το σύστημα S το οποίο θα δώσει $\Gamma \vdash S \rhd \Theta'; t_s \gg \langle G_1[\dots G_n[u, cond], \{identify \cup \tilde{p}\}\rangle$, όπου $cond = e \wedge true = e$ για ένα σύνολο δικαιωμάτων $\tilde{p}$. Ωστόσο κάτι τέτοιο θα έδινε μια διεπαφή η οποία δεν συμβαδίζει με την ιεραρχία και σκοπό της πολιτικής οπόταν $\langle H, u_H\rangle \nVdash \widetilde{HP}$ και έτσι $P \nVdash \Theta$. Παρόμοια προκύπτει και η περίπτωση από το δικαίωμα εγγραφής του βασικού τύπου πεδίου δομής της κατηγορίας T^p και χρήση του κανόνα από το σύστημα των τύπων (Out).

Έστω ότι $identify \notin \bigcup_{G \in \tilde{G}} \pi(\neg cond, G, t_s)\ cond = e, [\![e]\!] = false$ και $\exists x, y$ τέτοια ώστε $\Gamma \vdash x \rhd G[\tilde{T}], y\colon t_s.t \in \tilde{y}_T, t_s.t \in T^p$ και $P = if(e)\ then\ Q\ else\ x(\tilde{y}_T).P'$. Για να είμαστε σε θέση να έχουμε ένα περιβάλλον Δ για τη διεργασία P θα πρέπει να χρησιμοποιήσαμε το κανόνα του συστήματος των τύπων (In) για να μπορέσουμε να συμπεράνουμε ότι για το βασικό τύπο δομής t_s και τον αντίστοιχο τύπο πεδίου της $t_s.t$ $\Gamma \vdash P = x(\tilde{y}_T).P' \rhd \Delta \uplus \{t_s.t\colon(\{read\}, true).t_s\colon(\{identify\}, true)\}$ και τέλος με την εφαρμογή του κανόνα από το σύστημα των τύπων (If) για το βασικό τύπο της δομής T^p προκύπτει ότι $\Gamma \vdash P = if(e)\ then\ Q\ else\ x(\tilde{y}_T).P' \rhd T^p\colon(\{identify\}, true \wedge \neg e)$. Με μια σειρά εφαρμογής των κανόνων $(ParP), (ParS)$ και $(ResGP), (ResGS)$ θα είχαμε κατασκευάσει μια διεπαφή δικαιωμάτων Θ για το σύστημα S το οποίο θα δώσει $\Gamma \vdash S \rhd \Theta'; t \gg \langle G_1[\dots G_n[u, \neg cond], \{identify \cup \tilde{p}\}\rangle$, όπου $cond = \neg e \wedge true = \neg e$ για ένα σύνολο δικαιωμάτων $\tilde{p}$. Ωστόσο κάτι τέτοιο θα έδινε μια διεπαφή η οποία δεν συμβαδίζει με την ιεραρχία και σκοπό της πολιτικής οπόταν $\langle H, u_H\rangle \nVdash \widetilde{HP}$ και έτσι $P \nVdash \Theta$. Παρόμοια προκύπτει και η περίπτωση από το

δικαίωμα εγγραφής του βασικού τύπου πεδίου δομής της κατηγορίας T^p και χρήση του κανόνα από το σύστημα των τύπων (Out).

4. Η περίπτωση του κανόνα εσφαλμένης διεργασίας (6) προκύπτει από το συνδυασμό όλων των παραπάνω δυνατών περιπτώσεων ενεργειών και ικανοποίηση συνθηκών από όλους τους κανόνες και η παραβίαση εντοπίζεται όταν εφαρμόζεται ο κανόνας $(ResGP)$ ο οποίος αναθέτει σε όλους τους τύπους που έχουν παραχθεί μέχρι εκείνη τη στιγμή τον σκοπό u ο οποίος δεν είναι συμβατός με τη πολιτική ιδιωτικότητας οπόταν $\langle H, u_H \rangle \nVdash \widetilde{HP}$.

■

Όπως αναμενόταν βάσει και των παραπάνω στοιχείων εάν μια διεργασία είναι εσφαλμένη ως προς κάποια πολιτική ιδιωτικότητας $\mathcal{P}$ και αντίστοιχο περιβάλλον Γ, τότε και η αντίστοιχη διεπαφή Θ δεν ικανοποιεί την πολιτική ιδιωτικότητας $\mathcal{P}$.

Με τη διατύπωση του Λήμματος 2 έχουμε ξεκαθαρίσει την έννοια της ικανοποίησης μιας πολιτικής ιδιωτικότητας από ένα σύστημα, οι αποδείξεις παραπάνω επιβεβαιώνουν ότι η ικανοποίηση μιας πολιτικής από μια διατυπωμένη διεργασία προστατεύεται από τη σημασιολογία παραπάνω.

Ορισμός 8: Δομική αντιστοίχιση (Structural Congruence)
Έστω ≡ η μικρότερη αντιστοιχία η οποία ικανοποιεί το αντιμεταθετικό μονοειδές. (|,0) και τους κανόνες $(\nu\, x : T)0 \equiv 0, (\nu\, x : T_1)(\nu\, y : T_2)F \equiv (\nu\, y : T_2)(\nu\, x : T_1)F$ $(!\,\mathrm{P} \equiv \mathrm{P}|!\,\mathrm{P}, x \notin fn(F_2)$ συνεπάγεται ότι $(\nu\, x : T)F_1|F_2 \equiv (\nu\, x : T)(F_1|F_2)$.

Λήμμα 3

Εάν $F_1 \equiv F_2$ και $F_1 \xrightarrow{l} F_1'$ τότε $F_2 \xrightarrow{l} F_2'$ και $F_1' \equiv F_2'$ για κάποιο F_2'.
Απόδειξη: Η απόδειξη προκύπτει με επαγωγή στον ορισμό της Δομικής αντιστοίχισης.

Λήμμα 4: Αποδυνάμωση (Weakening)

1. Εάν $\Gamma \vdash x \rhd \mathrm{T}$ και $\mathrm{y} \notin \mathrm{dom}(\Gamma)$ τότε $\Gamma \cdot \mathrm{y}\colon \mathrm{T}' \vdash \mathrm{x} \rhd \mathrm{T}$.
2. Εάν $\Gamma \vdash \mathrm{P} \rhd \Delta$ και $\mathrm{y} \notin \mathrm{dom}(\Gamma)$ τότε $\Gamma \cdot \mathrm{y}\colon \mathrm{T} \vdash \mathrm{P} \rhd \Delta$.
3. Εάν $\Gamma \vdash \mathrm{S} \rhd \Theta$ και $\mathrm{y} \notin \mathrm{dom}(\Gamma)$ τότε $\Gamma \cdot \mathrm{y}\colon \mathrm{T} \vdash \mathrm{S} \rhd \Theta$.

Απόδειξη: Η απόδειξη αναφορικά με την πρώτη πρόταση ακολουθεί τον κανόνα του συστήματος τύπων ($Name$) ενώ οι αποδείξεις των προτάσεων 2 και 3 προκύπτουν με εφαρμογή επαγωγής στη σύνταξη των διεργασιών και των συστημάτων.

Το αντίστροφο της Αποδυνάμωσης για ένα περιβάλλον διατύπωσης των τύπων Γ είναι η έννοια της Ενδυνάμωσης.

Λήμμα 5: Ενδυνάμωση (Strengthening)

1. Εάν $\Gamma \cdot y{:}\,T' \vdash x \rhd T$ και $y \neq x$ τότε $\Gamma \vdash x \rhd T$.
2. Εάν $\Gamma \cdot y{:}\,T \vdash P \rhd \Delta$ και $y \notin \mathrm{fn}(P)$ τότε $\Gamma \vdash P \rhd \Delta$.
3. Εάν $\Gamma \cdot y{:}\,T \vdash S \rhd \Theta$ και $y \notin \mathrm{fn}(S)$ τότε $\Gamma \vdash S \rhd \Theta$.

Απόδειξη: Όπως και στην περίπτωση του Λήμματος της Αποδυνάμωσης, η απόδειξη της πρώτης πρότασης προκύπτει από τον κανόνα του συστήματος τύπων (Name) ενώ οι αποδείξεις των προτάσεων 2 και 3 προκύπτουν με εφαρμογή επαγωγής στη σύνταξη των διεργασιών και των συστημάτων.

Θεώρημα 1: Διατήρηση των Τύπων (Type Preservation)

1. Έστω ότι $\Gamma \vdash P \rhd \Delta$ και $P \xrightarrow{l} P'$ τότε $\Gamma \vdash P' \rhd \Delta'$ και $\Delta' \preccurlyeq \Delta$
2. Έστω ότι $\Gamma \vdash S \rhd \Theta$ και $S \xrightarrow{l} S'$ τότε $\Gamma \vdash S' \rhd \Theta'$ και $\Theta' \preccurlyeq \Theta$

Απόδειξη:

Ξεκινάμε την απόδειξη μας με την απόδειξη της πρότασης 1 του παρόντος Θεωρήματος. Αυτή θα προκύψει με επαγωγή στο μέγεθος της κατασκευής της μετάβασης.

Για το βασικό βήμα της επαγωγής μας θεωρούμε τις ακόλουθες δύο περιπτώσεις:

- Περίπτωση του κανόνα (Out): Έστω $P = \bar{x}\langle \tilde{z} \rangle.P$ και $P \xrightarrow{\bar{x}(\tilde{z})} P'$. Από την εφαρμογή του κανόνα (Out) του συστήματος των τύπων και υποθέτοντας ότι $\Gamma \vdash z_i \rhd T_i$ για κάθε $z_i \in \tilde{z}$ και $\tilde{z} = z_1 \ldots z_n$ με $n \in \mathbb{N}$ και $\Gamma \vdash x \rhd G[\tilde{T}]$, έχουμε ότι:

$$\frac{\Gamma \vdash P' \rhd \Delta'}{\Gamma \vdash \bar{x}\langle \tilde{z} \rangle.P' \rhd \Delta' \uplus \Delta^{w}_{T_i, i=1..n}}$$

Θεωρούμε ένα τυχαίο στοιχείο z της πλειάδας $\tilde{z}$. Εφόσον η σχέση $\Delta' \uplus \Delta_T^w$ εφαρμόζεται για όλα τα στοιχεία αυτής θα αποδείξουμε για ένα τυχαίο στοιχείο z το οποίο αντιπροσωπεύει όλα όσα εμπεριέχονται στο $\tilde{z}$.

Συγκεκριμένα υπάρχουν οι παρακάτω τέσσερις περιπτώσεις:

1. Εάν ο τύπος T του z δεν είναι βασικός τύπος t ούτε της μορφής $G'[\tilde{T}]$ τότε από τον ορισμό του $\Delta_{\mathrm{T}}^{\mathrm{w}}$ προκύπτει ότι $\Delta_{\mathrm{T}}^{\mathrm{w}} = \emptyset$. Ως αποτέλεσμα του προηγούμενου, $\Delta = \Delta'$ και τετριμμένα ισχύει ότι $\Delta \succcurlyeq \Delta'$.
2. Εάν ο τύπος T του z είναι βασικός τύπος t ανεξάρτητος δομής, τύπος δομής ή βασικός τύπος πεδίου δομής που ανήκει στην κατηγορία των T^n τότε προκύπτει ότι $\Delta_T^w = t : (\{write\}, true)$. Οπόταν $\Delta = \Delta' \uplus t: (\{write\}, true)$ για το οποίο προφανώς ισχύει ότι $\Delta \succcurlyeq \Delta'$.
3. Εάν ο τύπος T του z είναι βασικός τύπος t πεδίου της κατηγορίας T^p τότε $\Delta_T^w = t_s: (\{identify\}, true).t : (\{write\}, true)$. Οπόταν $\Delta = \Delta' \uplus t_s: (\{identify\}, true).t : (\{write\}, true)$ για το οποίο προφανώς ισχύει ότι $\Delta \succcurlyeq \Delta'$.
4. Εάν ο τύπος T του z είναι της μορφής $G'\left[G[\tilde{T}]\right]$ προκύπτει ότι $\Delta_T^w = t : (\{disclose\ G'\}, true)$. Έτσι $\Delta = \Delta' \uplus t : (\{disclose\ G'\}, true)$. για το οποίο προφανώς ισχύει ότι $\Delta \succcurlyeq \Delta'$.

- Περίπτωση του κανόνα (In): Έστω μια διεργασία $P = x(\tilde{y}_T).P'$ και $P \xrightarrow{x(\tilde{z})} P'\{^{z_i}/_{y_i}\}_{\forall i=1..n}$ όπου $\tilde{z} = z_1 \dots z_n, \tilde{y} = y_1 \dots y_n, \tilde{y}_T = y_1 : T_1 \dots . . y_n : T_n$ και n ∈ ℕ. Αρχικά παρατηρούμε ότι από το Θεώρημα της Αντικατάστασης, εάν $\Gamma \vdash \mathrm{P}'\{\mathrm{z_i}/\mathrm{y_i}\} \rhd \Delta'$ για κάθε ζεύγος τιμών (z_i, y_i) τότε $\Gamma \vdash P' \rhd \Delta'$. Επιπρόσθετα, από τον κανόνα του συστήματος των τύπων (In) και υποθέτοντας ότι το $\Gamma \vdash x \rhd G[\tilde{T}]$, έχουμε ότι

$$\frac{\Gamma \vdash \mathrm{P}' \rhd \Delta'}{\Gamma \vdash x(\tilde{z}).P' \rhd \Delta' \uplus \Delta^r_{T_{i,i=1..n}}}$$

Θεωρούμε ένα τυχαίο στοιχείο z της πλειάδας $\tilde{z}$. Εφόσον η σχέση $\Delta' \uplus \Delta_T^r$ εφαρμόζεται για όλα τα στοιχεία αυτής θα αποδείξουμε για ένα τυχαίο στοιχείο z το οποίο αντιπροσωπεύει όλα όσα εμπεριέχονται στο $\tilde{z}$.

Συγκεκριμένα υπάρχουν οι παρακάτω τέσσερις περιπτώσεις:

1. Εάν ο τύπος T του z δεν είναι βασικός τύπος t ούτε της μορφής $G'[\tilde{T}]$ τότε από τον ορισμό του $\Delta_{\mathrm{T}}^{\mathrm{r}}$ προκύπτει ότι $\Delta_{\mathrm{T}}^{\mathrm{r}} = \emptyset$. Ως αποτέλεσμα του προηγούμενου, $\Delta = \Delta'$ και τετριμμένα ισχύει ότι $\Delta \succcurlyeq \Delta'$.
2. Εάν ο τύπος T του z είναι βασικός τύπος t ανεξάρτητος δομής δεδομένων, τύπος δομής ή βασικός τύπος πεδίου δομής που ανήκει στην κατηγορία των T^n τότε προκύπτει ότι $\Delta_T^r = t : (\{read\}, true)$. Οπόταν $\Delta = \Delta' \uplus t : (\{read\}, true)$. για το οποίο προφανώς ισχύει ότι $\Delta \succcurlyeq \Delta'$.
3. Εάν ο τύπος T του z είναι βασικός τύπος t πεδίου της κατηγορίας T^p τότε $\Delta_T^r = t_s : (\{identify\}, true).t : (\{read\}, true)$ Οπόταν $\Delta = \Delta' \uplus t_s : (\{identify\}, true).t : (\{read\}, true)$ για το οποίο προφανώς ισχύει ότι $\Delta \succcurlyeq \Delta'$.
4. Εάν ο τύπος T του z είναι της μορφής $G'\left[G[\tilde{T}]\right]$ προκύπτει ότι $\Delta_T^w = t : (\{access\}, true)$. Έτσι $\Delta = \Delta' \uplus t : (\{access\}, true)$. για το οποίο προφανώς ισχύει ότι $\Delta \succcurlyeq \Delta'$.

Προχωρούμε στο βήμα της Επαγωγής:

- Περίπτωση του κανόνα (Com): Έστω $P_1|P_2 \xrightarrow{\tau} (\nu\, bn(l_1) \cup bn(l_2))(P_1'|P_2')$, όπου $P_1 \xrightarrow{l_1} P_1'$, $P_2 \xrightarrow{l_2} P_2'$ και $dual(l_1, l_2)$. Έστω $\Gamma' = \Gamma$, όταν $bn(l_1) \cup bn(l_2) = \emptyset$ και $\Gamma' = \Gamma \cdot y : T$ για κάθε $y{:}T \in \tilde{y}_T$, όταν $bn(l_1) \cup bn(l_2) = \tilde{y}$ και $\tilde{y}$ αποτελείται από τα ονόματα της πλειάδας $\tilde{y}_T$. Από επαγωγική υπόθεση έχουμε ότι:

$$\Gamma' \vdash P_1 \rhd \Delta_1, \Gamma' \vdash P_1' \rhd \Delta_1' \text{ και } \Delta_1 \succcurlyeq \Delta_1'$$
$$\Gamma' \vdash P_2 \rhd \Delta_2, \Gamma' \vdash P_2' \rhd \Delta_2' \text{ και } \Delta_2 \succcurlyeq \Delta_2'$$

  Από τον κανόνα του συστήματος των τύπων $(ParP)$ έχουμε ότι:

$$\frac{\Gamma' \vdash P_1 \rhd \Delta_1 \;\; \Gamma' \vdash P_2 \rhd \Delta_2}{\Gamma' \vdash P_1|P_2 \rhd \Delta_1 \uplus \Delta_2}$$

  και από το Λήμμα 5 (2) μπορούμε να συμπεράνουμε ότι $\Gamma \vdash P_1|P_2 \rhd \Delta_1 \uplus \Delta_2$. Ομοίως, με την εφαρμογή του κανόνα του συστήματος των τύπων $(ParP)$ παίρνουμε:

$$\frac{\Gamma' \vdash P_1' \rhd \Delta_1' \quad \Gamma' \vdash P_2' \rhd \Delta_2'}{\Gamma' \vdash P_1'|P_2' \rhd \Delta_1' \uplus \Delta_2'}$$

και ακολούθως από τον κανόνα του συστήματος των τύπων $(ResNP)$ παίρνουμε ότι $\Gamma \vdash \big(\nu\, bn(l_1) \cup bn(l_2)\big)(P_1'|P_2') \rhd \Delta_1' \uplus \Delta_2'$. Από τον ορισμό της σχέσης $\uplus$ συμπεραίνουμε ότι $\Delta_1 \uplus \Delta_2 \Subset \Delta_1' \uplus \Delta_2'$, και το αποτέλεσμα ακολουθεί.

- Περίπτωση των κανόνων $(ParL)$ και $(ParR)$: Αυτές οι περιπτώσεις είναι όμοιες με την απόδειξη που δόθηκε παραπάνω για τον κανόνα του (Com).

- Περίπτωση του κανόνα $(ResN)$: Έστω διεργασία $P = (\nu\, \tilde{x}_T)P'$ με $P \xrightarrow{l} (\nu\, \tilde{x}_T)P''$, $P' \xrightarrow{l} P''$ και $x \notin fn(l)$, για κάθε $x \in \tilde{x}_T$ και $\tilde{x}_\mathrm{T} = \mathrm{x_1}\colon \mathrm{T_1} \ldots \ldots \mathrm{x_n}\colon \mathrm{T_n}$. Από την επαγωγική υπόθεση, έχουμε ότι εάν $\Gamma \vdash P \rhd \Delta$, τότε:

$$\Gamma' \vdash P' \rhd \Delta, \Gamma' \vdash P'' \rhd \Delta' \text{ και } \Delta \Subset \Delta'$$

για $\Gamma' = \Gamma \cdot x : T$ για κάθε $x : T \in \tilde{x}_T$. Με την εφαρμογή του κανόνα $(ResNP)$, παρατηρούμε ότι:

$$\Gamma \vdash P \rhd \Delta, \Gamma \vdash (\nu\, \tilde{x}_T)P'' \rhd \Delta'$$

Εφόσον $\Delta \Subset \Delta'$ το αποτέλεσμα έπεται.

- Περίπτωση κανόνα $(Scope)$: Αυτή η περίπτωση κανόνα είναι όμοια με την προηγούμενη περίπτωση.

- Περίπτωση κανόνων $(True)$ και $(False)$: Προκύπτουν άμεσα από επαγωγική υπόθεση καθώς ο κανόνας του συστήματος των τύπων (If) μεταβάλλει μόνο το σύνολο των συνθηκών για τους τύπους.

- Περίπτωση κανόνα $(Alpha)$: Αυτή η περίπτωση παράγεται άμεσα από το Λήμμα της Αντικατάστασης

- Περίπτωση κανόνα $(Repl)$: Αυτή η περίπτωση κανόνα είναι όμοια με του κανόνα (Com).

