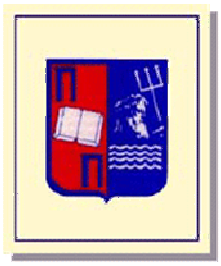
Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

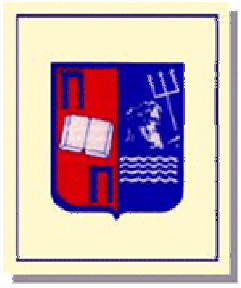


Μοντέλα Ασφάλειας και Εμπιστοσύνης για Συστήματα Κινητών Πρακτόρων Λογισμικού

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μιχαήλ Φ. Φραγκάκη

Πειραιάς, Ιούνιος 2011



Συμβουλευτική Επιτροπή

Επιβλέπων:
Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:
Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

Διατριβή για την απόκτηση Διδακτορικού Διπλώματος του Τμήματος Πληροφορικής

«Μοντέλα Ασφάλειας και Εμπιστοσύνης για Συστήματα Κινητών Πρακτόρων Λογισμικού»

Εξεταστική Επιτροπή:

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Χρήστος Δουληγέρης
Καθηγητής Πανεπιστημίου Πειραιώς

Θεμιστοκλής Παναγιωτόπουλος
Καθηγητής Πανεπιστημίου Πειραιώς

Στέφανος Γκρίτζαλης
Καθηγητής Πανεπιστημίου Αιγαίου

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Γεώργιος Καμπουράκης
Λέκτορας Πανεπιστημίου Αιγαίου

Παναγιώτης Κοτζανικολάου
Λέκτορας Πανεπιστημίου Πειραιώς

……

Μιχαήλ Φ. Φραγκάκης
Μηχανικός Πληροφοριακών και Επικοινωνιακών Συστημάτων Πανεπιστημίου Αιγαίου

Στους γονείς μου,
Φώτη και Ιουλία Φραγκάκη

Ευχαριστίες

Μια διδακτορική διατριβή είναι μια μακρόχρονη δοκιμασία σε ερευνητικό, ψυχολογικό και προσωπικό επίπεδο που ο καθένας βιώνει και αντιμετωπίζει με τρόπο διαφορετικό. Σε αυτή μου τη δοκιμασία υπήρξαν πολλοί άνθρωποι που με στήριξαν και συνέβαλαν στην ολοκλήρωσή της, είτε άμεσα είτε έμμεσα. Θα ήθελα να τους ευχαριστήσω όλους ειλικρινά και από τα βάθη της καρδιάς μου.

Πρωτίστως, θα ήθελα να ευχαριστήσω τον Καθηγητή κ. Νικόλαο Αλεξανδρή, επιβλέποντα της διδακτορικής μου διατριβής, για την πολύτιμη βοήθεια επιστημονική και ψυχολογική, που ακούραστα μου προσέφερε σε όλα τα στάδια της εκπόνησής της. Η συμβολή του υπήρξε ανεκτίμητη και μου άνοιξε νέους ορίζοντες, που με οδήγησαν στην ολοκλήρωση της παρούσας έρευνας.

Ευχαριστώ θερμά τους συνεπιβλέποντες της τριμελούς επιτροπής, Καθηγητή Χρήστο Δουληγέρη και Καθηγητή Θεμιστοκλή Παναγιωτόπουλο, για την αμέριστη συμπαράσταση και καθοδήγησή τους, καθώς και για τις πολύτιμες παρατηρήσεις και συμβουλές τους.

Ιδιαιτέρως θα ήθελα να ευχαριστήσω το μέλος της επταμελούς επιτροπής, Καθηγητή κ. Στέφανο Γκρίτζαλη και καθηγητή μου στις προπτυχιακές σπουδές στο τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου, που μου πρότεινε τη συγκεκριμένη ερευνητική κατεύθυνση. Ευχαριστώ, επίσης, τα μέλη της επταμελούς επιτροπής, Καθηγητή κ. Βασίλειο Χρυσικόπουλο, Λέκτορα κ. Γεώργιο Καμπουράκη και Λέκτορα κ. Παναγιώτη Κοτζανικολάου, για την τιμή που μου έκαναν να είναι μέλη της επταμελούς επιτροπής κρίσης της διατριβής μου.

Το Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς μου έδωσε τη δυνατότητα να πραγματοποιήσω το ερευνητικό μου έργο σε ένα άνετο και παραγωγικό ακαδημαϊκό περιβάλλον. Για αυτό και το ευχαριστώ.

Θα ήθελα, επιπλέον, να ευχαριστήσω τον Ομότιμο Καθηγητή Μιχάλη Γεωργιακόδη και τον Καθηγητή Φώτη Γεωργιακώδη για την συνεργασία και υποστήριξή τους κατά τη διάρκεια της διατριβής, η οποία έφτασε πολύ πέρα από τα

ακαδημαϊκά όρια. Όλο αυτό το διάστημα υπήρξαν για μένα Δάσκαλοι αλλά και πραγματικοί φίλοι.

Σημαντική υποστήριξη μου προσέφεραν όλα αυτά τα χρόνια οι φίλοι μου, άλλοι κοντά μου και άλλοι μακριά, οι οποίοι, με τον τρόπο του ο καθένας, φρόντιζαν να με παροτρύνουν να συνεχίσω την προσπάθειά μου. Επιπλέον, στάθηκαν δίπλα μου σε όλες τις προσωπικές μου δυσκολίες, τις οποίες με βοήθησαν να ξεπεράσω, ενίοτε με την συνδρομή ποικιλίας αλκοολούχων “σκευασμάτων”. Σας ευχαριστώ παιδιά!

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω ιδιαιτέρως τον αδερφό μου Μάρκο Φραγκάκη, Μηχανικό Ηλεκτρονικών Υπολογιστών, για την βοήθεια που μου προσέφερε σε κρίσιμα σημεία της διδακτορικής διατριβής, συχνά μάλιστα εις βάρους του δικού του, περιορισμένου, ελεύθερου χρόνου. Τα εύστοχα σχόλια και οι παρατηρήσεις του και, το κυριότερο, οι παροτρύνσεις του υπήρξαν πολύτιμες.

Κλείνοντας, ένα μεγάλο ευχαριστώ στους γονείς μου Φώτη και Ιουλία Φραγκάκη για την υλική, πνευματική, ψυχολογική και γαστρονομική υποστήριξη που μου προσέφεραν όλα αυτά τα χρόνια. Χωρίς τη στήριξή τους δεν θα ήταν δυνατή η εκπόνηση της διδακτορικής διατριβής αυτής και γι’ αυτό τους ευγνωμονώ.

Περιεχόμενα

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

1 ΕΙΣΑΓΩΓΗ

1.1 Πράκτορες Λογισμικού

Οι πράκτορες (agents) αποτελούν αυτόνομες μονάδες λογισμικού που είναι σχεδιασμένες να ενεργούν για λογαριασμό του δημιουργού τους με σκοπό τη διεκπεραίωση μιας συγκεκριμένης εργασίας. Στο πλαίσιο της λειτουργίας τους χρειάζεται να μπορούν να επικοινωνούν για τη συλλογή πληροφοριών ή την επιστροφή αποτελεσμάτων, ενώ συχνά απαιτείται η μετακίνησή τους σε διαφορετικές πλατφόρμες τρίτων προκειμένου να αποκτήσουν πρόσβαση σε διαφορετικά δεδομένα, καθώς και η συνεργασία με άλλους πράκτορες. Η λειτουργία τους χαρακτηρίζεται από αυτονομία και τη δυνατότητα να λαμβάνουν αποφάσεις ανάλογα με τις συνθήκες που επικρατούν στο περιβάλλον τους. Όπως όλες οι οντότητες λογισμικού απαιτούν για τη λειτουργία τους πόρους από την πλατφόρμα στην οποία είναι εγκατεστημένοι. Παρόμοιους πόρους απαιτούν όλοι οι πράκτορες σε μια πλατφόρμα, οι οποίοι είναι δυνατόν να είναι και ανταγωνιστικοί, ενώ πόροι απαιτούνται και για τη λειτουργία της ίδιας της πλατφόρμας.

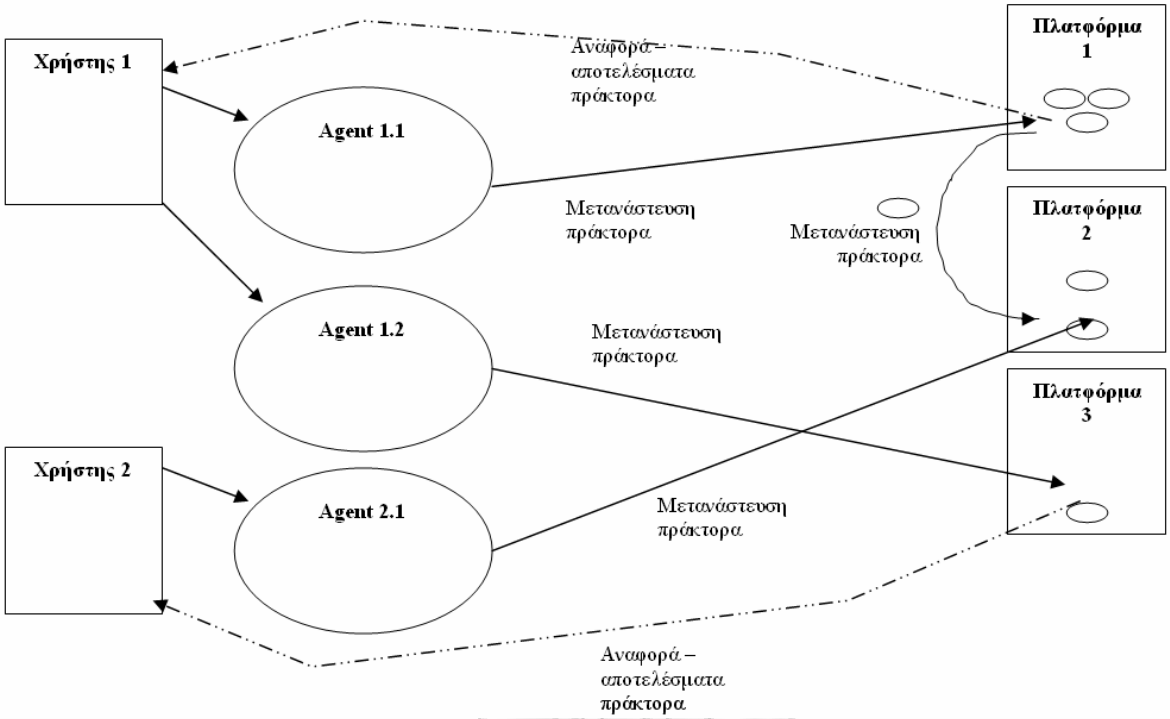
Έτσι, οι πράκτορες μπορούν να διαχωριστούν με βάση ορισμένα κριτήρια, μεταξύ των οποίων είναι η κινητικότητα, ο βαθμός αλληλεπίδρασης και η ευφυΐα τους [66]. Στην παρούσα διατριβή διαπραγματευόμαστε τα συστήματα κινητών πρακτόρων τα οποία χαρακτηρίζονται από υψηλό βαθμό κινητικότητας και αλληλεπίδρασης, κατάλληλα για δραστηριοποίηση στο Διαδίκτυο και πιο συγκεκριμένα με τα μοντέλα ασφάλειας και εμπιστοσύνης που αυτά υιοθετούν. Η επικέντρωση στο συγκεκριμένο τύπο πρακτόρων γίνεται καθώς έχουν υψηλές απαιτήσεις ασφάλειας, αφού ουσιαστικά αφορούν στην εκτέλεση ξένου κώδικα (foreign code) τοπικά και τη μετακίνησή του διαμέσου δικτύων ευρείας περιοχής (Wide Area Network - WAN). Αντίθετα, συστήματα στατικών πρακτόρων όπως αυτά που χρησιμοποιούνται σε εφαρμογές αισθητήρων δεν παρουσιάζουν ιδιαίτερο ενδιαφέρον από πλευράς ασφάλειας, καθώς συνήθως εκτελούνται στατικά εντός

κλειστού δικτύου, περιβάλλον απομονωμένο και, επομένως ιδιαίτερα ασφαλές. Επίσης, τα συστήματα κινητών πρακτόρων χαρακτηρίζονται συνήθως και από ευφυΐα, ανάλογα πάντα με τον προγραμματισμό τους, η οποία όμως είναι πέρα από το σκοπό της συγκεκριμένης διατριβής.

Σε γενικές γραμμές, στα συστήματα κινητών πρακτόρων οι χρήστες δημιουργούν διάφορους κινητούς πράκτορες, με διαφορετικές εφαρμογές, και στη συνέχεια τους στέλνουν σε απομακρυσμένες πλατφόρμες εκτέλεσης που συμμετέχουν στο συγκεκριμένο σύστημα πρακτόρων (Εικόνα 1). Οι πράκτορες εκτελούνται στις πλατφόρμες χρησιμοποιώντας τοπικούς πόρους, ενώ είναι δυνατόν να επιλέξουν να μεταναστεύσουν και σε άλλη πλατφόρμα, προκειμένου να συνεχίσουν τη λειτουργία τους, χωρίς την παρέμβαση του χρήστη. Οι πράκτορες μεταδίδουν τα αποτελέσματα της λειτουργίας τους στο χρήστη τους και όταν ολοκληρώσουν τη λειτουργία τους, παύουν να εκτελούνται.

Η τεχνολογία των κινητών πρακτόρων σχετίζεται με τα επιστημονικά αντικείμενα της Τεχνητής Νοημοσύνης και των Παράλληλων και Κατανεμημένων Συστημάτων [8], [9], καθώς οι πράκτορες πρέπει να διαθέτουν αυτονομία και να μπορούν να συνεργάζονται με άλλους πράκτορες ή διεργασίες συστήματος. Έτσι, στη λειτουργία τους εισάγονται θέματα ασφάλειας που κυριαρχούν στις εφαρμογές κινητού κώδικα. Ως αποτέλεσμα, στη λειτουργία τους εφαρμόζονται διάφοροι μηχανισμοί ασφαλείας, ανάλογα με τη χρήση και την έκταση του συστήματος, στους οποίους μηχανισμούς ασφαλείας και επικεντρώνεται η παρούσα διατριβή.

Πιο αναλυτικά εξετάζουμε τη λειτουργία συστημάτων πρακτόρων στο τρίτο κεφάλαιο της παρούσας διατριβής, όπου παρουσιάζονται ενδεικτικοί εκπρόσωποι συστημάτων πρακτόρων, μέσα από την ανάλυση των μοντέλων ασφάλειας και εμπιστοσύνης που υιοθετούν. Εκεί φαίνεται λεπτομερώς η διαφοροποίηση του κάθε συστήματος από το παραπάνω, απλουστευμένο, μοντέλο λειτουργίας, ως αποτέλεσμα της εξειδικευμένης λειτουργίας για την οποία σχεδιάστηκε το κάθε εξεταζόμενο σύστημα.



Εικόνα 1: Γενική λειτουργία συστημάτων κινητών πρακτόρων (αφαιρετικό μοντέλο).

1.2 Παρούσα Κατάσταση Τεχνολογίας

Τα συστήματα κινητών πρακτόρων περιλαμβάνουν επικοινωνίες μεταξύ πρακτόρων, καθώς και ένα σημαντικό βαθμό κινητικότητας των ίδιων των πρακτόρων. Για συγκεκριμένες ενέργειες απαιτείται να μετακινηθεί ένας πράκτορας, μαζί με τα δεδομένα του, διαμέσου ενός δικτύου ευρείας περιοχής. Ως αποτέλεσμα, ο πράκτορας πρέπει να είναι προστατευμένος από τυχόν κακόβουλες πλατφόρμες εκτέλεσης, που ενδέχεται να προσπαθήσουν να επηρεάσουν τη λειτουργία του ή να υποκλέψουν τα, πιθανώς εμπιστευτικά, δεδομένα του. Αντίστροφα, μια πλατφόρμα εκτέλεσης πρακτόρων πρέπει να είναι προστατευμένη ενάντια τυχόν κακόβουλων πρακτόρων. Επιπλέον, είναι δυνατόν ένας πράκτορας να κάνει επίθεση εναντίον κάποιου άλλου, στην ίδια ή ακόμη και σε διαφορετική, απομακρυσμένη πλατφόρμα.

Οι δημιουργοί συστημάτων πρακτόρων χρησιμοποιούν αρκετούς μηχανισμούς ασφαλείας που αντιμετωπίζουν ζητήματα αυθεντικοποίησης, εμπιστευτικότητας, ακεραιότητας δεδομένων και μηχανισμούς παρακολούθησης [3], [8], [10], [11]. Επιπλέον αυτών, το γεγονός ότι ένας πράκτορας ίσως χρειάζεται να λειτουργήσει σε ένα συνεχώς διαφοροποιούμενο περιβάλλον εισάγει την έννοια της εμπιστοσύνης στη λειτουργία των κινητών πρακτόρων. Η εμπιστοσύνη αντικατοπτρίζει την ανθρώπινη κοινωνική συμπεριφορά εκτίμησης ρίσκου, που κατευθύνεται από την ανάγκη για συνεργασία μέσα από την επικοινωνία και την αλληλεπίδραση για την επίτευξη ενός συγκεκριμένου σκοπού [10], [11], [12]. Αφορά σε υποθέσεις σχετικές με την ακεραιότητα ή την κακοβουλία των οντοτήτων που αποτελούν ένα σύστημα κινητών πρακτόρων. Αν και τέτοιες υποθέσεις κρίνονται απαραίτητες, κάποιες φορές ίσως οδηγήσουν στο να θεωρηθεί μια οντότητα του συστήματος ως αξιόπιστη και άρα ασφαλής για αλληλεπίδραση, ενώ στην πραγματικότητα δεν είναι. Σε τέτοιες περιπτώσεις η χρήση ακόμη και των πλέον σύγχρονων μηχανισμών ασφάλειας είναι άσκοπη.

Όσον αφορά την προτυποποίηση στο χώρο των κινητών πρακτόρων, υπάρχουν οργανισμοί που εργάζονται προς αυτή τη κατεύθυνση. Δύο από τους

σημαντικότερους είναι το Foundation for Intelligent Physical Agents – FIPA [15] και το Object Management Group – OMG [17]. Οι προδιαγραφές τους δημιουργήθηκαν παράλληλα και ως εκ τούτου είναι ασύμβατες. Το FIPA ασχολείται αποκλειστικά με πράκτορες λογισμικού και έχει παραγάγει προδιαγραφές που αφορούν κυρίως τη δια-λειτουργικότητα μεταξύ διαφορετικών συστημάτων πρακτόρων, τις επικοινωνίες και αρχιτεκτονικά στοιχεία [13], [16]. Αποτελεί ουσιαστικά, μια αφηρημένη αρχιτεκτονική που μπορεί να χρησιμοποιηθεί από διαφορετικές πλατφόρμες. Αντίθετα, το OMG αποτελεί οργανισμό προτυποποίησης σε ευρύτερα αντικείμενα και δεν αφορά μονάχα κινητούς πράκτορες όπως το FIPA. Για την ακρίβεια, στοχεύει στην παραγωγή γενικότερων προτύπων για κατανεμημένα συστήματα και η μοντελοποίηση και οι προδιαγραφές του εστιάζονται στις επικοινωνίες, τις πρακτικές ανάπτυξης, εστιάζοντας κυρίως στις διεπαφές μεταξύ των διαφόρων οντοτήτων σε ένα σύστημα [18], [22]. Σχετικά με τους κινητούς πράκτορες έχει παραγάγει το πρότυπο Mobile Agent System Interoperability Facilities Specification (MASIF).

Πιο συγκεκριμένα, στον τομέα τις ασφάλειας, η FIPA έχει παράγει μία μόνο σχετική προδιαγραφή (FIPA 98), η οποία όμως έχει ανακληθεί επισήμως ως παρωχημένη (obsolete) και δεν έχει αντικατασταθεί από νεότερη [14], αν και στοιχεία ασφάλειας περιέχονται στις ισχύουσες προδιαγραφές, ιδιαίτερα στις ασφάλειες επικοινωνιών. Από την πλευρά του OMG το πρότυπο MASIF δεν εξετάζει ανεξάρτητα τα θέματα ασφάλεια, που αφορούν τους κινητούς πράκτορες [18], [95]. Και αυτό έχει ενσωματώσει στοιχεία ασφάλειας στις επιμέρους προδιαγραφές του.

Και τα δύο πρότυπα, αν και υιοθετούνται από συστήματα πρακτόρων, χρησιμοποιούνται περισσότερο ως πρότυπα διαλειτουργικότητας και επικοινωνιών και όχι για τις δυνατότητες ασφάλειας και θεωρείται ότι δεν έχουν καταφέρει να προάγουν τη χρήση των πρακτόρων [34]. Τα τελευταία χρόνια σκοπός και των δύο οργανισμών είναι η σύγκλιση των προδιαγραφών τους σε ενιαίες, προκειμένου να προωθηθεί η τεχνολογία των κινητών πρακτόρων [18].

1.3 Χρήση - Βαθμός Καθιέρωσης

Η χρήση κινητών πρακτόρων μπορεί να αποφέρει οφέλη σε σημαντικό αριθμό δικτυακών εφαρμογών, σε σχέση με την πιο κλασική προσέγγιση client - server [60][61]. Μια λειτουργία που πρέπει να διεκπεραιωθεί σε ένα αριθμό απομακρυσμένων σταθμών αντί να κατευθύνεται κεντρικά (μοντέλο client – server) μπορεί να πραγματοποιηθεί με την αποστολή ενός πράκτορα, ο οποίος και θα μετακινηθεί στον καθένα από αυτούς και χρησιμοποιώντας παρεχόμενους πόρους θα την πραγματοποιήσει. Η διαφορετική αυτή προσέγγιση που προσφέρει η τεχνολογία των κινητών πρακτόρων προσφέρει τα παρακάτω πλεονεκτήματα [62]:

- **Μειωμένη χρήση δικτυακών πόρων**. Σε περιπτώσεις ανάγκης επεξεργασίας μεγάλων όγκων κατανεμημένων δεδομένων είναι προτιμότερο να μετακινήσουμε απλά τον πράκτορα που θα τα επεξεργαστεί τοπικά, παρά τα ίδια τα δεδομένα.
- **Αυτόνομη και ασύγχρονη λειτουργία**. Ένας πράκτορας μπορεί να εξακολουθεί να λειτουργεί, ανεξάρτητα από το δημιουργό του. Έτσι, μπορεί να χαθεί κάθε επικοινωνία και ο πράκτορας να συνεχίσει τη λειτουργία του με βάση τον προγραμματισμό του. Αργότερα, όταν η επικοινωνία αποκατασταθεί, αποστέλλονται τα αποτελέσματα της επεξεργασίας (χρήσιμη δυνατότητα σε στρατιωτικές και διαστημικές εφαρμογές [35]).
- **Προσαρμοστικότητα**. Ένας πράκτορας μπορεί να προσαρμόσει τη λειτουργία του με βάση το περιβάλλον του. Έτσι, είναι δυνατό να επιλέξει να μεταναστεύσει και να συνεχίσει τη λειτουργία του σε άλλη πλατφόρμα εάν διαπιστώσει έλλειψη πόρων συστήματος. Ως αποτέλεσμα μπορεί να χρησιμοποιηθούν για την εξισορρόπηση του φόρτου σε ένα δίκτυο (load balancing).
- **Ευκολία συντήρησης**. Σε περίπτωση αλλαγής λειτουργίας δεν απαιτείται η προσαρμογή όλων των οντοτήτων σε ένα σύστημα, παρά μόνο αλλαγές στον προγραμματισμό του πράκτορα. Στη συνέχεια

μεταναστεύει στις πλατφόρμες εκτέλεσης, στις οποίες χρησιμοποιώντας τους ίδιους πόρους, πραγματοποιεί τη νέα του λειτουργία.

Ανάλογα με τη φύση της εφαρμογής, τα πλεονεκτήματα αυτής της τεχνολογίας μπορεί να αποδειχθούν ιδιαίτερα κρίσιμα. Παρόλ' αυτά όμως, η χρήση των κινητών πρακτόρων είναι ιδιαίτερα περιορισμένη [34]. Οι λόγοι που περιορίζουν τη χρήση των πρακτόρων εντοπίζονται στα εγγενή κενά ασφάλειας που τους διακρίνουν [34]. Ουσιαστικά, ένας πράκτορας αποτελεί μια εφαρμογή η οποία μεταναστεύει και εκτελείται σε πλατφόρμα τρίτου. Οι κίνδυνοι ακεραιότητας που υπάρχουν καθιστούν απαγορευτική τη χρήση τους σε κρίσιμες εφαρμογές, όπως οι εμπορικές-εγχρήματες συναλλαγές. Από την έρευνά μας διαπιστώνουμε ότι βρίσκουν περιορισμένες εφαρμογές σε μικρά κυρίως συστήματα που λειτουργούν σε περιορισμένο ή ακόμη και κλειστό περιβάλλον [1], [2], [3], [4], [5], [34].

1.4 Σκοπός Έρευνας / Δομή Διατριβής

Η παρούσα διατριβή, λαμβάνοντας υπόψη τα πλεονεκτήματα που έχει η χρήση των πρακτόρων, θέτει ως σκοπό τη διερεύνηση του χώρου από τη σκοπιά της ασφάλειας. Πιο συγκεκριμένα, αποσκοπεί στη διερεύνηση των μοντέλων ασφάλειας και εμπιστοσύνης των κινητών πρακτόρων.

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στη τεχνολογία των κινητών πρακτόρων, παρουσιάζεται η παρούσα κατάσταση της τεχνολογίας στον τομέα που αφορά τα μοντέλα ασφάλειας και εμπιστοσύνης και ο βαθμός διείσδυσης των κινητών πρακτόρων σήμερα.

Στο δεύτερο κεφάλαιο παρατίθενται οι απαιτήσεις σε ασφάλεια που κρίνονται αναγκαίες για τη λειτουργία των πρακτόρων, σύμφωνα με τα υπάρχοντα πρότυπα, και αναπτύσσεται μια μεθοδολογία σύγκρισης των μοντέλων ασφάλειας και εμπιστοσύνης για τα διάφορα συστήματα πρακτόρων.

Στο τρίτο κεφάλαιο της διατριβής, και με χρήση της μεθοδολογίας σύγκρισης που αναπτύχθηκε στο προηγούμενο κεφάλαιο, γίνεται αποτύπωση και αξιολόγηση των μοντέλων ασφάλειας και εμπιστοσύνης που υλοποιούνται από αντιπροσωπευτικά συστήματα πρακτόρων. Με αυτόν τον τρόπο, εντοπίζονται οι απειλές που δεν λαμβάνονται υπόψη επαρκώς ή και αγνοούνται παντελώς. Μετά από ανάλυση ικανού αριθμού συστημάτων, προκύπτουν συμπεράσματα για το βαθμό προόδου της τεχνολογίας στο τομέα της ασφάλειας πρακτόρων. Τα συμπεράσματα αυτά παρατίθενται ξεχωριστά για κάθε τομέα που προβλέπει το μοντέλο σύγκρισης. Τέλος, επισημαίνονται τα σημεία που καλύπτονται ελλιπώς από τις διάφορες πλατφόρμες.

Στο τέταρτο κεφάλαιο προσδιορίζονται οι προδιαγραφές που πρέπει να πληροί ένα μοντέλο-πρότυπο ασφάλειας και εμπιστοσύνης κινητών πρακτόρων. Οι προδιαγραφές αυτές διαμορφώνονται στην τελική τους μορφή μετά την ανάλυση των υπαρχόντων συστημάτων και με χρήση των συμπερασμάτων της σύγκρισης. Με βάση τις τελικές αυτές προδιαγραφές γίνεται ο σχεδιασμός ενός θεωρητικού

καθολικού μοντέλου ασφάλειας και εμπιστοσύνης που επιτρέπει τη λειτουργία και συνεργασία των πρακτόρων κατά τρόπο εξασφαλισμένο.

Στο πέμπτο κεφάλαιο εξετάζεται η επίδραση που έχει στις επιδόσεις ενός συστήματος πρακτόρων η εφαρμογή του μοντέλου μας με την πραγματοποίηση μιας προσομοίωσης σε περιβάλλον εικονικού δικτύου. Κάτι τέτοιο κρίνεται απαραίτητο για να διερευνηθεί αφενός το κατά πόσο μπορεί, το προτεινόμενο μοντέλο, να είναι εφαρμόσιμο και αφετέρου να εντοπιστούν ενδεχόμενα προβλήματα του μοντέλου που χρήζουν βελτίωσης. Επίσης, αναλύονται οι λόγοι που οδήγησαν στη επιλογή της προσομοίωσης αντί μιας πραγματικής υλοποίησης, ως μεθόδου αξιολόγησης των επιδόσεων.

Στο έκτο κεφάλαιο, τέλος, παρουσιάζονται τα συμπεράσματα που εξήχθησαν κατά την πορεία της έρευνας και γίνεται αξιολόγησή τους. Τα συμπεράσματα αυτά αφορούν τόσο την υφιστάμενη κατάσταση της τεχνολογίας των κινητών πρακτόρων, όσο και την αξιολόγηση του προτεινόμενου μοντέλου ασφάλειας και εμπιστοσύνης. Επιπλέον, παρουσιάζονται μελλοντικές κατευθύνσεις τις οποίες είναι δυνατόν να ακολουθήσει η έρευνα, και οι λόγοι για τους οποίους αυτές προτείνονται.