Αυτό ολοκληρώνει την απόδειξη μας αναφορικά με την πρόταση (1) του παρόντος θεωρήματος.

Η απόδειξη της πρότασης (2) του θεωρήματος προκύπτει με επαγωγή παρόμοια με την απόδειξη που έχει δοθεί πιο πάνω στην πρόταση (1). Η επαγωγή γίνεται πάνω στο σύνολο των ενεργειών l αυτή τη φορά ωστόσο για τη κατασκευή ενός συστήματος.

- Περίπτωση του κανόνα (Com): Έστω $S_1|S_2 \xrightarrow{\tau} (\nu\ bn(l_1) \cup bn(l_2))(S_1' |S_2')$, όπου $S_1 \xrightarrow{l_1} S_1'$ και $S_2 \xrightarrow{l_2} S_2'$ και $dual(l_1, l_2)$. Έστω $\Gamma' = \Gamma$, όταν $bn(l_1) \cup bn(l_2) = \emptyset$ και $\Gamma' = \Gamma \cdot y : T$ για κάθε $y{:}T \in \tilde{y}_T$, όταν $bn(l_1) \cup bn(l_2) = \tilde{y}$ και $\tilde{y}$ αποτελείται από τα ονόματα της πλειάδας $\tilde{y}_T$. Από την επαγωγική υπόθεση έχουμε ότι:

$$\Gamma' \vdash S_1 \rhd \Theta_1, \Gamma' \vdash S_1' \rhd \Theta_1' \text{ και } \Theta_1 \succcurlyeq \Theta_1'$$
$$\Gamma' \vdash S_2 \rhd \Theta_2, \Gamma' \vdash S_2' \rhd \Theta_2' \text{ και } \Theta_2 \succcurlyeq \Theta_2'$$

Με την εφαρμογή του κανόνα του συστήματος των τύπων $(ParS)$ έχουμε ότι:

$$\frac{\Gamma' \vdash S_1 \rhd \Theta_1 \quad \Gamma' \vdash S_2 \rhd \Theta_2}{\Gamma' \vdash S_1|S_2 \rhd \Theta_1; \Theta_2}$$

και από το Λήμμα 5(3) μπορούμε άμεσα να συμπεράνουμε ότι $\Gamma \vdash S_1|S_2 \rhd \Theta_1; \Theta_2$. Ομοίως με την εφαρμογή του κανόνα του συστήματος των τύπων $(ParS)$ έχουμε:

$$\frac{\Gamma' \vdash S_1' \rhd \Theta_1' \quad \Gamma' \vdash S_2' \rhd \Theta_2'}{\Gamma' \vdash S_1'|S_2' \rhd \Theta_1'; \Theta_2'}$$

και ακολούθως από τον κανόνα του συστήματος των τύπων $(ResNS)$ έχουμε ότι $\Gamma \vdash \big(\nu\ bn(l_1) \cup bn(l_2)\big)(S_1'|S_2') \rhd \Theta_1'; \Theta_2'$. Από τον ορισμό του ; συμπεραίνουμε ότι το $\Theta_1; \Theta_2 \succcurlyeq \Theta_1'; \Theta_2'$ και το αποτέλεσμα προκύπτει άμεσα.

- Περίπτωση του κανόνα $(ParL)$ και $(ParR)$: Αυτές οι περιπτώσεις προκύπτουν αντίστοιχα με την προηγούμενη περίπτωση.

- Περίπτωση του κανόνα $(ResN)$: Έστω $S = (\nu\ \tilde{x}_T)S'$ όπου $S \xrightarrow{l} (\nu\tilde{x}_T\ )S''$, $S' \xrightarrow{l} S''S \xrightarrow{l} (\nu\tilde{x}_T\ )S'', S' \xrightarrow{l} S''$και $x \notin fn(l)$, για κάθε $x{:}T \in \tilde{x}_T$ και $\tilde{x}_T = x_1{:}T_1 \ldots\ldots x_n{:}T_n$.
  Από την επαγωγική υπόθεση, έχουμε ότι εάν $\Gamma \vdash S \rhd \Theta$, τότε:

$$\Gamma' \vdash S' \rhd \Theta, \Gamma' \vdash S'' \rhd \Theta' \text{ και } \Theta \geqslant \Theta'$$

για $\Gamma' = \Gamma \cdot x : T$ για κάθε $x{:}T \in \tilde{x}_T$. Τότε από τον κανόνα του συστήματος των τύπων $(ResNS)$, έχουμε:

$$\Gamma \vdash S \rhd \Theta, \Gamma \vdash (\nu \tilde{x}_T)S'' \rhd \Theta'$$

Εφόσον $\Theta \geqslant '$ το αποτέλεσμα έπεται.

- Περίπτωση του κανόνα $(Scope)$: Αυτή η περίπτωση κανόνα είναι ίδια με την περίπτωση του κανόνα $(ResNS)$ ενώ ταυτόχρονα εμπλέκει και το Λήμμα της Αποδυνάμωσης.

- Περίπτωση του κανόνα $(ResGS)$: Έστω ένα σύστημα $S = (\nu G)S'$ όπου $S \xrightarrow{l} (\nu G)S''$ και $S' \xrightarrow{l} S''$.
  Από την επαγωγική υπόθεση, έχουμε ότι εάν $\Gamma \vdash S \rhd \Theta$,τότε: $\Gamma' \vdash S' \rhd \Theta_1$, $\Gamma' \vdash S'' \rhd \Theta_1'$ και $\Theta_1 \geqslant \Theta_1'$ για $\Gamma' = \Gamma \cdot G$ και $\Theta = \mathrm{G} \bigoplus \Theta_1$. Τότε από τον κανόνα του συστήματος των τύπων $(ResGS)$, έχουμε:

  $$\Gamma \vdash S \rhd \Theta, \Gamma \vdash (\nu G)S'' \rhd \Theta'$$

  όπου $\Theta_1 = G \bigoplus \Theta_1'$, εφόσον $\Theta_1 \geqslant \Theta_1'$ το αποτέλεσμα έπεται.

- Η περίπτωση του $S = (\nu G)P\langle u \rangle$ είναι παρόμοια ωστόσο εμπλέκει τον κανόνα $(ResGP)$ αντί του κανόνα $(ResGS)$ του συστήματος των τύπων όπως στην περίπτωση της πρότασης (1) του Θεωρήματος.

- Περίπτωση κανόνα $(Alpha)$: Αυτή η περίπτωση παράγεται άμεσα από το Λήμμα της Αντικατάστασης.

■

Έτσι, όπως διατυπώνεται και από το παραπάνω θεώρημα θεωρούμε ότι οποτεδήποτε μια καλά τυπικά ορισμένη διεργασία εκτελέσει μια ενέργεια, αυτό οδηγεί σε μια αντίστοιχη καλά ορισμένη διεργασία. Το ίδιο ισχύει και στην περίπτωση του συστήματος ορίζοντας ότι όταν ένα σύστημα εκτελεί μια συγκεκριμένη ενέργεια τότε και αυτό οδηγεί σε ένα καλά ορισμένο σύστημα. Οι δύο σχετικές παραγόμενες διεπαφές για διεργασία και σύστημα Δ και Θ αντίστοιχα, ανάγονται σύμφωνα με το σχεσιακό τελεστή ≼ που

ορίσαμε παραπάνω και καταγράφει ότι ουδέποτε προκύπτουν επιπλέον δικαιώματα από αυτά που προκύπτουν από την τυπική καταγραφή τους μέσω του ελέγχου τύπων.

Αποτέλεσμα 2

Εάν $\mathcal{P} \vdash S$ και $S \xrightarrow{l} S'$ τότε $\mathcal{P} \vdash S'$

Θεώρημα 2: Ασφάλεια (Safety)

Εάν $\Gamma \vdash S \rhd \Theta, \mathcal{P} \Vdash \Theta$ και $S \xrightarrow{\iota}{}^{*} S'$ τότε το S' δεν είναι μια εσφαλμένη διεργασία έναντι της πολιτικής ιδιωτικότητας $\mathcal{P}$.

Απόδειξη:

Εάν $\Gamma \vdash S \rhd \Theta$ και $S \xrightarrow{\iota}{}^{*} S'$ τότε από το θεώρημα της Διατήρησης των Τύπων έχουμε $\Gamma \vdash S' \rhd \Theta'$ όπου $\Theta' \preccurlyeq \Theta$. Από το Λήμμα της Αντικατάστασης και εφόσον η διεπαφή Θ ικανοποιεί την πολιτική $\mathcal{P}$, $\mathcal{P} \Vdash \Theta$ τότε και η διεπαφή Θ', ικανοποιεί την πολιτική $\mathcal{P}$ $\mathcal{P} \Vdash \Theta'$. Έστω ότι το σύστημα S' είναι μια εσφαλμένη διεργασία ως προς τη πολιτική ιδιωτικότητας $\mathcal{P}$. Από το Λήμμα 2 έχουμε ότι η διεπαφή Θ' δεν ικανοποιεί την πολιτική $\mathcal{P}$, αυτό ωστόσο οδηγεί σε αντίφαση. Οπόταν το σύστημα S' δεν είναι μια εσφαλμένη διεργασία.

■

6.2 Εφαρμογή αποδείξεων ικανοποίησης πολιτικής

Θα χρησιμοποιήσουμε τις αποδείξεις που δώσαμε παραπάνω για τον έλεγχο ικανοποίησης πολιτικών ιδιωτικότητας από το προτεινόμενο πλαίσιο ελέγχου για να αποδείξουμε ότι το σύστημα που καταγράφηκε για το σενάριο του νοσοκομείου στο λογισμό της CP calculus ικανοποιεί την πολιτική που ορίζεται αντίστοιχα στο Κεφάλαιο 3. Η εξέταση γίνεται για σκοπούς της απόδειξης ικανοποίησης αλλά ταυτόχρονα χρησιμοποιούμε μια μικρή παραλλαγή των εφαρμοζόμενων δικαιωμάτων ώστε να αναδείξουμε και την περίπτωση της μη ικανοποίησης της πολιτικής.

Θα αποδείξουμε με τη χρήση των παραπάνω αποδείξεων ότι το σύστημα του νοσοκομείου ικανοποιεί την αντίστοιχη πολιτική ιδιωτικότητας που ορίζεται για αυτό. Η

παραγόμενη διεπαφή με τον έλεγχο των τύπων για το αντίστοιχο παράδειγμα ήταν η ακόλουθη:

$PDATA.Age \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Sex \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Name \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access\}\rangle;$

$PDATA \gg \langle Hospital[Nurse[diagnosis_h, true]], \{identify\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{write\}\rangle;$

$PDATA.Name \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{read\}\rangle;$

$PDATA \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{identify\}\rangle;$

$PDATA.Age \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access, read\}\rangle;$

$PDATA.Name \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

$PDATA.Sex \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

Συνεπώς έχουμε τα παρακάτω σύνολα ομάδων:

$\widetilde{G_1} = \langle Hospital, Nurse\rangle$

$\widetilde{G_2} = \langle Hospital, Doctor\rangle$

Διαχωρίζουμε τις διεπαφές των δικαιωμάτων στο σύνολο αυτών που αφορούν το βασικό τύπο του $PDATA$ και αυτών που αφορούν εσωτερικούς τύπους πεδίων του. Συνεπώς το πρώτο σύνολο για τον βασικό τύπο του PDATA περιλαμβάνει τα παρακάτω:

$PDATA \gg \langle Hospital[Nurse[diagnosis_h, true]], \{identify\}\rangle;$

$PDATA \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{identify\}\rangle;$

Ενώ για κάθε βασικό τύπο πεδίου της δομής του $PDATA$ θεωρούμε το ακόλουθο σύνολο από διεπαφές δικαιωμάτων:

$PDATA.Age \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Sex \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Name \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access, write\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Nurse[diagnosis_h, true]], \{access\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{write\}\rangle;$

$PDATA.Name \gg \langle Hospital[Doctor[diagnosis_h, age \geq 18]], \{read\}\rangle;$

$PDATA.Age \gg \langle Hospital[Doctor[diagnosis_h, true]], \{acces, read\}\rangle;$

$PDATA.Name \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

$PDATA.Sex \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

$PDATA.Diagnosis \gg \langle Hospital[Doctor[diagnosis_h, true]], \{access\}\rangle;$

Ως προς τον βασικό τύπο της δομής του $PDATA$ προκύπτουν τα εξής:

$perms_H(\widetilde{G_1}, diagnosis_h, true) = \{access, identify\}$

$perms_H(\widetilde{G_2}, diagnosis_h, age \geq 18) = \{access, identify\}$

Ως προς τον βασικό τύπο πεδίου δομής $PDATA.Name$ προκύπτουν τα εξής:

$perms_{HFP_1}(\widetilde{G_1}, diagnosis_h, true) = \{access, write\}$

$perms_{HFP_1}(\widetilde{G_2}, diagnosis_h, true) = \{access\}$

$perms_{HFP_1}(\widetilde{G_2}, diagnosis_h, age \geq 18) = \{access, read\}$

Ως προς τον βασικό τύπο πεδίου δομής $PDATA.Sex$ προκύπτουν τα εξής:

$perms_{HFP_2}(\widetilde{G_1}, diagnosis_h, true) = \{access, write\}$

$perms_{HFP_2}(\widetilde{G_2}, diagnosis_h, true) = \{access, read\}$

Ως προς τον βασικό τύπο πεδίου δομής $PDATA.Age$ προκύπτουν τα εξής:

$perms_{HFP_3}(\widetilde{G_1}, diagnosis_h, true) = \{access, write\}$

$perms_{HFP_3}(\widetilde{G_2}, diagnosis_h, true) = \{access, read\}$

Ως προς τον βασικό τύπο πεδίου δομής $PDATA.Diagnosis$ προκύπτουν τα εξής:

$perms_{HFP_4}(\widetilde{G_1}, diagnosis_h, true) = \{access\}$

$perms_{HFP_4}(\widetilde{G_2}, diagnosis_h, true) = \{access\}$

$perms_{HFP_4}(\widetilde{G_2}, diagnosis_h, age \geq 18) = \{access, write\}$

Όπως είναι προφανές από το παραπάνω τα δικαιώματα που ασκούνται στο σύστημα από τις διεργασίες που το αποτελούν πάνω στον τύπο της δομής αλλά και όλων των τύπων πεδίου της δομής για το σκοπό του σεναρίου και εκάστοτε συνθήκης είναι συμβατά με

την πολιτική που ορίζεται στο αντίστοιχο κεφάλαιο παραπάνω οπόταν η παραγόμενη διεπαφή δικαιωμάτων Θ ικανοποιεί την πολιτική από τον Ορισμό 4. Ως εκ τούτου το σύστημα που έχει παραγάγει τη συγκεκριμένη διεπαφή ικανοποιεί την πολιτική ιδιωτικότητας του σεναρίου γράφοντας και σχετικά $\mathcal{P} \vdash S$ από τον Ορισμό 6.

Για σκοπούς εμφάνισης της μη ικανοποίησης της πολιτικής από μια παραγόμενη διεπαφή ας θεωρήσουμε ότι η ομάδα Νοσοκόμος προσπαθεί να διαβάσει πληροφορία του βασικού τύπου της διάγνωσης χωρίς τον έλεγχο οποιασδήποτε έκφρασης. Μια τέτοια προσπάθεια θα οδηγούσε σε μια παραγόμενη διεπαφή η οποία θα περιελάβανε μεταξύ των όσων παράχθηκαν προηγουμένως το ακόλουθο:

$$PDATA.Diagnosis \gg \langle Hospital\big[Nurse[diagnosis_h, true]\big], \{read\}\rangle;$$

Σε μια τέτοια περίπτωση ωστόσο το σύνολο των ασκούμενων δικαιωμάτων βάση συνθήκης, εφόσον ο σκοπός παραμένει ο ίδιος με της πολιτικής η παραβίαση προέρχεται από εσφαλμένη χρήση δικαιωμάτων ως προς την ικανοποίηση μιας συνθήκης, στη συγκεκριμένη περίπτωση η μη ικανοποίηση οποιασδήποτε συνθήκης οπόταν συνθήκη $true$, δεν θα ήταν συμβατό με όσα ορίζει η πολιτική καθώς το δικαίωμα $read$ του βασικού τύπου πεδίου δομής της διάγνωσης δεν εμφανίζεται σε κανένα επίπεδο της ιεραρχίας της πολιτικής και συγκεκριμένα για τις ομάδες $Hospital$, $Nurse$ με συνθήκη $true$. Το προηγούμενο προκύπτει άμεσα από την εφαρμογή της βοηθητικής συνάρτησης π για ομαδοποίηση των δικαιωμάτων πολιτικής ως προς τον βασικό τύπο πεδίου του $PDATA.Diagnosis$ για την συνθήκη $true$ και τις ομάδες $Hospital$ και $Nurse$ αφού $\pi(true, Nurse, PDATA.Diagnosis) = \emptyset$ ως προς την ομάδα $Nurse$ και $\pi(true, Hospital, PDATA.Diagnosis) = \emptyset$.

Το νέο σύστημα αποτελεί εσφαλμένη διεργασία ως προς την ενέργεια εισόδου και το δικαίωμα $read$ και η νέα διεπαφή δικαιωμάτων Θ' δεν είναι συμβατή με την πολιτική. Ως αποτέλεσμα $\mathcal{P} \nVdash \Theta'$ που απευθείας οδηγεί στο γεγονός ότι το σύστημα που έχει παράξει την διεπαφή Θ' δεν σέβεται την πολιτική ιδιωτικότητας $\mathcal{P}$.

Κεφάλαιο 7

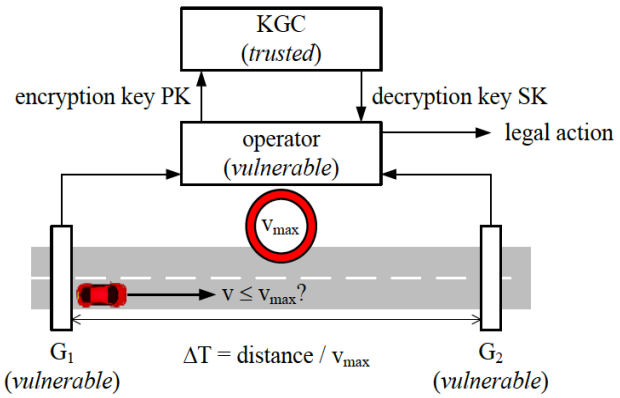
Περιπτώσεις Χρήσης

7.1 Ανίχνευση παραβίασης από υπέρβαση ορίου ταχύτητας

7.1.1 Περιγραφή

Η πρώτη περίπτωση χρήσης στην οποία και θα εφαρμόσουμε την προτεινόμενη μεθοδολογία για τον έλεγχο πολιτικών ιδιωτικότητας στα πλαίσια της παρούσας εργασίας προκύπτει μέσα από το [10]. Το σύστημα που περιγράφεται στο συγκεκριμένο άρθρο αφορά ένα σύστημα επιβολής προστίμου για υπέρβαση του ορίου ταχύτητας. Συγκεκριμένα, περιγράφεται η διαδικασία με την οποία σε αρκετές ευρωπαϊκές πόλεις

επιβάλλεται πρόστιμο υπέρβασης ορίου ταχύτητας στους οδηγούς. Αφαιρετικά το σύστημα αυτό λειτουργεί ως εξής, καθώς ένα όχημα περνά από σημεία ελέγχου που βρίσκονται τοποθετημένα στο δρόμο, καταγράφονται κάποια στοιχεία του και ο χρόνος στον οποίο έχει διέλθει. Αυτά χρησιμοποιούνται αργότερα για τον υπολογισμό της ύπαρξης ή όχι παραβίασης αναφορικά με υπέρβαση του ορίου ταχύτητας. Όταν το όχημα περάσει από ένα διαδοχικό σημείο ελέγχου τότε η διαδικασία καταγραφής των πληροφοριών του οχήματος επαναλαμβάνεται. Εκεί συνεργατικά τα δύο σημεία ελέγχου είναι υπεύθυνα να εξακριβώσουν κατά πόσο υπάρχει η οποιαδήποτε παραβίαση ορίου ταχύτητας. Σε περίπτωση παραβίασης, ένας κεντρικός διαχειριστής ($operator$) ενημερώνεται σχετικά από τα σημεία ελέγχου ($gantry$) με κρυπτογραφημένες ωστόσο για σκοπούς ασφάλειας πληροφορίες και αναλαμβάνει ευθύνη για τις περαιτέρω ενέργειες. Λόγω του ότι τα στοιχεία τα οποία παρέχονται σε αυτόν είναι κρυπτογραφημένα αυτός ζητά από το κέντρο παραγωγής κλειδιών ($Key\ Generator$ Center $-\ KGC$) τη μόνη έγκυρη μονάδα του συστήματος κλειδιά με τα οποία να μπορεί να αποκρυπτογραφήσει τις συγκεκριμένες πληροφορίες. Με τον όρο έγκυρη θεωρούμε τη μόνη οντότητα του συστήματος η οποία δεν θεωρείται ευάλωτη σε εξωτερικές επιθέσεις. Το κέντρο παραγωγής κλειδιών (KGC) με τη σειρά του ενημερώνει με το κλειδί αποκρυπτογράφησης το διαχειριστή ($operator$) ούτως ώστε να μπορεί να αποκρυπτογραφήσει τις πληροφορίες και να προβεί στις κατάλληλες νομικές ενέργειες. Το σενάριο που περιγράφεται περιέχει τη χρήση κάποιων δημοσιών κλειδιών τα οποία χρησιμοποιούνται για σκοπούς ασφαλείας των δεδομένων των οδηγών που καταχωρούνται στο σύστημα και τα οποία δημιουργούνται βάση των σχετικών πληροφοριών καταγραφής του οχήματος στα κέντρα ελέγχου. Σχηματικά η αναπαράσταση της λειτουργία του προαναφερθέντος συστήματος βρίσκεται Σχήμα 7.1



Σχήμα 7.1: Διαγραμματική αναπαράσταση σεναρίου

Ακολουθεί λεπτομερής περιγραφή των βημάτων που ακολουθούνται από κάθε οντότητα του συστήματος για την εξυπηρέτηση του παραπάνω σκοπού. Το σενάριο που εξετάζει τη συμπεριφορά του συστήματος αποτελείται από τα 2 σημεία ελέγχου GAN_1 και GAN_2, τον κεντρικό διαχειριστή που ενεργοποιείται όταν υπάρχει παραβίαση ορίου ταχύτητας και το αντίστοιχο κέντρο παραγωγής κλειδιών (KGC) το οποίο ενημερώνει τον διαχειριστή με τα κλειδιά αποκρυπτογράφησης στις περιπτώσεις παραβίασης.