Στη συνέχεια παρατίθεται βιβλιογραφική αναφορά των εργασιών και βιβλίων που χρησιμοποιήθηκαν ως υπόβαθρο στην υπάρχουσα διατριβή.

Τέλος, στο παράρτημα παρατίθενται οι πλήρεις αναφορές που λήφθηκαν κατά τη διάρκεια της προσομοίωσης.

2 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ – ΜΟΝΤΕΛΟ ΣΥΓΚΡΙΣΗΣ

2.1 Εισαγωγή

Στο παρόν κεφάλαιο γίνεται μια εισαγωγή στους κινδύνους που εμπλέκονται στη λειτουργία των συστημάτων κινητών πρακτόρων και στη συνέχεια παρατίθενται οι απαιτήσεις τους σε ασφάλεια, σύμφωνα με τα υπάρχοντα πρότυπα λειτουργίας. Τέλος, αναπτύσσεται μια μεθοδολογία σύγκρισης των μοντέλων ασφάλειας και εμπιστοσύνης το οποίο και χρησιμοποιείται στη συνέχεια για την ανάλυση συστημάτων πρακτόρων.

2.2 Κίνδυνοι Λειτουργίας Κινητών Πρακτόρων

Τα συστήματα κινητών πρακτόρων εμπεριέχουν επικοινωνίες μεταξύ πρακτόρων, καθώς και ένα σημαντικό βαθμό αυτονομίας και κινητικότητας. Προκειμένου να επιτευχθούν συγκεκριμένες εργασίες, κάποιες φορές είναι απαραίτητο ένας πράκτορας να μετακινηθεί, μαζί με τα δεδομένα που έχει συλλέξει/παραγάγει, μέσα από ένα κοινόχρηστο δίκτυο ευρείας περιοχής. Έτσι, ένας πράκτορας θα πρέπει να μπορεί να προστατεύεται από τυχόν κακόβουλες πλατφόρμες εκτέλεσης, που σκοπεύουν να αλλοιώσουν τη λειτουργία του ή/και τα (πιθανώς απόρρητα) δεδομένα του. Από την άλλη πλευρά, οι πλατφόρμες που παρέχουν υπηρεσίες φιλοξενίας πρακτόρων πρέπει να είναι προστατευμένες από κακόβουλους πράκτορες. Επιπλέον, κάποιες φορές είναι δυνατόν ένας πράκτορας να πραγματοποιήσει επίθεση εναντίον ενός άλλου πράκτορα που εκτελείται στην ίδια, ή ακόμη και σε διαφορετική πλατφόρμα.

Οι δημιουργοί συστημάτων πρακτόρων χρησιμοποιούν ποικίλες τεχνικές προκειμένου να επιλύσουν αυτά τα ζητήματα. Οι τεχνικές αυτές συνήθως αποτελούνται από μηχανισμούς αυθεντικοποίησης, εμπιστευτικότητας, ακεραιότητας δεδομένων καθώς και μηχανισμούς παρακολούθησης [1], [8], [10],

[11]. Επιπλέον της χρήσης μηχανισμών ασφάλειας, το γεγονός ότι ένας πράκτορας πρέπει να λειτουργήσει σε ένα δυναμικό περιβάλλον εισάγει την έννοια της εμπιστοσύνης. Η εμπιστοσύνη αντικατοπτρίζει την ανθρώπινη κοινωνική συμπεριφορά εκτίμησης ρίσκου, κατευθυνόμενη από την ανάγκη για συνεργασία μέσα από την επικοινωνία και την αλληλεπίδραση, προκειμένου να επιτευχθεί ένας συγκεκριμένος στόχος [10], [11], [12]. Περιλαμβάνει υποθέσεις σχετικά με το κατά πόσο οι διάφορες οντότητες που απαρτίζουν ένα σύστημα κινητών πρακτόρων είναι ασφαλείς για αλληλεπίδραση ή είναι κακόβουλες. Αν και οι υποθέσεις σχετικά με την αξιοπιστία είναι συχνά απαραίτητες, κάποιες φορές μπορεί να οδηγήσουν στο να θεωρηθεί μια οντότητα ως αξιόπιστη, και άρα υψηλής εμπιστοσύνης, ενώ στην πραγματικότητα να μην είναι. Σε μια τέτοια περίπτωση, η χρήση ακόμη και των πλέον σύγχρονων και ισχυρών μηχανισμών ασφάλειας είναι άσκοπη.

Οι κίνδυνοι ασφάλειας που προκύπτουν από την παραβίαση του πράκτορα ως οντότητα ή της πλατφόρμας στην οποία λειτουργεί, αφορούν στην απώλεια της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας των πληροφοριών, έννοιες οι οποίες ορίζονται όπως παρακάτω [68]:

- **Εμπιστευτικότητα** – Οι πληροφορίες που περιέχει ο πράκτορας πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Αυτές μπορεί να είναι στοιχεία που συλλέχθηκαν κατά τη διάρκεια της λειτουργίας του ή ακόμη και πληροφορίες που εισήγαγε ο δημιουργός του (π.χ. στοιχεία χρέωσης, αν πρόκειται για εμπορική εφαρμογή).
- **Ακεραιότητα** – Διασφάλιση της εγκυρότητας, ορθότητας και πληρότητας των δεδομένων κατά τη φάση της συλλογής, επεξεργασίας και παραγωγής του αποτελέσματος της επεξεργασίας τους από το πράκτορα.
- **Διαθεσιμότητα** – Τα δεδομένα και οι υπηρεσίες του πράκτορα πρέπει να είναι διαθέσιμα στις εξουσιοδοτημένες οντότητες για όσο χρονικό διάστημα προβλέπεται για την ολοκλήρωση της λειτουργίας του.

Η σημαντικότητα των παραπάνω κινδύνων προσδιορίζεται από την επίδρασή τους στη λειτουργία του πράκτορα και από την πιθανότητα εκδήλωσής τους.

Η επίδραση από την απώλεια της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας των πληροφοριών στη λειτουργία των πρακτόρων μπορεί

πρακτικά να οδηγήσει σε ποικίλες επιπτώσεις. Όπως προκύπτει από τα [67], [68], μπορεί να επιφέρει:

- Απώλεια ανταγωνιστικού πλεονεκτήματος σε σχέση με άλλους πράκτορες - υπηρεσίες.
- Λήψη λανθασμένων αποφάσεων από τον πράκτορα.
- Αδυναμία διεκπεραίωσης βασικών δραστηριοτήτων.
- Προσβολή της αξιοπιστίας και της εμπιστοσύνης προς τον πράκτορα, το δημιουργό του και τη πλατφόρμα λειτουργίας, ειδικά σε περίπτωση όπου χρησιμοποιείται προσαρμοστικό μοντέλο εμπιστοσύνης.
- Πιθανότητα για επιπλέον κόστος πέραν αυτού που δημιουργήθηκε από την αδυναμία ασφάλειας.
- Παραβίαση νομικού ή θεσμικού κανόνα ή μη τήρηση συμβατικής υποχρέωσης.
- Αδυναμία επαναλειτουργίας λόγω πολλών ανεκτέλεστων διαδικασιών οι οποίες δεν μπορούν να εκτελεστούν είτε λόγω χρονικού περιορισμού, είτε επειδή έχουν χαθεί.
- Πιθανότητα απάτης.
- Αδυναμία λειτουργίας λόγω απώλειας διαθεσιμότητας των πληροφοριακών πόρων που παρέχει η πλατφόρμα.

Οι παραπάνω κίνδυνοι θεωρούνται κρίσιμοι παράγοντες για την παρούσα περιορισμένη χρήση της τεχνολογίας των πρακτόρων [34].

2.3 Απαιτήσεις Ασφάλειας

Όπως αναφέραμε στο εισαγωγικό κεφάλαιο δεν υπάρχουν συγκεκριμένες ενεργές προδιαγραφές σχετικές με την ασφάλεια κινητών πρακτόρων. Παρόλ' αυτά όμως στις προδιαγραφές που έχει παραγάγει το FIPA, καθώς και σε εκείνες που βρίσκονται ακόμη σε προκαταρκτικό στάδιο [15], υπάρχουν κάποιες αρχές ασφάλειας που απαιτούνται από τα συμβατά συστήματα κινητών πρακτόρων. Ομοίως, και στη περίπτωση του OMG στις προδιαγραφές του περιλαμβάνονται κάποιοι βασικοί κανόνες ασφάλειας [17], [18]. Οι απαιτήσεις αυτές συνοψίζονται στους παρακάτω τομείς ασφάλειας [10]:

- Αυθεντικοποίηση (Authentication): Η δυνατότητα εξακρίβωσης της ταυτότητας των διαφόρων οντοτήτων που αποτελούν το σύστημα.
- Εξουσιοδότηση (Authorization): Με βάση την ταυτότητα μιας οντότητας να προσδιοριστεί ποιες πολιτικές πρόσβασης πρέπει να εφαρμοστούν στην οντότητα αυτή.
- Ακεραιότητα (Integrity): Η δυνατότητα να προσδιοριστεί εάν κάποιο τμήμα λογισμικού, μήνυμα ή άλλα δεδομένα έχουν τροποποιηθεί μετά την αποστολή τους από την αρχική πηγή.
- Ιδιωτικότητα (Privacy). Η δυνατότητα να εξασφαλιστεί ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να αποκτήσουν πρόσβαση σε κάποιο λογισμικό, μήνυμα ή άλλα δεδομένα. Για κάθε άλλη οντότητα η πληροφορία θα πρέπει να μένει κρυφή (obscured).

Επιπλέον, οι προδιαγραφές του FIPA και του OMG εισάγουν κάποιες υποθέσεις σχετικά με την εξ' ορισμού ασφάλεια που παρέχουν κάποια στοιχεία της πλατφόρμας εκτέλεσης, το οποίο μπορεί να θεωρηθεί ως ένα βασικό μοντέλο εμπιστοσύνης [1], [2], [17], [18].

Ακόμη, θεωρούμε ότι ένα μοντέλο ασφάλειας και εμπιστοσύνης οφείλει, για λόγους λειτουργικότητας, να ακολουθεί τις παρακάτω κατευθύνσεις:

1. Το μοντέλο θα πρέπει να είναι διεξοδικό. Πρέπει να καλύπτει όλους τους τομείς της λειτουργίας και τον κύκλο ζωής ενός πράκτορα, καθώς και θέματα επικοινωνιών και διαχείρισης, τόσο από τη πλευρά του πράκτορα όσο και από την πλευρά της πλατφόρμας εκτέλεσης.
2. Το μοντέλο θα πρέπει να καλύπτει τις παραδοχές στο θέμα της εμπιστοσύνης (trust model) μεταξύ των εμπλεκόμενων οντοτήτων, πέρα από τα τεχνικά χαρακτηριστικά ασφάλειας.
3. Θα πρέπει να είναι γενικό-αφαιρετικό, στα πρότυπα των υπαρχόντων προτύπων για κινητούς πράκτορες, ώστε να μπορεί να εφαρμοστεί σε υλοποιήσεις πρακτόρων που προορίζονται για ετερόκλητες χρήσεις. Έτσι, θα μπορεί να παρέχει ελευθερία στους κατασκευαστές να μπορούν να επιλέξουν μεταξύ διαφόρων μηχανισμών ασφάλειας ανάλογα με την εφαρμογή, με την προϋπόθεση να καλύπτονται οι ελάχιστες απαιτήσεις που θα θέτει το μοντέλο.

2.4 Μοντέλο Σύγκρισης

Με βάση τις απαιτήσεις που αναφέρθηκαν στην προηγούμενη παράγραφο, προτείνουμε μια λίστα κριτηρίων, ως μοντέλο σύγκρισης, με βάση το οποίο συγκρίνουμε τα μοντέλα ασφάλειας και εμπιστοσύνης συστημάτων κινητών πρακτόρων. Με αυτό τον τρόπο αποσκοπούμε στο να αναλύσουμε τους τρόπους με τους οποίους οι αρχές ασφάλειας ικανοποιούνται στα σημερινά συστήματα. Το μοντέλο αυτό πρέπει να καλύπτει τα θέματα ασφάλειας όλων των οντοτήτων που περιλαμβάνονται σε ένα σύστημα κινητών πρακτόρων: ασφάλεια πράκτορα, ασφάλεια πλατφόρμας εκτέλεσης, ασφάλεια δεδομένων και υποθέσεις εμπιστοσύνης μεταξύ τους (trust model) σε συνδυασμό με στοιχεία λειτουργικότητας. Έτσι, για το μοντέλο σύγκρισής μας, προτείνουμε τα παρακάτω κριτήρια με βάση τα οποία εξετάζονται στη συνέχεια τα συστήματα κινητών πρακτόρων:

1. **Ακεραιότητα πράκτορα** (agent integrity): Οι μηχανισμοί με τους οποίους ο κώδικας του πράκτορα καθώς και τα δεδομένα που φέρει προστατεύονται από κακόβουλες πλατφόρμες ή άλλους πράκτορες. Εξετάζεται η αποτελεσματικότητα των μεθόδων που υιοθετεί το κάθε εξεταζόμενο σύστημα και ο βαθμός με τον οποίο μπορούν να αντιμετωπίσουν τις διάφορες απειλές.
2. **Ακεραιότητα πλατφόρμας εκτέλεσης** (platform integrity): Οι μηχανισμοί με τους οποίους η πλατφόρμα εκτέλεσης προστατεύεται από τυχόν κακόβουλους πράκτορες, προκειμένου να μπορεί να συνεχίσει να παρέχει τις υπηρεσίες της.
3. **Ασφάλεια επικοινωνιών** (communications security): Τα κρυπτογραφικά μέσα τα οποία χρησιμοποιούνται για τη διασφάλιση των επικοινωνιών μεταξύ πρακτόρων, αλλά και των εξωτερικών επικοινωνιών. Η ανάλυση γίνεται σε συνδυασμό με τον τύπο δικτύου για τον οποίο προορίζεται το κάθε εξεταζόμενο σύστημα πρακτόρων.
4. **Μοντέλο αυθεντικοποίησης** (authentication scheme): Οι μηχανισμοί με τους οποίους οι οντότητες που απαρτίζουν ένα σύστημα πρακτόρων

αυθεντικοποιούνται μεταξύ τους. Εξετάζεται και κατά πόσο η αυθεντικοποίηση είναι αμοιβαία ή μονόπλευρη (π.χ. αν μονάχα ο πράκτορας αυθεντικοποιείται στην πλατφόρμα ή και αντίστροφα). Επίσης εξετάζεται το κατά πόσο γίνεται η χρήση ψηφιακών υπογραφών και από ποιες οντότητες καθώς και η χρήση πιστοποιητικών.

5. **Έλεγχος πρόσβασης** (access control): τα κριτήρια με τα οποία οι πόροι της πλατφόρμας κατανέμονται στους πράκτορες.
6. **Διαχείριση πόρων** (resource control): ο βαθμός με τον οποίο οι πόροι του συστήματος κατανέμονται αποδοτικά και δίκαια.
7. **Δυνατότητα μετανάστευσης** (migration capability): ο βαθμός κατά τον οποίο είναι δυνατόν ένας πράκτορας να μετακινηθεί σε μια άλλη πλατφόρμα και να συνεχίσει την εκτέλεσή του εκεί και μάλιστα κατά πόσο μπορεί να μετακινήσει την κατάσταση εκτέλεσής του (execution state) στη νέα πλατφόρμα. Η μετανάστευση με μεταφορά της πιο πρόσφατης κατάστασης εκτέλεσης ονομάζεται ισχυρή **(strong migration**), ενώ η μεταφορά περιορισμένων προκαθορισμένων σημείων της κατάστασης εκτέλεσης είναι η ασθενής μετανάστευση (**weak migration**). Αν και η δυνατότητα μετανάστευσης δεν αποτελεί κριτήριο ασφάλειας, την έχουμε εισάγει στο μοντέλο σύγκρισής μας καθώς θεωρείται απαραίτητη δυνατότητα για τους κινητούς πράκτορες. Η δυνατότητα, όμως, αυτή εισάγει νέες απαιτήσεις ασφάλειας στη λειτουργία ενός συστήματος πρακτόρων.
8. **Μοντέλο εμπιστοσύνης** (trust model): Προκειμένου να λειτουργήσει κάθε αρχιτεκτονική ασφάλειας, κάποιες οντότητες πρέπει να θεωρηθούν έμπιστες και ασφαλείς εξ ορισμού. Θα εξεταστούν ποιες είναι αυτές σε κάθε σύστημα και κατά πόσο αυτό είναι αποδοτικό από πλευράς ασφάλειας.
9. **Κεντρικοποιημένη διαχείριση ασφάλειας** (domain driven security): Εξετάζεται εάν υπάρχει κάποια κεντρική οντότητα που να ρυθμίζει θέματα ασφάλειας σε ένα δίκτυο κινητών πρακτόρων (Domain) από το οποίο θα λαμβάνουν οδηγίες ή θα λογοδοτούν οι διάφορες πλατφόρμες, οι πράκτορες και οι χρήστες που συμμετέχουν στο συγκεκριμένο σύστημα.

Πέρα από την ανάλυση με βάση τα παραπάνω κριτήρια επικεντρωνόμαστε περισσότερο στο μοντέλο εμπιστοσύνης, εξετάζοντάς το και με μια επιπλέον μέθοδο, πέρα από τα κριτήρια σύγκρισης που μόλις προτείναμε. Ο λόγος είναι ότι θεωρούμε ότι χρήζει περισσότερης διερεύνησης επειδή τυχόν προβλήματα σε αυτό αποτελούν ουσιαστικό λόγο για την περιορισμένη χρήση της τεχνολογίας [34]. Αναλύουμε τη συμπεριφορά του κάθε συστήματος κάτω από συγκεκριμένες απειλές που αφορούν στις υιοθετημένες υποθέσεις αξιοπιστίας των διαφόρων οντοτήτων. Επιπλέον, επιχειρούμε να αποφανθούμε ως προς το κατά πόσο κατάλληλο είναι το κάθε μοντέλο εμπιστοσύνης για λειτουργία σε ανοιχτά περιβάλλοντα.

Δεδομένου ότι επιθυμούμε να εμβαθύνουμε στο μοντέλο εμπιστοσύνης, τα χρησιμοποιούμενα σενάρια δεν αφορούν σε ευρύτερα θέματα ασφάλειας, όπως για παράδειγμα ακεραιότητα επικοινωνιών ή παραβιάσεις πρόσβασης. Αντίθετα, επικεντρωνόμαστε σε σενάρια που αναδεικνύουν τυχόν ανεπάρκειες του μοντέλου εμπιστοσύνης. Έτσι, εξετάζουμε τη συμπεριφορά των συστημάτων κινητών πρακτόρων κάτω από τα παρακάτω σενάρια απειλών:

- **Κακόβουλη συμπεριφορά ενός αυθεντικοποιημένου/ έμπιστου πράκτορα**. Συνήθως, το επίπεδο εμπιστοσύνης που αποδίδεται σε ένα πράκτορα βασίζεται στην ταυτότητα του ιδιοκτήτη του [1], [2]. Παρόλ’ αυτά το να ανήκει σε έμπιστο χρήστη δεν προλαμβάνει απαραίτητα έναν πράκτορα από το να παρουσιάσει κακόβουλη συμπεριφορά. Αυτός ο τύπος επίθεσης μπορεί να πραγματοποιηθεί είτε σκόπιμα, από τον έως τώρα έμπιστο χρήστη, είτε από μια τρίτη οντότητα που χρησιμοποιεί την ταυτότητα του έμπιστου χρήστη. Όποια και να είναι η αιτία, θέλουμε να διερευνήσουμε τη απόκριση του συστήμτος πρακτόρων καθώς και τις πιθανές επιπτώσεις στη λειτουργία του.
- **Η απειλή μια πλατφόρμας εκτέλεσης πρακτόρων να είναι ή να έγινε κακόβουλη**. Συνήθως η πλατφόρμα θεωρείται εξ ορισμού ως ασφαλής από τους πράκτορες [1], [2]. Ωστόσο, είναι δυνατόν μια πλατφόρμα να πραγματοποιήσει επίθεση στους πράκτορες που φιλοξενεί. Ομοίως με παραπάνω, αυτό μπορεί να συμβεί είτε επειδή η αρχικά νομότυπη (legitimate) πλατφόρμα έχει πέσει η ίδια θύμα κάποιας επίθεσης, είτε επειδή

ήταν προγραμματισμένο να γίνει κακόβουλη από την αρχή της λειτουργίας της. Σκοπός μας είναι να διερευνήσουμε την έκταση στην οποία μπορούν να καλύψουν τέτοιες απειλές τα μοντέλα ασφάλειας και εμπιστοσύνης των συστημάτων κινητών πρακτόρων που εξετάζουμε. Επίσης, γίνεται εκτίμηση των πιθανών συνεπειών μιας τέτοιας επίθεσης.

- **Λειτουργία κινητού πράκτορα σε ανοιχτό περιβάλλον**. Μολονότι δεν αποτελεί συγκεκριμένη απειλή, πιστεύουμε ότι είναι απαραίτητο να εξετάσουμε τη καταλληλότητα των μοντέλων εμπιστοσύνης για λειτουργία του συστήματος σε περιβάλλοντα όπου δεν υπάρχει κοινή διαχείριση ασφάλειας, όπως το Διαδίκτυο. Θέλουμε να εξετάσουμε κατά πόσο μια τέτοια λειτουργία μπορεί να υποστηριχθεί αποτελεσματικά.

2.5 Συμπεράσματα

Τα παραπάνω κριτήρια σε συνδυασμό με τα σενάρια απειλών χρησιμοποιούνται ως μοντέλο σύγκρισης για τις τεχνικές ασφάλειας που παρέχουν τα σημερινά συστήματα πρακτόρων. Θεωρούμε ότι ο συνδυασμός αυτός μπορεί να αποτυπώσει σφαιρικά το επίπεδο ασφάλειας του κάθε συστήματος που εξετάζεται, σε συνάρτηση με το επίπεδο λειτουργικότητας που αυτό προσφέρει. Τη μέθοδο αυτή χρησιμοποιούμε ως μηχανισμό εξαγωγής συμπερασμάτων για την παρούσα κατάσταση της τεχνολογίας των κινητών πρακτόρων όσον αφορά στα μοντέλα ασφάλειας και εμπιστοσύνης. Οι τυχόν ελλείψεις που εντοπίζονται κατά τη σύγκριση χρησιμοποιούνται στη συνέχεια για την πρόταση ενός νέου μοντέλου ασφάλειας και εμπιστοσύνης που τις καλύπτει, που επιπλέον πληροί και τις προδιαγραφές που έχουν τεθεί στο τέλος του πρώτου κεφαλαίου.

3 ΑΝΑΛΥΣΗ ΜΟΝΤΕΛΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο αναλύουμε συστήματα κινητών πρακτόρων χρησιμοποιώντας το μοντέλο σύγκρισης που προτείναμε στο προηγούμενο κεφάλαιο. Γίνεται αποτύπωση και αξιολόγηση των μοντέλων ασφάλειας και εμπιστοσύνης που υλοποιούν αντιπροσωπευτικά συστήματα πρακτόρων. Έτσι, εντοπίζονται οι απειλές που δεν λαμβάνονται υπόψη αποτελεσματικά ή ακόμη και καθόλου. Τέλος, εξάγονται συμπεράσματα για το βαθμό προόδου της τεχνολογίας στο τομέα της ασφάλειας πρακτόρων. Με βάση τα συμπεράσματα αυτά, στο επόμενο κεφάλαιο προχωρούμε στην πρόταση ενός μοντέλου ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες που να αντιμετωπίζει τις ελλείψεις που διαπιστώθηκαν.

3.2 Επιλογή Συστημάτων – Δομή Σύγκρισης

Όπως αναφέραμε και στην εισαγωγή, τα συστήματα που αναλύονται ανήκουν στη κατηγορία των κινητών πρακτόρων που είναι και εκείνη που παρουσιάζει τα μεγαλύτερα θέματα ασφάλειας λόγω ανταλλαγών δεδομένων μέσω μη ασφαλών δικτύων αλλά και μετακίνησης του ιδίου του πράκτορα. Έτσι, μεταξύ των δεκάδων συστημάτων πρακτόρων που υπάρχουν, έχουμε περιορίσει την επιλογή σε συστήματα που έχουν αναπτυχθεί λαμβάνοντας υπόψη τις ανάγκες ασφάλειας του χώρου και υλοποιούν ποικίλες τεχνικές ασφάλειας. Επιπλέον, θεωρήσαμε σημαντικό το να έχουν απασχολήσει ερευνητικά τη διεθνή επιστημονική κοινότητα. Σημαντικός παράγοντας στην επιλογή των συστημάτων ήταν να διαθέτουν επαρκή τεκμηρίωση (documentation) για τα υποσυστήματα και την αρχιτεκτονική τους, που, όμως, όπως διαπιστώθηκε στην πορεία της έρευνας,

δεν συμβαίνει πάντοτε. Τέλος, ο τύπος των συστημάτων έπρεπε να ποικίλει ώστε να καλύπτονται διαφορετικές εφαρμογές της τεχνολογίας των κινητών πρακτόρων.

Με βάση τα παραπάνω κριτήρια επιλέξαμε προς ανάλυση τα συστήματα κινητών πρακτόρων: **Grasshopper, JADE, Cougaar, Aglets, Nomads, Mansion, Havana, Concordia, D'Agents, Mole και Ara.** Συγκεκριμένα τα Grasshopper, Concordia και Aglets αποτελούν πλατφόρμες κινητών πρακτόρων γενικής χρήσης, των οποίων τα μοντέλα ασφάλειας και εμπιστοσύνης που υιοθετούν έχουν απασχολήσει εκτενώς την επιστημονική κοινότητα [19]-[22], [27], [29], [37]-[41]. Το JADE αποτελεί ένα σύγχρονο σύστημα γενικής χρήσης, το οποίο είναι υπό συνεχιζόμενη ανάπτυξη, με σημαντικά χαρακτηριστικά ασφάλειας [19], [21], [23], [24], [30]. Το NOMADS [49], [51] αποτελεί ένα ερευνητικό σύστημα το οποίο αρχικά ξεκίνησε υπό την χρηματοδότηση της DARPA και της NASA και το οποίο αποσκοπεί στην παροχή προηγμένης κινητικότητας και ελέγχου πόρων σε ένα ασφαλές περιβάλλον. Το Mansion [53], [54], [55] αποτελεί ένα ακόμη ερευνητικό πρόγραμμα, του οποίου ο σκοπός είναι η δημιουργία μιας αλυσίδας εμπιστοσύνης σε μεγάλα περιβάλλοντα. Το Cougaar [31], [32], [33]αποτελεί ένα σύστημα πρακτόρων ειδικού σκοπού, το οποίο και αυτό ξεκίνησε υπό τη χρηματοδότηση της DARPA. Ο σχεδιασμός του αφορούσε λειτουργία σε περιβάλλον υψηλού κινδύνου που επικρατεί στις στρατιωτικές εφαρμογές. Τέλος, το Havana αποτελεί ένα εμπορικό σύστημα κινητών πρακτόρων ειδικού σκοπού που αποσκοπεί στη δημιουργία ενός απολύτως έμπιστου περιβάλλοντος μέσα από τη δέσμευση των οντοτήτων με επιχειρηματικό συμβόλαιο του πραγματικού κόσμου.

Στην αρχή της ανάλυσης του κάθε πράκτορα παρουσιάζεται η αρχιτεκτονική του συστήματος σε επίπεδα, ξεκινώντας από τον ίδιο τον πράκτορα και προχωρώντας στην πλατφόρμα εκτέλεσής του (host) και, τέλος, στην παρουσίαση ολοκλήρου του “κόσμου” (Domain) που απαρτίζει το σύστημα. Η παρουσίαση γίνεται με έμφαση στα χαρακτηριστικά ασφάλειας του κάθε επιπέδου και επικεντρώνεται στα τμήματα που σχετίζονται περισσότερο με την ασφάλεια και λιγότερο με τη λειτουργικότητα του κάθε συστήματος.

Στη συνέχεια αναλύονται οι μέθοδοι με τις οποίες καλύπτονται τα κριτήρια σύγκρισης που θέσαμε στο προηγούμενο κεφάλαιο και τέλος εξετάζεται με ποιο

τρόπο αναμένεται να αντιδράσει το σύστημα στα τρία σενάρια απειλών του μοντέλου σύγκρισης. Μετά την ανάλυση των πρακτόρων αναλύονται συγκεντρωτικά τα αποτελέσματα και με τη χρήση πινάκων απεικονίζεται συγκριτικά η συμπεριφορά των υπό εξέταση συστημάτων. Τέλος, εξάγονται συμπεράσματα σχετικά με τις αδυναμίες και ελλείψεις των υπαρχόντων μοντέλων ασφάλειας και εμπιστοσύνης, με βάση τα οποία προχωρούμε στην πρόταση του δικού μας μοντέλου στο επόμενο κεφάλαιο.