Βήμα 1: Όταν κάποιο όχημα διέλθει από το σημείο ελέγχου GAN_1, σε χρόνο t_1, ο GAN_1, καταγράφει το σχετικό χρόνο διέλευσης του οχήματος και κάποια στοιχεία του οχήματος όπως οι πινακίδες εγγραφής. Αυτά τα στοιχεία αποθηκεύονται μαζί στη δομή των πληροφοριών του οχήματος οπόταν απαρτίζουν τα στοιχεία της δομής του. Στη συνέχεια και βάσει του χρόνου t_1 το σημείο ελέγχου υπολογίζει και αποθηκεύει στο σύστημα σαν ξεχωριστή πληροφορία ένα δημόσιο κλειδί PK_1 το οποίο χρησιμοποιείται κυρίως για σκοπούς ασφάλειας από εξωτερικές επιθέσεις. Σημαντικό να τονισθεί ότι το κάθε σημείο ελέγχου, κράτα αντίγραφο της λίστας από τα δημόσια κλειδιά PK_s τα οποία έχει δημιουργήσει πρόσφατα, τα οποία δίνονται από μια λίστα $L = \{\mathrm{PK}_1, \ldots \mathrm{PK}_\mathrm{N}\}$ και με τα οποία ελέγχει κατά πόσο υπάρχει η όχι παραβίαση ορίου ταχύτητας. Τα κλειδιά αυτά όπως και όλες οι άλλες πληροφορίες αποθηκεύονται προσωρινά σε μια μνήμη του σημείου ελέγχου για χρονικό διάστημα $\Delta\mathrm{T}$. Αυτό υπολογίζεται όπως και παραπάνω διαιρώντας την απόσταση διά τη μέγιστη επιτρεπτή ταχύτητα, το $\Delta\mathrm{T}$ αντανακλά τον ελάχιστο που χρειάζεται ένα όχημα για να διανύσει τη σταθερή απόσταση μεταξύ 2 σημείων ελέγχου με τη μέγιστη επιτρεπτή ταχύτητα. Αν για παράδειγμα η απόσταση μεταξύ των GAN_1 και GAN_2 είναι $5Km$ και το μέγιστο επιτρεπτό όριο ταχύτητας είναι $120\ Km/h$, τότε ο ελάχιστος χρόνος που απαιτείται για τη διάσχιση του παραπάνω κομματιού με επιτρεπτά όρια ταχύτητας είναι περίπου 150 δευτερόλεπτα. Τα δημόσια κλειδιά με χρονική διάρκεια $> \Delta T$ διαγράφονται αφού προφανώς δεν απασχολούν στην εξέταση υπέρβασης ορίου ταχύτητας.

Βήμα 2: Η διαδικασία που περιεγράφηκε στο Βήμα 1, επαναλαμβάνεται στο επόμενο σημείο ελέγχου GAN_2. Με το νέο υπολογισμό ωστόσο του καινούριου δημοσίου κλειδιού PK_2, τα σημεία ελέγχου, ελέγχουν μεταξύ τους αν το αντίστοιχο κλειδί του οχήματος από το πρώτο σημείο ελέγχου ή το δεύτερο είναι τα ίδια οπόταν υπάρχει η σχετική παραβίαση του ορίου ταχύτητας. Αυτό συμβαίνει μόνο όταν $t_2 - t_1 < \Delta T$ οπόταν και

τα δύο κλειδιά είναι ακόμα καταγεγραμμένα στις λίστες των δύο σημείων ελέγχου και μπορούν να ελεγχθούν μεταξύ τους. Εάν εντοπιστεί παραβίαση τα σημεία ελέγχου αποστέλλουν προς τον διαχειριστή τα κλειδιά τους και δημιουργούν κρυπτογραφημένα στοιχεία οχήματος τα οποία θα χρησιμοποιήσει ο διαχειριστής αργότερα για να προβεί στις κατάλληλες νομικές ενέργειες.

Βήμα 3: Με την ενημέρωση του ο διαχειριστής, ελέγχει εάν τα κλειδιά αυτά είναι τα ίδια οπόταν υπάρχει παραβίαση από υπέρβαση του ορίου ταχύτητας οπόταν και αποκαλύπτει προς το κέντρο παραγωγής κλειδιών τα πρωτεύοντα κλειδιά για τα οποία θα χρειαστεί ενημέρωση με το κλειδί αποκρυπτογράφησης.

Βήμα 4: Το κέντρο παραγωγής κλειδιών ενημερώνει με το κλειδί που μπορεί να χρησιμοποιηθεί για τη αποκρυπτογράφηση των στοιχείων του οχήματος τον διαχειριστή αν τα κλειδιά με τα οποία ενημερώθηκε από το διαχειριστή είναι τα ίδια οπόταν υπάρχει παραβίαση από υπέρβαση του ορίου ταχύτητας.

7.1.2 Πολιτική Ιδιωτικότητας

Η πολιτική ιδιωτικότητας ορίζει διάφορα δικαιώματα για το σύνολο των βασικών τύπων που αντιπροσωπεύουν τα δεδομένα που τυγχάνουν διαχείρισης στο σύστημα. Αρχικά ορίζουμε την ονομασία του συστήματος μας βάση και του παραδείγματος ως $Speed\ Limit\ System$ σε συντομία (SLS) και την ύπαρξη των ακόλουθων ομάδων που αντιπροσωπεύουν τις διάφορες οντότητες εσωτερικά αυτού. Ως εκ τούτου, για τα σημεία σημεία ελέγχου ορίζουμε την ομάδα GAN,για την κεντρική μονάδα του διαχειριστή ορίζουμε την ομάδα $OPER$ και την ομάδα KGC η οποία αφορά την κεντρική μονάδα παραγωγής κλειδιών προς το διαχειριστή. Ως αποτέλεσμα των παραπάνω η ιεραρχία των ομάδων εντός του συστήματος είναι η ακόλουθη $SLS[GAN, OPER, KGC]$. Ορίζουμε ως σκοπό του παρόντος σεναρίου τον έλεγχο οχημάτων για εντοπισμό παραβίασης από υπέρβαση ορίου ταχύτητας $speedCheck$. Για το σύνολο των δεδομένων που συναντήθηκαν παραπάνω ορίζουμε τους παρακάτω βασικούς τύπους.

1. Ο βασικός τύπος δομής δεδομένων του οχήματος ορίζεται ως $VDATA$ και αποτελείται από τους βασικούς τύπους πεδίων του $VDATA.VID, VDATA.Time$. Ο βασικός τύπος πεδίου του $VDATA.VID$ αναφέρεται στο αναγνωριστικό του

οχήματος ενώ ο βασικός τύπος πεδίου του $VDATA.Time$ αναφέρεται στο χρόνο στον οποίο έχει διέλθει το όχημα. Τα αντίστοιχα πεδία των παραπάνω τύπων είναι vid και $time$.

2. Ο βασικός τύπος που αναφέρεται στα κρυπτογραφημένα στοιχεία που καταγράφονται και αποστέλλονται στο διαχειριστή κάθε φορά που υπάρχει παραβίαση του ορίου ταχύτητας ορίζεται ως EED. Είναι τύπος που καταχωρείται ανεξάρτητα της παραπάνω δομής των στοιχείων του οχήματος.
3. Ο βασικός τύπος για τα δημόσια κλειδιά τα οποία παράγονται σε κάθε σημείο ελέγχου για σκοπούς κρυπτογράφησης των στοιχείων του οχήματος ορίζεται ως PK. Δεν αποθηκεύεται σε δομή ενώ από αυτό για ένα όχημα ορίζουμε τις τιμές όπως αυτές αναγράφονται σε κάθε σημείο ελέγχου pk_1 η οποία δημιουργείται από το πρώτο σημείο ελέγχου και pk_2 από το δεύτερο σημείο ελέγχου για τη διατύπωση της συνθήκης υπέρβασης ορίου ταχύτητας και παραβίασης στο σύστημα. Είναι τύπος που καταχωρείται ανεξάρτητα της παραπάνω δομής των στοιχείων του οχήματος
4. Ο βασικός τύπος του κλειδιού που απαιτείται για την αποκρυπτογράφηση των στοιχείων του οχήματος από το κεντρικό διαχειριστή στις περιπτώσεις παραβίασης του ορίου ταχύτητας ορίζεται ως SK. Θεωρείται ξεχωριστός τύπος ο οποίος δεν αφορά οποιαδήποτε δομή.

Ως προς τις κατηγορίες των βασικών τύπων πεδίων της δομής του $VDATA$. Ο χρόνος δεν μπορεί να οδηγήσει σε ταυτοποίηση ενός οχήματος ενώ τα στοιχεία του VID μπορούν να ταυτοποιήσουν μοναδικά ένα όχημα και ως εκ τούτου αυτά ανήκουν στην κατηγορία των τύπων ταυτοποίησης. Με τον παραπάνω διαχωρισμό έχουμε ότι για το σύνολο των βασικών τύπων πεδίου του $VDATA$ το σύνολο $T^n = \{VDATA.Time\}$ και το σύνολο $T^P = \{VDATA.VID\}$. Με τον καθορισμό των παραπάνω μπορούμε να δώσουμε και τη συνθήκη βάση της οποίας διαχωρίζονται τα δικαιώματα στο σύστημα και προκύπτει από τις τιμές του βασικού τύπου PK που καταγράφονται στα σημεία ελέγχου όταν αυτές είναι ίδιες οπόταν $cond: pk_1 == pk_2$.

Η πολιτική ιδιωτικότητας του συστήματος ορίζει τα παρακάτω αναφορικά με τους προαναφερθέντες βασικούς τύπους συνθήκη και σκοπό.

1. Τα σημεία ελέγχου δικαιούνται να λάβουν πρόσβαση στη δομή των πληροφοριών ενός οχήματος και να χειριστούν ανάλογα τους βασικούς τύπους της δομής εσωτερικά. Η πρόσβαση αυτή γίνεται χωρίς την ικανοποίηση κάποιας συνθήκης.
2. Όσον αφορά τα δεδομένα που αφορούν τους βασικούς τύπους πεδίων για τα στοιχεία του οχήματος $VDATA.\mathrm{VID}$ και χρόνου διέλευσης $VDATA.\mathrm{Time}$ αυτά αφορούν αποκλειστικά διαδικασίες και λειτουργίες του συστήματος που λαμβάνουν χώρα στα σημεία ελέγχου. Εκεί μπορούν να καταγραφούν, αναγνωστούν, παρέχοντας έτσι και το δικαίωμα ταυτοποίησης ενός οχήματος από το $VDATA.\mathrm{VID}$. Τα δικαιώματα αυτά ανατίθενται χωρίς την ανάγκη ικανοποίησης οποιασδήποτε συνθήκης.
3. Όσον αφορά τα δεδομένα που αφορούν τον βασικό τύπο του EED τα σημεία ελέγχου μπορούν να εγγράψουν και να αποκαλύψουν τέτοιες πληροφορίες προς το διαχειριστή μόνο στην περίπτωση υπέρβασης του ορίου ταχύτητας. Αυτός δικαιούται με τη σειρά του να αποκτήσει πρόσβαση σε αυτά και να τα διαβάσει όταν επιβεβαιωθεί η παραβίαση και έχει λάβει το κλειδί αποκρυπτογράφησης τους.
4. Όσον αφορά τα δεδομένα που αφορούν τον βασικό τύπο των δημόσιων κλειδιών κρυπτογράφησης (PK) όλοι δικαιούνται να λάβουν πρόσβαση και να τα διαβάσουν χωρίς την ικανοποίηση οποιασδήποτε συνθήκης για σκοπούς ελέγχου παραβίασης, ενώ το δικαίωμα εγγραφής παρέχεται αποκλειστικά και μόνο στα σημεία ελέγχου χωρίς την ικανοποίηση οποιασδήποτε συνθήκης. Τα δικαιώματα αποκάλυψης ορίζονται με τη σειρά των βημάτων παραπάνω οπόταν τα σημεία ελέγχου δικαιούνται να τα αποκαλύψουν σε περίπτωση παραβίασης και μόνο στο διαχειριστή και αυτός με τη σειρά του και πάλι στη περίπτωση παραβίασης δικαιούνται να τα αποκαλύψει προς τη μονάδα παραγωγής κλειδιών.
5. Όσον αφορά τον τελευταίο βασικό τύπο στο σύστημα μας αυτόν που αφορά τα δεδομένα των κλειδιών αποκρυπτογράφησης (SK) η μονάδα παραγωγής κλειδιών δικαιούται να το καταγράψει στις περιπτώσεις παραβίασης και να το αποκαλύψει προς το διαχειριστή ο οποίος δικαιούται πρόσβαση και ανάγνωση σε αυτά όταν υπάρχει παραβίαση.

Με τη διατύπωση και των παραπάνω είμαστε πλέον σε θέση να δώσουμε τις ιεραρχίες των δικαιωμάτων για τους βασικούς τύπους της δομής του $VDATA$ με τα επιμέρους

δικαιώματα για τους βασικούς τύπους των πεδίων του $VDATA.Time, VDATA.VID$ αλλά και του κάθε τύπου ανεξάρτητα δομής δηλαδή EED, PK, SK. Ως εκ τούτου, ορίζουμε την ιεραρχία δικαιωμάτων H_1 για το βασικό τύπο δομής $VDATA$. Ορίζουμε την ιεραρχία δικαιωμάτων H_2 η οποία αφορά το βασικό τύπο του EED, την ιεραρχία δικαιωμάτων H_3 η οποία αφορά τον βασικό τύπο του PK και τέλος την ιεραρχία δικαιωμάτων H_4 για τον βασικό τύπου του SK. Οι ιεραρχίες δικαιωμάτων H_2, H_3, H_4 εφόσον αφορούν βασικούς τύπους ανεξάρτητους δομής έχουν το σύνολο $\widetilde{FP} = \emptyset$. Σκοπός που συνοδεύει όλες τις παραπάνω ιεραρχίες όπως ορίσαμε και παραπάνω είναι το $speedCheck$.

$$H_1 = SLS[GAN: \left(true, \{access, identify\}, \langle \begin{matrix} VDATA.Time: \{access, read, write\}; \\ VDATA.VID: \{access, read, write\}; \end{matrix} \rangle\right)]$$

$$H_2 = SLS[GAN: (pk_1 == pk_2, \{write, disclose\ OPER\}),$$

$$OPER: (pk_1 == pk_2, \{access, read\})]$$

$$H_3 = SLS[GAN: (true, \{read, write, access\})(pk_1 == pk_2, \{disclose\ OPER\}),$$

$$OPER: (true, \{read, access\}, (pk_1 == pk_2, \{disclose\ KGC\}),$$

$$KGC: (true, \{read, access\})]$$

$$H_4 = SLS[OPER: (pk_1 == pk_2, \{read, access\}),$$

$$KGC: (pk_1 == pk_2, \{write, disclose\ OPER\})]$$

Τυπικά η πολιτική ιδιωτικότητας βάσει και των προαναφερθέντων ορίζεται ως ακολούθως. Ο σκοπός που συνοδεύει τις ιεραρχίες δικαιωμάτων όπως αναφέραμε και παραπάνω είναι ο έλεγχος για παραβίαση ορίου ταχύτητας $speedCheck$.

$$\mathcal{P} = \quad VDATA \gg \langle H_1, speedCheck \rangle; EED \gg \langle H_2, speedCheck \rangle;$$
$$PK \gg \langle H_3, speedCheck \rangle; SK \gg \langle H_4, speedCheck \rangle;$$

7.1.3 Μοντελοποίηση Συστήματος

Ακολουθεί η μοντελοποίηση του συστήματος αναφορικά με την επιβολή προστίμου από υπέρβαση του ορίου ταχύτητας για ένα όχημα. Οι ονομασίες των ομάδων ισχύουν από

παραπάνω.

$$S = (\nu\, SLS)\ ((\nu\, GAN)GN_1\langle speedCheck\rangle$$
$$|(\nu\, GAN)GN_2\langle speedCheck\rangle$$
$$|(\nu\, OPER)OPR\langle speedCheck\rangle$$
$$|(\nu\, KGC)KGC_1\langle speedCheck\rangle)$$

$$GN_1 = vdataCH(x{:}T_{Time}, y{:}T_{VID}).(\nu\, t_1{:}VDATA.Time, VID_1{:}VDATA.VID).\bar{x}\langle t_1\rangle.$$
$$\bar{y}\langle VID_1\rangle.(\nu\, PK_1{:}T_{PK}).(\nu\, pk_1{:}PK).\overline{PK_1}\langle pk_1\rangle.PK_2(pk_2{:}PK).$$
$$if\ (pk_1 == pk_2)\ then\ (\nu\, ED_1{:}T_{EED}).(\nu\, evd_1{:}EED).$$
$$\overline{ED_1}\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0$$

$$GN_2 = vvdataCH(xx{:}T_{Time}, yy{:}T_{VID}).(\nu\, t_2{:}VDATA.Time, VID_2{:}VDATA.VID).$$
$$\overline{xx}\langle t_2\rangle.\overline{yy}\langle VID_2\rangle.(\nu\, PK_2{:}T_{PK}).(\nu\, pk_2{:}PK).\overline{PK_2}\langle pk_2\rangle.PK_1(pk_1{:}PK).$$
$$if\ (pk_2 == pk_1)\ then\ (\nu\, ED_2{:}T_{EED}).(\nu\, evd_2{:}EED).$$
$$\overline{ED_2}\langle evd_2\rangle.\overline{STO_{2PK}}\langle PK_2\rangle.\overline{STO_{2EED}}\langle ED_2\rangle.0$$

$$OPR = STO_{1PK}(pkey_1{:}T_{PK}).STO_{2PK}(pkey_2{:}T_{PK}).pkey_1(pk_1{:}PK).$$
$$pkey_2(pk_2{:}PK).if(pk_1 == pk_2)\ then\ \overline{tokeyG}\langle pkey_1, pkey_2\rangle.$$
$$rcvSK(secKey{:}T_{SK}).secKey(sk{:}SK).STO_{1EED}(EVD_1{:}T_{EED}).EVD_1(ed{:}EED)$$
$$STO_{2EED}(EVD_2{:}T_{EED}).EVD_2(edd{:}EED).0$$

$$KGC_1 = tokeyG(xf{:}T_{PK}, xm{:}T_{PK}).xf(pk_1{:}PK).xm(pk_2{:}PK).$$
$$if(pk_1 == pk_2)\ then\ (\nu\, secretKey:\ T_{SK}).(\nu\, secK:SK).$$
$$\overline{secretKey}\langle secK\rangle.\overline{rcvSK}\langle secretKey\rangle.0$$

Η συμπεριφορά της διεργασίας για το σημείο ελέγχου 1 ορίζεται ως εξής. Αρχικά λαμβάνει πρόσβαση στη δομή και στα κανάλια χρόνου και στοιχείων οχήματος τα οποία ενημερώνει σχετικά με τις τιμές που αφορούν το όχημα για το οποίο εφαρμόζει έλεγχο. Το κανάλι της δομής έχει τύπο $T_{VDATA} = SLS[T_{Time}, T_{VID}]$ και τα εσωτερικά κανάλια είναι τα κανάλια για τα πεδία χρόνου και στοιχείων οχήματος με τύπο $SLS[VDATA.Time], SLS[VDATA.VID]$ αντίστοιχα. Με τα στοιχεία αυτά που λαμβάνει δημιουργεί το πρωτεύον κλειδί για το όχημα και το αντίστοιχο κανάλι τύπου $T_{PK} = SLS[PK]$. Αναμένει να λάβει είσοδο το κλειδί που έχει καταγράψει η διεργασία από το

δεύτερο σημείο ελέγχου σε ίδιας μορφής κανάλι και μετά την ανάγνωση της τιμής που λαμβάνει ελέγχει κατά πόσο η τιμή αυτή είναι η ίδια με αυτή που έχει καταγράψει ο ίδιος οπόταν υπάρχει παραβίαση του ορίου ταχύτητας. Τότε δημιουργεί το κανάλι και τη πληροφορία για τα στοιχεία παραβίασης που θα αποστείλει στο διαχειριστή. Το κανάλι αυτό έχει τύπο $T_{EED} = SLS[EED]$. Η ενημέρωση του διαχειριστή γίνεται μέσω καναλιών προς το διαχειριστή για τα παραπάνω στοιχεία και το πρωτεύον κλειδί οπόταν κανάλια με τύπο$T_{chOPEREED} = OPER[T_{EED}]$ και $T_{chOPERPK} = OPER[T_{PK}]$ αντίστοιχα.

Η διεργασία του σημείου ελέγχου 2 εφαρμόζει την ίδια συμπεριφορά με το αντίστοιχο στο ένα.

Η διεργασία του κεντρικού διαχειριστή αναμένει τα πρωτεύοντα κλειδιά του οχήματος ούτως ώστε να εξασφαλίσει την παραβίαση στο σύστημα μέσα από τα κανάλια που αναφέραμε παραπάνω. Εφόσον λάβει πρόσβαση σε αυτά τα διαβάσει ελέγχει την ισότητα τους και όταν εντοπίσει τη παραβίαση τότε αποκαλύπτει τα κλειδιά στη διεργασία του κέντρου παραγωγής κλειδιών ούτως ώστε να ενημερωθεί με το κλειδί αποκρυπτογράφησης των στοιχείων της παραβίασης που έχει λάβει ωστόσο δεν μπορεί να διαβάσει. Η αίτηση αυτή γίνεται μέσω του καναλιού με τύπο $T_{chKGC} = KGC[T_{PK}, T_{PK}]$ και αναμένει είσοδο από το κέντρο παραγωγής κλειδιών μέσω καναλιού με τύπο $T_{chOPERSK} = OPER[T_{SK}]$. Το κανάλι T_{SK} περιέχει το κλειδί αποκρυπτογράφησης οπόταν έχει τύπο $T_{SK} = SLS[SK]$. Εφόσον το παραλάβει τότε διαβάζει τα στοιχεία παραβίασης από το όχημα από τα κανάλια που ανέμενε σαν είσοδο από τα σημεία ελέγχου.

Η διεργασία του κέντρου παραγωγής κλειδιών αναμένει ενημέρωση από τα κλειδιά για τη παραβίαση μέσω του καναλιού που περιεγράφηκε παραπάνω από το διαχειριστή τα διαβάζει και εάν είναι τα ίδια οπόταν υπάρχει παραβίαση τότε καταγράφει αποκαλύπτει το κλειδί αποκρυπτογράφησης στη διεργασία του κεντρικού διαχειριστή.

Οι βασικοί τύποι για τις πληροφορίες και δομή ισχύουν από παραπάνω οπόταν $VDATA = \{time: VDATA.Time, vid: VDATA.VID\}, ED, PK, SK$.

7.1.4 Έλεγχος Τύπων

Για την εκτέλεση του ελέγχου τύπων θεωρείται το περιβάλλον Γ το οποίο ισούται με:

$$\Gamma = vdataCH: T_{VDATA} \cdot x: T_{Time} \cdot y: T_{VID} \cdot PK_1: T_{PK} \cdot pk_1: PK \cdot ED_1: T_{EED} \cdot evd_1: EED$$
$$\cdot STO_{1PK}: T_{chOPERPK} \cdot STO_{2PK}: T_{chPERPK} \cdot STO_{1EED}: T_{chOPEREED} \cdot xx: T_{Time}$$
$$\cdot STO_{2EED}: T_{chOPEREED} \cdot T_{chOPERPK} \cdot t_1: VDATA.Time \cdot VID_1: VDATA.VID$$
$$\cdot vvdataCH: T_{VDATA} \cdot yy: T_{VID} \cdot PK_2: T_{PK} \cdot pk_2: PK \cdot ED_2: T_{EED} \cdot evd_2: EED$$
$$\cdot EVD_1: T_{EED} \cdot EVD_2: T_{EED} \cdot ed: EED \cdot EVD_2: T_{EED} \cdot edd: EED \cdot t_2: VDATA.Time$$
$$\cdot VID_2: VDATA.VID \cdot pkey_1: T_{PK} \cdot pkey_2: T_{PK} \cdot tokeyG: T_{chKGC} \cdot secKey: T_{SK}$$
$$\cdot sk: SK \cdot xf: T_{PK} \cdot xm: T_{PK} \cdot secretKey: T_{SK} \cdot secK: SK \cdot rcvSK: T_{chOPERSK}$$

Για τη διεργασία

$$GN_1 = vdataCH(x: T_{Time}, y: T_{VID}).(\nu\ t_1: VDATA.Time, VID_1: VDATA.VID).\bar{x}\langle t_1\rangle.$$
$$\bar{y}\langle VID_1\rangle.(\nu\ PK_1: T_{PK}).(\nu\ pk_1: PK).\overline{PK_1}\langle pk_1\rangle.PK_2(pk_2: PK).$$
$$if\ (pk_1 == pk_2)\ then\ (\nu\ ED_1: T_{EED}).(\nu\ evd_1: EED).$$
$$\overline{ED_1}\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0$$

έχουμε τα εξής:

$$\Gamma \vdash 0 \rhd \emptyset, true$$

$(κανόνας\ Nil)$

$$\Gamma \vdash \overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$$
$$EED: (\{disclose\ OPER\}, true)$$

$(κανόνας\ Out)$

$$\Gamma \vdash \overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$$
$$PK: (\{disclose\ OPER\}, true).$$
$$EED: (\{disclose\ OPER\}, true)$$

$(κανόνας\ Out)$

$$\Gamma \vdash \overline{ED_1}\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$$
$$PK: (\{disclose\ OPER\}, true).$$
$$EED: (\{write, disclose\ OPER\}, true)$$

$(κανόνας\ Out)$

$$\Gamma \vdash if\ (pk_1 == pk_2)\ then\ (\nu\ ED_1: T_{EED}).(\nu\ evd_1: EED).$$
$$\overline{ED_1}\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$$
$$PK: (\{disclose\ OPER\}, pk_1 == pk_2).$$
$$EED: (\{write, disclose\ OPER\}, pk_1 == pk_2)$$

$(κανόνας\ If, κανόνας\ ResNP)$

$\Gamma \vdash PK_2(pk_2{:}\,PK).\,if\ (pk_1 == pk_2)\ then\ (\nu\ ED_1{:}\,T_{EED}).\,(\nu\ evd_1{:}\,EED).$

$\overline{ED}_1\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$

$PK{:}\,(\{read\}, true).$

$PK : (\{disclose\ OPER\}, pk_1 == pk_2).$

$EED{:}\,(\{write, disclose\ OPER\}, pk_1 == pk_2)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash \overline{PK}_1\langle pk_1\rangle.PK_2(pk_2{:}\,PK).\,if\ (pk_1 == pk_2)\ then\ (\nu\ ED_1{:}\,T_{EED}).\,(\nu\ evd_1{:}\,EED).$

$\overline{ED}_1\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$

$PK{:}\,(\{write, read\}, true).$

$PK : (\{disclose\ OPER\}, pk_1 == pk_2).$

$EED{:}\,(\{write, disclose\ OPER\}, pk_1 == pk_2)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash \bar{y}\langle VID_1\rangle.(\nu\ PK_1{:}\,T_{PK}).(\nu\ pk_1{:}\,PK).\overline{PK}_1\langle pk_1\rangle.PK_2(pk_2{:}\,PK).$

$if\ (pk_1 == pk_2)\ then\ (\nu\ ED_1{:}\,T_{EED}).\,(\nu\ evd_1{:}\,EED).$

$\overline{ED}_1\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$

$VDATA.VID{:}\,(\{write\}, true).$

$VDATA{:}\,(\{identify\}, true).$

$PK{:}\,(\{write, read\}, true).$

$PK : (\{disclose\ OPER\}, pk_1 == pk_2).$

$EED{:}\,(\{write, disclose\ OPER\}, pk_1 == pk_2)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out, \kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP)$

$\Gamma \vdash \bar{x}\langle t_1\rangle.\bar{y}\langle VID_1\rangle.(\nu\ PK_1{:}\,T_{PK}).(\nu\ pk_1{:}\,PK).\overline{PK}_1\langle pk_1\rangle.PK_2(pk_2{:}\,PK).$

$if(pk_1 == pk_2)\ then\ (\nu\ ED_1{:}\,T_{EED}).\,(\nu\ evd_1{:}\,EED).$

$\overline{ED}_1\langle evd_1\rangle.\overline{STO_{1PK}}\langle PK_1\rangle.\overline{STO_{1EED}}\langle ED_1\rangle.0 \rhd$

$VDATA.Time{:}\,(\{write\}, true).$

$VDATA.VID{:}\,(\{write\}, true).$

$VDATA{:}\,(\{identify\}, true).$

$PK{:}\,(\{write, read\}, true).$

$PK : (\{disclose\ OPER\}, pk_1 == pk_2).$

$EED{:}\,(\{write, disclose\ OPER\}, pk_1 == pk_2)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash vdataCH(x{:}\,T_{Time}, y{:}\,T_{VID}).(\nu\ t_1{:}\,VDATA.Time, VID_1{:}\,VDATA.VID).\bar{x}\langle t_1\rangle.$

$\bar{y}\langle VID_1\rangle.(\nu\ PK_1{:}T_{PK}).(\nu\ pk_1{:}PK).\overline{\overline{PK}_1}\langle pk_1\rangle.PK_2(pk_2{:}PK).$

$if\ (pk_1 == pk_2)\ then\ (\nu\ ED_1{:}T_{EED}).(\nu\ evd_1{:}EED).$

$\overline{\overline{ED}_1}\langle evd_1\rangle.\overline{\overline{STO_{1PK}}}\langle PK_1\rangle.\overline{\overline{STO_{1EED}}}\langle ED_1\rangle.0 \rhd$

$VDATA.Time{:}(\{access, write\}, true).$

$VDATA.VID{:}(\{access, write\}, true).$

$VDATA{:}(\{identify\}, true).$

$PK{:}(\{write, read\}, true).$

$PK : (\{disclose\ OPER\}, pk_1 == pk_2).$

$EED{:}(\{write, disclose\ OPER\}, pk_1 == pk_2)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In, \kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP)$

$\Gamma \vdash (\nu\ \mathrm{GAN})GN_1\langle speedCheck\rangle \rhd$

$VDATA.Time \gg \langle GAN[speedCheck, true], \{access, write\}\rangle;$

$VDATA.VID \gg \langle GAN[speedCheck, true], \{access, write\}\rangle;$

$VDATA \gg \langle GAN[speedCheck, true], \{identify\}\rangle;$

$PK \gg \langle GAN[speedCheck, true], \{write, read\}\rangle;$

$PK \gg \langle GAN[speedCheck, pk_1 == pk_2], \{disclose\ OPER\}\rangle;$

$EED \gg \langle GAN[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResGP)$

Η συμπεριφορά του GN_2, ορίζεται αντίστοιχα του GN_1 οπόταν ο έλεγχος των τύπων δίνει ακριβώς την ίδια διεπαφή αναφορικά με τα ασκούμενα δικαιώματα στο σύνολο των βασικών τύπων.

Προχωρούμε στον έλεγχο τύπων για τη διεργασία του OPR.

$OPR = STO_{1PK}(pkey_1{:}T_{PK}).STO_{2PK}(pkey_2{:}T_{PK}).pkey_1(pk_1{:}PK).$

$pkey_2(pk_2{:}PK).if(pk_1 == pk_2)\ then\ \overline{\overline{tokeyG}}\langle pkey_1, pkey_2\rangle.$

$rcvSK(secKey{:}T_{SK}).secKey(sk{:}SK).STO_{1EED}(EVD_1{:}T_{EED}).EVD_1(ed{:}EED)$

$STO_{2EED}(EVD_2{:}T_{EED}).EVD_2(edd{:}EED).0$

όπου έχουμε τα παρακάτω:

$\Gamma \vdash\ 0\ \rhd\ \emptyset, true$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Nil)$

$\Gamma \vdash EVD_2(edd{:}EED).0 \rhd EED{:}(\{read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash STO_{2EED}(EVD_2{:}\,T_{EED}).\,EVD_2(edd{:}\,EED).\,0 \rhd EED{:}\,(\{access, read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash EVD_1(ed{:}\,EED).STO_{2EED}(EVD_2{:}\,T_{EED}).\,EVD_2(edd{:}\,EED).\,0 \rhd$
$EED{:}\,(\{access, read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash STO_{1EED}(EVD_1{:}\,T_{EED}).\,EVD_1(ed{:}\,EED)$
$STO_{2EED}(EVD_2{:}\,T_{EED}).\,EVD_2(edd{:}\,EED).\,0 \rhd$
$EED{:}\,(\{access, read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash secKey(sk{:}\,SK).\,STO_{1EED}(EVD_1{:}\,T_{EED}).\,EVD_1(ed{:}\,EED)$
$STO_{2EED}(EVD_2{:}\,T_{EED}).\,EVD_2(edd{:}\,EED).\,0 \rhd$
$EED{:}\,(\{access, read\}, true).$
$SK{:}\,(\{read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash rcvSK(secKey{:}\,T_{SK}).\,secKey(sk{:}\,SK).\,STO_{1EED}(EVD_1{:}\,T_{EED}).\,EVD_1(ed{:}\,EED)$
$STO_{2EED}(EVD_2{:}\,T_{EED}).\,EVD_2(edd{:}\,EED).\,0 \rhd$
$EED{:}\,(\{access, read\}, true).$
$SK{:}\,(\{access, read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash \overline{tokeyG}\langle pkey_1, pkey_2\rangle.$
$rcvSK(secKey{:}\,T_{SK}).\,secKey(sk{:}\,SK).\,STO_{1EED}(EVD_1{:}\,T_{EED}).\,EVD_1(ed{:}\,EED)$
$STO_{2EED}(EVD_2{:}\,T_{EED}).\,EVD_2(edd{:}\,EED).\,0 \rhd$
$EED{:}\,(\{access, read\}, true).$
$SK{:}\,(\{access, read\}, true).$
$PK{:}\,(\{disclose\ KGC\}, true)$

$(κανόνας\ Out)$

$\Gamma \vdash if\,(pk_1 == pk_2)\ then\ \overline{tokeyG}\langle pkey_1, pkey_2\rangle.$
$rcvSK(secKey{:}\,T_{SK}).\,secKey(sk{:}\,SK).\,STO_{1EED}(EVD_1{:}\,T_{EED}).\,EVD_1(ed{:}\,EED)$
$STO_{2EED}(EVD_2{:}\,T_{EED}).\,EVD_2(edd{:}\,EED).\,0 \rhd$
$EED{:}\,(\{access, read\}, pk_1 == pk_2).$
$SK{:}\,(\{access, read\}, pk_1 == pk_2).$
$PK{:}\,(\{disclose\ KGC\}, pk_1 == pk_2)$ $(κανόνας\ If)$

$\Gamma \vdash pkey_2(pk_2{:}PK).\, if\,(pk_1 == pk_2)\ then\ \overline{tokeyG}\langle pkey_1, pkey_2\rangle.$

$rcvSK(secKey{:}T_{SK}).\, secKey(sk{:}SK).\, STO_{1EED}(EVD_1{:}T_{ED}).\, EVD_1(ed{:}EED)$

$STO_{2EED}(EVD_2{:}T_{EED}).\, EVD_2(edd{:}EED).\, 0 \rhd$

$EED{:}(\{access, read\}, pk_1 == pk_2).$

$SK{:}(\{access, read\}, pk_1 == pk_2).$

$PK{:}(\{disclose\ KGC\}, pk_1 == pk_2).$

$PK{:}(\{read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash pkey_1(pk_1{:}PK).$

$pkey_2(pk_2{:}PK).\, if\,(pk_1 == pk_2)\ then\ \overline{tokeyG}\langle pkey_1, pkey_2\rangle.$

$rcvSK(secKey{:}T_{SK}).\, secKey(sk{:}SK).\, STO_{1EED}(EVD_1{:}T_{EED}).\, EVD_1(ed{:}EED)$

$STO_{2EED}(EVD_2{:}T_{EED}).\, EVD_2(edd{:}EED).\, 0 \rhd$

$EED{:}(\{access, read\}, pk_1 == pk_2).$

$SK{:}(\{access, read\}, pk_1 == pk_2).$

$PK{:}(\{disclose\ KGC\}, pk_1 == pk_2).$

$PK{:}(\{read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash STO_{2PK}(pkey_2{:}T_{PK}).\, pkey_1(pk_1{:}PK).$

$pkey_2(pk_2{:}PK).\, if\,(pk_1 == pk_2)\ then\ \overline{tokeyG}\langle pkey_1, pkey_2\rangle.$

$rcvSK(secKey{:}T_{SK}).\, secKey(sk{:}SK).\, STO_{1EED}(EVD_1{:}T_{EED}).\, EVD_1(ed{:}EED)$

$STO_{2EED}(EVD_2{:}T_{EED}).\, EVD_2(edd{:}EED).\, 0 \rhd$

$EED{:}(\{access, read\}, pk_1 == pk_2).$

$SK{:}(\{access, read\}, pk_1 == pk_2).$

$PK{:}(\{disclose\ KGC\}, pk_1 == pk_2).$

$PK{:}(\{access, read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash STO_{1PK}(pkey_1{:}T_{PK}).\, STO_{2PK}(pkey_2{:}T_{PK}).\, pkey_1(pk_1{:}PK).$

$pkey_2(pk_2{:}PK).\, if\,(pk_1 == pk_2)\ then\ \overline{tokeyG}\langle pkey_1, pkey_2\rangle.$

$rcvSK(secKey{:}T_{SK}).\, secKey(sk{:}SK).\, STO_{1EED}(EVD_1{:}T_{EED}).\, EVD_1(ed{:}EED)$

$STO_{2EED}(EVD_2{:}T_{EED}).\, EVD_2(edd{:}EED).\, 0 \rhd$

$EED{:}(\{access, read\}, pk_1 == pk_2).$

$SK{:}(\{access, read\}, pk_1 == pk_2).$

$PK: (\{disclose\ KGC\}, pk_1 == pk_2).$

$PK: (\{access, read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash (\nu\ OPER) OPR\langle speedCheck\rangle \rhd$

$EED \gg \langle OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$SK \gg \langle OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$PK \gg \langle OPER[speedCheck, pk_1 == pk_2], \{disclose\ KGC\}\rangle;$

$PK \gg \langle OPER[speedCheck, true], \{access, read\}\rangle;$

$(κανόνας\ ResGP)$

Συνεχίζουμε με τη διεργασία

$KGC_1 = tokeyG(xf: T_{PK}, xm: T_{PK}).\ xf(pk_1: PK).\ xm(pk_2: PK).$

$if(pk_1 == pk_2)\ then\ (\nu\ secretKey :\ T_{SK}).\ (\nu\ secK : SK).$

$\overline{secretKey}\langle secK\rangle.\ \overline{rcvSK}\langle secretKey\rangle.\ 0$

όπου παίρνουμε:

$\Gamma \vdash\ 0\ \rhd\ \emptyset, true$

$(κανόνας\ Nil)$

$\Gamma \vdash \overline{rcvSK}\langle secretKey\rangle.\ 0 \rhd SK: (\{disclose\ OPER\}, true)$