Προτού προχωρήσουμε στην ανάλυση των συστημάτων παραθέτουμε πιο αναλυτικά τα επίπεδα των συστημάτων κινητών πρακτόρων. Επειδή η αρχιτεκτονική που ακολουθεί το κάθε σύστημα συχνά διαφοροποιείται αρκετά και ο βαθμός πολυπλοκότητας κυμαίνεται, ενδέχεται κάποιες από τις οντότητες που απεικονίζουν τα επίπεδα να απουσιάζουν ή να απαιτούνται άλλα ενδιάμεσα επίπεδα για τη σωστή απεικόνισή τους.

Έτσι, η ευρύτερη οντότητα της κάθε πλατφόρμας θα αποτελεί το **διάγραμμα πλαίσιο** που απεικονίζει συνήθως ολόκληρο τον κόσμο λειτουργίας του κάθε συστήματος. Οι επιμέρους οντότητες απεικονίζονται στα **διαγράμματα επιπέδου 1, 2, 3 και 4.** Συγκεκριμένα, στα κατώτερα διαγράμματα (επίπεδο 4) απεικονίζεται ο ίδιος ο πράκτορας. Η διαγραμματική απεικόνιση επικεντρώνεται στα τμήματα που έχουν να κάνουν με την ασφάλεια και λιγότερο με τη λειτουργικότητα του συστήματος πρακτόρων. Οι οντότητες που απεικονίζουμε διαγραμματικά είναι:

Επικράτεια (Domain) – διάγραμμα Πλαίσιο: Συνήθως αποτελείται από ένα ευρύτερο δίκτυο πλατφορμών εκτέλεσης πρακτόρων με κάποιου είδους κοινή διαχείριση (πχ LAN οργανισμού). Αποτελεί το συνολικό κόσμο λειτουργίας ενός συστήματος κινητών πρακτόρων.

Κατανεμημένη πλατφόρμα εκτέλεσης – διάγραμμα επιπέδου 1: Οι επιμέρους λειτουργίες μιας πλατφόρμας μπορεί να κατανέμονται σε πολλαπλά μηχανήματα (host) ενός δικτύου. Η συγκεκριμένη οντότητα αποτελεί την εικονική ομαδοποίησή τους. Συνήθως όλες οι υπηρεσίες μιας πλατφόρμας παρέχονται από ένα μηχάνημα οπότε και τις περισσότερες φορές αυτή ο οντότητα ταυτίζεται με τη πλατφόρμα. Σε αυτές τις περιπτώσεις τα διαγράμματα επιπέδου 1 και 2 θα ταυτίζονται.

Πλατφόρμα εκτέλεσης (Agent System) – διάγραμμα επιπέδου 2: Ένα μηχάνημα εκτέλεσης όπου τρέχει το περιβάλλον εκτέλεσης των πρακτόρων και παρέχει υπηρεσίες φιλοξενίας.

Τοποθεσία πλατφόρμας (Place) – διάγραμμα επιπέδου 3: Μια εικονική ομαδοποίηση πρακτόρων σε μια πλατφόρμα για καλύτερη διαχείριση παρόμοιων πρακτόρων. Συχνά δεν υφίσταται και ταυτίζεται με τον πράκτορα. Σε αυτές τις περιπτώσεις τα διαγράμματα επιπέδου 3 και 4 ταυτίζονται.

Πράκτορας (Agent) – διάγραμμα επιπέδου 4: Η οντότητα του καθεαυτού πράκτορα με την εσωτερική του δομή.

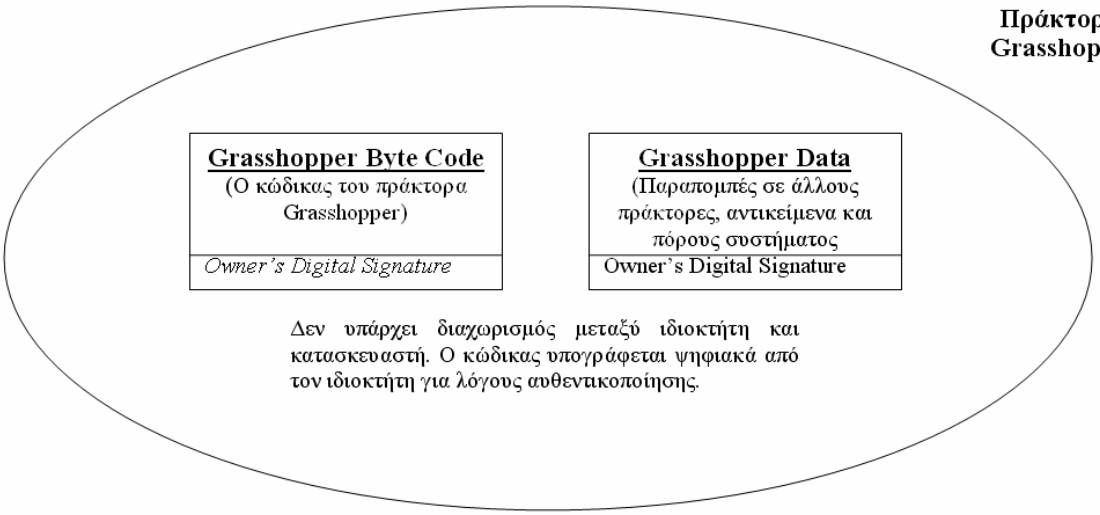
Λόγω της χρήσης επιπέδων, στα διαγράμματα ανώτερου επιπέδου εμπεριέχονται σε σμίκρυνση οι οντότητες του αμέσως κατώτερου και απεικονίζεται ο τρόπος που αυτές αλληλεπιδρούν. Έτσι για παράδειγμα, στο διάγραμμα πλαίσιο, που απεικονίζει ολόκληρο τον κόσμο λειτουργίας του συστήματος πρακτόρων, απεικονίζονται πλατφόρμες εκτέλεσης (διαγράμματα επιπέδου 1 ή 2) με τις αλληλεπιδράσεις τους. Ομοίως, μέσα στο διάγραμμα επιπέδου 2, που αναπαριστά την πλατφόρμα εκτέλεσης, εμφανίζονται πράκτορες ή ομαδοποιήσεις πρακτόρων (διαγράμματα επιπέδου 4 ή 3) και πώς αυτοί αλληλεπιδρούν. Μετά την παρουσίαση των συστημάτων, στην παράγραφο με τα αποτελέσματα σύγκρισης της αρχιτεκτονικής ανά επίπεδο, απεικονίζονται συγκριτικά οι οντότητες που υιοθετεί το κάθε σύστημα (Πίνακας 1, σελ.92).

3.3 Ανάλυση Συστημάτων Κινητών Πρακτόρων

3.3.1 Grasshopper

Το σύστημα πρακτόρων Grasshopper αναπτύχθηκε από την GMD FOKUS, διανέμεται από την IKV++ και αφορά σε εφαρμογές ηλεκτρονικού εμπορίου, ανάκτησης πληροφορίας, τηλεπικοινωνίες και κινητά υπολογιστικά συστήματα (mobile computing). Είναι συμβατό με τις προδιαγραφές της FIPA καθώς και με της OMG και κάνει διαχωρισμό των μηχανισμών ασφάλειας σε εσωτερικούς και εξωτερικούς. Η παρακάτω ανάλυση στηρίχθηκε στα [19]-[22].

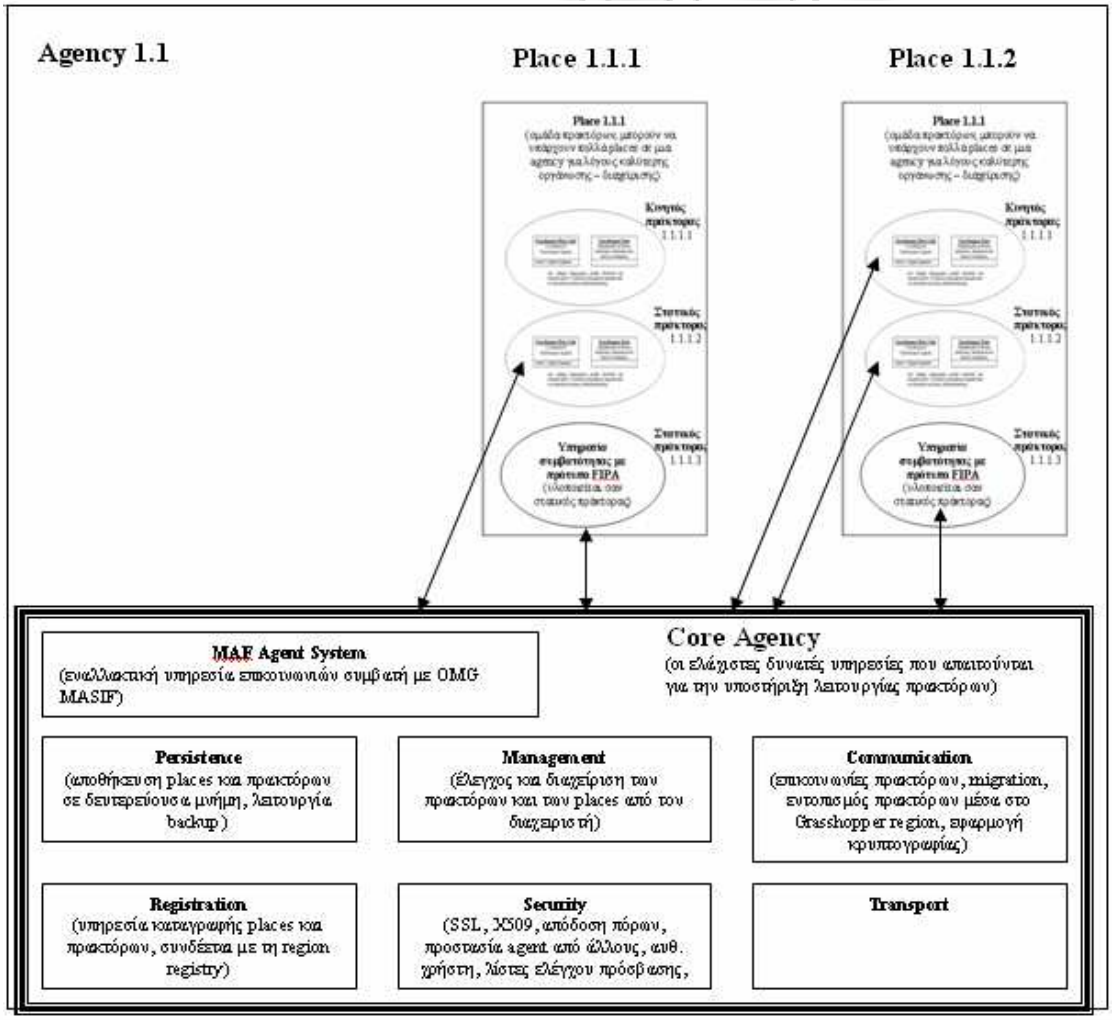
Ο πράκτορας Grasshopper (Εικόνα 2) κατά τη δημιουργία του αποτελείται από τον κώδικα και τα δεδομένα του, με τη ψηφιακή υπογραφή του ιδιοκτήτη, ενώ δεν γίνεται διαχωρισμός μεταξύ προγραμματιστή και δημιουργού. Ο πράκτορας ενδέχεται να είναι κινητός ή σταθερός. Ακολουθεί απλούστατη σχεδίαση και ονομάζεται Υπηρεσία και βασίζεται στη Java. Τα πάντα του παρέχονται ως εξωτερικές υπηρεσίες από την πλατφόρμα. Οι υπηρεσίες αυτές θεωρούνται στατικοί πράκτορες.



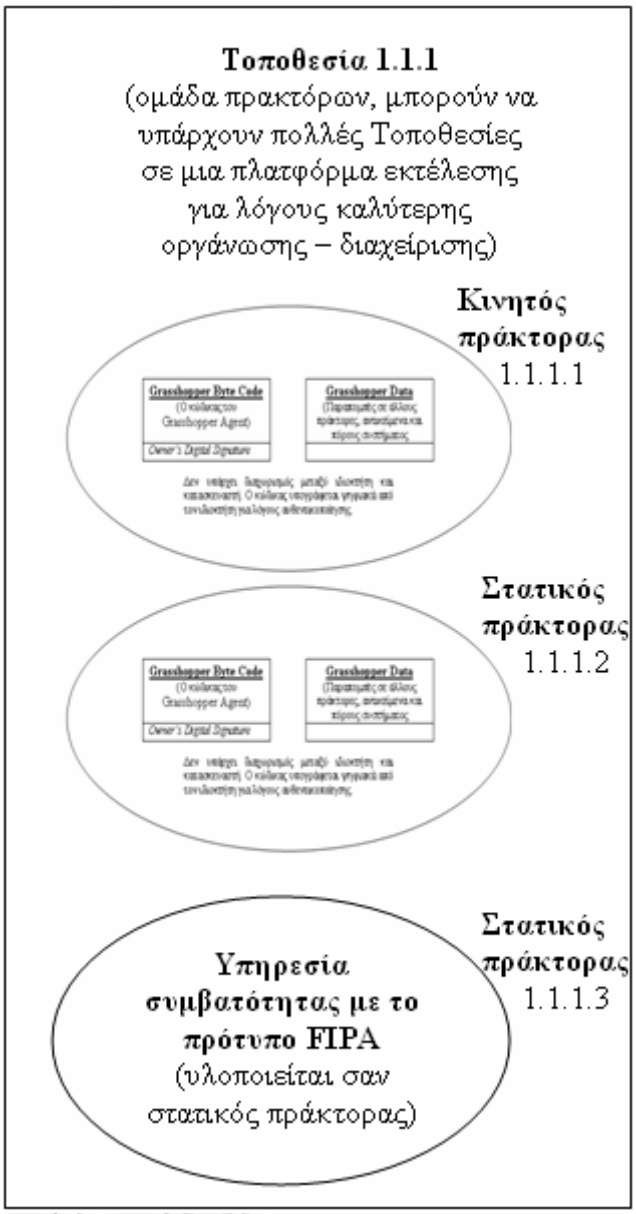
Εικόνα 2 – Διάγραμμα επιπέδου 4: Ένας πράκτορας Grasshopper.

Το μηχάνημα εκτέλεσης των πρακτόρων Grasshopper ονομάζεται Agency (Εικόνα 3). Εδώ υποστηρίζονται ομαδοποιήσεις πρακτόρων με κοινή αντιμετώπιση

που ονομάζεται Place (Εικόνα 4). Οι πράκτορες υποχρεωτικά πρέπει να ανήκουν σε κάποια Τοποθεσία (Place). Η πλατφόρμα εκτέλεσης (Agency - Εικόνα 5) τρέχει την Java Virtual Machine (JVM) και παρέχει όλες τις υπηρεσίες υποστήριξης: επικοινωνίες πρακτόρων, μετανάστευση, εντοπισμό πρακτόρων μέσα στην επικράτεια Grasshopper (Region), εφαρμογή κρυπτογραφίας, Secure Sockets Layer (SSL), πιστοποιητικά τύπου X509, απόδοση πόρων, προστασία του πράκτορα από άλλους, αυθεντικοποίηση χρήστη, λίστες ελέγχου πρόσβασης, υπηρεσία καταγραφής Places και πρακτόρων, σύνδεση με τη Region Registry, αποθήκευση Places και πρακτόρων στη δευτερεύουσα μνήμη και λειτουργία backup και υπηρεσίες συμβατότητας με MASIF και FIPA. Σημειώνεται ότι οι πόροι του συστήματος θεωρούνται στατικοί πράκτορες και επομένως ανήκουν σε Τοποθεσία.

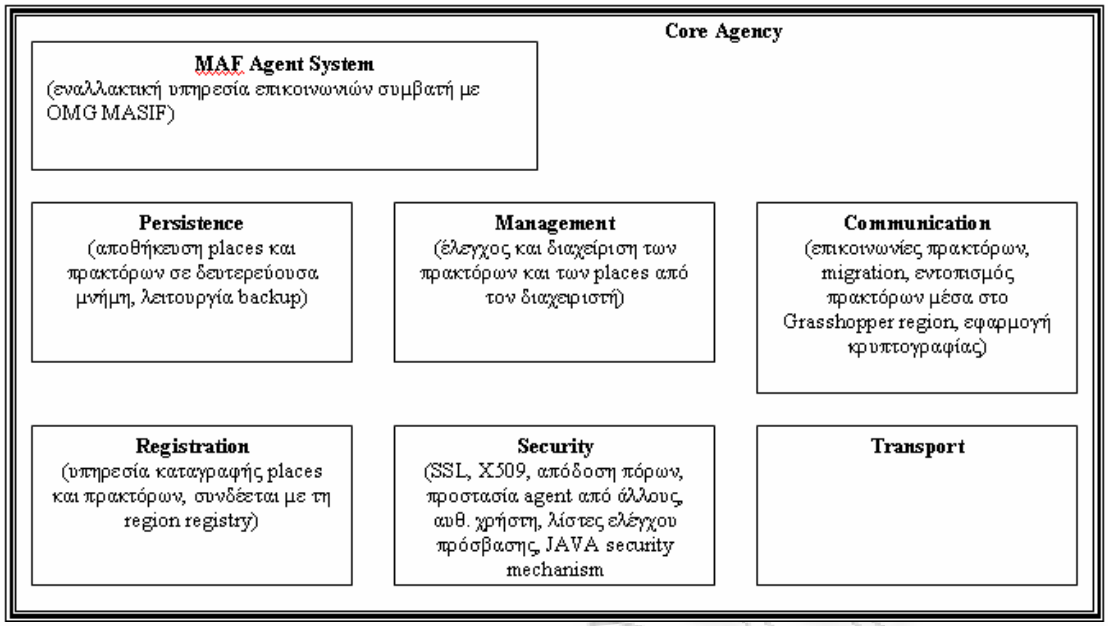


Εικόνα 3 - Διάγραμμα επιπέδου 1: Η πλατφόρμα εκτέλεσης (Agency) των πρακτόρων Grasshopper.

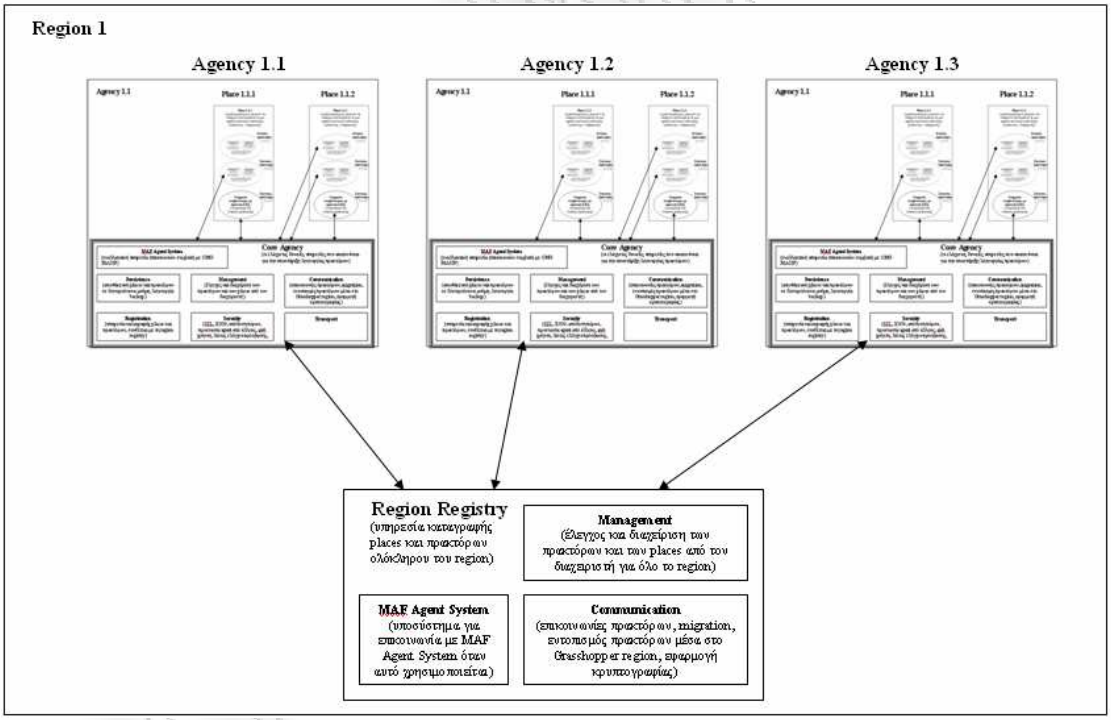


Εικόνα 4 - Διάγραμμα επιπέδου 2 (α): Μια τοποθεσία (Place) Grasshopper.

Στο Grasshopper η ανώτερη επικράτεια ορίζεται το Region (Εικόνα 6). Και εδώ υπάρχει κεντρικοποιημένη διαχείριση από το Region Registry από όπου ελέγχονται όλες οι λειτουργίες ασφάλειας. Παρέχεται έλεγχος και διαχείριση των πρακτόρων και των Places από τον διαχειριστή για όλο το Region καθώς και για τις επικοινωνίες πρακτόρων, τη μετανάστευση, τον εντοπισμός πρακτόρων μέσα στο Grasshopper Region και ρύθμιση του επιπέδου κρυπτογραφίας.



Εικόνα 5 - Διάγραμμα επιπέδου 2 (b): Διάγραμμα επιπέδου 2 (b): οι ελάχιστες δυνατές υπηρεσίες που απαιτούνται για την υποστήριξη λειτουργίας πρακτόρων



Εικόνα 6 - Διάγραμμα - Πλαίσιο: Μια ομάδα agencies με κοινούς στόχους λειτουργίας - ασφάλειας

Ανάλυση με Βάση τα Κριτήρια Σύγκρισης

Η εσωτερική ασφάλεια στηρίζεται στους μηχανισμούς που παρέχει η Java Virtual Machine (JVM) και συγκεκριμένα το Java Sandbox [21]. Σκοπεύει να προστατεύσει την πλατφόρμα και τους πόρους της από κακόβουλους πράκτορες, καθώς και να παρέχει προστασία σε συναλλαγές μεταξύ πρακτόρων. Ο έλεγχος πρόσβασης παρέχεται, επίσης, μέσω των μηχανισμών της Java. Κάθε πράκτορας φέρει την ψηφιακή υπογραφή του ιδιοκτήτη του, που χρησιμοποιείται για υπηρεσίες αυθεντικοποίησης και ακεραιότητας του πράκτορα. Ο έλεγχος πρόσβασης πραγματοποιείται με βάση την ταυτότητα του χρήστη που βρίσκεται πίσω από μια οντότητα, ενώ για λόγους καλύτερης διαχείρισης γίνεται η χρήση ομάδων χρηστών με αντίστοιχα δικαιώματα (user groups). Η αυθεντικοποίηση των οντοτήτων είναι αμοιβαία (mutual authentication). Αυτή η πολιτική αποτελεί ουσιαστικά μια λίστα ελέγχου πρόσβασης (access control list), όπου κάθε αντικείμενο αποτελεί μια καταχώρηση στη λίστα. Όλα τα αντικείμενα διαθέτουν το δικό τους σύνολο δικαιωμάτων πρόσβασης στα κύρια υποσυστήματα της πλατφόρμας εκτέλεσης Grasshopper. Κάθε φορά που ζητείται πρόσβαση σε ένα πόρο, η πλατφόρμα ελέγχει εάν η οντότητα που το διεκδικεί αποτελεί κάποιο έμπιστο υποσύστημα (πχ ο πυρήνας του συστήματος - Grasshopper core) ή ένας πράκτορας. Δίδεται πρόσβαση στα υποσυστήματα της πλατφόρμας, καθώς το μοντέλο εμπιστοσύνης του Grasshopper υποθέτει ότι είναι έμπιστα. Στη περίπτωση που η οντότητα που κάνει την αίτηση είναι πράκτορας, το σύστημα εξάγει το σύνολο των δικαιωμάτων του, καθώς και τα δικαιώματα που αποδίδονται σε κάποιο γκρουπ στο οποίο ανήκει. Εάν η πρόσβαση στον πόρο συστήματος που ζητείται περιλαμβάνεται στα δικαιώματα αυτά, δίδεται πρόσβαση στον πράκτορα. Σε διαφορετική περίπτωση εμφανίζεται μήνυμα λάθους. Η διαχείριση πόρων επιτυγχάνεται με τους μηχανισμούς που παρέχει η Java, οι οποίοι επιτρέπουν τον έλεγχο των περισσότερων πόρων του συστήματος.

Η εξωτερική ασφάλεια περιλαμβάνει αλληλεπιδράσεις υποσυστημάτων της πλατφόρμας με οντότητες εκτός πλατφόρμας. Βασίζεται σε τυποποιημένες τεχνικές ασφάλειας επικοινωνιών όπως το Secure Sockets Layer (SSL) και τα πιστοποιητικά

X.509 [22]. Το SSL παρέχει υπηρεσίες εμπιστευτικότητας, αυθεντικοποίησης (με ανταλλαγή πιστοποιητικών) και ακεραιότητας δεδομένων. Σε γενικές γραμμές το επίπεδο ασφάλειας σε μια πλατφόρμα (εσωτερικά και εξωτερικά) η οποία ανήκει σε μια επικράτεια ρυθμίζεται κεντρικοποιημένα από το Region Registry. Όσον αφορά στη δυνατότητα μετανάστευσης, το Grasshopper παρέχει δυνατότητα ισχυρής μετανάστευσης.

Ανάλυση με Βάση Σενάρια Απειλών

Στο Grasshopper οι πράκτορες κληρονομούν τα δικαιώματα πρόσβασης των ιδιοκτητών τους. Έτσι, αν ένας χρήστης είναι έμπιστος τότε και οι πράκτορές του θεωρούνται έμπιστοι. [20], [21], [19]. Στο πρώτο σενάριο, όπου ένας έμπιστος πράκτορας συμπεριφέρεται κακόβουλα, το Grasshopper στηρίζεται αποκλειστικά στους μηχανισμούς ασφάλειας της JVM. Παρόλο που αυτοί μπορούν να προστατεύσουν σε κάποιο βαθμό τους άλλους πράκτορες που εκτελούνται στην ίδια πλατφόρμα, η ίδια η πλατφόρμα παραμένει εκτεθειμένη. Ο κακόβουλος πράκτορας, έχοντας ήδη αυθεντικοποιηθεί, έχει αποκτήσει πρόσβαση σε πόρους του συστήματος. Ανάλογα με τον προγραμματισμό του, ο πράκτορας μπορεί να προσπαθήσει να παραβιάσει την ακεραιότητα της πλατφόρμας, να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα ή να πραγματοποιήσει επίθεση άρνησης υπηρεσιών (Denial of Service)

Αντίθετα, η JVM δεν είναι σχεδιασμένη για να προστατεύει ένα πράκτορα στο σενάριο που αυτός εκτελείται σε κακόβουλη πλατφόρμα. Σε αυτή την περίπτωση, η ακεραιότητα του πράκτορα και τα δεδομένα που φέρει μπορεί εύκολα να εκτεθούν ή και να αλλοιωθούν, καθώς το μοντέλο ασφάλειας του Grasshoppers δεν λαμβάνει υπόψη του αυτό τον τύπο απειλής [20], [21].

Το Grasshopper ορίζει μια παγκόσμια οντότητα, το Region, μέσα στην οποία οι πράκτορες κινούνται και λειτουργούν και όπου το επίπεδο ασφάλειας ρυθμίζεται κεντρικά [21], [22]. Παρόλο που το Grasshopper Region θεωρείται έμπιστο από τις οντότητες εντός των ορίων του, δεν μπορεί να θεωρηθεί ως ένα ανοιχτό περιβάλλον. Αυτό είναι προφανές, καθώς πρακτικά δεν υποστηρίζεται λειτουργία

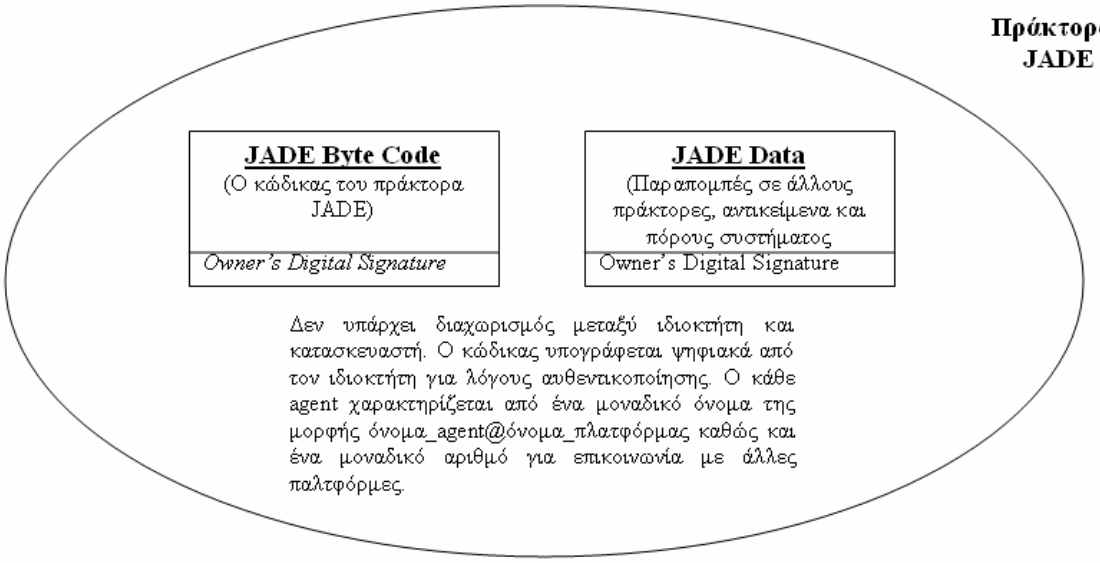
μεταξύ διαφορετικών Region, κάτι που καθιστά το μοντέλο ασφάλειας και εμπιστοσύνης του Grasshopper ακατάλληλο για λειτουργία σε ανοιχτά περιβάλλοντα.

Πρέπει να σημειώσουμε ότι έχουν πραγματοποιηθεί επιτυχώς επιθέσεις σε συστήματα Grasshopper [20]. Πιο συγκεκριμένα έχουν γίνει επιθέσεις έμπιστου κώδικα (trusted code base attacks), επιθέσεις στο γραφικό περιβάλλον του χρήστη (graphic user interface attacks), επιθέσεις σε ιδιότητες του συστήματος (system properties attacks) και επιθέσεις πολιτικών συστήματος (policy system attacks), οι οποίες χρησιμοποιούν έμπιστες κλάσεις της Java (trusted Java classes) και ατελείς ή μη ασφαλείς μεθόδους (incomplete or unsecured methods).

3.3.2 JADE

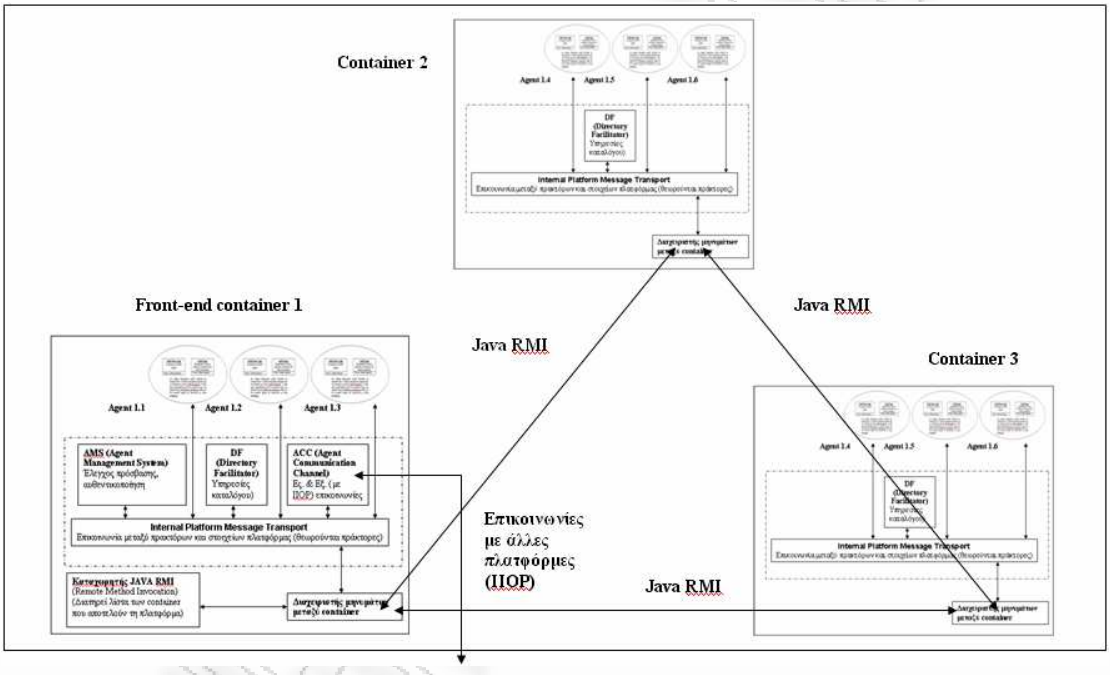
Το Java Agent DEvelopment framework (JADE) αποτελεί μια πλατφόρμα λογισμικού που άρχισε να διανέμεται από την TILab (πλέον Jade Software Corporation Limited), και αποσκοπεί στην απλοποίηση της ανάπτυξης αλληλοσυνεργαζόμενων συστημάτων κινητών πρακτόρων συμβατών με το πρότυπο FIPA. Πέρα από τη συμμόρφωση στο πρότυπο σκοπεύει στην παροχή εκτεταμένων υπηρεσιών [23]. Οι μηχανισμοί ασφαλείας του JADE παρέχονται μέσα από ένα πρόσθετο (add-on) που ονομάζεται JADE-S.

Ο πράκτορας JADE κατά τη δημιουργία του αποτελείται από τον κώδικα και τα δεδομένα του, με την ψηφιακή υπογραφή του ιδιοκτήτη, ενώ δεν γίνεται διαχωρισμός μεταξύ ιδιοκτήτη και προγραμματιστή – δημιουργού (Εικόνα 7). Και εδώ ο σχεδιασμός είναι απλούστατος και βασίζεται στους μηχανισμούς της Java. Οι βασικές υπηρεσίες της πλατφόρμας θεωρούνται ως στατικοί πράκτορες που εκτελούνται στην πλατφόρμα και παρέχουν τις υπηρεσίες της πλατφόρμας στους υπόλοιπους πράκτορες που μεταναστεύουν εκεί. Το JADE είναι συμβατό με τα πρότυπα της FIPA και της OMG.

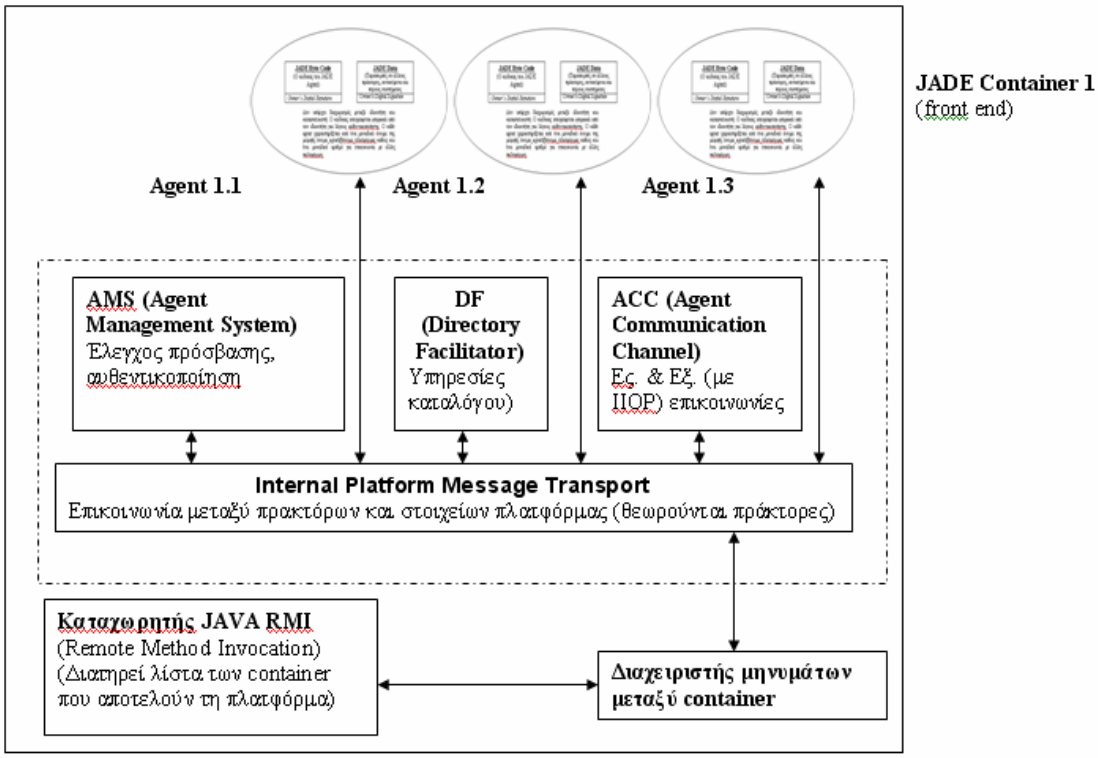


Εικόνα 7 - Διάγραμμα επιπέδου 4: Ένας πράκτορας JADE.

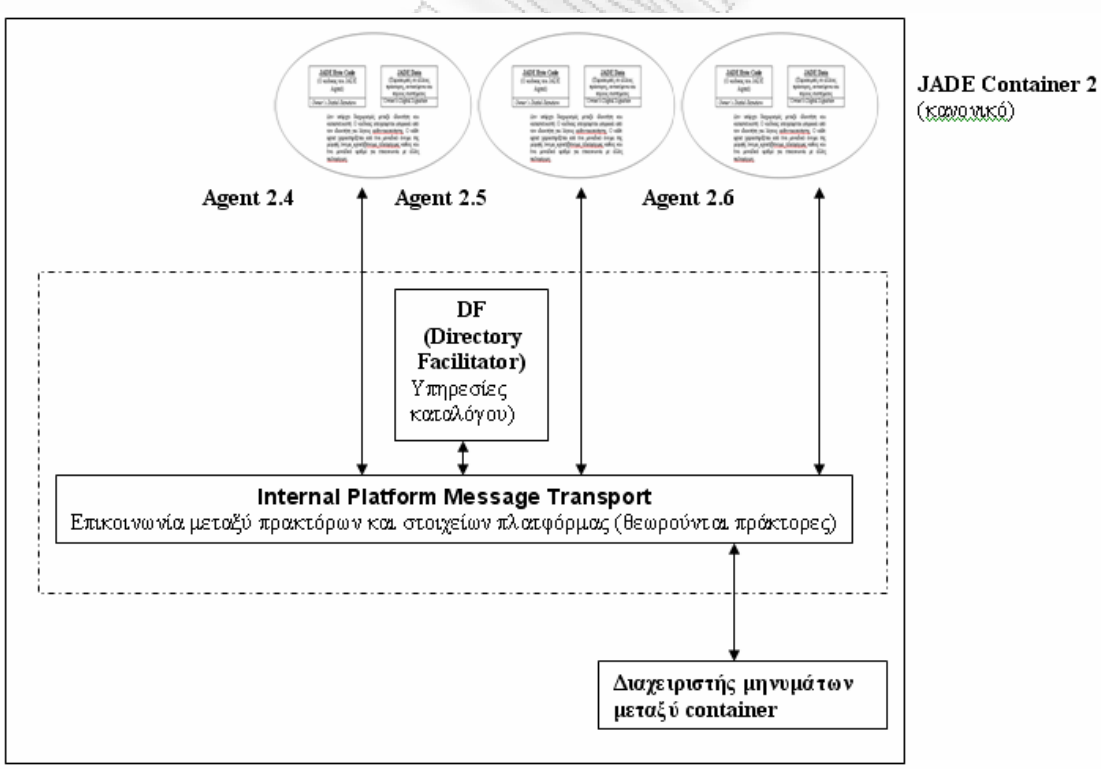
Το μηχάνημα εκτέλεσης JADE ονομάζεται JADE Container (Εικόνα 8). Δεν υποστηρίζεται ομαδοποίηση πρακτόρων με κοινή αντιμετώπιση. Υπάρχουν 2 είδη Container, τα front-end (Εικόνα 9), που παρέχουν κανονικά όλες τις υπηρεσίες, και τα απλά, με μειωμένες δυνατότητες όπου απλά επιτρέπουν να εκτελούνται πράκτορες (Εικόνα 10). Τα front-end containers τρέχουν JVM και παρέχουν: έλεγχο πρόσβασης, αυθεντικοποίηση, υπηρεσίες καταλόγου, εσωτερικές και εξωτερικές επικοινωνίες με χρήση του πρωτοκόλλου IIOP της OMG, επικοινωνία μεταξύ πρακτόρων και στοιχείων πλατφόρμας και τον καταχωρητή των Container (Εικόνα 9). Όλα τα μέρη του Container θεωρούνται στατικοί πράκτορες.



Εικόνα 8 – Διάγραμμα επιπέδου 1: Μια πλατφόρμα εκτέλεσης JADE, η οποία είναι κατανεμημένη καθώς έχει 2 ήδη container.

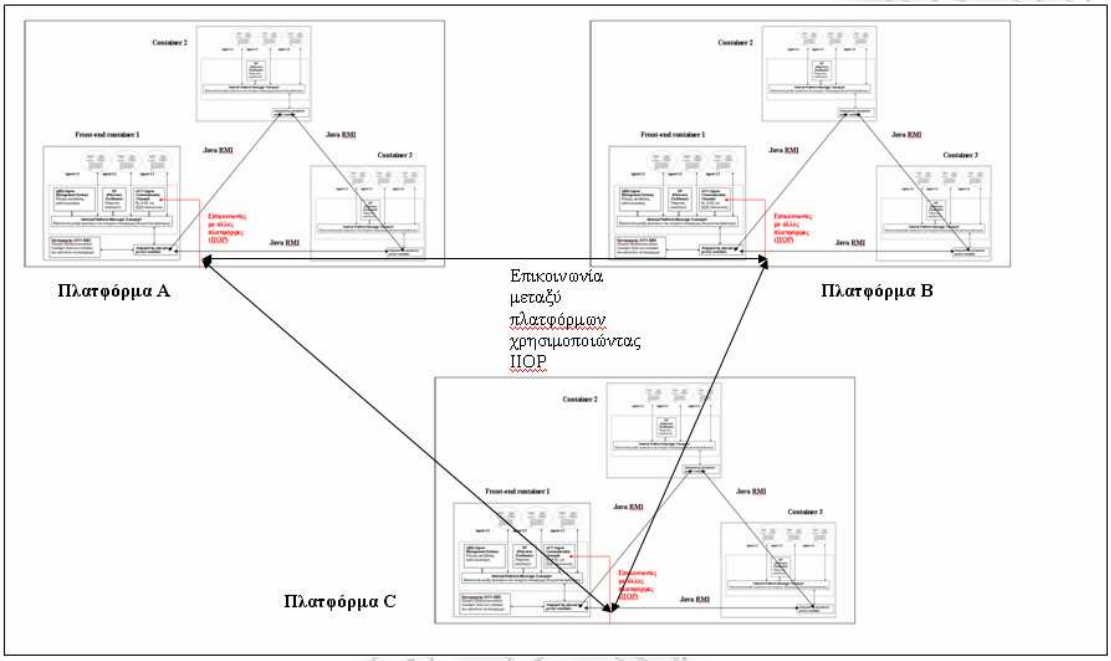


Εικόνα 9 – Διάγραμμα επιπέδου 2: Το front-end container στο οποίο βασίζεται η πλατφόρμα



Εικόνα 10 – Διάγραμμα επιπέδου 2 (συνέχεια): Ένα επιμέρους container μιας πλατφόρμας

Στο JADE δεν ορίζεται ανώτερη οντότητα από τη πλατφόρμα. Απλά υπάρχουν συνεργαζόμενες πλατφόρμες σε περιβάλλον δικτύου. Δεν υπάρχει κεντρικοποιημένη διαχείριση, είναι όμως δυνατή η επικοινωνία μεταξύ διαφορετικών servers, οπότε και η επικοινωνία αυτή απεικονίζεται καταχρηστικά ως διάγραμμα ανώτερου επιπέδου (Εικόνα 11).



Εικόνα 11 – Διάγραμμα Πλαίσιο: Πλατφόρμες εκτέλεσης JADE που αλληλεπιδρούν μεταξύ τους.

Ανάλυση με Βάση τα Κριτήρια Σύγκρισης

Στο JADE η ακεραιότητα του πράκτορα εξασφαλίζεται από την ψηφιακή υπογραφή του ιδιοκτήτη, που χρησιμοποιείται επιπλέον και για παροχή υπηρεσιών αυθεντικοποίησης. Ένας αυθεντικοποιημένος χρήστης θεωρείται έμπιστος, όπως και οι ενέργειες και τα αντικείμενα που παράγει (πράκτορες) [19], [21], [24], [30]. Η πλατφόρμα προστατεύεται και εδώ από το μηχανισμό Java Sandbox και θεωρείται ως έμπιστη από τους πράκτορες. Ο μηχανισμός αυθεντικοποίησης του JADE βασίζεται στην υπηρεσία Java Authentication and Authorization Service (JAAS), που επιβάλλει έλεγχο πρόσβασης σε επίπεδο χρήστη. Παρέχονται πολλά υποσυστήματα εισόδου στο σύστημα είτε με βάση το λειτουργικό σύστημα που χρησιμοποιείται (UNIX, Windows) ή ανεξάρτητα από αυτό (όπως ο Kerberos και simple authentication module) [25].

Το JADE χρησιμοποιεί το πρότυπο επικοινωνιών που προβλέπεται από το πρότυπο της FIPA, την Agent Communication Language (ACL) [42]. Ένα τυπικό σύστημα JADE είναι μια πλατφόρμα με πολλούς αυθεντικοποιημένους χρήστες στους οποίους μπορεί να ανήκουν διάφορα υποσυστήματα. Με βάση τα δικαιώματα που αποδίδονται στον κάθε χρήστη, κάποιες ενέργειες γίνονται επιτρεπτές και άλλες όχι. Οι υπηρεσίες της πλατφόρμας και οι πόροι του συστήματος (π.χ υπηρεσίες καταλόγου, δικτυακοί πόροι, πρόσβαση σε αρχεία) μπορεί να αποδοθούν επιλεκτικά. Ο έλεγχος πόρων γίνεται από την JVM. Η πολιτική απόδοσης δικαιωμάτων στο JADE είναι αρκετά ευέλικτη ώστε να μπορεί να διαχειριστεί ακόμη και κατανεμημένα συστήματα πρακτόρων [24].

Τα μηνύματα ACL προστατεύονται, μέσω του προτύπου SSL, ανεξάρτητα από το αν οι πράκτορες που επικοινωνούν τρέχουν στην ίδια ή σε διαφορετική πλατφόρμα. Πιο συγκεκριμένα, μπορεί να κρυπτογραφηθούν και να φέρουν υπογραφές, προκειμένου να διασφαλιστεί η ακεραιότητα, το απόρρητο της επικοινωνίας και η αυθεντικοποίηση του αποστολέα [24]. Σε υψηλότερο επίπεδο ο χρήστης μπορεί να επιλέξει οι πράκτορές του να χρησιμοποιούν τεχνικές ασφάλειας, χωρίς όμως να χρειάζεται να ασχοληθεί με τις τεχνικές λεπτομέρειες των παραμέτρων ασφαλείας.

Το JADE υποστηρίζει μετανάστευση του κώδικα του πράκτορα καθώς και της κατάστασης εκτέλεσής του (ισχυρή μετανάστευση), επιτρέποντάς του να συνεχίσει την εκτέλεσή του σε άλλη πλατφόρμα από το σημείο που είχε σταματήσει. Όπως είδαμε προηγουμένως, στο JADE, τα διάφορα υποσυστήματα της πλατφόρμας είναι δυνατόν να κατανεμηθούν σε πολλούς host, τα containers. Εν τούτοις, όμως δεν υπάρχει καθορισμένη παγκόσμια οντότητα που να επιτρέπει κεντρικοποιημένη διαχείριση των λειτουργιών ασφάλειας. Το κύριο container (Front–End – Εικόνα 9) της πλατφόρμας είναι υπεύθυνο για όλες τις λειτουργίες ασφάλειας.

Ανάλυση με Βάση Σενάρια Απειλών

Η χρήση της JVM βοηθάει στην προστασία της πλατφόρμας και των πόρων της από κακόβουλους πράκτορες, και σε συναλλαγές μεταξύ πρακτόρων. Καθώς οι πράκτορες JADE κληρονομούν τα δικαιώματα του ιδιοκτήτη τους, στη περίπτωση ενός έμπιστου χρήστη, οι πράκτορές του θεωρούνται έμπιστοι [19], [21]. Στο σενάριο του έμπιστου πράκτορα που συμπεριφέρεται κακόβουλα, το JADE στηρίζεται μονάχα στους μηχανισμούς της JVM. Όπως είδαμε, αυτό μπορεί να απομονώσει έως ένα σημείο άλλους πράκτορες που τρέχουν στην ίδια πλατφόρμα, αλλά η πλατφόρμα καθαυτή παραμένει εκτεθειμένη. Ο κακόβουλος πράκτορας, έχοντας περάσει το στάδιο της αυθεντικοποίησης έχει αποκτήσει πρόσβαση σε πόρους συστήματος. Σε αυτό το στάδιο, ο τύπος της επίθεσης που θα πραγματοποιήσει και η έκταση της ζημίας που θα προκαλέσει εξαρτάται βασικά από το τι έχει προγραμματιστεί ο πράκτορας να κάνει

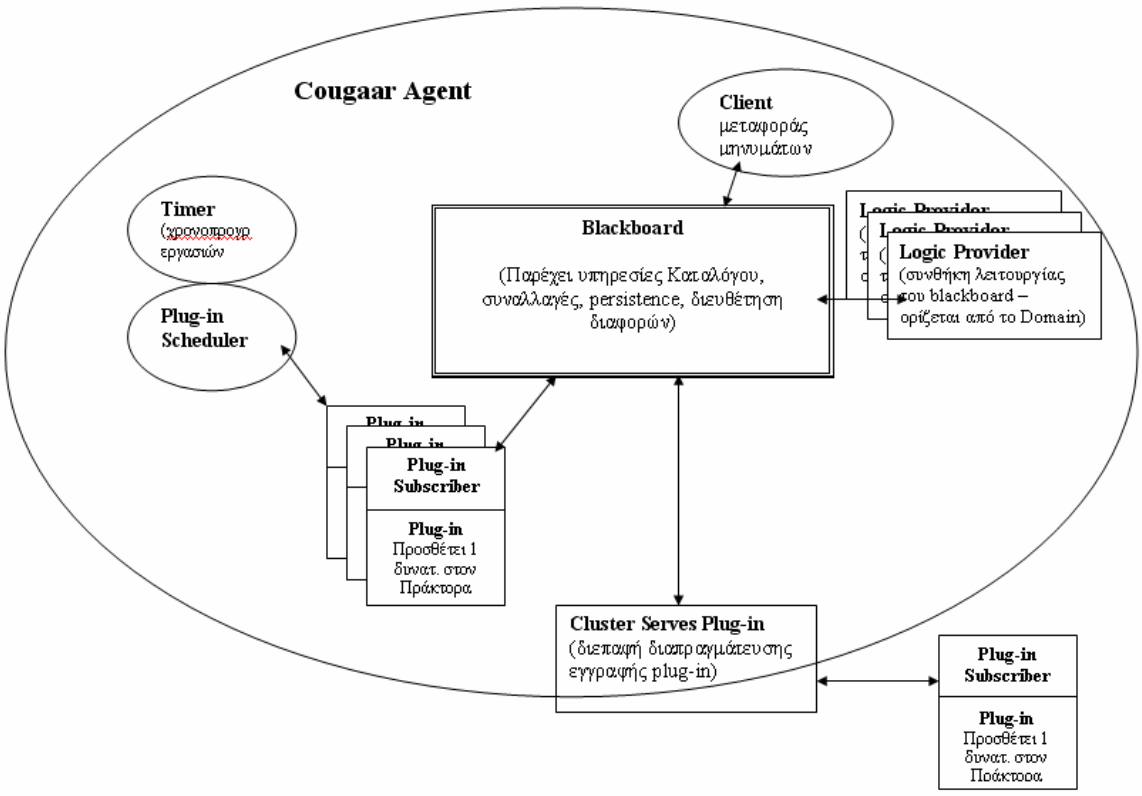
Και στη περίπτωση του JADE, η JVM δεν είναι σχεδιασμένη να προστατεύσει ένα πράκτορα από την κακόβουλη πλατφόρμα στην οποία εκτελείται, καθώς το Java Sandbox δεν είναι σχεδιασμένο για αυτή τη χρήση. Έτσι μπορούμε α πούμε ότι το μοντέλο ασφάλειας και εμπιστοσύνης του JADE δεν λαμβάνει υπόψη του αυτό τον τύπο απειλής [21][30]

Είδαμε παραπάνω, στην ανάλυση των επιπέδων του JADE, ότι δεν ορίζονται οντότητες υψηλότερου επιπέδου από την πλατφόρμα [23], [30]. Παρόλ’ αυτά όμως, τα διάφορα υποσυστήματα της πλατφόρμας είναι κατανεμημένα σε διάφορα container σε ένα δίκτυο και μεταξύ αυτών το Front–End container είναι υπεύθυνο για όλες τις λειτουργίες ασφάλειας. Αυτή η προσέγγιση δημιουργεί ένα έμπιστο περιβάλλον, αλλά ταυτόχρονα υποδηλώνει ξεκάθαρα ότι απαιτείται κάποιου είδους κοινή διαχείριση όλων των host. Δεδομένης αυτής της απαίτησης το μοντέλο εμπιστοσύνης του JADE δεν κρίνεται κατάλληλο για λειτουργία σε ανοιχτά περιβάλλοντα.

3.3.3 Cougaar

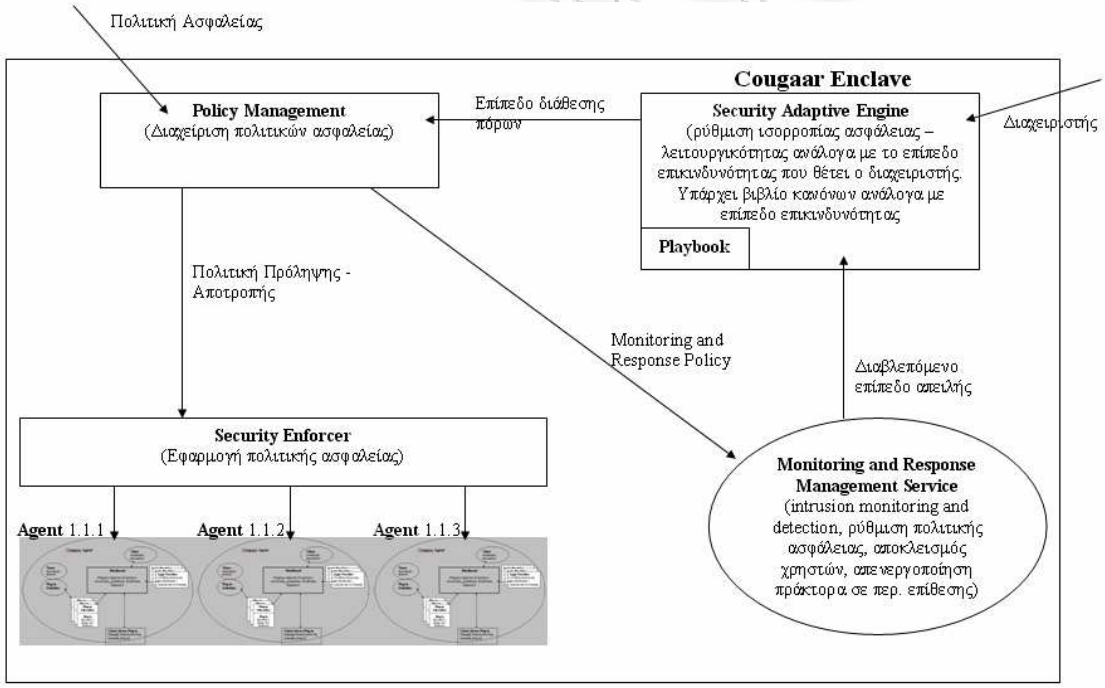
Το Cognitive Agent Architecture (Cougaar) αναπτύχθηκε από την Cougaar Software Inc ως μέρος των προγραμμάτων DARPA ALP [32]και UltraLog [32]. Είναι σχεδιασμένο για να πληροί τις προδιαγραφές ισχυρής ασφάλειας και διαβαθμιστικότητας (scalability) που απαιτούνται σε συνθήκες πολέμου [32]. Βασίζεται και αυτό στην Java.

Ο πράκτορας Cougaar (Εικόνα 12) ακολουθεί σύνθετη σχεδίαση και επιτρέπει την χρήση προσθέτων λογισμικού (plug-ins). Αποτελεί υλοποίηση του ερευνητικού προγράμματος άμυνας DARPA και έχει αναπτυχθεί με κύριο γνώμονα την ασφάλεια. Οι περισσότερες κύριες λειτουργίες είναι ενσωματωμένες μέσα στον πράκτορα για λόγους αυτονομίας και ασφάλειας. Υπηρεσίες καταλόγου, ασφαλούς αποθήκευσης, υπηρεσίες μηνυμάτων, χρονοπρογραμματισμός εργασιών και προσθήκη πρόσθετων λογισμικού περιλαμβάνονται εντός του πράκτορα.