$(κανόνας\ Out)$

$\Gamma \vdash \overline{secretKey}\langle secK\rangle.\ \overline{rcvSK}\langle secretKey\rangle.\ 0 \rhd$

$SK: (\{write, disclose\ OPER\}, true)$

$(κανόνας\ Out)$

$\Gamma \vdash (\nu\ secretKey :\ T_{SK}).\ (\nu\ secK : SK).$

$\overline{secretKey}\langle secK\rangle.\ \overline{rcvSK}\langle secretKey\rangle.\ 0 \rhd$

$SK: (\{write, disclose\ OPER\}, true)$

$(κανόνας\ ResNP)$

$\Gamma \vdash if(pk_1 == pk_2)\ then\ (\nu\ secretKey :\ T_{SK}).\ (\nu\ secK : SK).$

$\overline{secretKey}\langle secK\rangle.\ \overline{rcvSK}\langle secretKey\rangle.\ 0 \rhd$

$SK: (\{write, disclose\ OPER\}, pk_1 == pk_2)$

$(κανόνας\ If)$

$\Gamma \vdash xm(pk_2: PK).$

$if(pk_1 == pk_2)\ then\ (\nu\ secretKey :\ T_{SK}).\ (\nu\ secK : SK).$

$\overline{secretKey}\langle secK\rangle.\overline{rcvSK}\langle secretKey\rangle.0 \rhd$

$SK: (\{write, disclose\ OPER\}, pk_1 == pk_2).$

$PK: (\{read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash xf(pk_1: PK).xm(pk_2: PK).$

$if(pk_1 == pk_2)\ then\ (\nu\ secretKey :\ T_{SK}).(\nu\ secK : SK).$

$\overline{secretKey}\langle secK\rangle.\overline{rcvSK}\langle secretKey\rangle.0 \rhd$

$SK: (\{write, disclose\ OPER\}, pk_1 == pk_2).$

$PK: (\{read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash tokeyG(xf: T_{PK}, xm: T_{PK}).xf(pk_1: PK).xm(pk_2: PK).$

$if(pk_1 == pk_2)\ then\ (\nu\ secretKey :\ T_{SK}).(\nu\ secK : SK).$

$\overline{secretKey}\langle secK\rangle.\overline{rcvSK}\langle secretKey\rangle.0 \rhd$

$SK: (\{write, disclose\ OPER\}, pk_1 == pk_2).$

$PK: (\{access, read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash (\nu\ \mathrm{KGC})KGC_1\langle speedCheck\rangle \rhd$

$SK \gg \langle KGC[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$PK \gg \langle KGC[speedCheck, true], \{access, read\}\rangle;$

$(κανόνας\ ResGP)$

Συνδυάζοντας τα παραπάνω παίρνουμε:

$\Gamma \vdash (\nu\ \mathrm{GAN})\mathrm{GN}_1\langle speedCheck\rangle$

$|(\nu\ \mathrm{GAN})\mathrm{GN}_2\langle speedCheck\rangle$

$|(\nu\ \mathrm{OPER})\mathrm{OPR}\langle speedCheck\rangle$

$|(\nu\ \mathrm{KGC})KGC_1\langle speedCheck\rangle \rhd$

$VDATA.Time \gg \langle GAN[speedCheck, true], \{access, write\}\rangle;$

$VDATA.VID \gg \langle GAN[speedCheck, true], \{access, write\}\rangle;$

$VDATA \gg \langle GAN[speedCheck, true], \{identify\}\rangle;$

$PK \gg \langle GAN[speedCheck, true], \{write, read\}\rangle;$

$PK \gg \langle GAN[speedCheck, pk_1 == pk_2], \{disclose\ OPER\}\rangle;$

$EED \gg \langle GAN[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$EED \gg \langle OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$SK \gg \langle OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$PK \gg \langle OPER[speedCheck, pk_1 == pk_2], \{disclose\ KGC\}\rangle;$

$PK \gg \langle OPER[speedCheck, true], \{access, read\}\rangle;$

$SK \gg \langle KGC[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$PK \gg \langle KGC[speedCheck, true], \{access, read\}\rangle;$

$(κανόνας\ ParS)$

Τέλος για το σύστημα (S)

$S = (\nu\ SLS)\ ((\nu\ \mathrm{GAN})\mathrm{GN}_1\langle speedCheck\rangle$

$|(\nu\ \mathrm{GAN})\mathrm{GN}_2\langle speedCheck\rangle$

$|(\nu\ \mathrm{OPER})\mathrm{OPR}\langle speedCheck\rangle$

$|(\nu\ \mathrm{KGC})\mathrm{KGC}_1\langle speedCheck\rangle)$

έχουμε ότι:

$\Gamma \vdash S \rhd$

$VDATA.Time \gg \langle SLS[GAN[speedCheck, true]], \{access, write\}\rangle;$

$VDATA.VID \gg \langle SLS[GAN[speedCheck, true], \{access, write\}\rangle;$

$VDATA \gg \langle SLS[GAN[speedCheck, true], \{identify\}\rangle;$

$PK \gg \langle SLS[GAN[speedCheck, true], \{write, read\}\rangle;$

$PK \gg \langle SLS[GAN[speedCheck, pk_1 == pk_2], \{disclose\ OPER\}\rangle;$

$EED \gg \langle SLS[GAN[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$EED \gg \langle SLS[OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$SK \gg \langle SLS[OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$PK \gg \langle SLS[OPER[speedCheck, pk_1 == pk_2], \{disclose\ KGC\}\rangle;$

$PK \gg \langle SLS[OPER[speedCheck, true], \{access, read\}\rangle;$

$SK \gg \langle SLS[KGC[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$PK \gg \langle SLS[KGC[speedCheck, true], \{access, read\}\rangle;$

$(κανόνας\ ResGS)$

7.1.5 Έλεγχος Συμμόρφωσης με την πολιτική ιδιωτικότητας

Θα αποδείξουμε ότι το παραπάνω σύστημα ικανοποιεί την πολιτική ιδιωτικότητας της παρούσας περίπτωσης χρήσης.

Η διεπαφή δικαιωμάτων που προέκυψε για το σύστημα πιο πάνω είναι η ακόλουθη.

$VDATA.Time \gg \langle SLS[GAN[speedCheck, true]], \{access, write\}\rangle;$

$VDATA.VID \gg \langle SLS[GAN[speedCheck, true], \{access, write\}\rangle;$

$VDATA \gg \langle SLS[GAN[speedCheck, true], \{identify\}\rangle;$

$PK \gg \langle SLS[GAN[speedCheck, true], \{write, read\}\rangle;$

$PK \gg \langle SLS[GAN[speedCheck, pk_1 == pk_2], \{disclose\ OPER\}\rangle;$

$EED \gg \langle SLS[GAN[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$EED \gg \langle SLS[OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$SK \gg \langle SLS[OPER[speedCheck, pk_1 == pk_2], \{access, read\}\rangle;$

$PK \gg \langle SLS[OPER[speedCheck, pk_1 == pk_2], \{disclose\ KGC\}\rangle;$

$PK \gg \langle SLS[OPER[speedCheck, true], \{access, read\}\rangle;$

$SK \gg \langle SLS[KGC[speedCheck, pk_1 == pk_2], \{write, disclose\ OPER\}\rangle;$

$PK \gg \langle SLS[KGC[speedCheck, true], \{access, read\}\rangle;$

Συνεπώς έχουμε τα παρακάτω σύνολα ομάδων:

$\widetilde{G_1} = \langle SLS, GAN\rangle$

$\widetilde{G_2} = \langle SLS, OPER\rangle$

$\widetilde{G_3} = \langle SLS, KGC\rangle$

Εξετάζουμε αρχικά το βασικό τύπο της δομής του $VDATA$ και τους αντίστοιχα βασικούς τύπους πεδίων του $VDATA.Time, VDATA.VID$.

Για το σκοπό αυτό το σύνολο των διεπαφών του $VDATA$ περιέχει τα παρακάτω:

$VDATA \gg \langle SLS[GAN[speedCheck, true]], \{identify\}\rangle;$

Αντίστοιχα το σύνολο των διεπαφών για τους βασικούς τύπους πεδίων του $VDATA$ περιέχει τα εξής:

$VDATA.Time \gg \langle SLS\big[GAN[speedCheck, true]\big], \{access, write\}\rangle;$

$VDATA.VID \gg \langle SLS[GAN[speedCheck, true]], \{access, write\}\rangle;$

Για τον βασικό τύπο του $VDATA$ μέσω της συνάρτησης $perms_{H_1}$ προκύπτουν τα ακόλουθα.

$perms_{H_1}\big(\widetilde{G_1}, speedCheck, true\big) = \{access, identify\}$

Για τον βασικό τύπο πεδίου του $VDATA.Time$ μέσω της συνάρτησης HFP_1 προκύπτουν τα ακόλουθα:

$perms_{HFP_1}(\widetilde{G_1}, speedCheck, true) = \{access, read, write\}$

Για τον βασικό τύπο πεδίου του $VDATA.VID$ μέσω της συνάρτησης HFP_2 προκύπτουν τα ακόλουθα:

$perms_{HFP_2}(\widetilde{G_1}, speedCheck, true) = \{access, read, write\}$

Για τον βασικό τύπο αναφορικά του EED και μέσω της συνάρτησης $perms_{H_2}$ προκύπτουν τα ακόλουθα:

$perms_{H_2}(\widetilde{G_1}, speedCheck, pk_1 == pk_2) = \{write, disclose\ OPER\}$

$perms_{H_2}(\widetilde{G_2}, speedCheck, pk_1 == pk_2) = \{read, access\}$

Για τον βασικό τύπο αναφορικά με το PK μέσω της συνάρτησης $perms_{H_3}$ προκύπτουν τα ακόλουθα:

$perms_{H_3}(H, \widetilde{G_1}, speedCheck, true) = \{read, write, access\}$

$perms_{H_3}(H, \widetilde{G_1}, speedCheck, pk_1 == pk_2) = \{read, write, access, disclose\ OPER\}$

$perms_{H_3}(H, \widetilde{G_2}, speedCheck, true) = \{read, access\}$

$perms_{H_3}(H, \widetilde{G_2}, speedCheck, pk_1 == pk_2) = \{read, access, disclose\ KGC\}$

$perms_{H_3}(H, \widetilde{G_3}, speedCheck, true) = \{read, access\}$

Για τον βασικό τύπο αναφορικά με το SK, μέσω της συνάρτησης $perms_{H_4}$ προκύπτουν τα ακόλουθα:

$perms_{H_4} = (\widetilde{G_2}, speedCheck, pk_1 == pk_2) = \{read, access\}$

$perms_{H_4} = (\widetilde{G_3}, speedCheck, pk_1 == pk_2) = \{write, disclose\ OPER\}$

Όπως είναι προφανές από τα παραπάνω, τα δικαιώματα που ασκούνται στο σύστημα από τις ομάδες που το αποτελούν βάσει του συγκεκριμένου σκοπού και εκάστοτε συνθήκης, για όλους τους τύπους που καθορίστηκαν και τυγχάνουν διαχείρισης σε αυτό, είναι συμβατά με τα όσα επιτρέπονται από την πολιτική ιδιωτικότητας $\mathcal{P}$ και ως εκ τούτου έχουμε από τον Ορισμό 4 ότι $\mathcal{P} \Vdash \Theta$. Εφόσον η διεπαφή Θ έχει παραχθεί από το

σύστημα της παρούσας περίπτωσης χρήσης μπορούμε να συμπεράνουμε άμεσα από τον Ορισμό 6 ότι $\mathcal{P} \vdash S$.

7.2 Ιστοσελίδα The World Disney Center

7.2.1 Περιγραφή

Το ακρωνύμιο COPPA αναφέρεται στο Children's Online Privacy Protection Act [2] αποτελεί νομοθεσία η οποία καθορίζει τους τρόπους με τους οποίους ένα διαδικτυακό σύστημα παροχής υπηρεσιών σε παιδιά, με τον όρο παιδιά εννοούμε άτομα με ηλικία μικρότερη των 13 ετών, πρέπει να συμπεριφέρεται και να παρέχει μηχανισμούς οι οποίοι να διασφαλίζουν την ιδιωτικότητα των παιδιών. Ως νομοθεσία, πρέπει να γίνεται σεβαστή από όλα τα διαδικτυακά συστήματα τα οποία συλλέγουν και επεξεργάζονται πληροφορίες που αφορούν παιδιά.

Ένας από τους σημαντικότερους κανόνες του COPPA και ο οποίος θα μας απασχολήσει στο συγκεκριμένο παράδειγμα χρήσης καθώς δίνει την υπό συνθήκη παροχή δικαιωμάτων είναι το *Verifiable Parental Consent (VPC)* το οποίο αναφέρει σχετικά το ακόλουθο. Πριν ένα σύστημα συλλέξει, χρησιμοποιήσει ή αποκαλύψει προσωπικές πληροφορίες παιδιών, ο διαχειριστής του συστήματος θα πρέπει οπωσδήποτε να εξασφαλίσει τη γονική συναίνεση από το γονέα του παιδιού. Ο διαχειριστής για να μπορεί να εξασφαλίσει τη γονική συναίνεση από το γονέα του παιδιού δικαιούται να λάβει το όνομα του παιδιού αποκλειστικά χωρίς επίθετο για να μην προσδιορίζει μοναδικά κάποιο από αυτά και ένα τρόπο για ηλεκτρονική επικοινωνία με το γονέα. Συνεπώς, παρατηρούμε ότι υπάρχει μια διαφοροποίησή ως πρός την παροχή δικαιωμάτων από την ικανοποίηση κάποιων συνθηκών όπως η ηλικία του παιδιού αλλά και η εξασφάλιση γονικής συναίνεσης για αυτό και ενσωματώνεται το συγκεκριμένο παράδειγμα στα πλαίσια της παρούσας εργασίας καθώς καλύπτει το προτεινόμενο πλαίσιο διαχωρισμό δικαιωμάτων βάσει συνθηκών. Μια ιστοσελίδα η οποία ικανοποιεί πλήρως τις απαιτήσεις οι οποίες ορίζονται από το COPPA, είναι η ιστοσελίδα της The Walt Disney Company [13], η οποία ασχολείται με παιδιά καθώς είναι ιστοσελίδα η οποία παρέχει υπηρεσίες που απευθύνονται σε παιδιά. Πάνω στη συγκεκριμένη πολιτική θα δώσουμε τη συγκεκριμένη περίπτωση χρήσης της μεθοδολογίας μας για τον τυπικό έλεγχο πολιτικών ιδιωτικότητα από συστήματα. Το σενάριο που θα μας απασχολήσει

αφορά την διαδικασία με την οποία είναι δυνατό να γίνει εγγραφή των παιδιών στην ιστοσελίδα του $TWDC$. Αρχικά θα δώσουμε την τυπική διατύπωση της πολιτικής του συστήματος βάσει σκοπού και συνθηκών για τη διαδικασία της εγγραφής των παιδιών όπως αυτή εμφανίζεται στην ιστοσελίδα της $TWDC$. Στη συνέχεια θα δώσουμε τη μοντελοποίηση του συστήματος το οποίο χειρίζεται την εγγραφή των παιδιών σε υπηρεσίες της συγκεκριμένης ιστοσελίδας και τέλος με την εφαρμογή του συστήματος των τύπων θα είμαστε σε θέση να αποδείξουμε την ικανοποίηση της πολιτικής από το σύστημα εγγραφών.

7.2.2 Πολιτική Ιδιωτικότητας

Προτού προχωρήσουμε στην τυπική διατύπωση της πολιτικής η οποία ορίζεται και στην αντίστοιχη ιστοσελίδα θα ορίσουμε τις ομάδες για την ιεραρχία των ομάδων του παρόντος σεναρίου. Ορίζουμε στο υψηλότερο επίπεδο την ονομασία της ομάδας του συστήματος με το ακρωνύμιο του τίτλου της The Walt Disney Company, $TWDC$. Ορίζουμε την ομάδα $Operator$, η οποία αναφέρεται στους υπεύθυνους διαχείρισης της ιστοσελίδας, την ομάδα $Child$ η οποία αναφέρεται στην ομάδα των παιδιών που επιθυμούν να εγγραφούν στο σύστημα της ιστοσελίδας και την ομάδα $Parent$ η οποία αναφέρεται στο γονέα του παιδιού ο οποίος θα πρέπει να δώσει τη συναίνεση του πριν γίνει η οποιαδήποτε συλλογή δεδομένων από τον κάποιο στην ομάδα διαχείρισης της ιστοσελίδας για κάποιο παιδί. Συνεπώς η ιεραρχία των ομάδων εντός του συστήματος του είναι η ακόλουθη $TWDC$ $[Operator, Child, Parent]$.

Τα παιδιά μπορούν να εγγραφούν σε μια από τις υπηρεσίες της ιστοσελίδας για διάφορους σκοπούς όπως παρακολούθηση εφαρμογών με παιδικό περιεχόμενο, αλληλεπίδραση με ηλεκτρονικά παιχνίδια ή και συμμετοχή σε συζητήσεις με παιδιά της ηλικίας τους . Ο σκοπός κατ' επέκταση της λειτουργίας της συγκεκριμένης ιστοσελίδας για το παρόν σενάριο αναφέρεται στη διαδικασία εγγραφής για αυτό ορίζουμε ως το σκοπό της συγκεκριμένης πολιτικής την εγγραφή των παιδιών η οποία σχετικά δίνεται μέσα από το $Registration$.

Στο σύστημα καταχωρούνται τα παρακάτω δεδομένα για τα οποία ορίζονται και οι αντίστοιχοι βασικοί τύποι. Στο παρών σύστημα τα δεδομένα δεν αποθηκεύονται σε μια δομή αλλά το καθένα ξεχωριστά λόγω και της διαδικασίας που ακολουθείται. Ως εκ

τούτου οι βασικοί τύποι είναι ανεξάρτητοι δομής. Το πρώτο δεδομένο το οποίο αφορά τα παιδιά και διαχωρίζει και τα δικαιώματα παρακάτω ορίζοντας και σχετική συνθήκη για αυτό είναι η ηλικία τους για αυτό ορίζουμε τον βασικό τύπο του $Childage$. Ακολούθως για σκοπούς επικοινωνίας με το γονέα και εξασφάλιση της συναίνεσης του ορίζουμε τον βασικού τύπο $Email$ ο οποίος αφορά τα στοιχεία επικοινωνίας με τον γονιό. Ο βασικός τύπος $ParPerm$ αναφέρεται στην έγκριση η όχι της εγγραφής του παιδιού από το γονέα και ο τελευταίος βασικός τύπος του $ChildData$ αφορά πληροφορίες του παιδιού που καταχωρούνται στο σύστημα όταν ολοκληρώνεται η εγγραφή του και αυτό είναι εφικτό μετά την εξασφάλιση σχετικής έγκρισης από το γονιό. Όσον αφορά τις συνθήκες της πολιτικής αυτές ορίζονται βάσει των βασικών τύπων του $Childage$ και ParPerm και μέσα από τις μεταβλητές τιμές για αυτούς $childage$ και $parPerm$. Η πρώτη συνθήκη αναφέρεται στην ανάγκη εξασφάλισης γονικής συναίνεσης όταν το παιδί είναι κάτω των 13 ετών και δια αυτού ορίζεται η συνθήκη $cond_1: childage < 13$. Εφόσον το παιδί είναι κάτω των 13 τότε η δεύτερη συνθήκη για την εξασφάλιση συγκεκριμένων δικαιωμάτων αφορά την εξασφάλιση γονικής συναίνεσης και ορίζεται στην πολιτική ως $cond_2: parPerm == yes$.

Η πολιτική ιδιωτικότητας ορίζει τα παρακάτω αναφορικά με τους προαναφερθέντες βασικούς τύπους και συνθήκες.

1. Όσον αφορά δεδομένα που αφορούν την ηλικία των παιδιών και τον αντίστοιχο βασικό τύπο του $Childage$ η ομάδα παιδιού δικαιούται το πλήρες σύνολο δικαιωμάτων με το δικαίωμα αποκάλυψης να ορίζεται ως προς την ομάδα των διαχειριστών της ιστοσελίδας, και εννοείται χωρίς την ταυτοποίηση αφού ο βασικός τύπος αυτός δεν είναι δομής ενώ δεν περιορίζεται υπό οποιαδήποτε συνθήκη. Οι διαχειριστές δικαιούνται με την αποκάλυψη της ηλικίας σε αυτούς να λάβουν το πρόσβαση και να το διαβάσουν χωρίς και πάλι οποιοδήποτε περιορισμό συνθήκης.
2. Όσον αφορά δεδομένα που αφορούν την ηλεκτρονική διεύθυνση του γονέα και τον αντίστοιχο βασικού τύπου του $Email$ για την ομάδα των παιδιών ισχύουν αντίστοιχα των παραπάνω με το τύπο $Childage$, από την άλλη όμως οι διαχειριστές του συστήματος δικαιούνται πρόσβαση σε αυτά μόνο όταν η ηλικία

του παιδιού είναι τέτοια που να το επιβάλλει δηλαδή, μικρότερη των 13 ετών και ικανοποιείται η αντίστοιχη συνθήκη της πολιτικής.