Εικόνα 12 – Διάγραμμα επιπέδου 3: Ένας πράκτορας της πλατφόρμας Cougaar

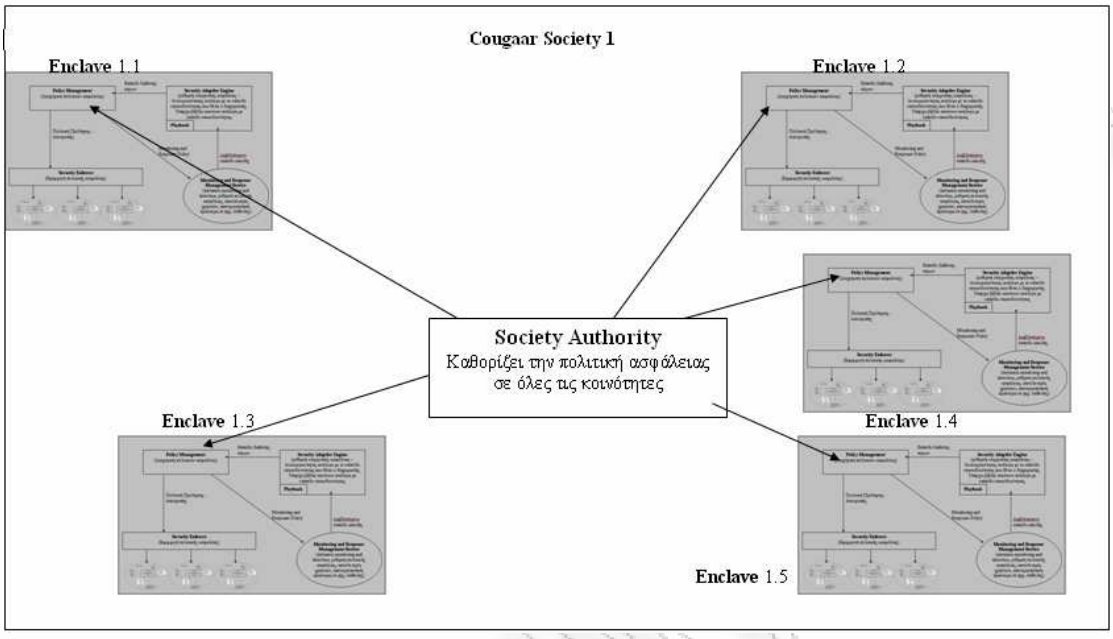
Το μηχάνημα εκτέλεσης Cougaar ονομάζεται Cougaar Node (Εικόνα 13). Υποστηρίζεται ομαδοποίηση πρακτόρων με βάση τις υπηρεσίες που παρέχουν, η οποία ονομάζεται Cougaar Enclave (Κοινότητα). Η ομαδοποίηση αυτή μπορεί να επεκτείνεται και σε άλλες πλατφόρμες εκτέλεσης. Διαθέτει προσαρμοστικό μηχανισμό ασφάλειας που ρυθμίζει την ισορροπία ασφάλειας – λειτουργικότητας ανάλογα με το επίπεδο επικινδυνότητας που θέτει ο διαχειριστής. Υπάρχει βιβλίο κανόνων ανάλογα με επίπεδο επικινδυνότητας. Παρέχεται μηχανισμός παρακολούθησης και εντοπισμού εισβολών (Intrusion Monitoring and Detection) που ονομάζεται μηχανισμός Παρακολούθησης και Απόκρισης (Monitor and Response), ρύθμιση πολιτικής ασφάλειας, αποκλεισμός χρηστών, απενεργοποίηση πράκτορα σε περίπτωση επίθεσης, και Πολιτική Πρόληψης – Αποτροπής (Monitoring and Response Policy).



Εικόνα 13 – Διάγραμμα επιπέδου 2 και 1 (ταυτίζονται): Μια κοινότητα Cougaar και ο προσαρμοστικός μηχανισμός ασφάλειας

Στο Cougaar η ανώτερη οντότητα είναι η Cougaar Society (Κοινωνία - Εικόνα 14). Το Cougaar διαθέτει ισχυρή κεντρικοποιημένη διαχείριση, η οποία στο ανώτερο επίπεδο εποπτεύει όλες τις λειτουργίες μέσω της Society Authority. Καθορίζεται η πολιτική ασφάλειας σε όλες τις Κοινότητες και όλα γίνονται μέσω

αυτής. Συνολικά, διαθέτει τυπική κεντρικοποιημένη οργάνωση αμυντικού συστήματος.



Εικόνα 14 – Διάγραμμα Πλαίσιο: Μια Κοινωνία Cougaar (DARPA)

Ανάλυση με Βάση τα Κριτήρια Σύγκρισης

Το επίπεδο ασφάλειας του Cougaar είναι προσαρμοστικό. Ανάλογα με τον τύπο της εφαρμογής που υλοποιείται πάνω στο Cougaar, οι μηχανισμοί ασφάλειας μπορεί να είναι ενεργοποιημένοι ή όχι. Οι πράκτορες μπορεί να είναι υπογεγραμμένοι ψηφιακά από το χρήστη διασφαλίζοντας την ακεραιότητά τους. Υποστηρίζεται αμοιβαία αυθεντικοποίηση, η οποία υλοποιείται είτε με την ανταλλαγή προκαθορισμένων συνθηματικών είτε με τη χρήση ψηφιακών πιστοποιητικών. Ο έλεγχος πρόσβασης γίνεται με βάση την ταυτότητα της οντότητας (χρήστης, πράκτορας ή πρόσθετο λογισμικό) [31] και τον πόρο στον οποίο ζητείται πρόσβαση. Το Cougaar υποστηρίζει χρήση ομαδοποιήσεων οντοτήτων και πόρων για πιο αποτελεσματική απόδοση πόρων. Η πολιτική εξουσιοδότησης της κάθε εφαρμογής παράγεται από τον δημιουργό της και επιβάλλεται από τον Policy Domain Manager. Η πλατφόρμα εκτέλεσης Cougaar προστατεύεται από το Java Sandbox, και, επιπρόσθετα, από μηχανισμό ανίχνευσης εισβολών (Intrusion Detection mechanism) [31].

Το Cougaar υποστηρίζει κρυπτογραφία και ψηφιακές υπογραφές για όλες τις επικοινωνίες, εσωτερικές και εξωτερικές. Ανοιχτά πρότυπα κρυπτογραφίας μπορούν να χρησιμοποιηθούν, καθώς και κρυπτογραφία δημοσίου κλειδιού (public key infrastructure - PKI) και Αρχές Πιστοποιητικών (Certificate Authorities - CA). Εάν απαιτείται, επιπρόσθετοι κρυπτογραφικοί μηχανισμοί από αυτούς που παρέχονται μπορεί να προστεθούν από τις εφαρμογές [31], [32]. Το Cougaar παρέχει πλήρεις υπηρεσίες μετανάστευσης, αφού υποστηρίζει ισχυρή μετανάστευση. Το μοντέλο εμπιστοσύνης καθορίζεται από τις ανάγκες αυθεντικοποίησης που ορίζει η κάθε εφαρμογή. Γενικά, ένας αυθεντικοποιημένος πράκτορας θεωρείται ότι είναι έμπιστος, όπως και η πλατφόρμα εκτέλεσης θεωρείται εξ ορισμού έμπιστη από τους πράκτορες. Το Cougaar περιλαμβάνει το μηχανισμό Παρακολούθησης και Απόκρισης, ο οποίος συλλέγει και αναλύει δεδομένα από διάφορες οντότητες, με σκοπό να εντοπίσει πιθανές επιθέσεις και ανάλογα ρυθμίζει δυναμικά το επίπεδο ασφάλειας. Καθώς πρόκειται για στρατιωτική εφαρμογή το Cougaar υλοποιεί κεντρικοποιημένη διαχείριση μέσα στον κόσμο που ορίζει (Society) μέσω της Society Authority. Αυτή είναι επιφορτισμένη με τη ρύθμιση της πολιτικής για το κάθε μηχάνημα εκτέλεσης (Node – Εικόνα 13).

Το βασικό χαρακτηριστικό του Cougaar είναι ο μηχανισμός προσαρμοστικής ασφάλειας που διαθέτει (Security Adaptive Engine). Ο συγκεκριμένος μηχανισμός εντοπίζει τους σημαντικούς πόρους (assets) για την κάθε εφαρμογή και, στη συνέχεια, δημιουργεί σενάρια πιθανών επιθέσεων στο σύστημα και το σκοπό τους, εντοπίζει αδυναμίες των εφαρμογών, παράγει μια λίστα με κατάλληλα αντίμετρα με το κόστος του καθενός και τέλος επιβάλλει μια ομάδα αντίμετρων που εξισορροπούν το συνολικό επίπεδο ασφάλειας με το υπολογιστικό κόστος που αυτά συνεπάγονται. Η Security Adaptive Engine κρίνεται απαραίτητη, καθώς η επιβολή του μέγιστου επιπέδου ασφάλειας σε όλες ανεξαιρέτως τις εφαρμογές μπορεί να επιφέρει σημαντικό αντίκτυπο στις επιδόσεις της πλατφόρμας εκτέλεσης [32], [33].

Ανάλυση με Βάση Σενάρια Απειλών

Αναφέραμε τη διαφοροποίηση του Cougaar από τα προηγούμενα συστήματα κινητών πρακτόρων όσον αφορά στη διαμόρφωση του μοντέλου ασφάλειας και εμπιστοσύνης που υιοθετεί, με τη χρήση της προσαρμοστικής Security Adaptive Engine, το ρυθμιζόμενο μοντέλο εμπιστοσύνης και το μηχανισμό ανίχνευσης εισβολών [35].

Αποτέλεσμα αυτής της προσέγγισης είναι το γεγονός ότι η πλατφόρμα εκτέλεσης του Cougaar προστατεύεται εκτός από το μηχανισμό Java Sandbox και από το μηχανισμό ανίχνευσης εισβολών που διαθέτει. Ανάλογα με την πολιτική ασφαλείας και τη συμπεριφορά του πράκτορα λαμβάνονται τα αντίστοιχα μέτρα για την προστασία της ακεραιότητας της πλατφόρμας [32]

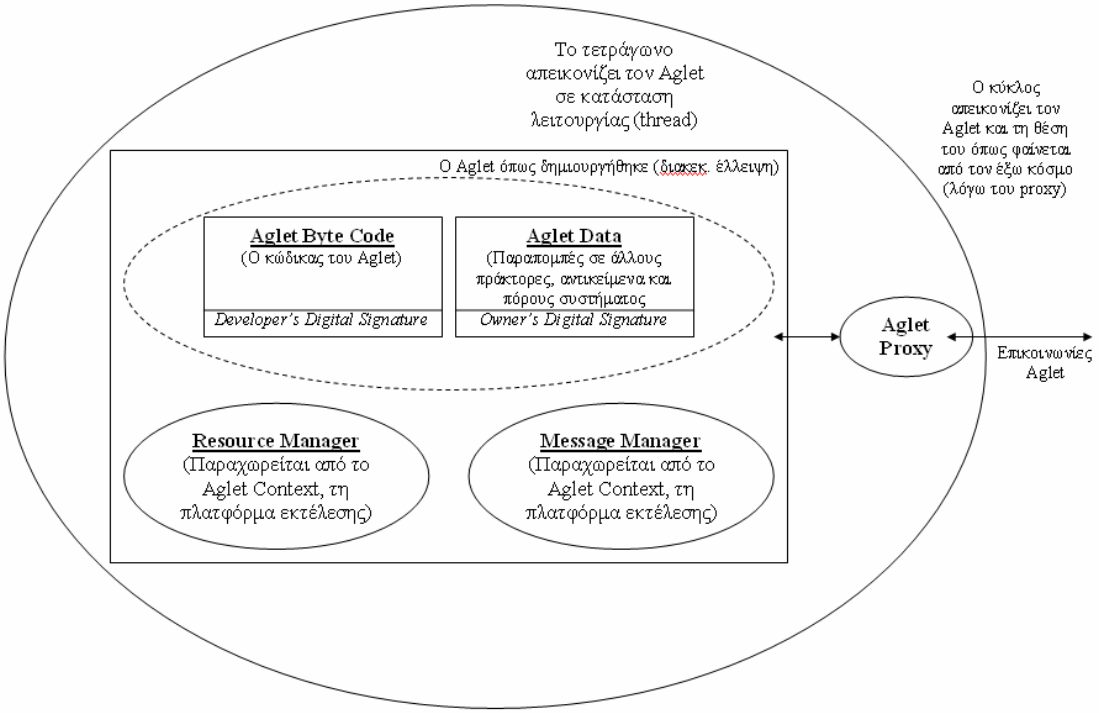
Σχετικά με το σενάριο της απειλής της κακόβουλης πλατφόρμας το Cougaar δεν λαμβάνει ιδιαίτερα μέτρα. Τα περισσότερα μέτρα ασφάλειας που υλοποιεί απευθύνονται σε απειλές που προέρχονται από πράκτορες ή εξωτερικές απειλές. Εντούτοις, χαρακτηριστικά όπως η αμοιβαία αυθεντικοποίηση σε συνδυασμό με το γεγονός ότι το Cougaar προορίζεται για λειτουργία στο κλειστό δικτυακό περιβάλλον των στρατιωτικών εφαρμογών, μειώνουν σημαντικά την πιθανότητα να εκδηλωθεί η συγκεκριμένη απειλή.

Είδαμε ότι το Cougaar υλοποιεί αυστηρά κεντρικοποιημένη διαχείριση στον κόσμο που ορίζει (Society) μέσω της Society Authority, το οποίο συνεπάγεται από τη στρατιωτική φύση της εφαρμογής. Ως αποτέλεσμα αυτής της προσέγγισης το συνολικό επίπεδο ασφάλειας αυξάνεται, καθώς όλες οι λειτουργίες πραγματοποιούνται σε ένα ελεγχόμενο περιβάλλον. Έτσι όμως, όπως και στην περίπτωση του Grasshopper, το μοντέλο εμπιστοσύνης του Cougaar κρίνεται ακατάλληλο για εφαρμογές σε ανοιχτά περιβάλλοντα.

3.3.4 Aglets

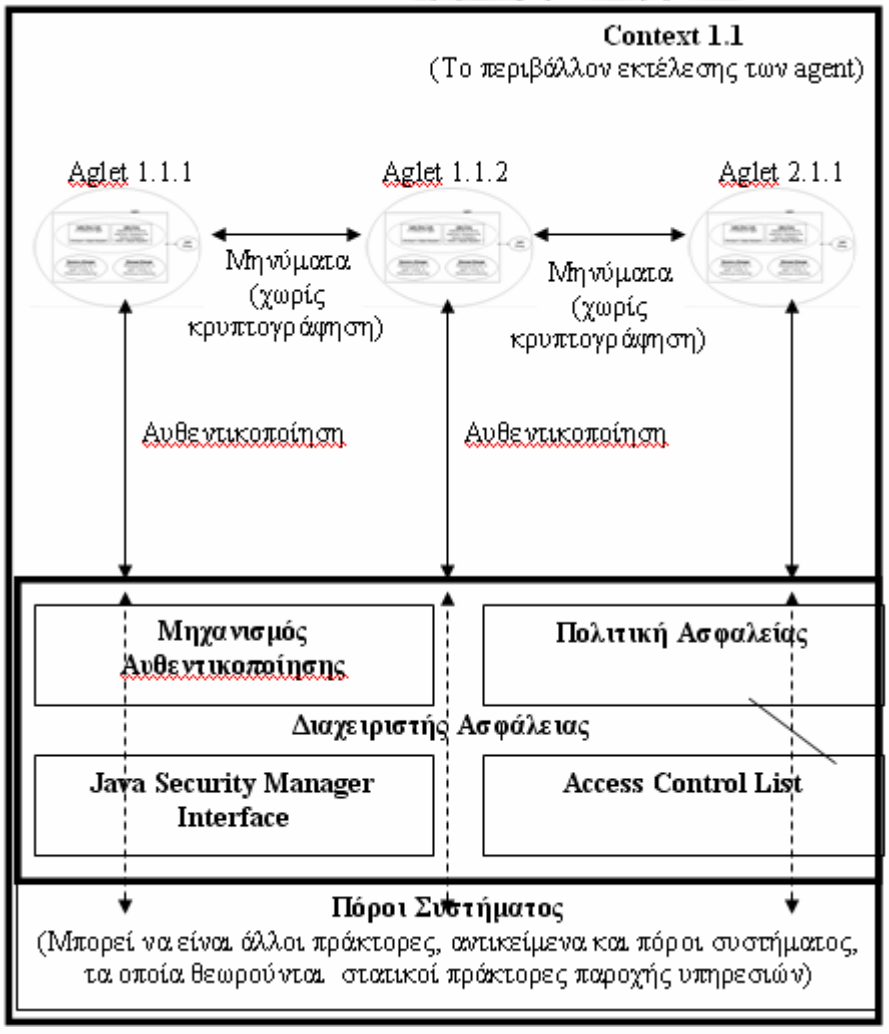
Το IBM Aglets Workbench αναπτύχθηκε αρχικά από το Tokyo Research Laboratory της εταιρίας IBM [43], και, πλέον, αποτελεί έργο ανοιχτού κώδικα (open source project). Αποτελεί μια πλατφόρμα κινητών πρακτόρων γενικού σκοπού και είναι σχεδιασμένο να παρέχει ένα εύκολο προγραμματιστικό περιβάλλον, αξιόπιστες επικοινωνίες και επαρκή χαρακτηριστικά ασφάλειας. Προορίζεται για χρήση στο Διαδίκτυο και βασίζεται στην Java [43], [44].

Ο πράκτορας Aglet κατά τη δημιουργία του αποτελείται από τον κώδικα, με τη ψηφιακή υπογραφή του προγραμματιστή του, και τα δεδομένα του, με τη ψηφιακή υπογραφή του ιδιοκτήτη (Εικόνα 15). Σε κατάσταση λειτουργίας (thread - εσωτερικό ορθογώνιο) διαθέτει ένα Resource Manager και ένα Message Manager που παραχωρούνται από το Aglet Context, την πλατφόρμα εκτέλεσης. Ο πράκτορας πραγματοποιεί όλες του τις επικοινωνίες μέσω ενός διακομιστή μεσολάβησης (proxy) οπότε από τον έξω κόσμο φαίνεται όπως η εξωτερική έλλειψη.



Εικόνα 15 – Διάγραμμα επιπέδου 3: Ένας πράκτορας Aglet.

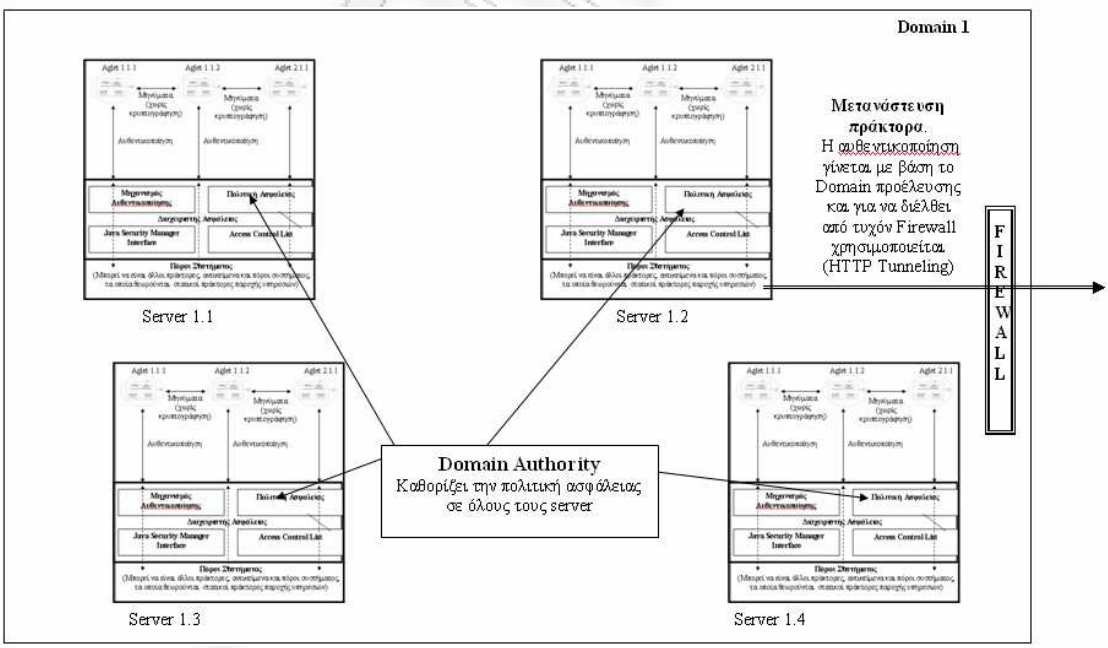
Το μηχάνημα εκτέλεσης των Aglet ονομάζεται Tahiti Server (Εικόνα 16). Ορίζεται μια μοναδική ομάδα μέσα στο server που περιλαμβάνει όλους τους πράκτορες και ονομάζεται Context. Δεν υποστηρίζεται ομαδοποίηση πρακτόρων με κοινή αντιμετώπιση οπότε καιτα διαγράμματα επιπέδου 1 και 2 ταυτίζονται λόγω ταύτισης ορισμού Server και Context. Ο server τρέχει JVM και ο διαχειριστής ασφαλείας που ενσωματώνει παρέχει υπηρεσίες αυθεντικοποίησης και ελέγχου πρόσβασης και εργαλείο διαχείρισης πολιτικής ασφαλείας (Εικόνα 17). Ο διαχειριστής δεν είναι δυνατό να τροποποιηθεί μετά την εγκατάστασή του. Οι εσωτερικές επικοινωνίες των πρακτόρων δεν κρυπτογραφούνται, ενώ μπορούν να τρέξουν πράκτορες από άλλες πλατφόρμες αλλά με περιορισμένα δικαιώματα.



Εικόνα 16 – Διάγραμμα επιπέδου 2: Το Aglet Context σε έναν Tahiti Server.

Εικόνα 17: Ο Διαχειριστής Ασφάλειας της πλατφόρμας Aglet

Στα Aglet ως ανώτερη οντότητα ορίζεται το Aglet Domain (Εικόνα 18). Υπάρχει η κεντρική οντότητα Domain Authority που καθορίζει την πολιτική ασφάλειας σε όλους τους εξυπηρετητές. Υποστηρίζεται λειτουργία μετανάστευσης σε διαφορετικό Domain και προβλέπεται η ύπαρξη Firewall ανεξάρτητου από τη λειτουργία των server για τη προστασία της περιμέτρου. Κατά τη μετανάστευση η αυθεντικοποίηση γίνεται με βάση το Domain προέλευσης και για να διέλθει από το Firewall χρησιμοποιείται HTTP Tunneling.



Εικόνα 18 - Διάγραμμα Πλαίσιο: Ένα Aglet Domain με τον διαχειριστή του.

Ανάλυση με Βάση τα Κριτήρια Σύγκρισης

Στα Aglets γίνεται διάκριση μεταξύ του κατασκευαστή του πράκτορα και του ιδιοκτήτη του [44], αν και στην πράξη δεν αποκλείεται να πρόκειται για την ίδια οντότητα. Η ακεραιότητα του πράκτορα επιτυγχάνεται με την υπογραφή του κώδικα του πράκτορα από τον κατασκευαστή του (τα δεδομένα του δεν είναι δυνατόν να φέρουν υπογραφή αφού συνεχώς αλλάζουν). Επιπλέον, κάθε πράκτορας υλοποιεί ένα διακομιστή μεσολάβησης, ο οποίος απομονώνει τον ίδιο τον πράκτορα από τις άλλες οντότητες στο σύστημα. Τα Aglets επιδιώκουν να διασφαλίσουν την ακεραιότητα του πράκτορα και της πλατφόρμας σε δύο επίπεδα. Κατά πρώτον, γίνεται χρήση ενός εργαλείου εντοπισμού εισβολών που βασίζεται σε αποτίμηση των κινδύνων και των αντίμετρών τους (audit information analysis) για να προστατεύσει τόσο τον πράκτορα όσο και την πλατφόρμα εκτέλεσης [47]. Δεύτερον, γίνεται χρήση των εγγενών μηχανισμών της Java Virtual Machine [46]. Στα Aglets όλα τα υποσυστήματα μέσα στο κόσμο που ορίζεται θεωρούνται έμπιστα και φέρουν ένα κοινό μυστικό κλειδί. Το ίδιο αυτό κλειδί χρησιμοποιείται για τον υπολογισμό του Message Integrity Code (MIC) που παρέχει ακεραιότητα μετάδοσης στις επικοινωνίες [44], [46].

Το κοινό κλειδί χρησιμοποιείται για την αυθεντικοποίηση μεταξύ διακομιστών Aglet οι οποίοι ανταλλάσσουν Message Authentication Codes (MACs). Οι χρήστες αυθεντικοποιούνται στον server με τη χρήση του κλασικού μοντέλου ονόματος χρήστη/συνθηματικού πρόσβασης. Οι αυθεντικοποιημένοι χρήστες και οι πράκτορές τους θεωρούνται ότι είναι έμπιστοι. Ο έλεγχος πρόσβασης βασίζεται στην ταυτότητα του ιδιοκτήτη του πράκτορα και στην Επικράτεια προέλευσής του. Λίστες ελέγχου πρόσβασης χρησιμοποιούνται για τον καθορισμό των δικαιωμάτων του κάθε πράκτορα πάνω στους πόρους της πλατφόρμας [46]. Οι πράκτορες Aglet φέρουν προτιμήσεις για το επίπεδο ασφάλειας, οι οποίες περιλαμβάνουν προτιμήσεις για τα δικαιώματα πρόσβασης. Δεν υλοποιείται κάποιος μηχανισμός καταγραφής και απόδοσης ευθυνών (accounting mechanism) και η διαχείριση πόρων επιτυγχάνεται μέσα από τους μηχανισμούς που παρέχει η Java [20].

Τα Aglets, αν και αρχικά υποστήριζαν μονάχα ασθενή μετανάστευση [44], πλέον υποστηρίζουν δυνατότητα ισχυρής μετανάστευσης χρησιμοποιώντας ένα παράλληλο μηχανισμό μεταφοράς της κατάστασης εκτέλεσης του κώδικα [91]. Η μετανάστευση πραγματοποιείται με τη χρήση της τεχνικής HTTP tunnelling για την παράκαμψη τυχόν firewall μεταξύ των server που λαμβάνει χώρα η μετανάστευση.

Στην Επικράτεια των Aglet (Aglet Domain) η πολιτική ασφάλειας διαμορφώνεται από την κεντρική Domain Authority. Η συγκεκριμένη οντότητα είναι υπεύθυνη για τη δημιουργία και την διανομή του κοινού μυστικού κλειδιού του Domain, καθώς και για τον καθορισμό των δικαιωμάτων πρόσβασης του κάθε χρήστη.

Ανάλυση με Βάση Σενάρια Απειλών

Είδαμε προηγουμένως ότι τα Aglets επιχειρούν να προστατεύσουν την πλατφόρμα, χρησιμοποιώντας εκτός από το Java Sandbox και το μηχανισμό εντοπισμού απειλών [20], [43], [47]. Η χρήση του εργαλείου αυτού μετριάζει την αδυναμία των μηχανισμών ασφαλείας της JVM για την αντιμετώπιση απειλών από κακόβουλους αυθεντικοποιημένους/έμπιστους πράκτορες.

Επιπλέον, είδαμε ότι στα Aglets όλα τα μέρη του συστήματος πρακτόρων μέσα σε ένα Domain θεωρούνται έμπιστα και χρησιμοποιούν ένα κοινό μυστικό κλειδί για λόγους αυθεντικοποίησης και εξασφάλισης επικοινωνιών [20][46]. Φέροντας αυτό το κλειδί, η πλατφόρμα θεωρείται εξ ορισμού έμπιστη από τον πράκτορα, ανεξάρτητα από την πιθανότητα να έχει γίνει κακόβουλη. Ως μέσο αυτοπροστασίας ο κάθε πράκτορας περιλαμβάνει το διακομιστή μεσολάβησης, που απομονώνει τον καθαυτό πράκτορα από τις υπόλοιπες οντότητες σε ένα σύστημα. Αυτός ο μηχανισμός ασφάλειας, αν και χρήσιμος για αλληλεπιδράσεις μεταξύ πρακτόρων, ίσως να μην αποδειχθεί εξίσου αποτελεσματικός στο σενάριο της κακόβουλης πλατφόρμας εκτέλεσης, καθώς ο ίδιος ο διακομιστής μεσολάβησης εκτελείται στην πλατφόρμα.

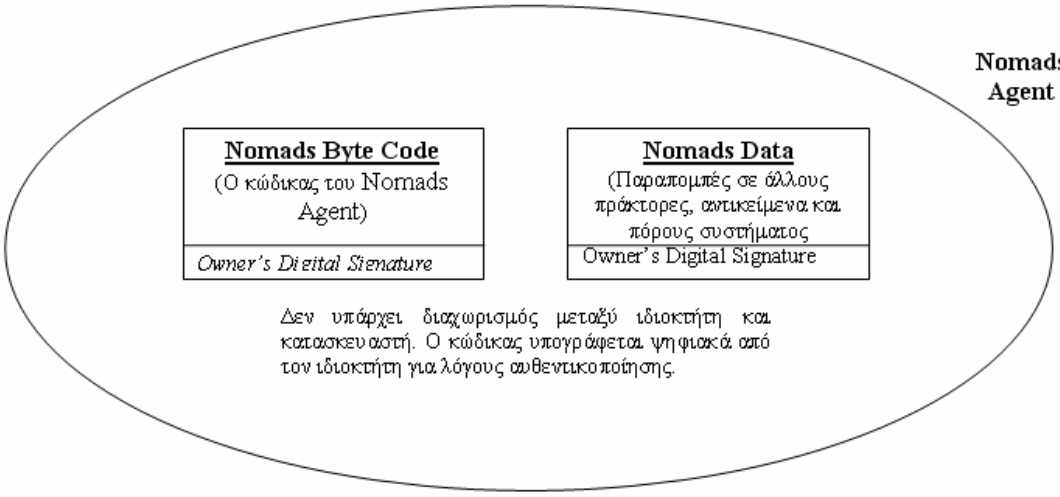
Το σύστημα κινητών πρακτόρων Aglets είναι σχεδιασμένο για χρήση διαμέσου του Διαδικτύου ως μέσο επικοινωνίας, αλλά αυτό δεν πρέπει να συγχέεται

με λειτουργία σε ανοιχτό περιβάλλον. Στην πραγματικότητα οι οντότητες των Aglets είναι σχεδιασμένες για λειτουργία μονάχα μέσα σε ένα αυστηρά καθορισμένο Domain. Συγκεκριμένα, μοιράζονται την ίδια πολιτική ασφάλειας και το κοινό μυστικό κλειδί. Η εφαρμογή αυτής της κοινής διαχείρισης ασφάλειας, και ακόμη περισσότερο η ύπαρξη ενός μονάχα κλειδιού για όλες τις οντότητες υποδηλώνει ότι τα Aglets προορίζονται για χρήση μεταξύ έμπιστων οντοτήτων, με κάποιου είδους κοινό υπόβαθρο και σαφέστατα σε μικρή κλίμακα. Έτσι, η λειτουργία σε ανοιχτό περιβάλλον είναι έξω από το σκοπό του μοντέλου εμπιστοσύνης των Aglets.