3. Όσον αφορά δεδομένα που αφορούν την παροχή γονικής συναίνεσης και τον αντίστοιχο βασικό τύπου του $ParPerm$ για την ολοκλήρωση εγγραφής του παιδιού σε υπηρεσίες της ιστοσελίδας η ομάδα του γονιού δικαιούται όλα τα δικαιώματα αφού είναι στοιχείο του, χωρίς την ταυτοποίηση, και ο διαχειριστής λαμβάνει πρόσβαση σε αυτό μόνο όταν και πάλι το παιδί είναι ανήλικο.
4. Όσον αφορά δεδομένα που αφορούν την ολοκλήρωση της εγγραφής των παιδιών και τον αντίστοιχο βασικό τύπου του $ChildData$ η ομάδα του παιδιού δικαιούται όλα τα δικαιώματα αφού είναι στοιχείο του, χωρίς την ταυτοποίηση. Το δικαίωμα πρόσβασης και ανάγνωσης και εγγραφής τους ξεχωριστά στο σύστημα από τους διαχειριστές γίνεται εφικτή μόνο όταν ικανοποιούνται και οι δύο συνθήκες της πολιτικής.

Με τη διατύπωση των παραπάνω είμαστε πλέον σε θέση να δώσουμε τις ιεραρχίες των δικαιωμάτων για τους βασικούς τύπους της πολιτικής. Ως εκ τούτου, ορίζουμε την ιεραρχία δικαιωμάτων για την διατύπωση της πολιτικής. Ορίζουμε την ιεραρχία δικαιωμάτων H_1 η οποία αφορά το βασικό τύπο του $Childage$ την ιεραρχία δικαιωμάτων H_2 η οποία αφορά το βασικό τύπο του $Email$, την ιεραρχία δικαιωμάτων H_3 η οποία αφορά τον βασικό τύπο του $ParPerm$ και τέλος την ιεραρχία δικαιωμάτων H_4 για το βασικό τύπο του $ChildData$. Εφόσον κανένας βασικός τύπος δεν αναφέρεται σε βασικό τύπο δομής το σύνολο του $\widetilde{FP} = \emptyset$ σε όλες τις περιπτώσεις.

$H_1 = TWDC[Operator: (true, \{access, read\}),$

$Child: (true, \{access, read, write, disclose\ Operator\}]$

$H_2 = TWDC[Operator: (childage < 13, \{access, read\}),$

$Child: (true, \{access, read, write, disclose\ Operator\}]$

$H_3 = TWDC[Operator: (childage < 13, \{access, read\}),$

$Parent: (true, \{access, read, write, disclose\ Operator\}]$

$$\mathrm{H}_4 = WDC[Operator: \begin{pmatrix} parPerm == yes \wedge childage < 13, \\ \{access, read, write\} \end{pmatrix},$$

$$Child: (true, \{access, read, write, disclose\ Opertor\}]$$

Ο σκοπός που συνοδεύει κάθε ιεραρχία δικαιωμάτων παραπάνω είναι ο σκοπός της εγγραφής και ως εκ τούτου τυπικά η διατύπωση της πολιτικής βάσει και των όσων έχουν καταγραφεί παραπάνω ολοκληρώνεται ως ακολούθως.

$\mathcal{P} = Childage \gg \langle H_1, Registration \rangle;$
$Email \gg \langle H_2, Registration \rangle;$
$ParPerm \gg \langle H_3, Registration \rangle;$
$ChildData \gg \langle H_4, Registration \rangle;$

7.2.3 Μοντελοποίηση Συστήματος

Ακολουθεί η μοντελοποίηση του συστήματος εγγραφής για ένα παιδί από την ομάδα των παιδιών για το οποίο γίνεται λήψη της γονικής συναίνεσης ένα διαχειριστή στα πλαίσια του συστήματος διαχείρισης εγγραφών και τη διεργασία του γονέα που αφορά το γονέα του παιδιού. Η μοντελοποίηση γίνεται με τη χρήση της CP calculus.

Το σύστημα ορίζεται ως:

$S = (\nu\ TWDC)\ ((\nu\ Operator) oper\langle Registration \rangle$
$\mid (\nu\ Child) child\langle Registration \rangle$
$\mid (\nu\ Parent) parent\langle Registration \rangle)$

$oper = get_{age}(age_{ch}: T_{childage}).\ age_{ch}(childage: Childage).$
$if\ (childage < 13)\ then\ get_{email}(mail: T_{email}).\ mail(parent_{email}: Email).$
$get_{perm}(permission: T_{parPerm}).\ permission(parPerm: ParPerm).$
$if\ (parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$
$rdata(childDat: ChildData).\ \overline{recordData}\langle childDat \rangle.\ 0$

$child = (\nu\ myAge: T_{childage}).\ (\nu\ mage: Childage).\ \overline{myAge}\langle mage \rangle.$
$\overline{get_{age}}\langle myAge \rangle.\ (\nu\ mpMail: T_{email}).\ (\nu\ mMail: Email).\ \overline{mpMail}\langle mMail \rangle.$
$\overline{get_{email}}\langle mpMail \rangle.\ (\nu\ myData: T_{childdata}).\ (\nu\ mData: ChildData).$

$$\overline{mData}\langle mData\rangle.\,\overline{get_{data}}\langle myData\rangle.\,0$$

$$parent = \left(\nu\ mPerm{:}\,T_{parPerm}\right)(\nu\ perm{:}\,ParPerm).\,\overline{mPerm}\langle perm\rangle.$$
$$\overline{get_{perm}}\langle mPerm\rangle.\,0$$

Η συμπεριφορά της διεργασίας του διαχειριστή ορίζεται ως εξής. Για σκοπούς της εγγραφής αναμένει σαν πρώτη είσοδο το κανάλι που αφορά τη ηλικία του παιδιού που επιθυμεί να εγγραφεί στο σύστημα. Όταν λάβει την ηλικία την διαβάζει και ελέγχει κατά πόσο αυτή είναι μικρότερη των 13 οπόταν και αναμένει από το παιδί το κανάλι αναφορικά με τα στοιχεία επικοινωνίας με το γονιό. Υπό την ικανοποίηση της ίδιας συνθήκης αναμένει και το κανάλι που αναφέρεται στη γονική συναίνεση και αφού την διαβάσει και εξακριβώσει τη θετική τιμή της τότε λαμβάνει τα στοιχεία του παιδιού για να τα καταχωρήσει στο σύστημα.

Η συμπεριφορά της διεργασίας του παιδιού ορίζεται ως εξής, το παιδί αποστέλλει το σύνολο των στοιχείων του προς το διαχειριστή εγγράφοντας τη πληροφορία αυτή σε κατάλληλα κανάλια ενημέρωσης.

Ο συμπεριφορά της διεργασίας του γονιού ορίζεται ως εξής, συγκεκριμένα ο γονέας εγγράφει και αποστέλλει στα κατάλληλα κανάλια την πληροφορία αναφορικά με την παροχή ή όχι σχετικής άδειας για το παιδί του προς το διαχειριστή.

Το κανάλι συντονισμού για την ηλικία ανάμεσα σε παιδί και διαχειριστή είναι το κανάλι με τύπο $T_{chchildage} = Operator\left[T_{childage}\right]$ όπου το εσωτερικό κανάλι δίνει πρόσβαση στη ηλικία του παιδιού και έχει τύπο $T_{childage} = TWDC[Childage]$.

Το κανάλι συντονισμού για την ηλεκτρονική διεύθυνση ανάμεσα σε παιδί και διαχειριστή είναι το κανάλι με τύπο $T_{chemail} = Operator[T_{email}]$ όπου το εσωτερικό κανάλι δίνει πρόσβαση στην ηλεκτρονική διεύθυνση επικοινωνίας και έχει τύπο $T_{email} = TWDC[Email]$.

Το κανάλι συντονισμού για την παροχή γονικής άδειας ανάμεσα σε γονέα και διαχειριστή

είναι το κανάλι με τύπο $T_{chparperm} = Operator[T_{parPerm}]$ όπου το εσωτερικό κανάλι δίνει πρόσβαση στην άδεια και έχει τύπο $T_{parPerm} = TWDC[ParPerm]$.

Το κανάλι συντονισμού για την παροχή των δεδομένων ολοκλήρωσης εγγραφής ανάμεσα σε παιδί και διαχειριστή έχει τύπο $T_{chchilddata} = Operator[T_{childdata}]$ όπου το εσωτερικό κανάλι είναι κανάλι που δίνει πρόσβαση στα στοιχεία αυτά και έχει τύπο $T_{childdata} = TWDC[ChildData]$.

Ισχύει το σύνολο των βασικών τύπων για τις αντίστοιχες πληροφορίες παραπάνω $Childage, ParPerm, Email, ChildData$.

7.2.4 Έλεγχος Τύπων

Για την εκτέλεση του ελέγχου τύπων θεωρείται το περιβάλλον Γ το οποίο ισούται με:

$$\begin{aligned}\Gamma = {} & get_{age}: T_{chchildage} \cdot age_{ch}: T_{childage} \cdot get_{email}: T_{chemail} \cdot recordData: T_{childdata} \\ & \cdot childage: Childage \cdot mail: T_{email} \cdot parent_{email}: Email \cdot permission: T_{parPerm} \\ & \cdot parPerm: ParPerm \cdot rdata: T_{childdata} \cdot childData: ChildData \\ & \cdot get_{perm}: T_{chparPerm} \cdot recordData: T_{childdata} \cdot get_{data}: T_{chchilddata} \\ & \cdot mage: Childage \cdot mpMail: T_{email} \cdot mMail: Email \cdot myData: T_{childdata} \\ & \cdot mData: ChildData \cdot mPerm: T_{parPerm} \cdot parPerm: ParPerm \\ & \cdot myAge: T_{childage}\end{aligned}$$

Από τη διεργασία

$$\begin{aligned}oper = {} & get_{age}(age_{ch}: T_{childage}).\, age_{ch}(childage: Childage). \\ & if\,(childage < 13)\ then\ get_{email}(mail: T_{email}).\, mail(parent_{email}: Email). \\ & get_{perm}(permission: T_{parPerm}).\, permission(parPerm: ParPerm). \\ & if\,(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}). \\ & rdata(childData: ChildData).\, \overline{recordData}\langle childData\rangle.\, 0\end{aligned}$$

έχουμε:

$\Gamma \vdash 0 \ \triangleright\ \emptyset, true$ $(κανόνας\ Nil)$

$\Gamma \vdash \overline{recordData}\langle childData\rangle.\, 0 \ \triangleright\ ChildData: (\{write\}, true)$ $(κανόνας\ Out)$

$\Gamma \vdash rdata(childData: ChildData).\, \overline{recordData}\langle childData\rangle.\, 0 \ \triangleright$

$ChildData: (\{read, write\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash get_{data}(rdata: T_{childdata}).$
$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \triangleright$
$ChildData: (\{access, read, write\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$
$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \triangleright$
$ChildData: (\{access, read, write\}, parPerm == yes)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ If)$

$\Gamma \vdash permission(parPerm: ParPerm).$
$if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$
$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \triangleright$
$ChildData: (\{access, read, write\}, parPerm == yes).$
$ParPerm: (\{read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash get_{perm}(permission: T_{parPerm}).permission(parPerm: ParPerm).$
$if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$
$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \triangleright$
$ChildData: (\{access, read, write\}, parPerm == yes).$
$ParPerm: (\{access, read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash mail(parent_{email}: Email).$
$get_{perm}(permission: T_{parPerm}).permission(parPerm: ParPerm).$
$if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$
$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \triangleright$
$ChildData: (\{access, read, write\}, parPerm == yes).$
$ParPerm: (\{access, read\}, true).$
$Email: (\{read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash get_{email}(mail: T_{email}).mail(parent_{email}: Email).$
$get_{perm}(permission: T_{parPerm}).permission(parPerm: ParPerm).$

$if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$

$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \rhd$

$ChildData: (\{access, read, write\}, parPerm == yes).$

$ParPerm: (\{access, read\}, true).$

$Email: (\{access, read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash if(childage < 13)\ then\ get_{email}(mail: T_{email}).mail(parent_{email}: Email).$

$get_{perm}(permission: T_{parPerm}).permission(parPerm: ParPerm).$

$if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$

$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \rhd$

$ChildData: (\{access, read, write\}, parPerm == yes \wedge childage < 13).$

$ParPerm: (\{access, read\}, childage < 13).$

$Email: (\{access, read\}, childage < 13)$

$(κανόνας\ If)$

$\Gamma \vdash age_{ch}(childage: Childage).$

$if(childage < 13)\ then\ get_{email}(mail: T_{email}).mail(parent_{email}: Email).$

$get_{perm}(permission: T_{parPerm}).permission(parPerm: ParPerm).$

$if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$

$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \rhd$

$ChildData: (\{access, read, write\}, parPerm == yes \wedge childage < 13).$

$ParPerm: (\{access, read\}, childage < 13).$

$Email: (\{access, read\}, childage < 13).$

$Childage: (\{read\}, true)$

$(κανόνας\ In)$

$\Gamma \vdash get_{age}(age_{ch}: T_{childage}).age_{ch}(childage: Childage).$

$if(childage < 13) then\ get_{email}(mail: T_{email}).mail(parent_{email}: Email).$

$get_{perm}(permission: T_{parPerm}).permission(parPerm: ParPerm).$

$if(parPerm == yes)\ then\ get_{data}(rdata: T_{childdata}).$

$rdata(childData: ChildData).\overline{recordData}\langle childData\rangle.0 \rhd$

$ChildData: (\{access, read, write\}, parPerm == yes \wedge childage < 13).$

$ParPerm: (\{access, read\}, childage < 13).$

$Email: (\{access, read\}, childage < 13).$

$Childage: (\{access, read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash (\nu\ Operator) oper\langle Registration\rangle \rhd$

$ChildData \gg \langle {}^{Operator[Registration, parPerm == yes \wedge childage < 13],}_{\{access, read, write\}} \rangle;$

$ParPerm \gg \langle Operator[Registration, childage < 13], \{access, read\}\rangle;$

$Email \gg \langle Operator[Registration, childage < 13], \{access, read\}\rangle;$

$Childage \gg \langle Operator[Registration, true], \{access, read\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResGP)$

Συνεχίζουμε με τη διεργασία

$child = (\nu\ myAge: T_{childage}).(\nu\ mage: Childage).\overline{myAge}\langle mage\rangle.$

$\overline{get_{age}}\langle myAge\rangle.(\nu\ mpMail: T_{email}).(\nu\ mMail: Email).\overline{mpMail}\langle mMail\rangle.$

$\overline{get_{email}}\langle mpMail\rangle.(\nu\ myData: T_{childdata}).(\nu\ mData: ChildData).$

$\overline{myData}\langle mData\rangle.\overline{get_{data}}\langle myData\rangle.0$

όπου παίρνουμε:

$\Gamma \vdash 0 \rhd \emptyset, true$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Nil)$

$\Gamma \vdash \overline{get_{data}}(childData: T_{childdata}).0 \rhd$

$ChildData: (\{disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash \overline{myData}\langle mData\rangle.\overline{get_{data}}\langle myData\rangle.0 \rhd$

$ChildData: (\{write, disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash \overline{get_{email}}\langle mpMail\rangle.$

$(\nu\ myData: T_{childdata}).(\nu\ mData: ChildData).\overline{myData}\langle mData\rangle.$

$\overline{get_{data}}\langle myData\rangle.0 \rhd$

$ChildData: (\{write, disclose\ Operator\}, true).$

$Email: (\{disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out, \kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP)$

$\Gamma \vdash \overline{mpMail}\langle mMail\rangle.\overline{get_{email}}\langle mpMail\rangle.$

$(\nu\ myData: T_{childdata}).(\nu\ mData: ChildData).\overline{myData}\langle mData\rangle.$

$\overline{get_{data}}\langle myData\rangle.0 \rhd$

$ChildData: (\{write, disclose\ Operator\}, true).$

$Email : (\{write, disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash \overline{get_{age}}\langle myAge\rangle.$

$(\nu\ mpMail: T_{email}).(\nu\ mMail: Email).\overline{mpMail}\langle mMail\rangle.\overline{get_{email}}\langle mpMail\rangle.$

$(\nu\ myData: T_{childdata}).(\nu\ mData: ChildData).\overline{myData}\langle mData\rangle.$

$\overline{get_{data}}\langle myData\rangle.0 \rhd$

$ChildData: (\{write, disclose\ Operator\}, true).$

$Email : (\{write, disclose\ Operator\}, true).$

$Childage : (\{disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out, \kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP)$

$\Gamma \vdash (\nu\ myAge: T_{childage}).(\nu\ mage: Childage).\overline{myAge}\langle mage\rangle.\overline{get_{age}}\langle myAge\rangle.$

$(\nu\ mpMail: T_{email}).(\nu\ mMail: Email).\overline{mpMail}\langle mMail\rangle.\overline{get_{email}}\langle mpMail\rangle.$

$(\nu\ myData: T_{childdata}).(\nu\ mData: ChildData).\overline{myData}\langle mData\rangle.$

$\overline{get_{data}}\langle myData\rangle.0 \rhd$

$ChildData: (\{write, disclose\ Operator\}, true).$

$Email : (\{write, disclose\ Operator\}, true).$

$Childage : (\{write, disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP, \kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash (\nu\ Child)child\langle Registration\rangle \rhd$

$ChildData \gg \langle Child[Registration, true], \{write, disclose\ Operator\}\rangle;$

$Email \gg \langle Child[Registration, true], \{write, disclose\ Operator\}\rangle;$

$Childage \gg \langle Child[Registration, true], \{write, disclose\ Operator\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResGP)$

Συνεχίζουμε με τη διεργασία

$parent = (\nu\ mPerm: T_{parPerm})(\nu\ perm: ParPerm).\overline{mPerm}\langle perm\rangle.$

$\overline{get_{perm}}\langle mPerm\rangle.0$

όπου παίρνουμε:

$\Gamma \vdash 0 \rhd \emptyset, true$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Nil)$

$\Gamma \vdash \overline{get_{perm}}\langle mPerm\rangle.0 \rhd ParPerm : (\{disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash \overline{mPerm}\langle perm\rangle.\,\overline{get_{perm}}\langle mPerm\rangle.\,0 \rhd$

$ParPerm : (\{write, disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash \big(\nu\ mPerm{:}\,T_{parPerm}\big)(\nu\ perm{:}\,ParPerm).\,\overline{mPerm}\langle perm\rangle.$

$\overline{get_{perm}}\langle mPerm\rangle.\,0 \rhd$

$ParPerm : (\{write, disclose\ Operator\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP)$

$\Gamma \vdash (\nu\ Parent)parent\langle Registration\rangle \rhd$

$ParPerm \gg \langle Parent[Registration, true], \{write, disclose\ Operator\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResGP)$

Συνδυάζοντας τα παραπάνω έχουμε ότι:

$\Gamma \vdash (\nu\ Operator)oper\langle Registration\rangle$

$|(\nu\ Child)child\langle Registration\rangle$

$|(\nu\ Parent)parent\langle Registration\rangle) \rhd$

$ChildData \gg \langle^{Operator[Registration,\, parPerm == yes \wedge childage < 13],}_{\{access, read, write\}}\rangle;$

$ParPerm \gg \langle Operator[Registration, childage < 13], \{access, read\}\rangle;$

$Email \gg \langle Operator[Registration, childage < 13], \{access, read\}\rangle;$

$Childage \gg \langle Operator[Registration, true], \{access, read\}\rangle;$

$ChildData \gg \langle Child[Registration, true], \{write, disclose\ Operator\}\rangle;$

$Email \gg \langle Child[Registration, true], \{write, disclose\ Operator\}\rangle;$

$Childage \gg \langle Child[Registration, true], \{write, disclose\ Operator\}\rangle;$

$ParPerm \gg \langle Parent[Registration, true], \{write, disclose\ Operator\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ParS)$

Τέλος για το σύστημα (S) έχουμε:

$S = (\nu\ TWDC)(\nu\ Operator)oper\langle Registration\rangle$

$|\ (\nu\ Child)child\langle Registration\rangle$

$|(\nu\ Parent)parent\langle Registration\rangle)$

$\Gamma \vdash S \rhd$

$ChildData \gg \langle^{TWDC[Operator[Registration,\, parPerm == yes \wedge childage < 13]],}_{\{access, read, write\}}\rangle;$

$ParPerm \gg \langle TWDC[Operator[Registration, childage < 13]], \{access, read\}\rangle;$

$Email \gg \langle TWDC[Operator[Registration, childage < 13]], \{access, read\}\rangle;$

$Childage \gg \langle TWDC[Operator[Registration, true]], \{access, read\}\rangle;$

$ChildData \gg \langle TWDC[Child[Registration, true]], \{write, diclose\ Operator\}\rangle;$

$Email \gg \langle TWDC[Child[Registration, true]], \{write, disclose\ Operator\}\rangle;$

$Childage \gg \langle TWDC[Child[Registration, true]], \{write, disclose\ Operator\}\rangle;$

$ParPerm \gg \langle TWDC[Parent[Registration, true]], \{write, disclose\ Operator\}\rangle;$

$(κανόνας\ ResGS)$

7.2.5 Έλεγχος Συμμόρφωσης με την πολιτική ιδιωτικότητας

Θα αποδείξουμε ότι το παραπάνω σύστημα ικανοποιεί την πολιτική ιδιωτικότητας της παρούσας περίπτωσης χρήσης.