3.3.5 Nomads

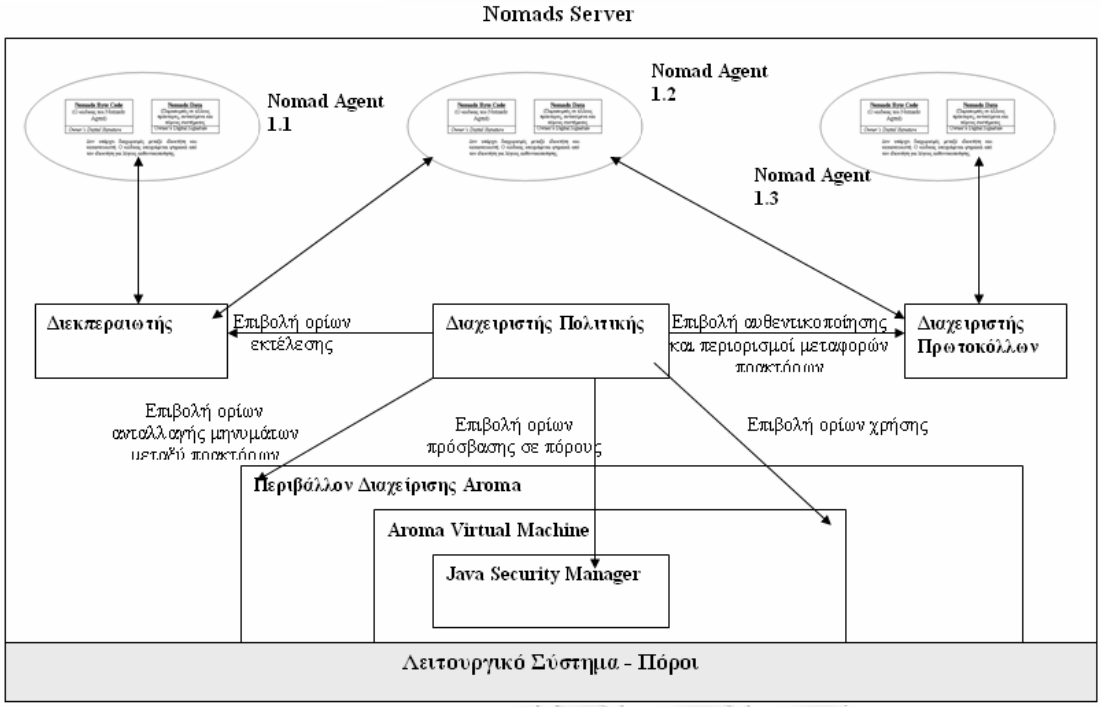
Η πλατφόρμα πρακτόρων Nomads διανέμεται από το Institute for Human and Machine Cognition Research Institute του πανεπιστημίου της Florida και έχει χρηματοδοτηθεί από τα προγράμματα Control of Agent Based Systems της DARPA, το NASA Aviation Extranet και από την National Technology Alliance. Σκοπεύει στην παροχή ισχυρής κινητικότητας με πολλαπλές χρήσεις καθώς και στην παροχή ασφαλούς περιβάλλοντος εκτέλεσης για τους πράκτορες [49], [51].

Ο πράκτορας Nomads κατά τη δημιουργία του αποτελείται από το κώδικα και τα δεδομένα του, με τη ψηφιακή υπογραφή του ιδιοκτήτη, ενώ δεν γίνεται διαχωρισμός με τον προγραμματιστή – δημιουργό (Εικόνα 19). Μπορεί να είναι κινητός ή σταθερός. Ο σχεδιασμός είναι απλούστατος και βασίζεται στους μηχανισμούς της Java. Οι βασικές υπηρεσίες της πλατφόρμας θεωρούνται στατικοί πράκτορες.



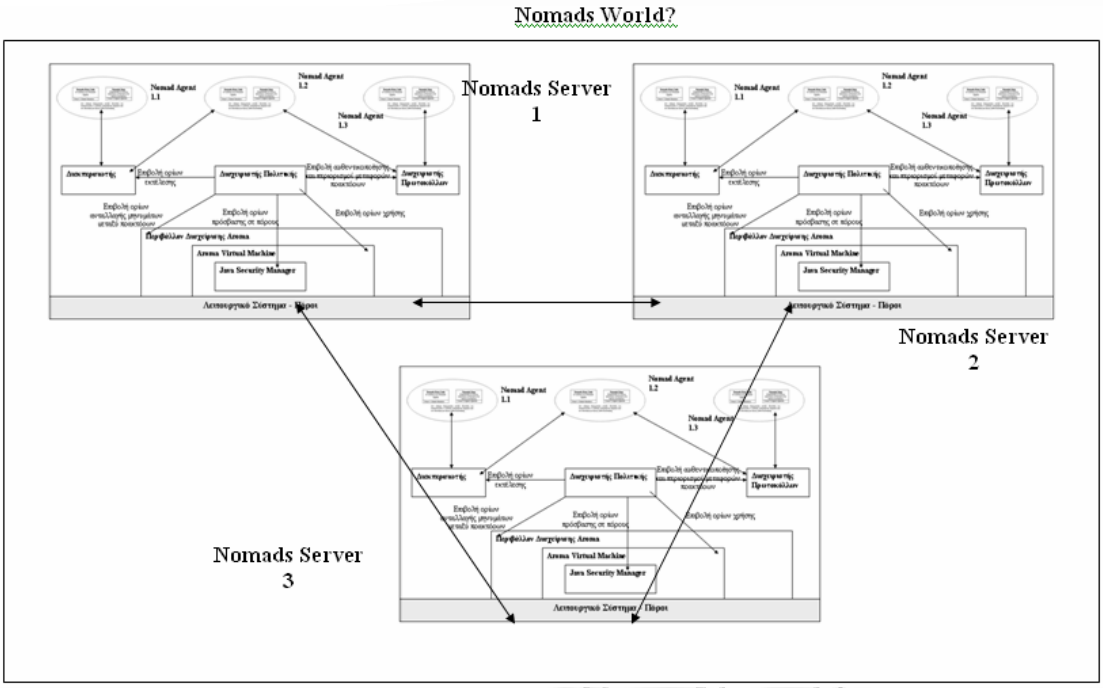
Εικόνα 19 – Διάγραμμα επιπέδου 4: Ένας πράκτορας Nomads.

Το μηχάνημα εκτέλεσης των Nomads ονομάζεται Nomads Server (Εικόνα 20). Δεν υποστηρίζεται ομαδοποίηση πρακτόρων με κοινή αντιμετώπιση εντός του server. Χρησιμοποιεί Java και τρέχει μια τροποποιημένη έκδοση της JVM που ονομάζεται Aroma Virtual Machine. Ολόκληρο περιβάλλον εκτέλεσης που παρέχει ο server ονομάζεται Oasis Execution Environment. Παρέχονται οι μηχανισμοί ασφάλειας της Java ενώ διατίθεται διαχειριστής πολιτικής, που είναι υπεύθυνος για επιβολή αυθεντικοποίησης και περιορισμούς στις μεταφορών πρακτόρων, επιβολή ορίων εκτέλεσης, επιβολή ορίων πρόσβασης σε πόρους και ανταλλαγή μηνυμάτων. Στο διάγραμμα (Εικόνα 20) απεικονίζεται η επιβολή περιορισμών ασφάλειας από το Διαχειριστή πολιτικής ενώ διακρίνεται ότι χρησιμοποιούνται οι μηχανισμοί ασφάλειας της Java.



Εικόνα 20 – Διάγραμμα επιπέδου 2: Ένας Server Nomad.

Στο Nomads δεν ορίζεται ανώτερη οντότητα από το server. Δεν υπάρχει κεντρικοποιημένη διαχείριση, είναι όμως δυνατή η επικοινωνία και η μετανάστευση μεταξύ διαφορετικών server, οπότε και απεικονίζονται καταχρηστικά σαν διάγραμμα ανώτερου επιπέδου (Εικόνα 21).



Εικόνα 21 – Διάγραμμα Πλαίσιο: Επικοινωνία μεταξύ διαφορετικών server σε ένα δίκτυο (δεν ορίζεται ανώτερη οντότητα από τον server).

Ανάλυση με Βάση τα Κριτήρια Σύγκρισης

Η φιλοσοφία που ακολουθεί το Nomads είναι να παρέχει ένα τυπικό σύστημα κινητών πρακτόρων με βάση την Java παρέχοντας όμως δύο σημαντικές βελτιώσεις: ισχυρή κινητικότητα και λεπτομερέστατο έλεγχο πόρων. Για να επιτύχει αυτούς τους στόχους χρησιμοποιεί μια τροποποιημένη έκδοση της JVM την Aroma Virtual Machine (AVM) και το περιβάλλον εκτέλεσης Oasis. Θέματα ασφάλειας όπως ακεραιότητα πράκτορα, πλατφόρμας και επικοινωνιών αναλύονται κάπως συνοπτικά στη σχετική βιβλιογραφία [48], [49], [50], [51]. Η ακεραιότητα της πλατφόρμας επιδιώκεται με τη χρήση της εικονικής μηχανής Oasis, καθώς και με την αφαίρεση των πόρων που έχουν αποδοθεί σε πράκτορες που συμπεριφέρονται κακόβουλα.

Η τεκμηρίωση του Nomads δεν δηλώνει ρητά ποιες κρυπτογραφικές χρησιμοποιεί, αλλά αναφέρει ότι η εξασφάλιση των επικοινωνιών στηρίζεται σε ασφαλή κανάλια και αλγόριθμους αυθεντικοποίησης που παρέχονται από τη Java και το λειτουργικό σύστημα. Ο έλεγχος πρόσβασης βασίζεται στην ταυτότητα του πράκτορα και είναι αλληλένδετος με τη διαδικασία αυθεντικοποίησης [50]. Ο

έλεγχος πρόσβασης, ο έλεγχος πόρων και εκτέλεσης καθώς και ο έλεγχος μεταφορών ορίζονται από το διαχειριστή του συστήματος στον Policy Manager, ανεξάρτητα για κάθε χρήστη ή με βάση ομάδες χρηστών [48], [52]. Αν και δεν ορίζεται κάποια ανώτερη οντότητα από την πλατφόρμα εκτέλεσης, υπονοείται η ύπαρξη ενός κεντρικού διαχειριστή ασφάλειας [50].

Ο μηχανισμός διαχείρισης πόρων είναι δυναμικός και χρησιμοποιείται για την επιβολή περιορισμών πρόσβασης στους πόρους που ένας πράκτορας μπορεί αποκτήσει, αλλά επίσης και στο επίπεδο πρόσβασης σε κάθε πόρο. Πιο συγκεκριμένα, υπάρχει διάκριση μεταξύ ποσοτικών ορίων πρόσβασης και ορίων ρυθμού πρόσβασης. Όρια ρυθμού πρόσβασης ορίζονται στην εγγραφή/ανάγνωση στο δίσκο, στη χρήση του δικτύου, στη χρήση του κεντρικού επεξεργαστή (CPU) και στις εισόδους / εξόδους του συστήματος (I/O). Τα ποσοτικά όρια περιλαμβάνουν τα συνολικά byte ανάγνωσης / εγγραφής στο δίσκο ή στο δίκτυο. Ο τρόπος με τον οποίο παραχωρείται στους κινητούς πράκτορες πρόσβαση στην CPU μπορεί να ρυθμιστεί με βάση πολλαπλά κριτήρια, όπως υψηλού επιπέδου ποσοστικό όριο ή ακόμη και σε χαμηλό επίπεδο ως προς το ποσό του κώδικα που εκτελείται σε συγκεκριμένο χρονικό διάστημα [50]. Η ποσότητα των πόρων που έχει αποδοθεί σε έναν πράκτορα μπορεί να αλλάξει ακόμη και κατά τη διάρκεια της εκτέλεσης [48].

Υποστηρίζεται ισχυρή καθώς και εξαναγκαστική μετανάστευση. Το συγκεκριμένο χαρακτηριστικό αποτελεί ένα μηχανισμό ισχυρής μετανάστευσης, κατά τη χρήση του οποίου η εκτέλεση του πράκτορα διακόπτεται και συνεχίζει σε διαφορετική πλατφόρμα εκτέλεσης. Η όλη διαδικασία είναι διαφανής ως προς τον πράκτορα που μεταναστεύει [52] και χρησιμοποιείται σε περιπτώσεις τερματισμού της λειτουργίας της πλατφόρμας ή για λόγους εξισορρόπησης φόρτου στο δίκτυο.

Το μοντέλο εμπιστοσύνης που υιοθετεί το Nomads δεν ορίζεται ρητά. Από την σχετική βιβλιογραφία [48], [49], [50], [51] μπορούμε να καταλήξουμε στο συμπέρασμα ότι η πλατφόρμα θεωρείται ως έμπιστη και οι οντότητες που ανήκουν στο ίδιο domain θεωρούνται αμοιβαία ως έμπιστες [50].

Ανάλυση με Βάση Σενάρια Απειλών

Εξετάσαμε την ιδιαιτερότητα του Nomads όσον αφορά στη δυνατότητα ισχυρής μετανάστευσης και λεπτομερούς διαχείρισης πόρων, ενώ είδαμε ότι τις επιτυγχάνει χρησιμοποιώντας της Aroma Virtual Machine και το περιβάλλον εκτέλεσης Oasis.

Το Nomads χρησιμοποιεί αυτούς τους μηχανισμούς προκειμένου να αντιμετωπίσει την απειλή ενός κακόβουλου πράκτορα. Επιπλέον, το Nomads αντιμετωπίζει την απειλή και με ένα δεύτερο τρόπο. Η εξειδικευμένη φύση της AVM επιτρέπει δυναμικό έλεγχο κατά την εκτέλεση του πράκτορα επιβάλλοντας όχι μόνο όρια ρυθμού αλλά και ποσοτικά. Έτσι, στην περίπτωση που ένας πράκτορας αρχίσει να συμπεριφέρεται κακόβουλα η AVM μπορεί να περιορίσει ή και να αφαιρέσει τους πόρους που του έχουν αποδοθεί, λειτουργώντας ουσιαστικά σαν ένας μηχανισμός εντοπισμού εισβολών που βασίζεται στη διαχείριση πόρων.

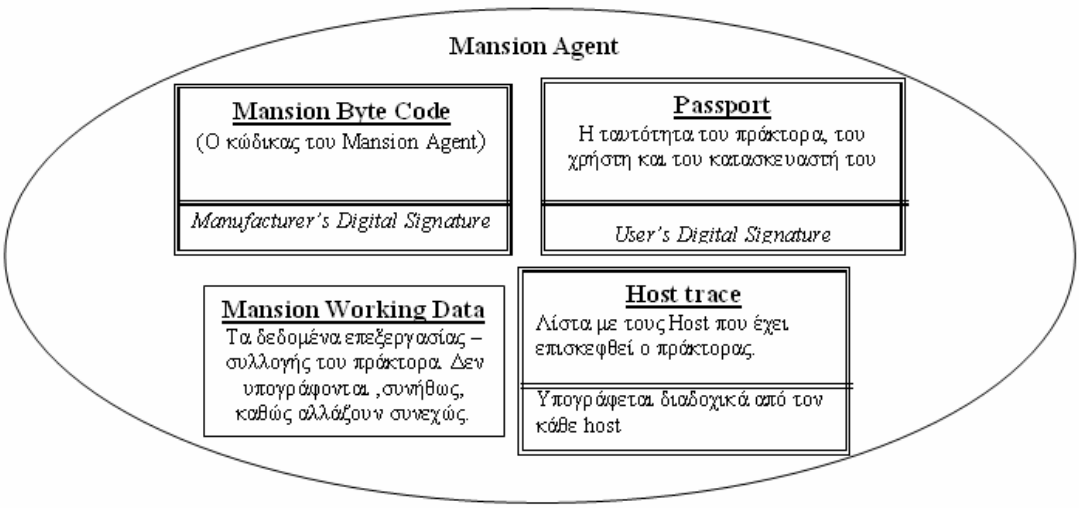
Κύρια προσφορά του Nomads αποτελούν οι βελτιώσεις εκτέλεσης που προσφέρει και τα χαρακτηριστικά ασφάλειας που όμως απευθύνονται κυρίως σε απειλές που προέρχονται από πράκτορες [4]. Έτσι, η πλατφόρμα θεωρείται εξ ορισμού ως ασφαλής και έμπιστη και η απειλή της κακόβουλης πλατφόρμας δεν λαμβάνεται υπόψη. Σε μια τέτοια περίπτωση ο πράκτορας παραμένει εκτεθειμένος.

Αν και τα Nomads δεν ορίζουν κάποια ανώτερη οντότητα από την πλατφόρμα εκτέλεσης, απεικονίζει πολλαπλά host με εξαναγκασμένη μετανάστευση πρακτόρων μεταξύ τους, για λόγους εξισορρόπησης φόρτου, η οποία μπορεί να πραγματοποιείται ακόμη και δια μέσου ενός ανοιχτού δικτύου [52]. Αυτό υπονοεί ένα κατανεμημένο σύστημα με κοινό υπόβαθρο για όλες τις συνεργαζόμενες πλατφόρμες, παράλληλα με κοινή διαχείριση ασφάλειας με σκοπό τη διαμόρφωση ενός ασφαλούς-έμπιστου περιβάλλοντος. Έτσι καταλήγουμε στο συμπέρασμα ότι η αρχιτεκτονική των Nomads δεν είναι σχεδιασμένη για λειτουργία σε ανοιχτά περιβάλλοντα.

3.3.6 Mansion

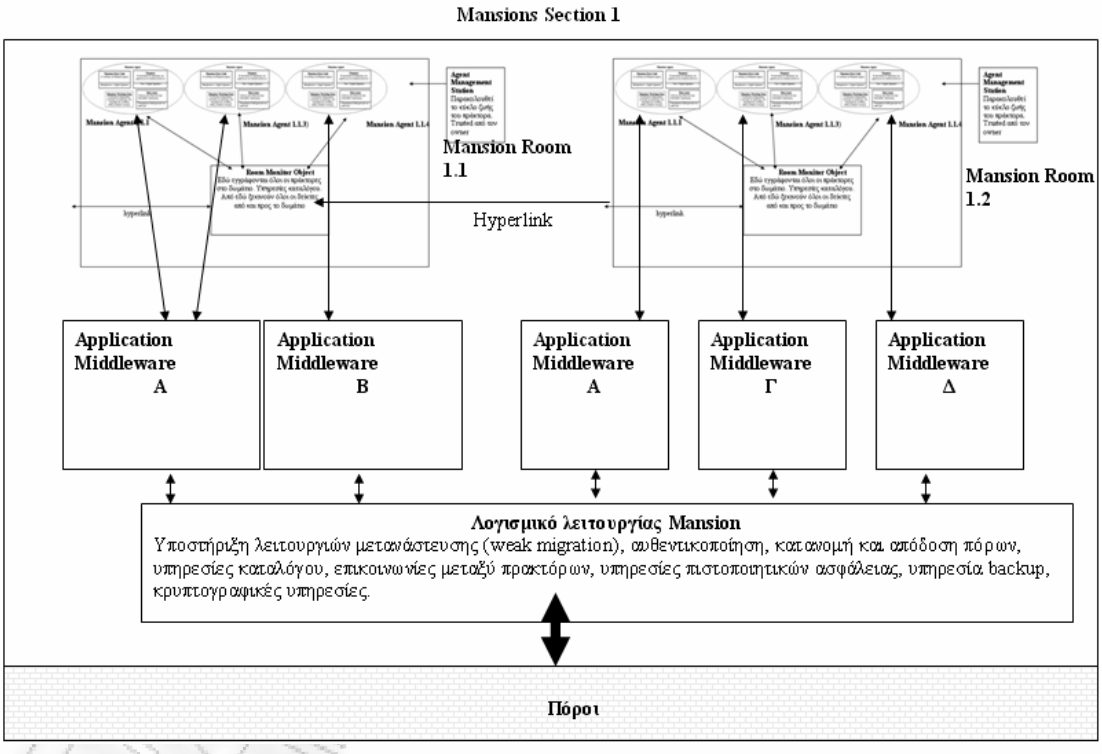
Το Mansion είναι ένα σύστημα κινητών πρακτόρων που αποτελεί προϊόν ερευνητικού προγράμματος του Πανεπιστημίου Vrije του Amsterdam. Αποσκοπεί στο να είναι κλιμακούμενο (scalability) και να παρέχει ασφάλεια σε εφαρμογές μεγάλης έκτασης [53]-[55]. Το κύριο χαρακτηριστικό του Mansion είναι η εισαγωγή ενός κόσμου (World) με πολλαπλά δωμάτια και ζώνες (rooms and zones), με τα οποία ένας πράκτορας μπορεί να αλληλεπιδρά. Το Mansion δημιουργεί μια σύνθετη ιεραρχία εμπιστοσύνης, βασιζόμενη στο κλειδί του ιδιοκτήτη του κόσμου (World Owner). Διάφορα δωμάτια και ζώνες μπορεί να δημιουργηθούν μέσα στον ίδιο κόσμο, χωρίς όμως απαραίτητα να θεωρούνται μεταξύ τους ως έμπιστα [54].

Ο πράκτορας Mansion έχει σχεδιαστεί παρόμοια με τον Ara (παράγραφος 3.3.8.4 Ara). Αποτελείται και αυτός από τον κώδικα, τα δεδομένα του, το "διαβατήριο" με τα στοιχεία του και το ιστορικό των host που έχει επισκεφθεί (Εικόνα 22). Ο κώδικας υπογράφεται ψηφιακά από τον κατασκευαστή και το διαβατήριο από τον χρήστη. Ο σχεδιασμός του πράκτορα περιλαμβάνει τα στατικά μέρη, τα οποία και υπογράφονται ψηφιακά και τα μεταβλητά τα οποία δεν είναι δυνατό να υπογραφούν. Υποστηρίζεται ισχυρή μετανάστευση.

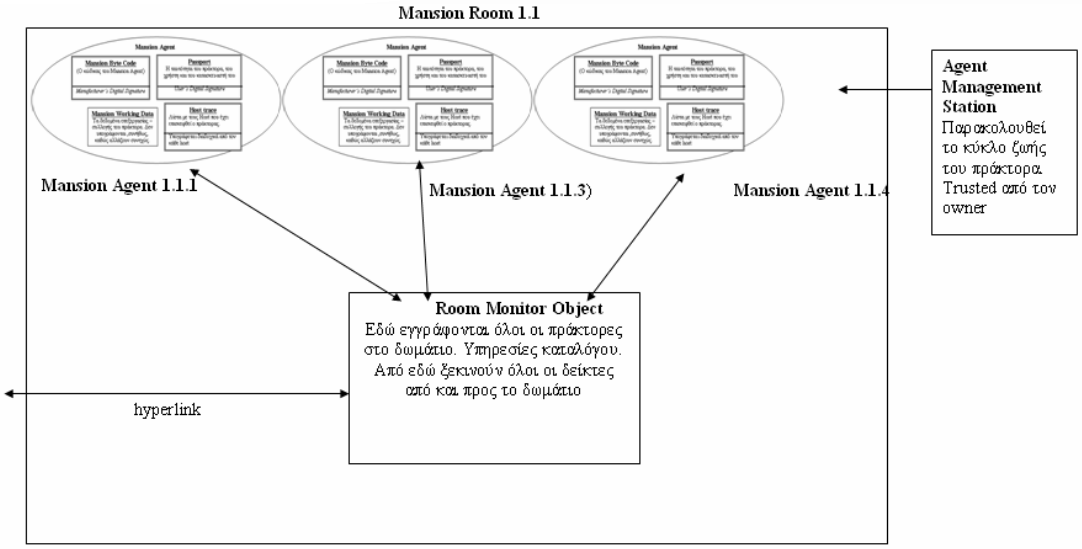


Εικόνα 22 – Διάγραμμα επιπέδου 4: Ένας πράκτορας Mansion.

Το μηχάνημα εκτέλεσης των Mansion δεν ορίζεται. Αποτελεί ένα τελείως δικτυακό και κατανεμημένο σύστημα στο οποίο έχει νόημα μόνον η κατανεμημένη πλατφόρμα που ονομάζεται Section (Εικόνα 23). Αυτή απλώνεται σε πολλά μηχανήματα, τα οποία έχουν κοινή διαχείριση. Υποστηρίζεται ομαδοποίηση πρακτόρων μέσα σε ένα Section που ονομάζεται Room, αλλά, και πάλι, δεν απαιτείται η συγκέντρωση όλων των πρακτόρων του σε ένα φυσικό μηχάνημα εκτέλεσης (Εικόνα 24). Όλες οι υπηρεσίες της πλατφόρμας υλοποιούνται σε επίπεδο Section και περιλαμβάνουν τις τυπικές υπηρεσίες υποστήριξης λειτουργιών μετανάστευσης, αυθεντικοποίησης, κατανομής και απόδοσης πόρων, υπηρεσίες καταλόγου, επικοινωνίες μεταξύ πρακτόρων, υπηρεσίες πιστοποιητικών ασφάλειας, υπηρεσία backup και κρυπτογραφικές υπηρεσίες.

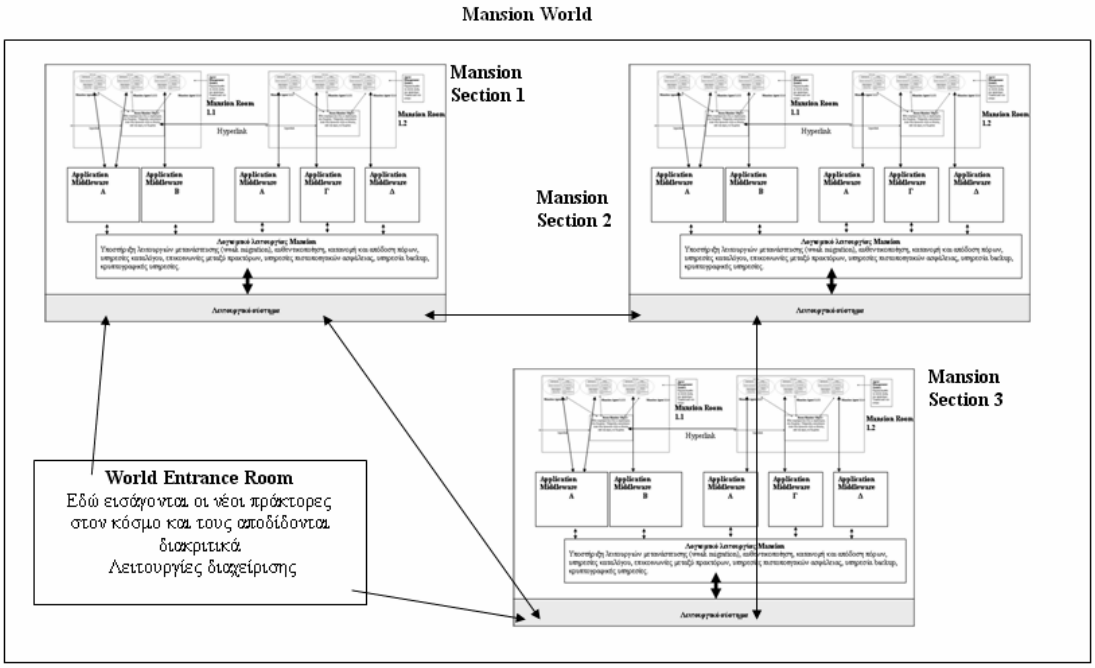


Εικόνα 23 – Διάγραμμα Επιπέδου 1: Ένα Section της πλατφόρμας Mansion.



Εικόνα 24 – Διάγραμμα επιπέδου 3: Ένα δωμάτιο πρακτόρων.