Η διεπαφή δικαιωμάτων που προέκυψε για το σύστημα πιο πάνω είναι η ακόλουθη.

$ChildData \gg \langle {}^{TWDC[Operator[Registration, parPerm == yes \wedge childage < 13]]}_{\{access, read, write\}} \rangle;$

$ParPerm \gg \langle TWDC[Operator[Registration, childage < 13]], \{access, read\}\rangle;$

$Email \gg \langle TWDC[Operator[Registration, childage < 13]], \{access, read\}\rangle;$

$Childage \gg \langle TWDC[Operator[Registration, true]], \{access, read\}\rangle;$

$ChildData \gg \langle TWDC[Child[Registration, true]], \{write, disclose\ Operator\}\rangle;$

$Email \gg \langle TWDC[Child[Registration, true]], \{write, disclose\ Operator\}\rangle;$

$Childage \gg \langle TWDC[Child[Registration, true]], \{write, disclose\ Operator\}\rangle;$

$ParPerm \gg \langle TWDC[Parent[Registration, true]], \{write, disclose\ Operator\}\rangle;$

Συνεπώς έχουμε τα παρακάτω σύνολα ομάδων:

$\widetilde{G_1} = \langle TWDC, Operator\rangle$

$\widetilde{G_2} = \langle TWDC, Child\rangle$

$\widetilde{G_3} = \langle TWDC, Parent\rangle$

Το σημείο b. ως προς την ικανοποίηση της πολιτικής εκάστοτε τύπου ικανοποιείται τετριμμένα καθώς το σύνολο $\widetilde{HP_f} = \emptyset$ και οι βασικοί τύποι είναι ανεξάρτητοι δομής.

Για τον βασικό τύπο του $Childage$ μέσω της συνάρτησης $perms_{H_1}$ προκύπτουν τα ακόλουθα:

$perms_{H_1}(\widetilde{G_1}, Registration, true) = \{access, read\}$

$perms_{H_1}(\widetilde{G_2}, Registration, true) = \{access, read, write, disclose\ Operator\}$

Για τον βασικό τύπο του $Email$ μέσω της συνάρτησης $perms_{H_2}$ προκύπτουν τα ακόλουθα:

$perms_{H_2}(\widetilde{G_1}, Registration, childage < 13) = \{access, read\}$

$perms_{H_2}(\widetilde{G_2}, Registration, true) = \{access, read, write, disclose\ Operator\}$

Για τον βασικό τύπο του $ParPerm$ μέσω της συνάρτησης $perms_{H_3}$ προκύπτουν τα ακόλουθα:

$perms_{H_3}(\widetilde{G_1}, Registration, childage < 13) = \{access, read\}$

$perms_{H_3}(\widetilde{G_3}, Registration, true) = \{access, read, write, disclose\ Operator\}$

Για τον βασικό τύπο του$ChildData$ μέσω της συνάρτησης $perms_{H_4}$ προκύπτουν τα ακόλουθα:

$perms_{H_4}(\widetilde{G_1}, Registration, parPerm == yes \wedge childage < 13) =$

$\{read, write, access\}$

$perms_{H_4}(\widetilde{G_2}, Registration, true) = \{access, read, write, disclose\ Operator\}$

Όπως είναι προφανές από τα παραπάνω τα δικαιώματα που ασκούνται στο σύστημα από τις ομάδες που το αποτελούν βάση του συγκεκριμένου σκοπού και εκάστοτε συνθήκης, για όλους τους τύπους που καθορίστηκαν και τυγχάνουν διαχείρισης σε αυτό, είναι συμβατά με τα όσα επιτρέπονται από την πολιτική ιδιωτικότητας $\mathcal{P}$ και ως εκ τούτου έχουμε από τον Ορισμό 4 ότι $\mathcal{P} \Vdash \Theta$. Εφόσον η διεπαφή Θ έχει παραχθεί από το σύστημα της παρούσας περίπτωσης χρήσης μπορούμε να συμπεράνουμε άμεσα από τον Ορισμό 6 ότι $\mathcal{P} \vdash S$.

7.3 Εφαρμογή Ginger

7.3.1 Περιγραφή

Η τρίτη και τελευταία περίπτωση χρήσης προκύπτει μέσα από το [3]. Στο συγκεκριμένο άρθρο οι συγγραφείς προτείνουν ένα πλαίσιο ελέγχου πρόσβασης το οποίο αφορά εφαρμογές οι οποίες συναντώνται στην αυτοκινητοβιομηχανία. Οι εφαρμογές αυτές

συνδυάζουν πληροφοριακές δυνατότητες με τη χρήση υποδομών δικτύου όπως ($UMTS, LTE, 802.11x$ κ.τ.λ) για την εξυπηρέτηση των οδηγών και την όσο το δυνατό καλύτερη παροχή υπηρεσιών στα οχήματα τους. Μερικά παραδείγματα τέτοιων εφαρμογών είναι εφαρμογές ενημέρωσης καιρού, υπηρεσίες βάσει τοποθεσίας όπως καθοδήγηση μέσω χαρτών πλοήγησης αλλά και πιο σύνθετες εφαρμογές όπως υπηρεσίες "Pay as you drive", όπου οδηγός του οχήματος πληρώνει ανάλογα των χιλιομέτρων που έχει διανύσει με κάποιο όχημα. Αυτές οι εφαρμογές αποκτούν πρόσβαση σε προσωπικές πληροφορίες του οδηγού και του οχήματος του όπως η τοποθεσία του οχήματος, η ταχύτητα του, αλλά και στοιχεία του οδηγού. Σκοπός τους είναι να επωφεληθούν της ύπαρξης διαφόρων αισθητήρων στα οχήματα των οδηγών ούτως ώστε να παρέχουν σε αυτούς μια όσο το δυνατό καλύτερη εμπειρία οδήγησης. Η πρόσβαση ωστόσο σε ευαίσθητα δεδομένα θεωρείται αρκετά σημαντικά αφού εγείρονται διάφορα ζητήματα ασφάλειας και ιδιωτικότητας. Υπάρχουν συγκεκριμένες απαιτήσεις από τον κάθε οδηγό αλλά και εταιρείες οχημάτων για το ποιες πληροφορίες του οχήματος μπορούν να είναι προσβάσιμες και οι οποίες πρέπει να λαμβάνονται υπόψιν στα της λειτουργίας τέτοιων εφαρμογών. Λαμβάνοντας υπόψιν τα παραπάνω το $Ginger$ είναι ένας μηχανισμός ο οποίος προσπαθεί να διασφαλίσει μέσω ελέγχου πρόσβασης και παροχής δικαιωμάτων την απαιτούμενη ασφάλεια ενώ παρέχει και μηχανισμούς ιδιωτικότητας για τέτοιου είδους εφαρμογές. Για τους σκοπούς της συγκεκριμένης περίπτωσης χρήσης θα επικεντρωθούμε στο μηχανισμό του $Ginger$ που προκύπτει με την εφαρμογή αλγορίθμων συσκότισης σε δεδομένα όταν αυτά δεν είναι επιτρεπτό να αποκαλύπτονται λόγω απαίτησης ιδιωτικότητας αλλά θεωρούνται απαραίτητα για τη λειτουργικότητα συγκεκριμένων εφαρμογών.

Περιγραφή σεναρίου περίπτωσης χρήσης

Το σενάριο που περιγράφεται και το οποίο εξετάζουμε αναφέρεται σε μια εφαρμογή η οποία ενημερώνει τις καιρικές συνθήκες που επικρατούν στην περιοχή του οχήματος έχοντας πρόσβαση στην ακριβή τοποθεσία του. Μια τέτοια εφαρμογή ενεργοποιείται λαμβάνοντας πρόσβαση στην τρέχουσα τοποθεσία του οχήματος και αποστέλλοντας τη σε ένα απομακρυσμένο εξυπηρετητή ο οποίος με τη σειρά του ενημερώνει την εφαρμογή για τις καιρικές συνθήκες της τρέχουσας τοποθεσίας. Η συγκεκριμένη εφαρμογή απαιτεί πρόσβαση στην τοποθεσία του οχήματος αλλά και στο διαδίκτυο για να είναι σε θέση να επικοινωνήσει με τον απομακρυσμένο εξυπηρετητή. Για τους σκοπούς του

παραδείγματος θα επικεντρωθούμε αποκλειστικά στην ανάγκη του για χρήση της τοποθεσίας του οχήματος. Ταυτόχρονα ένας χρήστης για σκοπούς διασφάλισης της ιδιωτικότητας του επιθυμεί τη μη αποκάλυψή της τρέχουσας τοποθεσίας του. Έτσι επιθυμεί μεν την ενημέρωση για τις καιρικές συνθήκες που επικρατούν στην περιοχή που βρίσκεται ωστόσο δεν θέλει αυτή να γίνεται με τη χρήση της πραγματικής τοποθεσίας του οχήματος. Για να επιτευχθεί αυτό μια λύση που προτείνεται από το $Ginger$ είναι η χρήση μηχανισμών συσκότισης οι οποίοι θα επιτύχουν με τη σειρά τους τη μη αποκάλυψη της ακριβούς τοποθεσίας αλλά μιας συσκοτισμένης μορφής τοποθεσίας η οποία να επιτρέπει από τη μια την ενημέρωση του καιρού αλλά ταυτόχρονα να μην είναι η ίδια με την ακριβή τοποθεσία του οχήματος.

Σκοπός μας στο παρών σημείο είναι να δούμε πώς η προτεινόμενη μεθοδολογία της παρούσας εργασίας θα μπορούσε να ελέγξει και να διασφαλίσει ότι η ιδιωτικότητα του χρήστη ικανοποιείται με τη χρήση τέτοιων μηχανισμών.

7.3.2 Πολιτική Ιδιωτικότητας

Η διατύπωση της πολιτικής ιδιωτικότητας τυπικά θα γίνει βάση των απαιτήσεων του χρήστη και η οποία θα θέλαμε να ικανοποιείται από το σύστημα στο οποίο συμμετέχουν ο μηχανισμός του $Ginger$ και η εφαρμογή ενημέρωσης του καιρού στο όχημα. Ορίζουμε ως την ομάδα του συστήματος την ομάδα Weather Service Application σε συντομία WSA, οι ομάδες που ανήκουν σε αυτό είναι η εφαρμογή του $Ginger$ και η οποία δίνεται μέσα από την ομάδα $Ginger$ και η εφαρμογή του καιρού που δίνεται από την ομάδα $WeatherApp$. Επομένως η σχετική ιεραρχία των ομάδων ορίζεται ως $WSA[Ginger, WeatherApp]$. Ορίζουμε ότι σκοπός του συγκεκριμένου σεναρίου είναι η καταγραφή του καιρού ορίζοντας το σχετικό σκοπό ως $weatherRecord$. Θεωρούμε ότι στο σύστημα συναντάμε δύο βασικούς τύπους ευαίσθητων δεδομένων και οι οποίοι περιγράφουν με τη σειρά τους την ακριβή τοποθεσία του οχήματος και την τοποθεσία του οχήματος μετά από την εφαρμογή αλγορίθμων συσκότισης. Για το σκοπό αυτό ορίζουμε τους ακόλουθους βασικούς τύπους : $ExactLocation$ και $ObfLocation$ με τις αντίστοιχες καταχωρήσεις τους να ορίζονται ως $exactLocation, obfLocation$. Εφόσον οι δύο βασικοί τύποι δεν αναφέρονται σε δομή δεδομένων θεωρούμε ότι ο τύπος τους για την ανάθεση των δικαιωμάτων μέσα από την ιεραρχία παρακάτω είναι ανεξαρτήτως δομής.

Για την υπό συνθήκη παροχή δικαιωμάτων ορίζουμε τη συνθήκη η οποία ελέγχει κατά πόσο η τιμή κρυπτογράφησης της τοποθεσίας που δίνεται μέσα από τη τιμή του $obfLocation$ για το τύπο της συσκοτισμένης τοποθεσίας έχει τιμή, όπως αυτή ορίζεται και στην αντίστοιχη περίπτωση χρήσης μεγαλύτερη από μια σταθερά τιμή X, όπου η σταθερά τιμή X αναπαριστά τα ικανοποιητικά επίπεδα συσκότισης μιας τοποθεσίας σεβόμενα την ιδιωτικότητα του χρήστη για τη μη αποκάλυψη της παρούσας τοποθεσίας του και υπολογισμό των καιρικών συνθηκών. Έτσι η συνθήκη που ορίζουμε στο σύστημα μας είναι:

$$cond: obfLocation > X$$

Η πολιτική ιδιωτικότητας ορίζει τα παρακάτω αναφορικά με τους προαναφερθέντες βασικούς τύπους και συνθήκες:

1. Όσον αφορά δεδομένα που αφορούν την ακριβή τοποθεσία του οχήματος και τον αντίστοιχο βασικό τύπο του $ExactLocation$ η ομάδα της εφαρμογής του $Ginger$ δικαιούται να λάβει πρόσβαση σε αυτή και να τη διαβάσει οποτεδήποτε χωρίς την ανάγκη ικανοποίησης οποιασδήποτε συνθήκης.
2. Όσον αφορά δεδομένα που αφορούν την τοποθεσία του οχήματος μετά την εφαρμογή των αλγορίθμων συσκότισης και τον αντίστοιχο βασικό τύπο του $ObfLocation$ η ομάδα της εφαρμογής του $Ginger$ δικαιούται πλήρες σύνολο δικαιωμάτων καθώς είναι στοιχείο που δημιουργείται από την ίδια, χωρίς το δικαίωμα ταυτοποίησης αφού δεν είναι τύπος δομής ενώ το δικαίωμα αποκάλυψης αφορά την εφαρμογή ενημέρωσης καιρού. Η εφαρμογή του καιρού με τη σειρά της δικαιούται πρόσβαση και ανάγνωση της συγκεκριμένης πληροφορίας ενώ δικαιούται την αποκάλυψη της προς ένα απομακρυσμένο εξυπηρετητή μόνο όταν ικανοποιείται η συνθήκη της πολιτικής.

Με τη διατύπωση και των παραπάνω είμαστε πλέον σε θέση να δώσουμε τις ιεραρχίες των δικαιωμάτων για τους βασικούς τύπους των δεδομένων. Ως εκ τούτου, ορίζουμε την ιεραρχία δικαιωμάτων H_1 η οποία αφορά το βασικό τύπο του $ExactLocation$ και την ιεραρχία δικαιωμάτων H_2 η οποία αφορά το βασικό τύπο του $ObfLocation$. Εφόσον οι βασικοί τύποι αυτοί είναι ανεξάρτητοι δομής το σύνολο ανάθεσης δικαιωμάτων σε βασικούς τύπους πεδίου δομής $\widetilde{FP} = \emptyset$.

$$H_1 = WSA[Ginger: (true, \{access, read\})]$$

$$H_2 = WSA[Ginger: (true, \{access, read, write, disclose\ WeatherApp\}),$$

$$WeatheApp: \{(true, \{access, read\}),$$

$$(obfLocation > X, \{disclose\ RemoteServer\})]$$

Ο σκοπός που συνοδεύει κάθε ιεραρχία δικαιωμάτων παραπάνω είναι ο σκοπός της ενημέρωσης του καιρού $weatherRecord$ και ως εκ τούτου τυπικά η διατύπωση της πολιτικής βάσει και των όσων έχουν καταγραφεί παραπάνω ολοκληρώνεται ως ακολούθως.

$$\mathcal{P} = ExactLocation \gg \langle H_1, weatherRecord \rangle;$$
$$ObfLocation \gg \langle H_2, weatherRecord \rangle$$

7.3.3 Μοντελοποίηση Συστήματος

Το παρακάτω σύστημα μοντελοποιεί τη συμπεριφορά του συστήματος που συνδυάζει τη διεργασία για την εφαρμογή του $Ginger, GIN$ και τη διεργασία για την εφαρμογή του καιρού $WeatherApp, WA$. Η διεργασία GIN διαβάζει από το όχημα στο κανάλι που περιλαμβάνει την ακριβή τοποθεσία του οχήματος το οποίο έχει τύπο $T_{ExactLocation} = WSA[ExactLocation]$ στα πλαίσια του συστήματος και αφότου ενημερωθεί για τη τιμή της δημιουργεί ένα κανάλι και συγκεκριμένη τιμή για τη τοποθεσία μετά την εφαρμογή των αλγορίθμων συσκότισης το κανάλι έχει τύπο $T_{ObfLocation} = WSA[ObfLocation]$ στα πλαίσια του συστήματος ενώ το αποκαλύπτει μέσω του καναλιού σύνδεσης του με τη διεργασία WA το οποίο έχει τύπο $T_{chObfLocationW} = WeatherApp[T_{ObfLocation}]$. Η διεργασία του WA διαβάζει τη πληροφορία που της αποκαλύπτεται μέσω του παραπάνω καναλιού και ελέγχει εάν η τιμή της είναι ικανοποιητική άρα μεγαλύτερη από μια τιμή X οπόταν και την αποκαλύπτει μέσω καναλιού προς τον απομακρυσμένο εξυπηρετητή που έχει τύπο $T_{chObfLocationR} = RemoteServer[T_{ObfLocation}]$. Για τα δεδομένα των τοποθεσιών ισχύουν οι βασικοί τύποι $ExactLocation, ObfLocation.$ Οι ομάδες είναι αντίστοιχα αυτών που ορίσαμε παραπάνω.

$$S = (\nu\ WSA)((\nu\ Ginger)GIN\langle weatherRecord\rangle$$
$$|(\nu\ WeatherApp)WA\langle weatherRecord\rangle)$$

$$GIN = ExLoc(rExactLocation{:}\ T_{ExctLocation}).$$
$$rExactLocation(x{:}\ ExactLocation).\left(\nu\ ObfRegister{:}\ T_{ObfLocation}\right).$$
$$(\nu\ obfloc{:}\ ObfLocation).\overline{ObfRegister}\langle obfloc\rangle.$$
$$\overline{toWeatherApp}\langle ObfRegister\rangle.\ 0$$

$$\mathrm{WA} = toWeatherApp\left(y{:}\ T_{ObfLocation}\right).y(obflocation{:}\ ObfLocation).$$
$$if\,(obflocation > X)\ then\ toRemoteServer(y).\ 0$$

7.3.4 Έλεγχος Τύπων

Για την εκτέλεση του ελέγχου τύπων θεωρείται το περιβάλλον Γ το οποίο ισούται με

$$\Gamma = ExLoc{:}\ T_{ExactLocation}\cdot rExactLocation{:}\ T_{ExactLocation}$$
$$\cdot ObfRegister{:}\ T_{ObfLocation}\cdot toWeatherApp{:}\ T_{chObfLocationW}$$
$$\cdot toRemoteServer{:}\ T_{chObfLocationR}\cdot y{:}\ T_{ObfLocation}\cdot obflocation{:}\ ObfLocation$$
$$\cdot obfloc{:}\ ObfLocation$$

Για τη διεργασία

$$GIN = ExLoc(rExactLocation{:}\ T_{ExactLocation}).$$
$$rExactLocation(x{:}\ ExactLocation).\left(\nu\ ObfRegister{:}\ T_{ObfLocation}\right).$$
$$(\nu\ obfloc{:}\ ObfLocation).\overline{ObfRegister}\langle obfloc\rangle.$$
$$\overline{toWeatherApp}\langle ObfRegister\rangle.\ 0$$

έχουμε τα εξής:

$$\Gamma \vdash\ 0\ \rhd\ \emptyset, true$$

$$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Nil)$$

$$\Gamma \vdash\ \overline{toWeatherApp}\langle ObfRegister\rangle.\ 0\ \rhd$$
$$ObfLocation{:}\ (\{disclose\ Weather\ App\}, true)$$

$$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$$

$$\Gamma \vdash \overline{ObfRegister}\langle obfloc\rangle.\overline{toWeatherApp}\langle ObfRegister\rangle.\ 0\ \ \rhd$$
$$ObfLocation{:}\ (\{write, disclose\ WeatherApp\}, true)$$

$$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$$

$$\Gamma \vdash rExactLocation(x{:}\ ExactLocation).$$

$(\nu\ ObfRegister: T_{ObfLocation}).(\nu\ obfloc: ObfLocation).$

$\overline{ObfRegister}\langle obfloc\rangle.\overline{toWeatherApp}\langle ObfRegister\rangle.0 \rhd$

$ExactLocation: (\{read\}, true).$

$ObfLocation: (\{write, disclose\ WeatherApp\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In, \kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResNP)$

$\Gamma \vdash ExLoc(rExactLocation: T_{ExactLocation}).rExactLocation(x: ExactLocation).$

$(\nu\ ObfRegister: T_{ObfLocation}).(\nu\ obfloc: ObfLocation).$

$\overline{ObfRegister}\langle obfloc\rangle.\overline{toWeatherApp}\langle ObfRegister\rangle.0 \rhd$

$ExactLocation: (\{access, read\}, true).$

$ObfLocation: (\{write, disclose\ WeatherApp\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash (\nu\ Ginger)\mathrm{GIN}\langle weatherRecord\rangle \rhd$

$ExactLocation \gg \langle Ginger[weatherRecord, true], \{access, read\}\rangle;$

$ObfLocation \gg \langle Ginger[weatherRecord, true], \{write, disclose\ WeatherApp\}\rangle;$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResGP)$

Συνεχίζουμε με τη διεργασία

$\mathrm{WA} = toWeatherApp(y: T_{ObfLocation}).y(obflocation: ObfLocation).$

$if(obflocation > X)\ then\ toRemoteServer(y).0$

όπου παίρνουμε:

$\Gamma \vdash 0 \rhd \emptyset, true$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Nil)$

$\Gamma \vdash \overline{toRemoteServer}\langle y\rangle.0 \rhd$

$ObfLocation: (\{disclose\ RemoteServer\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ Out)$

$\Gamma \vdash if(obflocation > X) then\ \overline{toRemoteServer}\langle y\rangle.0 \rhd$

$ObfLocation: (\{disclose\ RemoteServer\}, obfLocation > X)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ If)$

$\Gamma \vdash y(obflocation: ObfLocation).if(obflocation > X)$

$then\ \overline{toRemoteServer}\langle y\rangle.0 \rhd$

$ObfLocation: (\{disclose\ RemoteServer\}, obfLocation > X).$

$ObfLocation: (\{read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash toWeatherApp\big(y{:}T_{ObfLocation}\big).\, y(obfLocation{:}\, ObfLocation).$

$if\,(obfLocation > X)then\ \overline{toRemoteServer}\langle y\rangle.\,0 \rhd$

$ObfLocation{:}\,(\{disclose\ RemoteServer\}, obfLocation > X).$

$ObfLocation{:}\,(\{access, read\}, true)$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ In)$

$\Gamma \vdash (\nu\ WeatherApp)WA\langle weatherRecord\rangle \rhd$

$ObfLocation \gg \langle \text{WeatherApp}[weatherRecord, obfLocation > X]\rangle,$

$\{disclose\ RemoteServer\};$

$ObfLocation \gg \langle \text{WeatherApp}[weatherRecord, true]\rangle, \{access, read\};$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ \ ResGP)$

Συνδυάζοντας τα παραπάνω προκύπτει ότι:

$\Gamma \vdash ((\nu\ Ginger)GIN\langle weatherRecord\rangle$

$|(\nu\ WeatherApp)WA\langle weatherRecord\rangle) \rhd$

$ExactLocation \gg \langle Ginger[weatherRecord, true]\rangle, \{access, read\};$

$ObfLocation \gg \langle Ginger[weatherRecord, true]\rangle, \{write, disclose\ WeatherApp\};$

$ObfLocation \gg \langle \text{WeatherApp}[weatherRecord, obfLocation > X]\rangle,$

$\{disclose\ RemoteServer\};$

$ObfLocation \gg \langle \text{WeatherApp}[weatherRecord, true]\rangle, \{access, read\};$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ \ ParS)$

Τέλος για το σύστημα (S) έχουμε ότι:

$S = (\nu\ WSA)((\nu\ Ginger)GIN\langle weatherRecord\rangle$

$|(\nu\ WeatherApp)WA\langle weatherRecord\rangle)$

$\Gamma \vdash S \rhd$

$ExactLocation \gg \langle WSA[Ginger[weatherRecord, true]]\rangle, \{access, read\};$

$ObfLocation \gg \langle WSA[Ginger[weatherRecord, true]]\rangle, \{write, disclose\ WeatherApp\};$

$ObfLocation \gg \langle WSA[\text{WeatherApp}[weatherRecord, obfLocation > X]]\rangle,$

$\{disclose\ RemoteServer\};$

$ObfLocation \gg \langle \text{WSA}[\text{WeatherApp}[weatherRecord, true]]\rangle, \{access, read\};$

$(\kappa\alpha\nu\acute{o}\nu\alpha\varsigma\ ResGS)$

7.3.5 Έλεγχος Συμμόρφωσης με την πολιτική ιδιωτικότητας

Θα αποδείξουμε ότι το παραπάνω σύστημα ικανοποιεί την πολιτική ιδιωτικότητας της παρούσας περίπτωσης χρήσης. Η διεπαφή δικαιωμάτων που προέκυψε για το σύστημα

πιο πάνω είναι η ακόλουθη.

$ExactLocation \gg \langle WSA[Ginger[weatherRecord, true]]\rangle, \{access, read\};$

$ObfLocation \gg \langle WSA[Ginger[weatherRcord, true]]\rangle, \{write, disclose\ WeatherApp\};$

$ObfLocation \gg \langle WSA[\text{WeatherApp}[weatherRecord, obfLocation > X]]\rangle,$
$\{disclose\ RemoteServer\};$

$ObfLocation \gg \langle \text{WSA}[\text{WeatherApp}[weatherRecord, true]]\rangle, \{access, read\};$

Συνεπώς έχουμε τα παρακάτω σύνολα ομάδων:

$\widetilde{G_1} = \langle WSA, Ginger\rangle$

$\widetilde{G_2} = \langle WSA, WeatherApp\rangle$

Το σημείο b. ως προς την ικανοποίηση της πολιτικής εκάστοτε τύπου παρακάτω ισχύει τετριμμένα καθώς το σύνολο $\widetilde{HP_f} = \emptyset$ και οι βασικοί τύποι είναι ανεξάρτητοι δομής.

Για τον βασικό τύπο της ακριβούς τοποθεσίας $ExactLocation$ μέσω της συνάρτησης $perms_{H_1}$ προκύπτουν τα ακόλουθα:

$perms_{H_1}(\widetilde{G_1}, weatherRecord, true) = \{access, read\}$

Για τον βασικό τύπο της συσκοτισμένης τοποθεσίας $ObfLocation$ μέσω της συνάρτησης $perms_{H_2}$ προκύπτουν τα ακόλουθα:

$perms_{H_2}(\widetilde{G_1}, weatherRecord, true) = \{access, read, write, disclose\ WeatherApp\}$

$perms_{H_2}(\widetilde{G_2}, weatherRecord, true) = \{access, read\}$

$perms_{H_2}(\widetilde{G_2}, weatherRecord, obfLocation > X)$
$= \{access, read, disclose\ RemoteServer\}$

Όπως είναι προφανές από τα παραπάνω τα δικαιώματα που ασκούνται στο σύστημα από τις ομάδες που το αποτελούν βάση του συγκεκριμένου σκοπού και εκάστοτε συνθήκης, για όλους τους τύπους που καθορίστηκαν και τυγχάνουν διαχείρισης σε αυτό, είναι συμβατά με τα όσα επιτρέπονται από την πολιτική ιδιωτικότητας $\mathcal{P}$ και ως εκ τούτου έχουμε από τον Ορισμό 4 ότι $\mathcal{P} \Vdash \Theta$. Εφόσον η διεπαφή Θ έχει παραχθεί από το σύστημα της παρούσας περίπτωσης χρήσης μπορούμε να συμπεράνουμε άμεσα από τον Ορισμό 6 ότι $\mathcal{P} \vdash S$.

Κεφάλαιο 8

Συμπεράσματα

8.1 Συμπεράσματα

Η ιδιωτικότητα αποτελεί αναπόσπαστο κομμάτι της σημερινής τεχνολογικής προόδου καθώς όλο και περισσότερα συστήματα ασχολούνται με την συλλογή ευαίσθητων πληροφοριών. Τα άτομα απαιτούν και θέλουν η ιδιωτικότητα τους και σημαντικές πληροφορίες που τους αφορούν να τυγχάνουν του δέοντος σεβασμού από τα διάφορα συστήματα τα οποία ασχολούνται με τέτοιες πληροφορίες. Όλα τα συστήματα πρέπει και συνήθως συνοδεύονται από πολιτικές ιδιωτικότητας που καθορίζουν τους τρόπους με τους οποίους χειρίζονται τέτοιου είδους πληροφορίες. Για την περαιτέρω ικανοποίηση του αισθήματος της ιδιωτικότητας από τα άτομα θεωρείται αναγκαία η ύπαρξη εργαλείων τα οποία να μπορούν να ελέγχουν πως όντως συστήματα τα οποία ορίζουν την συμπεριφορά τους μέσω κάποιων πολιτικών ιδιωτικότητας συμπεριφέρονται με τρόπο ο οποίος να σέβεται την πολιτική αυτή.

Η παρούσα διπλωματική εργασία επεκτείνει ένα υφιστάμενο πλαίσιο ελέγχου πολιτικών ιδιωτικότητας από υποψήφια συστήματα με την χρήση τύπων. Συγκεκριμένα το πλαίσιο ελέγχου αυτό ενισχύθηκε βάσει παρατηρήσεων που προέκυψαν από την εξέταση διαφόρων πολιτικών ιδιωτικότητας ούτως ώστε να μπορεί να συλλάβει όσο το δυνατό καλύτερα απαιτήσεις αυτών. Λόγω της επέκτασης ως προς την τυπική διατύπωση των πολιτικών ιδιωτικότητας θεωρήθηκε αναγκαία η αναπροσαρμογή του λογισμού για την μοντελοποίηση των συστημάτων για τον λόγο αυτό προτάθηκε ο λογισμός της CP calculus, την οποία συνοδεύει ένα σύστημα τύπων για την παραγωγή των διεπαφών από ασκούμενα δικαιώματα εντός των διαφόρων συστημάτων και τα οποία επιτρέπουν με την καταγραφή των αποδείξεων αναφορικά με την ικανοποίηση των πολιτικών ιδιωτικότητας, τον έλεγχο του κατά πόσο συστήματα ικανοποιούν αυτές.

Οι επεκτάσεις που έγιναν αφορούσαν τα παρακάτω σημεία. Ως πρώτο σημείο επέκτασης αποτέλεσε η επέκταση της διατύπωσης πολιτικών ιδιωτικότητας με την ενσωμάτωση βασικών τύπων που αποτελούν πεδία συγκεκριμένων δομών από πληροφορίες και τον καθορισμό αντίστοιχων τύπων δομής. Η διαχείριση τους οδήγησε στην ανάγκη επέκτασης του λογισμού με την δυνατότητα μεταφοράς πολλαπλών στοιχείων δια μέσου των καναλιών αφού πλέον υπάρχει η δυνατότητα μεταφοράς δομών πληροφοριών μέσα από τα κανάλια του λογισμού. Επιπρόσθετα ως προς την διατύπωση των πολιτικών ιδιωτικότητας ενσωματώθηκε η έννοια της συνθήκης ο οποία εντοπίζεται σε διάφορα παραδείγματα πολιτικών ιδιωτικότητας. Οι συνθήκες όπως διατυπώνουμε και στο Κεφάλαιο 3 για τις Πολιτικές Ιδιωτικότητας αποτελεί μια από τις παραμέτρους που θεωρούνται απαραίτητες για τον καθορισμό πολιτικών ιδιωτικότητας. Η ενσωμάτωση των συνθηκών αποτέλεσε ένα από τα σημαντικότερα σημεία της παρούσας διπλωματικής εργασίας καθώς η ενσωμάτωση αυτών απαίτησε τον καθορισμό τελεστών στο λογισμό αλλά και αντίστοιχα κανόνων του συστήματος των τύπων όπως επίσης και οι αποδείξεις ικανοποίησης πολιτικών ιδιωτικότητας γίνονται συνδυάζοντας πέραν τον όσο υπάρχουν την δυνατότητα πολλαπλής μεταφοράς πληροφοριών στα κανάλια αλλά και των συνθηκών.

Μετά και από σχετική μελέτη αναφορικά με απειλές που προκύπτουν από την συλλογή και συνάθροιση πληροφοριών καθορίστηκε ένα νέο δικαίωμα το $identify$ το οποίο προκύπτει με την χρήση δομών πληροφοριών. Αυτό επιτρέπει την ταυτοποίηση μιας οντότητας από μια δομή όταν γίνεται πρόσβαση σε χαρακτηριστικό πεδίο μιας δομής το οποίο μπορεί να προσδιορίσει μοναδικά κάποια οντότητα. Η σχετική κατηγοριοποίηση των βασικών τύπων πεδίων μετά και από σχετική μελέτη πολιτικών ιδιωτικότητας αλλά και άρθρων ως προς διάφορες μορφές δεδομένων αποτέλεσε επέκταση της παρούσας διπλωματικής εργασίας. Το προτεινόμενο πλαίσιο της παρούσας εργασίας χαρακτηρίζεται από τις έννοιες της ασφάλειας και αξιοπιστίας όπως αυτό προκύπτει μέσα από το σύνολο των αποδείξεων που διατυπώνονται στο Κεφάλαιο 6. Το ενισχυμένο πλέον πλαίσιο ελέγχου εφαρμόζεται σε διάφορα ρεαλιστικά παραδείγματα οπόταν και μπορεί να αξιοποιηθεί πλήρως, ενώ καλύπτει μέσω και των επεκτάσεων που δίνονται περισσότερα παραδείγματα για έλεγχο πολιτικών αφού λαμβάνονται υπόψιν περισσότερες παραμέτρους ως προς την διατύπωση και έλεγχο τους.

Τέλος όσον αφορά το πλαίσιο ελέγχου που ορίζουμε παραπάνω αξίζει να σημειώσουμε στο παρών σημείο τις παρακάτω παραδοχές. Κάθε φορά που ορίζεται μια δομή και ανατίθεται ένα σύνολο από βασικούς τύπους σε αυτή προσδιορίζει μια συγκεκριμένη οντότητα αυτής, οπόταν στις περιπτώσεις όπου είναι δυνατό ένα σύστημα να λαμβάνει πρόσβαση και να χειρίζεται περισσότερες οντότητες της ίδιας δομής τότε ορίζονται διαφορετικοί τύποι για τη κάθε οντότητα ούτως ώστε να είναι εφικτός ο έλεγχος τύπων με τις κατάλληλες συνθήκες τιμών κάθε φορά. Ταυτόχρονα θεωρούμε πως η πρόσβαση σε δομές γίνεται με την λήψη των καναλιών που αφορούν όλους τους βασικούς τύπους πεδίων της εσωτερικά ενώ αυτό που διαφοροποιείται είναι το σύνολο των ενεργειών στα κανάλια που έχουν ληφθεί μέσω της δομής.

8.2 Μελλοντική Εργασία

Η παρούσα εργασία μπορεί να επεκταθεί σε διάφορους τομείς καθώς οι πολιτικές ιδιωτικότητας ολοένα και αναπροσαρμόζονται προσθέτοντας επιπρόσθετα στοιχεία ως προς τη διατύπωση τους. Μια πρώτη κατεύθυνση η οποία μπορεί να ενσωματωθεί και αφορά το τελευταίο σημείο ως προς τα χαρακτηριστικά των πολιτικών ιδιωτικότητας είναι οι υποχρεώσεις. Η ενσωμάτωση δηλαδή τυπικών ορισμών και στοιχείων τα οποία να επιβάλλουν συγκεκριμένες ενέργειες μετά από την χρήση κάποιων πληροφοριών τόσο σε επίπεδο πολιτικής όσο και λογισμού για τη μοντελοποίηση των διαφόρων συστημάτων.

Επιπρόσθετα το παρόν πλαίσιο θα μπορούσε να επεκταθεί με την ενσωμάτωση επιπρόσθετων δικαιωμάτων τα οποία προκύπτουν μέσα από διάφορες άλλες κατηγορίες απειλών ως προς την ιδιωτικότητα και αντίστοιχα αναπροσαρμογή του λογισμού για την μοντελοποίηση των συστημάτων.

Το υφιστάμενο πλαίσιο είναι επεκτάσιμο ωστόσο οι οποιεσδήποτε επεκτάσεις μπορούν να γίνουν μετά από κατάλληλη μελέτη και κατανόηση ολόκληρου του πλαισίου ελέγχου. Το δύσκολο κομμάτι αναφορικά με την επέκταση του υφιστάμενου πλαισίου ελέγχου προκύπτει από την ανάγκη προσεχτικής αναπροσαρμογής του συνόλου των αποδείξεων ορθότητας, ασφάλειας και ικανοποίησης πολιτικής, καθότι θεωρείται απαραίτητη προϋπόθεση η διασφάλιση του ότι αυτές οι έννοιες θα χαρακτηρίζουν την οποιαδήποτε μελλοντική επέκταση.

Βιβλιογραφία

[1] Cardelli, Luca, Giorgio Ghelli, και Andrew D. Gordon. 2005. «Secrecy and group creation.» *Information and Computation* 196 (2): 127-155.

[2] *Children's Online Privacy Protection Rule ("COPPA").* Accessed: August 7, 2015. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[3] Herges, David, Naim Asaj, Bastian Könings, Florian Schaub, και Michael Weber. 2012. «Ginger: An Access Control Framework for Telematics Applications.» *Trust, Security and Privacy in Computing and Communications (TrustCom).* Liverpool: IEEE. 474-481.

[4] Kokkinofta, Eleni, και Anna Philippou. 2015. «Type Checking Purpose-Based Privacy Policies in the π-calculus.» *Web Services, Formal Methods, and Behavioral Types.* Madrid: Springer. 122-142.

[5] Kouzapas, Dimitrios, και Anna Philippou. 2015. «Type Checking Privacy Policies in the π-calculus.» *Formal Techniques for Distributed Objects, Components, and Systems.* Grenoble: Springer International Publishing. 181-195.

[6] Kumaraguru, Ponnurangam, Lorrie Faith Cranor, Jorge Lobo, και Seraphin B. Calo. 2007. «A survey of privacy policy languages.» *Workshop on Usable IT Security Management (USM 07).* ACM.

[7] McCallister, Erika, Timothy Grance, και Karen A. Scarfone. 2010. «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).» Στο *Special Publication*.

[8] Milner, Robin. 1993. *The Polyadic π-Calculus: a Tutorial.* Τόμ. 94, σε *Logic and Algebra of Specification*, 203-246. Springer Berlin Heidelberg.

[9] Milner, Robin, Joachim Parrow, και David Walker. 1992. «A Calculus of Mobile Processes.» *Information and Computation* 100: 1-40.

[10] Rass, Stefan, Peter Schartner, Patrick Horster, και Alexander Abl. 2014. «Privacy-Preserving Speed-Limit Enforcement.» *Journal of Traffic and Logistics Engineering* 2: 26-44.

[11] *Sprout Social, Inc. Privacy Policy.* Accessed: April 1, 2015. http://sproutsocial.com/privacy-policy.

[12] *Teux Daux.* Accessed: February 7, 2013. https://teuxdeux.com/privacy.

[13] *The Walt Disney Company Privacy Center.* Accessed: December 11, 2015. https://disneyprivacycenter.com/privacy-policy-translations/english/#DIMGQuestion6.

[14] Tschantz , Michael Carl, και Jeannette M. Wing. 2009. *Formal methods for privacy.* Springer.

[15] Westin, Alan F. 1968. «Privacy and freedom.» *Washington and Lee Law Review* 25 (1): 166.