Στο Mansion η ανώτερη οντότητα είναι ο Κόσμος (World - Εικόνα 25). Διαθέτει κεντρικοποιημένη διαχείριση και δέντρο εμπιστοσύνης. Ο κόσμος μπορεί να δημιουργηθεί στο εσωτερικό δίκτυο ενός οργανισμού όπου είναι πρακτικά εφαρμόσιμο το συγκεκριμένο μοντέλο διαχείρισης. Είναι χαρακτηριστικό ότι ακόμη και για την εισαγωγή ενός νέου πράκτορα στον Κόσμο πρέπει να εισαχθεί από το World Entrance Room, το οποίο επιτελεί τις κεντρικές λειτουργίες διαχείρισης.



Εικόνα 25 – Διάγραμμα πλαίσιο: Ο «κόσμος» του Mansion.

Ανάλυση με Βάση τα Κριτήρια Σύγκρισης

Το Mansion διαμορφώνει ένα κόσμο με πολλαπλά δωμάτια και ζώνες στα οποία μπορεί να κινηθεί ένας πράκτορας. Όλες οι οντότητες μέσα σε αυτόν τον κόσμο (Mansion World) διαθέτουν ένα ζεύγος ιδιωτικού και δημοσίου κλειδιού. Είναι δυνατόν για τον προγραμματισμό ολόκληρης της πλατφόρμας να χρησιμοποιηθούν διάφορες γλώσσες προγραμματισμού, μεταξύ των οποίων η Java, η Python και η Safe-Tcl [54]. Οι πράκτορες προστατεύονται από τους μηχανισμούς της εικονικής μηχανής καθώς και από την ψηφιακή υπογραφή του χρήστη. Το Mansion διαθέτει μια διαχειριστική υπηρεσία πρακτόρων (Agent Management Service), η οποία είναι υπεύθυνη για τη διατήρηση αρχείου με όλες τις ενέργειες των πρακτόρων κατά τη διάρκεια του κύκλου ζωής του. Επιπλέον, δρα ως μεσάζοντας για όλες τις επικοινωνίες με τον πράκτορα. Γίνεται χρήση ενός συστήματος ελέγχου (audit system) σε συνδυασμό με ένα πρωτόκολλο διαπομπής (handoff protocol) για τη διασφάλιση της διαδικασίας μετανάστευσης. Η πλατφόρμα προστατεύεται με τη χρήση του Java Sandbox που επιτρέπει την εκτέλεση μη έμπιστου κώδικα [54], [55]. Η ασφάλεια των επικοινωνιών επιδιώκεται με τη χρήση κρυπτογραφικών μεθόδων όπως το SSL.

Όλες οι οντότητες, καθώς και τα τμήματα που απαρτίζουν τον κόσμο των Mansion, αυθεντικοποιούνται αμοιβαία με τη χρήση υπογραφών και πιστοποιητικών (Self-certifying Identifiers). Το Mansion σκοπεύει στη δημιουργία μιας υποδομής εμπιστοσύνης (trust infrastructure) βασισμένης στο κλειδί του ιδιοκτήτη του κόσμου (World Owner). Ο έλεγχος πρόσβασης επιτυγχάνεται και σε αυτό τα σύστημα κινητών πρακτόρων με τη χρήση λιστών πρόσβασης. Αυτές οι λίστες είναι δυνατόν να διαφέρουν μεταξύ διαφορετικών ζωνών και δωματίων, ανάλογα με τις υποθέσεις εμπιστοσύνης (trust assumptions) που θεσπίζει ο κάθε τοπικός διαχειριστής [55]. Η διαχείριση πόρων πραγματοποιείται μέσω του λειτουργικού συστήματος και της εικονικής μηχανής που χρησιμοποιείται. Ένας πράκτορας μπορεί να αποκτήσει πρόσβαση μονάχα σε πόρους του δωματίου στο οποίο λειτουργεί [54]. Παρέχεται δυνατότητα ισχυρής μετανάστευσης, αν και μονάχα μεταξύ δωματίων με προϋπάρχοντα υπερσύνδεσμο μεταξύ τους. Ο

ιδιοκτήτης του κόσμου παρέχει ένα σημείο ένταξης στον κόσμο για τα δωμάτια και μπορεί να θεωρηθεί ως ένας κεντρικοποιημένος διαχειριστής ασφάλειας. Παρολ' αυτά, όμως, οι επιμέρους διαχειριστές δωματίων και ζωνών μπορεί να υιοθετήσουν την δική τους πολιτική ασφάλειας και τις δικές τους υποθέσεις εμπιστοσύνης – αξιοπιστίας.

Ανάλυση με Βάση Σενάρια Απειλών

Είδαμε προηγουμένως ότι το Mansion επιδιώκει την ακεραιότητα της πλατφόρμας πέρα από τη χρήση των μηχανισμών της εικονικής μηχανής με τη χρήση του μηχανισμού Agent Management Service (AMS). Η υπηρεσία αυτή είναι υπεύθυνη για την καταγραφή των κινήσεων του πράκτορα κατά τη διάρκεια της ζωής του. Έτσι, στην περίπτωση ενός κακόβουλου πράκτορα η AMS καταγράφει την συμπεριφορά και τη συσχετίζει με τον ιδιοκτήτη του πράκτορα και το επίπεδο εμπιστοσύνης που του αποδίδεται [54].

Σχετικά με την απειλή μιας κακόβουλης πλατφόρμας, το Mansion δεν λαμβάνει ιδιαίτερα μέτρα. Ένας πράκτορας επιτρέπεται να μεταναστεύσει μονάχα μεταξύ προκαθορισμένων τοποθεσιών, ανάλογα με τις σχέσεις εμπιστοσύνης που έχουν μεταξύ τους τα διάφορα μέρη του κόσμου. Έτσι, ο πράκτορας θεωρεί την πλατφόρμα εκτέλεσης εξ ορισμού ως έμπιστη, μια υπόθεση που τον καθιστά εκτεθειμένο στην περίπτωση που η πλατφόρμα αποδειχθεί κακόβουλη.

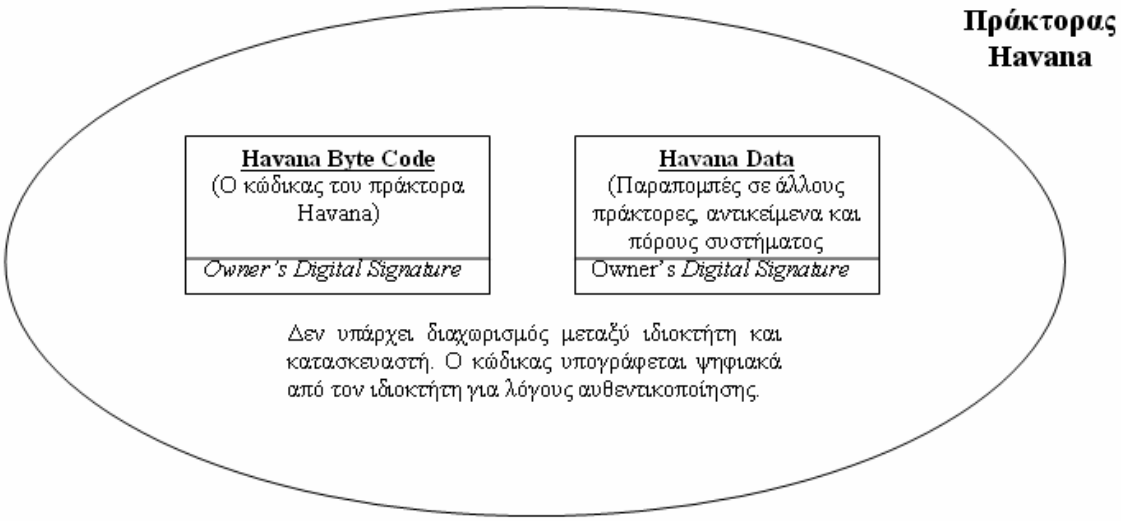
Το σύστημα κινητών πρακτόρων Mansion είναι και αυτό σχεδιασμένο για χρήση στο Διαδίκτυο, χρησιμοποιώντας το όμως απλά ως μέσο μετάδοσης, κάτι που δεν συνεπάγεται απαραίτητα λειτουργία σε ανοιχτό περιβάλλον. Είδαμε, επίσης, ότι Mansion δημιουργεί μια αλυσίδα εμπιστοσύνης με βάση το κλειδί του ιδιοκτήτη του κόσμου, αλλά είναι δυνατόν τα διάφορα δωμάτια και ζώνες να έχουν τη δική τους διαχείριση ασφάλειας που με τη σειρά της καθορίζει τη δική της, μοναδική, πολιτική εμπιστοσύνης απέναντι στις άλλες οντότητες. Αυτό το πολύπλοκο μοντέλο ιεραρχίας εμπιστοσύνης αντικατοπτρίζει τις σχέσεις που επικρατούν και στον πραγματικό κόσμο. Όμως, αυτό το μοντέλο έχει το αρνητικό ότι ένας πράκτορας μπορεί να λειτουργήσει πρακτικά μονάχα σε μέρη του κόσμου που θεωρούνται

έμπιστα από το μέρος προέλευσης του πράκτορα και όχι σε ολόκληρο τον κόσμο. Έτσι, συμπεραίνουμε ότι το μοντέλο ασφάλειας και εμπιστοσύνης που υιοθετεί το Mansion δεν υποστηρίζει λειτουργία σε ανοιχτά περιβάλλοντα.

3.3.7 Havana

Το Havana είναι ένα σύστημα κινητών πρακτόρων που αναπτύχθηκε από το πανεπιστήμιο του Guelph στον Καναδά. Αποσκοπεί στην παροχή όχι μόνο μιας πλατφόρμας εκτέλεσης, αλλά και ενός νέου επιχειρηματικού μοντέλου (business model) για την ενσωμάτωση της τεχνολογίας κινητών πρακτόρων σε υπάρχοντες διαδικτυακούς servers [56]-[58]. Το Havana προτείνει μια κλειστή αρχιτεκτονική στην οποία όλες οι οντότητες δεσμεύονται μεταξύ τους με ένα επικερδές επιχειρηματικό συμβόλαιο [58]. Οι πράκτορες είναι στην πραγματικότητα αγοραστικοί πράκτορες (shopping agents) που εισάγονται μέσα στον κόσμο του Havana μέσω μιας πύλης (Gateway). Οι μεταναστεύσεις λαμβάνουν χώρα μεταξύ της Gateway και των εμπορικών servers (Business servers) των διαφόρων διαδικτυακών εμπόρων που συμμετέχουν στο σύστημα.

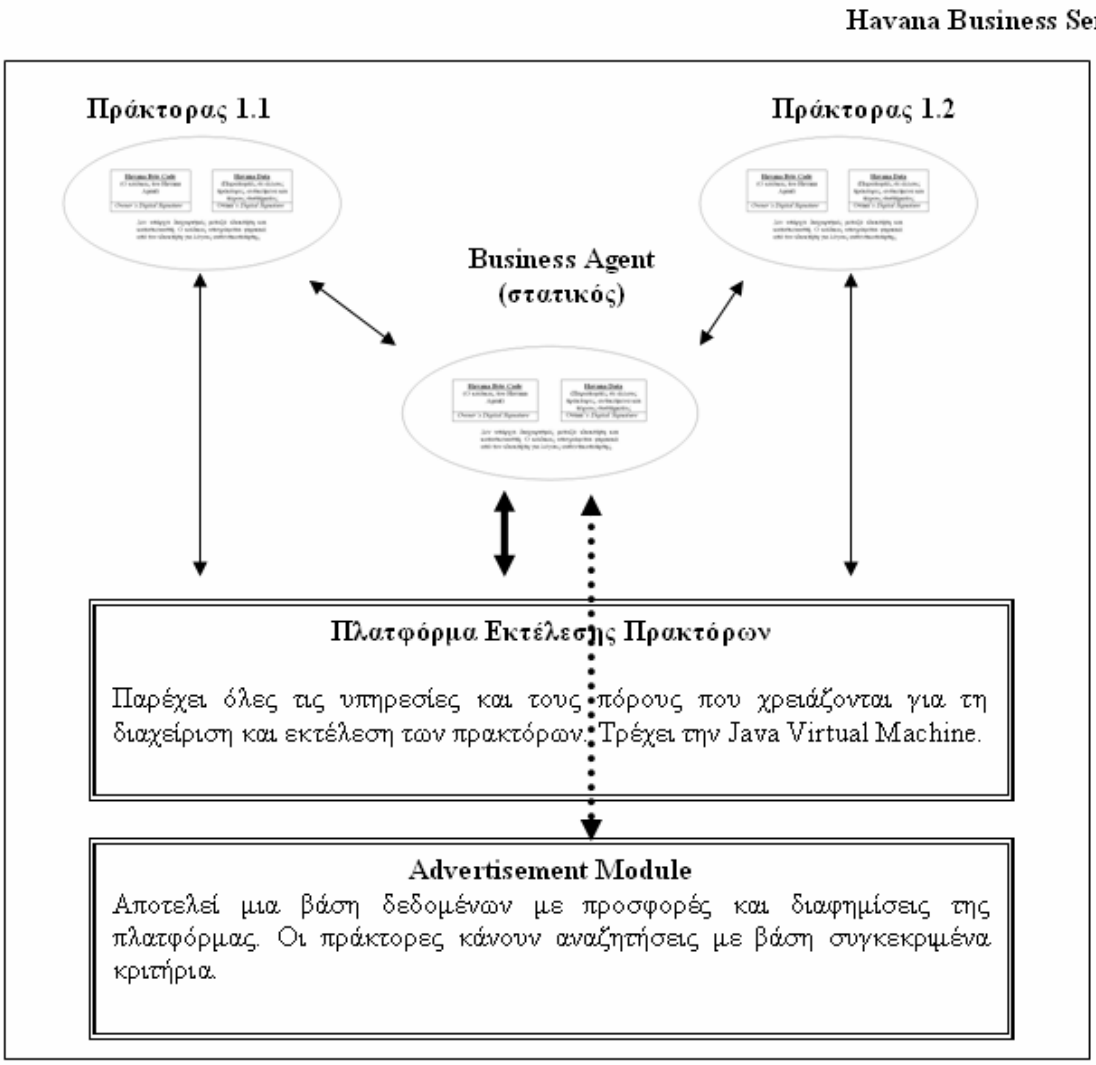
Ο πράκτορας Havana (Εικόνα 26) κατά τη δημιουργία του αποτελείται από τον κώδικα και τα δεδομένα του, με τη ψηφιακή υπογραφή του ιδιοκτήτη, ενώ δεν γίνεται διαχωρισμός με τον προγραμματιστή – δημιουργό. Αποτελεί έναν πράκτορα αγορών (shopping agent). Ακολουθεί απλούστατη σχεδίαση και δημιουργείται από τον χρήστη μέσω της Gateway χρησιμοποιώντας ένα GUI με δυνατότητες παραμετροποίησης. Καθώς ο κώδικας του πράκτορα δημιουργείται αυτοματοποιημένα, ο χρήστης δεν μπορεί να εισάγει μη εγκεκριμένο κώδικα.



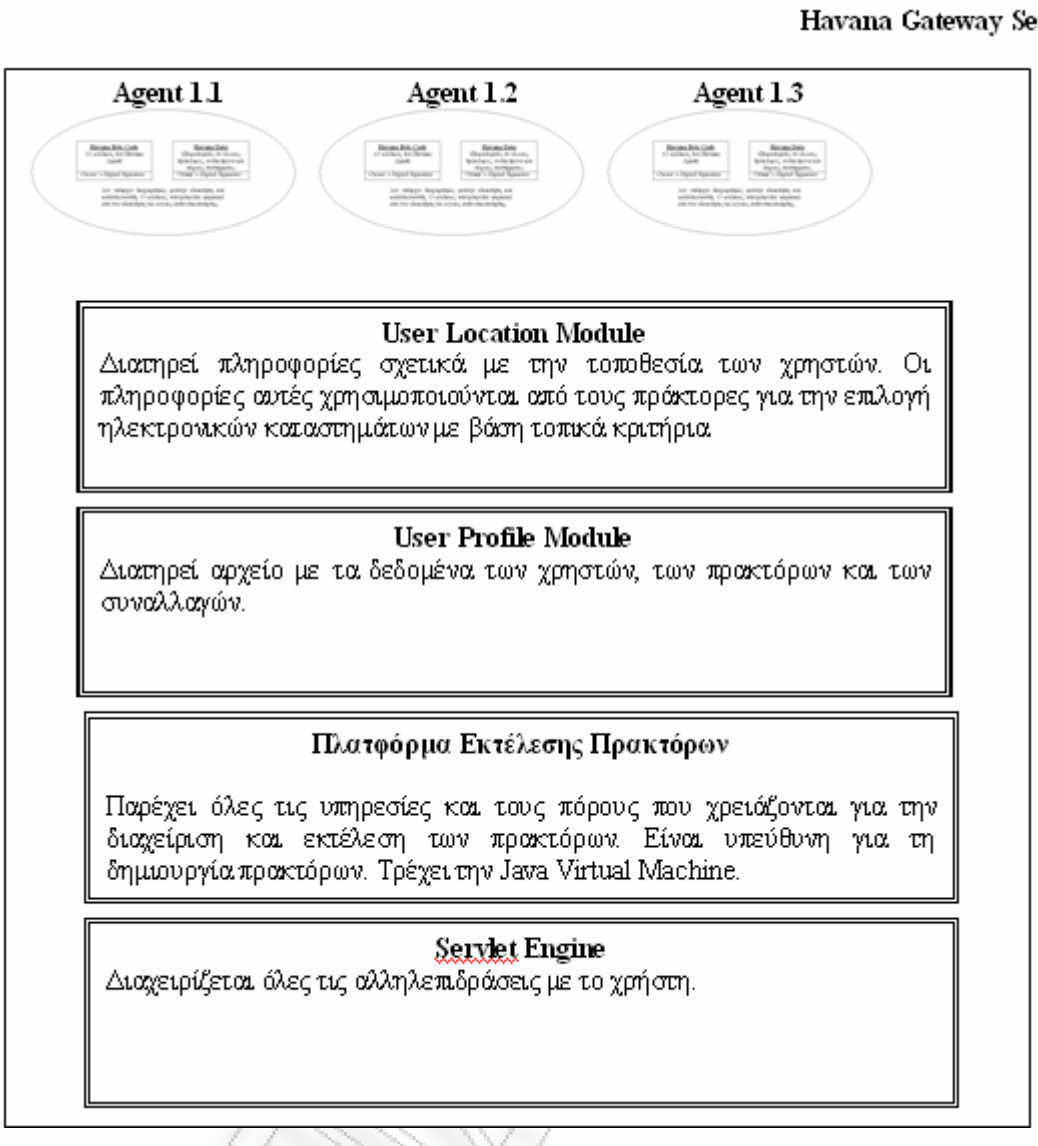
Εικόνα 26 – Διάγραμμα επιπέδου 3: Ένας πράκτορας Havana.

Ορίζονται δύο είδη πλατφόρμας, η πύλη (Εικόνα 28) που είναι μονάχα μία και οι Business servers (Εικόνα 27) που είναι όσοι και οι διαδικτυακοί έμποροι που συμμετέχουν στο σύστημα Havana. Οι Business servers αποτελούν ουσιαστικά την πλατφόρμα εκτέλεσης των πρακτόρων στα ηλεκτρονικά καταστήματα και έχουν απλό σχεδιασμό. Αποσκοπούν μονάχα στην παροχή των υπηρεσιών που απαιτούνται για την εκτέλεση των πρακτόρων και υπηρεσιών καταλόγου, που επιτρέπουν την πραγματοποίηση εμπορικών αναζητήσεων και αγορών και τις οποίες παρέχει μέσω του στατικού Business Agent.

Η Gateway, αντιθέτως, έχει πιο σύνθετη δομή, ως αποτέλεσμα του κεντρικού ρόλου που αναλαμβάνει. Αποτελεί την πλατφόρμα δημιουργίας και εκτέλεσης των πρακτόρων. Είναι ο κεντρικός διαχειριστής του δικτύου Havana και είναι υπεύθυνη για τη διαχείριση χρηστών, εμπόρων και πρακτόρων, ενώ όλες οι διαδικασίες στο σύστημα λαμβάνουν χώρα μέσω αυτής.

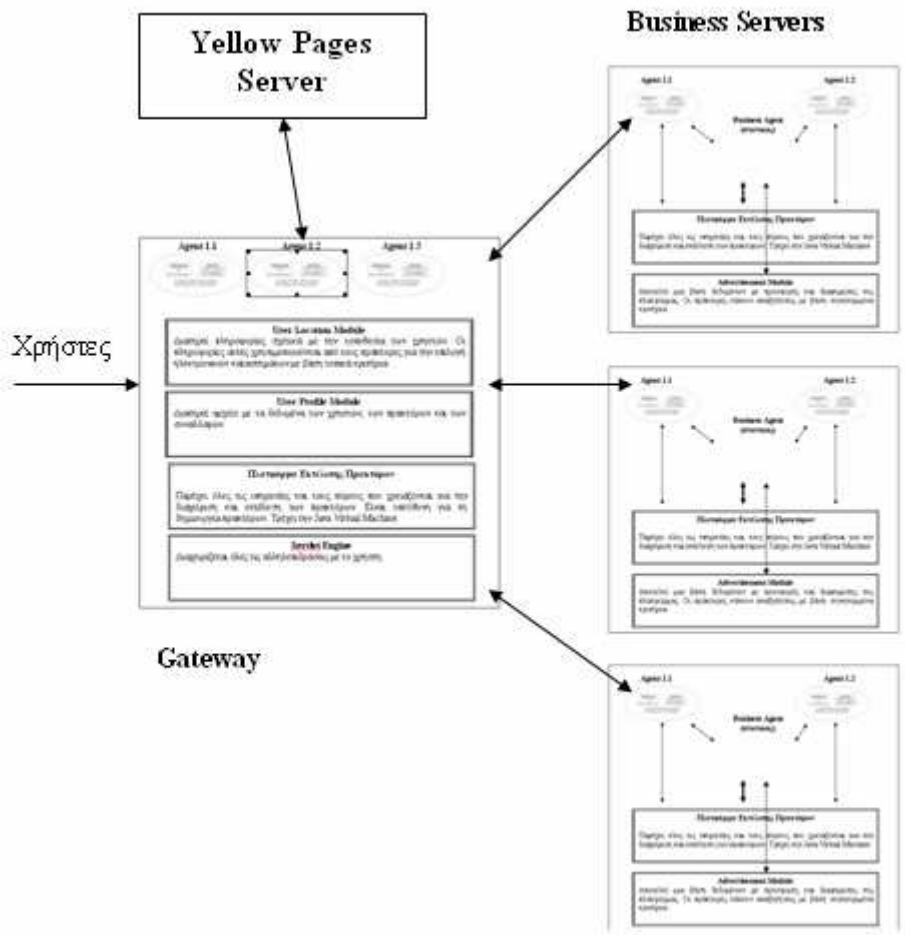


Εικόνα 27 – Διάγραμμα επιπέδου 1: Ένας Business Server Havana.



Εικόνα 28 – Διάγραμμα επιπέδου 1: Ένας Gateway Server Havana.

Στο Havana ανώτερη οντότητα Επικράτειας ορίζεται η Havana Platform (Εικόνα 29). Υπάρχει αυστηρά κεντρικοποιημένη διαχείριση, μέσω της Gateway, σε ένα δίκτυο Havana και απεικονίζεται μέσα στο διάγραμμα ανώτερου επιπέδου. Ο κόσμος του Havana αποτελείται από την Gateway που είναι η είσοδος στο σύστημα και ο κεντρικός διαχειριστής, τους Business Servers των ηλεκτρονικών καταστημάτων και τη βάση δεδομένων Yellow Pages, που κρατάει το αρχείο με τα ηλεκτρονικά καταστήματα. Οι χρήστες καθώς και όλες οι οντότητες που συμμετέχουν σε μια Havana Platform δεσμεύονται από πραγματικό συμβόλαιο.



Εικόνα 29 – Διάγραμμα Πλαίσιο: Η Havana Platform.

Ανάλυση με Βάση τα Κριτήρια Σύγκρισης

Το κύριο χαρακτηριστικό του Havana είναι το μοντέλο της εμπιστοσύνης του. Οποιαδήποτε κακόβουλη συμπεριφορά κατά τη διάρκεια των συναλλαγών συνεπάγεται το σπάσιμο της εμπορικής συμφωνίας. Ο πράκτορας και οι πλατφόρμες της Gateway και των εμπορικών server φέρουν υπογραφές προκειμένου να διασφαλίσουν την ακεραιότητά τους. Με την ολοκλήρωση των εργασιών του ένας πράκτορας μεταδίδει τα αποτελέσματά του πίσω στην Gateway, για την παροχή υπηρεσιών μη αποποίησης (non repudiation services). Αυτό συμβαίνει ώστε να μπορούν να εντοπιστούν τυχόν αλλοιώσεις από μελλοντικές πλατφόρμες φιλοξενίας, κάτι που θα επιφέρει την παραβίαση του συμβολαίου.

Καθώς το Havana βασίζεται στην Java, η πλατφόρμα προστατεύεται από κακόβουλους ή δυσλειτουργικούς πράκτορες από τον Java Security Manager. Οι επικοινωνίες διασφαλίζονται με τη χρήση κρυπτογραφίας δημόσιου / ιδιωτικού κλειδιού [56]. Επιβάλλεται αμοιβαία αυθεντικοποίηση όλων των οντοτήτων με τη χρήση ψηφιακών υπογραφών. Αυτό συνεπάγεται στο να θεωρείται ο κόσμος του Havana ως έμπιστος, επιτρέποντας έτσι τη δημιουργία μιας αμοιβαία επωφελούς σχέσης όπου καμία μη εξουσιοδοτημένη οντότητα δεν μπορεί να εισέλθει [57], [58]. Ο έλεγχος πρόσβασης βασίζεται σε λίστες εγγεγραμμένων χρηστών και Business Servers, οι οποίες διατηρούνται από την Gateway [56]. Η διαχείριση πόρων επιβάλλεται από τον Java Security Manager. Το Havana υποστηρίζει ισχυρή κρυπτογραφία για τη μεταφορά του πράκτορα μαζί με τα δεδομένα του σε νέους εμπόρους. Το Havana αποτελεί ένα κλειστό περιβάλλον με κεντρική διαχείριση ασφάλειας. Η Gateway είναι υπεύθυνη για την εγγραφή και εξουσιοδότηση χρηστών – πελατών, πρακτόρων και εμπόρων και αποτελεί τον κεντρικό διαχειριστή και για θέματα ασφάλειας.

Ανάλυση με Βάση Σενάρια Απειλών

Το Havana βασίζεται στην Java, οπότε και η πλατφόρμα προστατεύεται από κακόβουλους πράκτορες από τους μηχανισμούς που παρέχει η JVM, χωρίς να υλοποιούνται πρόσθετοι μηχανισμοί. Η ουσιαστική ασφάλεια που διαθέτει, όμως, το Havana είναι το επιχειρηματικό συμβόλαιο που δεσμεύει τις οντότητες. Επομένως, ένας κακόβουλος πράκτορας ενδέχεται να παραβιάσει την ακεραιότητα της πλατφόρμας, αλλά κάτι τέτοιο θα έχει άμεσο αντίκτυπο στον ιδιοκτήτη του.

Το μοντέλο εμπιστοσύνης του Havana θεωρεί μια αυθεντικοποιημένη πλατφόρμα ότι είναι έμπιστη. Βεβαίως είναι δυνατόν μια έως τώρα νόμιμη πλατφόρμα να μετατραπεί σε κακόβουλη (για λόγους που εξετάσαμε στο δεύτερο κεφάλαιο). Σε αυτή την περίπτωση είναι τεχνικά δυνατόν να παραβιάσει την ακεραιότητα ενός πράκτορα, ακόμη και να επηρεάσει την αγοραστική του δραστηριότητα προς όφελος του ιδιοκτήτη της. Όμως το Havana παρέχει ισχυρές υπηρεσίες μη αποποίησης, καθώς όλες οι ενέργειες αναφέρονται και καταγράφονται

από την Gateway. Έτσι, και στην απειλή της κακόβουλης πλατφόρμας η ουσιαστική ασφάλεια προέρχεται από τις συνέπειες που θα έχει στον πραγματικό κόσμο μια οντότητα αν αθετήσει το εμπορικό συμβόλαιο που τη δεσμεύει.

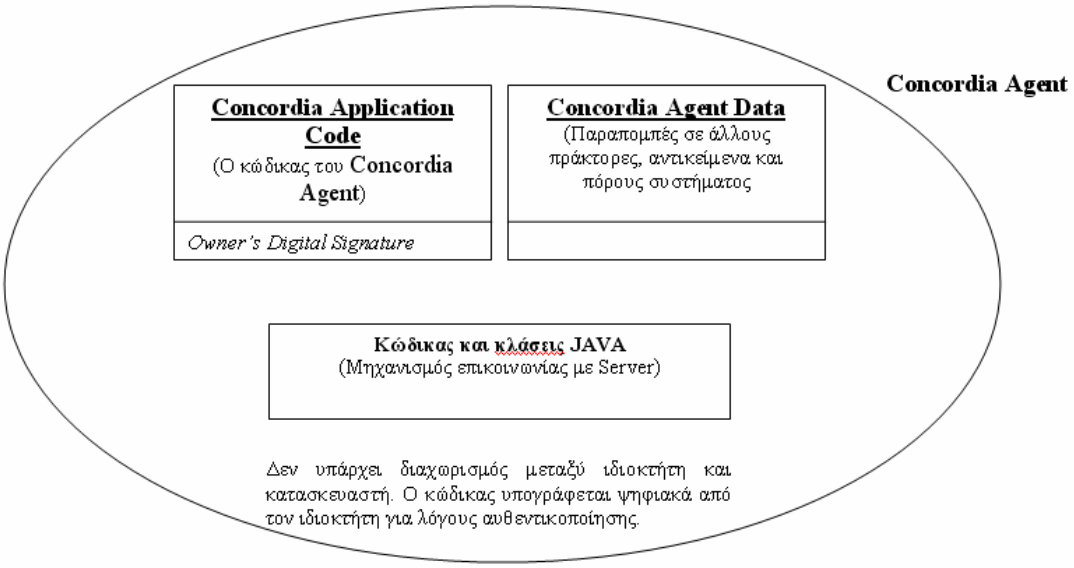
Το Havana είναι κατάλληλο για χρήση σε ανοιχτά δίκτυα με τις διάφορες οντότητες που εμπλέκονται να έχουν τη δική τους ανεξάρτητη διαχείριση ασφάλειας, καθώς πρόκειται για διαφορετικά διαδικτυακά καταστήματα [57], [58]. Όμως, καθώς η Gateway διαχειρίζεται κεντρικά τη λειτουργία του συστήματος και ειδικά τα θέματα ασφάλειας σε όλες τις αλληλεπιδράσεις, αναλαμβάνει το ρόλο κεντρικού διαχειριστή ασφάλειας. Αυτό καθιστά τον κόσμο του Havana ένα κλειστό περιβάλλον όπου μάλιστα οι οντότητες που τον απαρτίζουν δεσμεύονται και με συμβόλαιο. Αυτό δημιουργεί έναν ασφαλή και έμπιστο κόσμο όπου μπορούν να πραγματοποιηθούν κερδοφόρες συναλλαγές και στον οποίο δεν μπορούν να εισέλθουν μη εξουσιοδοτημένες οντότητες.

3.3.8 Άλλα Συστήματα Πρακτόρων

3.3.8.1 Concordia

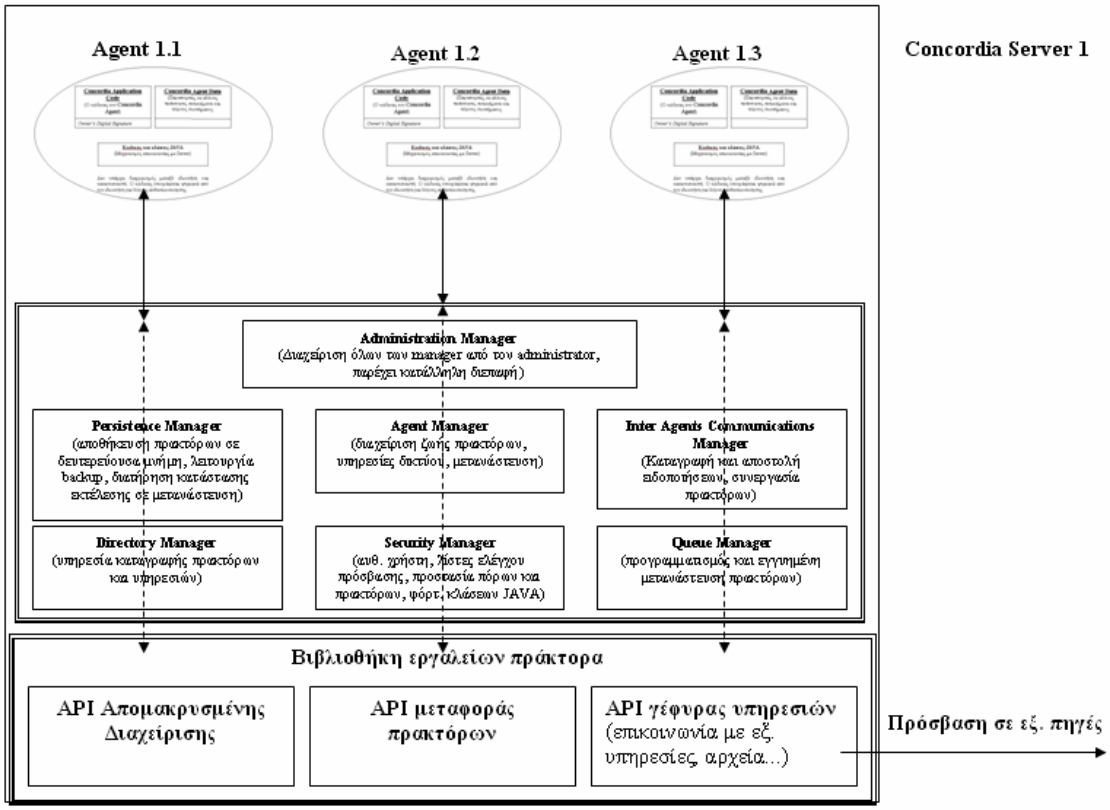
Το Concordia αποτελεί μια πλατφόρμα κινητών πρακτόρων που αναπτύχθηκε από το Electronic Information Center της Mitsubishi [26], [38]. Σχεδιάστηκε για να προσφέρει κινητικότητα πρακτόρων και συνεργασία, αξιόπιστες επικοινωνίες και ασφάλεια. Είναι και αυτό βασισμένο στην Java.

Ο πράκτορας Concordia κατά τη δημιουργία του αποτελείται από τον κώδικα, τα δεδομένα του, καθώς και κάποιες κλάσεις JAVA (Εικόνα 30). Μόνον ο κώδικας υπογράφεται ψηφιακά, ενώ και εδώ δεν γίνεται διαχωρισμός με τον προγραμματιστή - δημιουργό. Ο πράκτορας ενδέχεται να είναι κινητός ή σταθερός και ακολουθεί απλούστατη σχεδίαση.



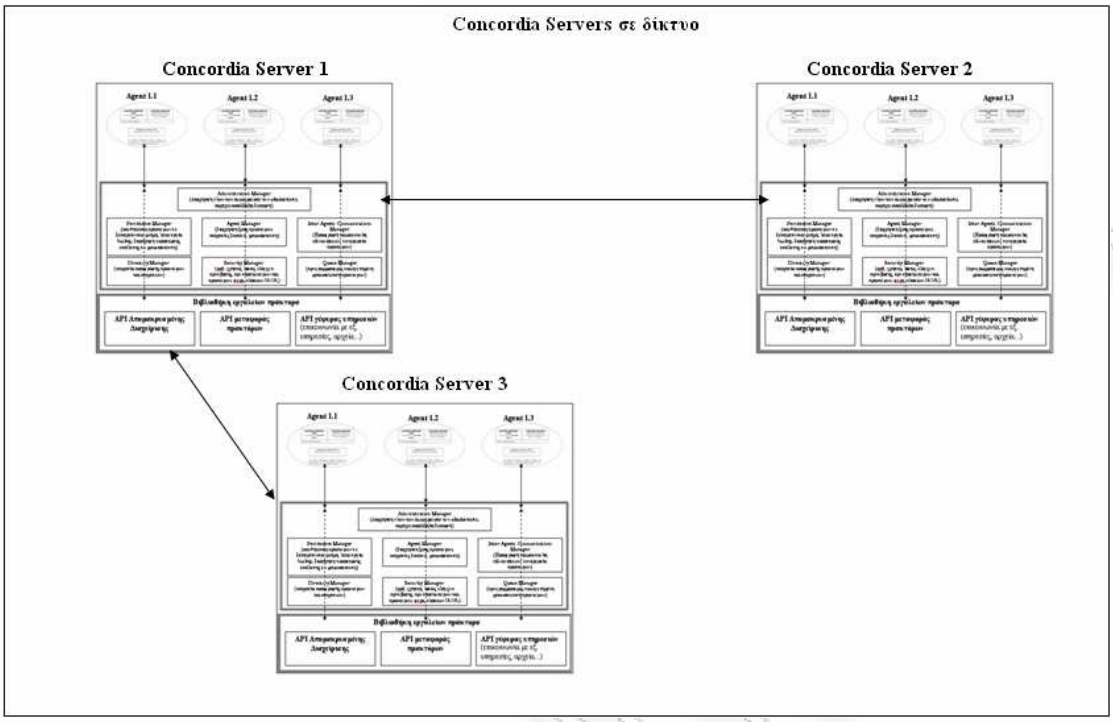
Εικόνα 30 - Διάγραμμα επιπέδου 3: Ένας πράκτορας του συστήματος Concordia

Το μηχάνημα εκτέλεσης Concordia ονομάζεται Concordia Server (Εικόνα 31). Δεν υποστηρίζεται ομαδοποίηση πρακτόρων με κοινή αντιμετώπιση. Ο Server τρέχει JVM και παρέχει όλες τις υπηρεσίες υποστήριξης: αποθήκευση πρακτόρων σε δευτερεύουσα μνήμη, λειτουργία backup, διατήρηση κατάστασης εκτέλεσης κατά τη μετανάστευση, διαχείριση ζωής πρακτόρων, υπηρεσίες δικτύου, καταγραφή και αποστολή ειδοποιήσεων, συνεργασία πρακτόρων, υπηρεσία καταγραφής πρακτόρων και υπηρεσιών, αυθεντικοποίηση χρήστη, λίστες ελέγχου πρόσβασης, προστασία πόρων και πρακτόρων, φόρτωση κλάσεων JAVA και προγραμματισμό και εγγυημένη μετανάστευση πρακτόρων.



Εικόνα 31 – Διάγραμμα επιπέδου 1: Ένας Server Concordia – η πλατφόρμα εκτέλεσης των πρακτόρων.

Στο Concordia δεν υφίσταται η ανώτερη οντότητα από τον server. Δεν υπάρχει κεντρικοποιημένη διαχείριση, είναι όμως δυνατή η επικοινωνία μεταξύ διαφορετικών server, οπότε και απεικονίζεται καταχρηστικά σαν διάγραμμα ανώτερου επιπέδου (Εικόνα 32).



Εικόνα 32 – Διάγραμμα Πλαίσιο: Επικοινωνία μεταξύ διαφορετικών server σε ένα δίκτυο.

Το Concordia αποσκοπεί στην προστασία των κινητών πρακτόρων και των δεδομένων τους, καθώς και στην προστασία των πόρων της πλατφόρμας. Αυτό επιτυγχάνεται, εν μέρει, με τη χρήση του μηχανισμού Java Sandbox. Όλες οι επικοινωνίες, όπως και η μετανάστευση του πράκτορα, είναι δυνατόν να προστατευθούν με τη χρήση του SSL [28]. Όταν ο πράκτορας δεν εκτελείται αποθηκεύεται σε κρυπτογραφημένη μορφή. Ο έλεγχος πρόσβασης πραγματοποιείται μέσω της JVM και περιλαμβάνει τη χρήση ενός τυπικού συστήματος ελέγχου πρόσβασης με βάση την ταυτότητα των χρηστών. Κάθε πράκτορας έχει μια ταυτότητα που δηλώνει τον ιδιοκτήτη του, και φέρει την ψηφιακή του υπογραφή. Μετά την αυθεντικοποίηση ένας πράκτορας μπορεί να θεωρηθεί ως έμπιστος ή μη έμπιστος. Η πλατφόρμα θεωρείται εξ ορισμού ως έμπιστη από τον πράκτορα, καθώς και ένας πράκτορας που ανήκει σε τοπικό χρήστη (της ίδιας πλατφόρμας) θεωρείται έμπιστος από την πλατφόρμα.

Το Concordia χρησιμοποιεί τον Queue Manager [26] ο οποίος χειρίζεται την διαδικασία της μετανάστευσης. Παρέχει υπηρεσίες ασφαλούς μετανάστευσης μέσα από το Διαδίκτυο χρησιμοποιώντας ένα πρωτόκολλο χειραψίας με δύο φάσεις, καθώς και υπηρεσίες διακομιστή μεσολάβησης. Η μετανάστευση που παρέχεται

είναι ασθενής, αφού ο πράκτορας μπορεί να μεταναστεύσει μονάχα σε προκαθορισμένα στάδια της διαδικασίας εκτέλεσης.

Ο διαχειριστής ασφάλειας (Security Manager) θεωρεί κάθε τοπικό πράκτορα ως έμπιστο και επιτρέπει αυτόματα την εκτέλεσή του. Στην περίπτωση ξένου πράκτορα, ο διαχειριστής ασφάλειας διαπιστώνει αρχικά αν πρόκειται για πράκτορα Concordia ή όχι. Στη συνέχεια, δίνει πρόσβαση στους πόρους της πλατφόρμας, ανάλογα με τα δικαιώματα του χρήστη του πράκτορα. Η διαχείριση πόρων πραγματοποιείται σε επίπεδο JVM και λειτουργικού συστήματος

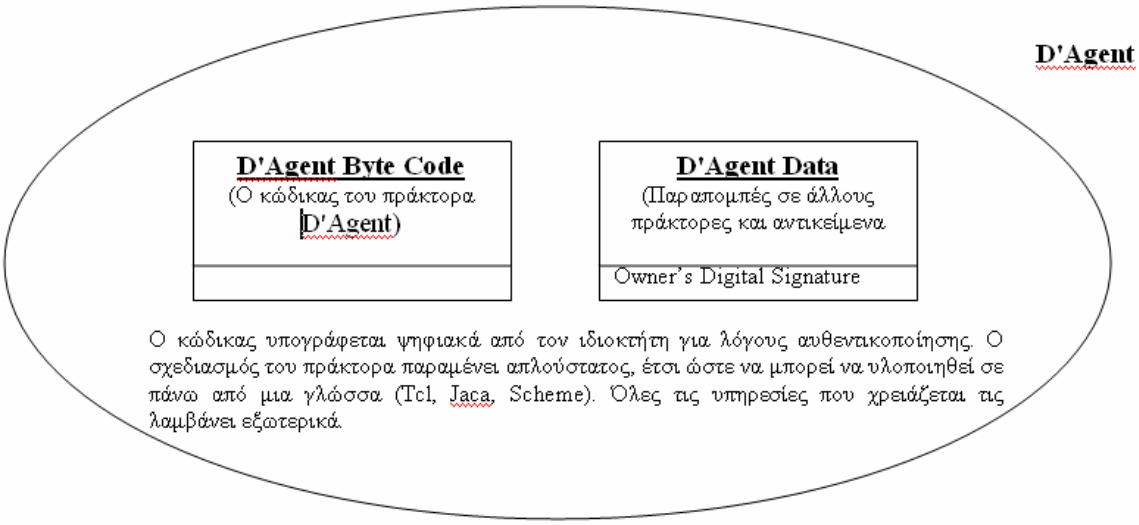
Η αρχιτεκτονική του Concordia δεν ορίζει ανώτερη οντότητα από το μηχάνημα εκτέλεσης (server - Εικόνα 31), το οποίο σημαίνει ότι δεν ορίζεται επίσημα κάποια οντότητα κεντρικού ελέγχου ασφάλειας. Παρόλ' αυτά είναι δυνατόν να υπάρχουν συνεργαζόμενοι Concordia Servers σε ένα δίκτυο, το οποίο υποδηλώνει την ύπαρξη κάποιας σχέσης μεταξύ τους καθώς και κοινής διαχείρισης. Το Concordia υποστηρίζει αρκετές καθιερωμένες υπηρεσίες ασφάλειας, αλλά δεν υιοθετεί κάποια συγκεκριμένη πολιτική ασφάλειας, ούτε παρέχει τα μέσα για την ενσωμάτωση κάποιας [27].

3.3.8.2 D' Agents

Οι D' Agents αποτελούν μια πλατφόρμα κινητών πρακτόρων που αναπτύχθηκε ερευνητικά από το Πανεπιστήμιο του Dartmouth. Σχεδιάστηκε για να προσφέρει μηχανισμούς ασφάλειας και λειτουργία μέσω κινητών και ασταθών δικτύων, ενώ χρηματοδοτήθηκε από τις αμερικανικές στρατιωτικές υπηρεσίες (Office of Naval Research, Air Force Office of Scientific Research, Department of Defense, DARPA) [81], [82].

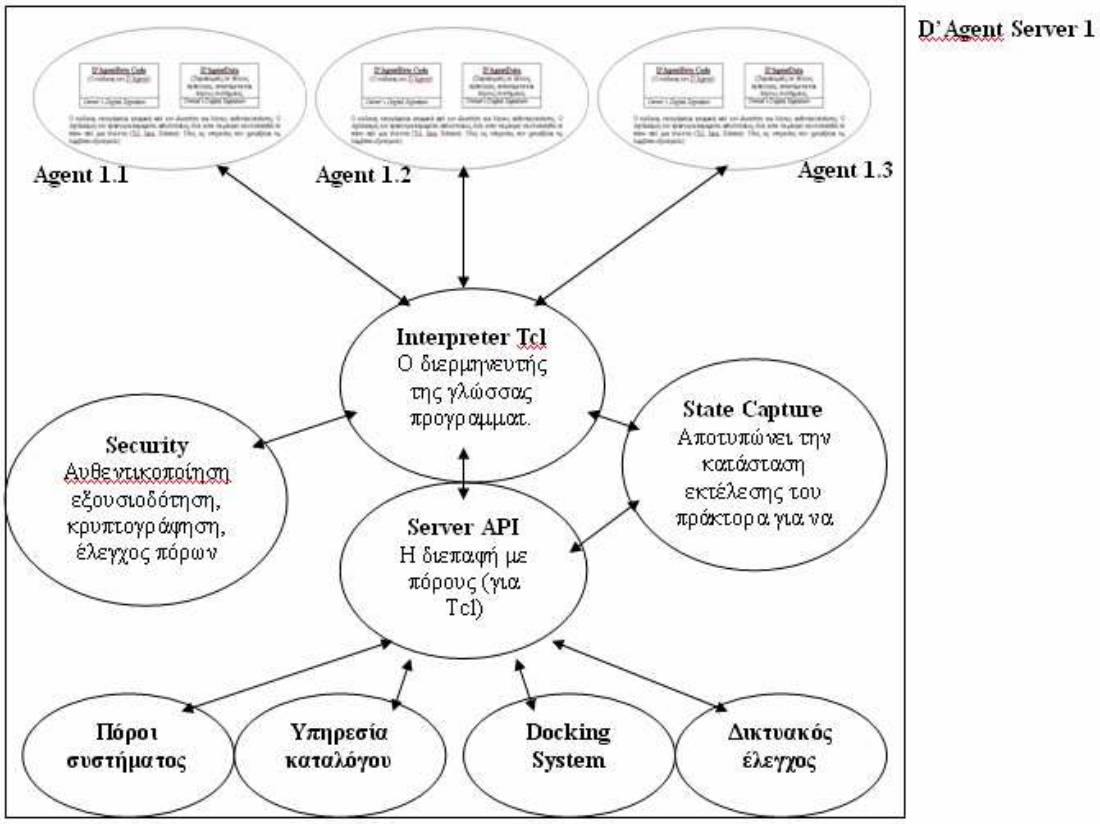
Ο πράκτορας D' Agent αποτελείται από τον κώδικα και τα δεδομένα του (Εικόνα 33). Ο κώδικας και τα δεδομένα υπογράφονται ψηφιακά από τον ιδιοκτήτη για λόγους αυθεντικοποίησης ενώ και στους D'Agents δεν γίνεται διαχωρισμός με τον προγραμματιστή – δημιουργό. Ο σχεδιασμός του πράκτορα παραμένει απλούστατος, έτσι ώστε να μπορεί να υλοποιηθεί σε πάνω από μια γλώσσα (Tcl,

Java, Scheme). Όλες τις υπηρεσίες που χρειάζεται τις λαμβάνει εξωτερικά της πλατφόρμας και θεωρούνται στατικοί πράκτορες.



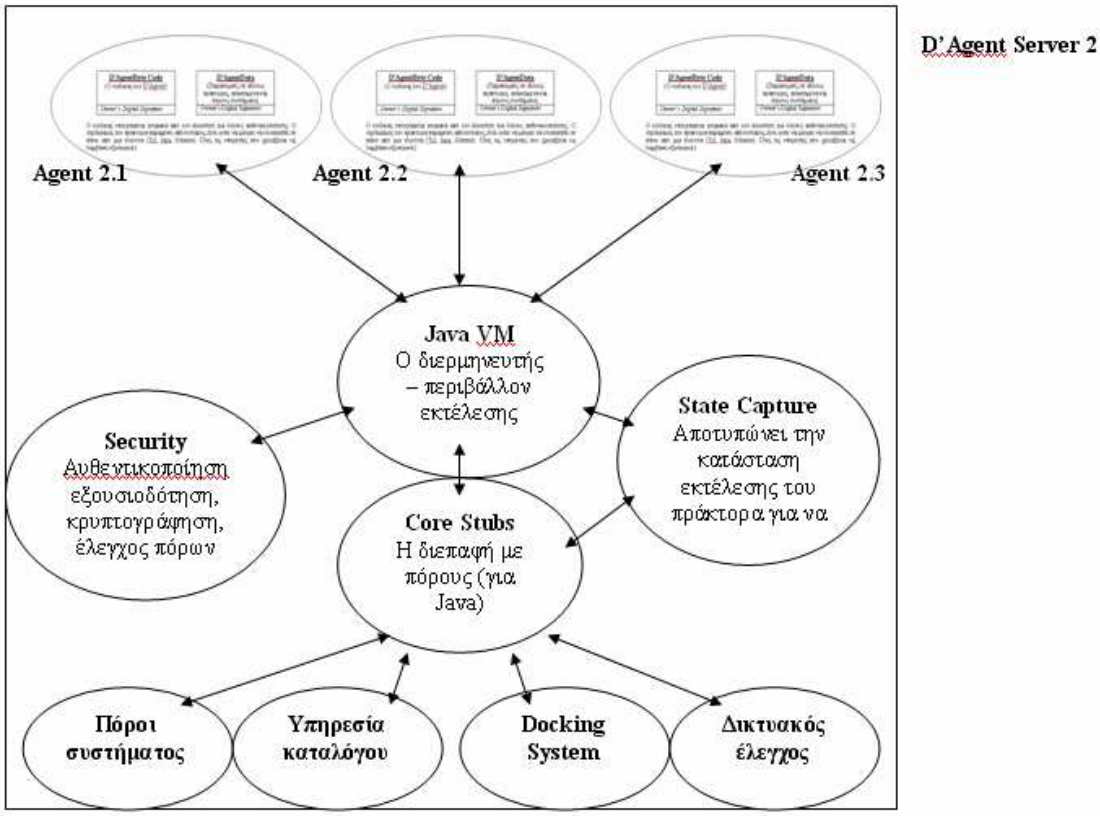
Εικόνα 33 – Διάγραμμα επιπέδου 4: Ένας πράκτορας D'Agent.

Το μηχάνημα εκτέλεσης των D'Agent ονομάζεται D'Agent Server. Δεν υποστηρίζεται ομαδοποίηση πρακτόρων με κοινή αντιμετώπιση. Εδώ υπάρχει η ιδιαιτερότητα ότι υποστηρίζονται τρεις γλώσσες υλοποίησης (Java, Tcl, Scheme) οπότε και ο server διαφοροποιείται ελαφρώς ανάλογα με τη γλώσσα. Υπάρχουν δύο είδη server ένας για Java και ένας για Scheme και Tcl (Εικόνα 34, Εικόνα 35). Και οι δύο παρέχουν αυθεντικοποίηση, εξουσιοδότηση, κρυπτογράφηση, έλεγχος πόρων, διεπαφή με πόρους (διαφορετική για κάθε γλώσσα), υπηρεσίες καταλόγου, δικτυακό έλεγχο, διερμηνευτές της γλώσσας προγραμματισμού ή της JVM και αποτύπωση της κατάστασης εκτέλεσης του πράκτορα προκειμένου να μεταναστεύσει. Στους D'Agent οι υπηρεσίες της πλατφόρμας θεωρούνται στατικοί πράκτορες και οπότε λαμβάνουν αυξημένους πόρους και μεγαλύτερο επίπεδο εμπιστοσύνης.

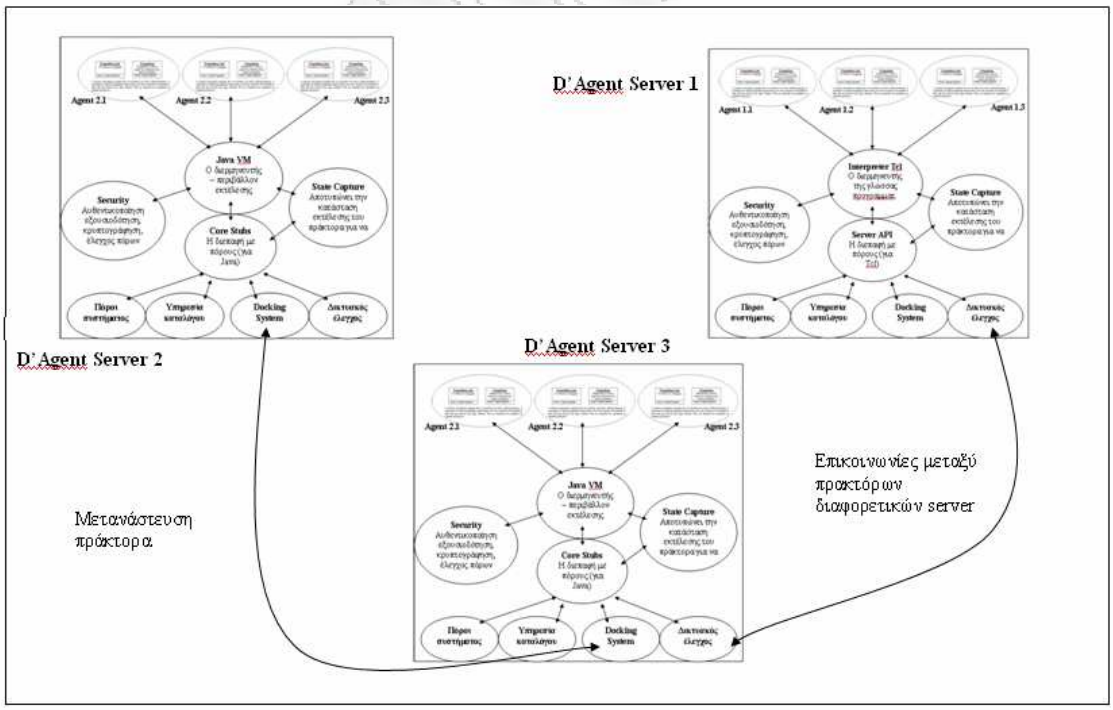


Εικόνα 34 – Διάγραμμα επιπέδου 2: Ένας D'Agent server που τρέχει πράκτορες υλοποιημένους σε Tcl / Scheme

Στους D'Agents δεν ορίζεται ανώτερη οντότητα από το server. Και εδώ δεν υπάρχει κεντρικοποιημένη διαχείριση, είναι όμως δυνατή η επικοινωνία και η μετανάστευση μεταξύ διαφορετικών server, οπότε και απεικονίζεται καταχρηστικά σαν διάγραμμα ανώτερου επιπέδου (Εικόνα 36).



Εικόνα 35 – Διάγραμμα επιπέδου 2 (συνέχεια): Ένας D'Agent server που τρέχει πράκτορες υλοποιημένους σε Java.

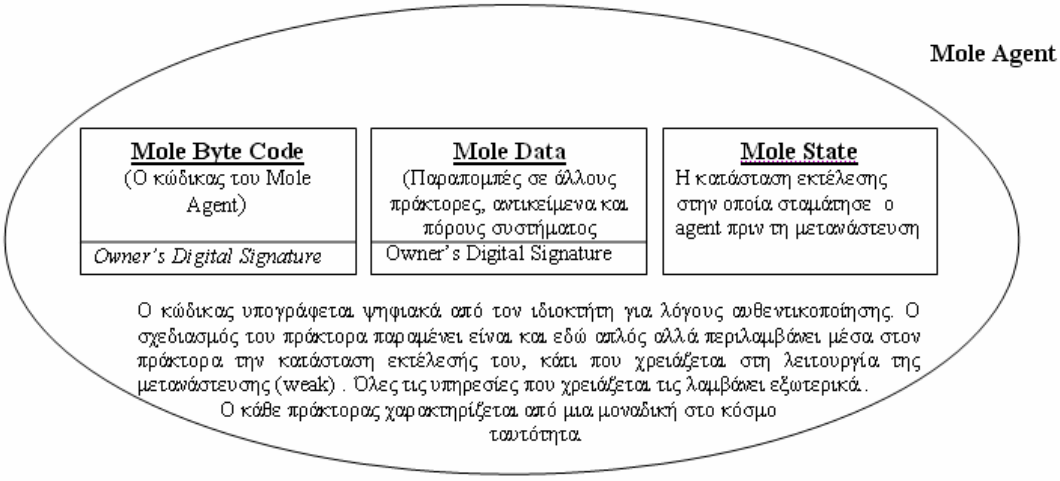


Εικόνα 36 – Διάγραμμα Πλαίσιο: Επικοινωνία μεταξύ διαφορετικών server σε ένα δίκτυο.

3.3.8.3 Mole

Το σύστημα κινητών πρακτόρων Mole αναπτύχθηκε από το Πανεπιστήμιο της Στουτγκάρδης με σκοπό την δημιουργία ενός συστήματος γενικής χρήσης βασισμένο στη Java [83], [84].

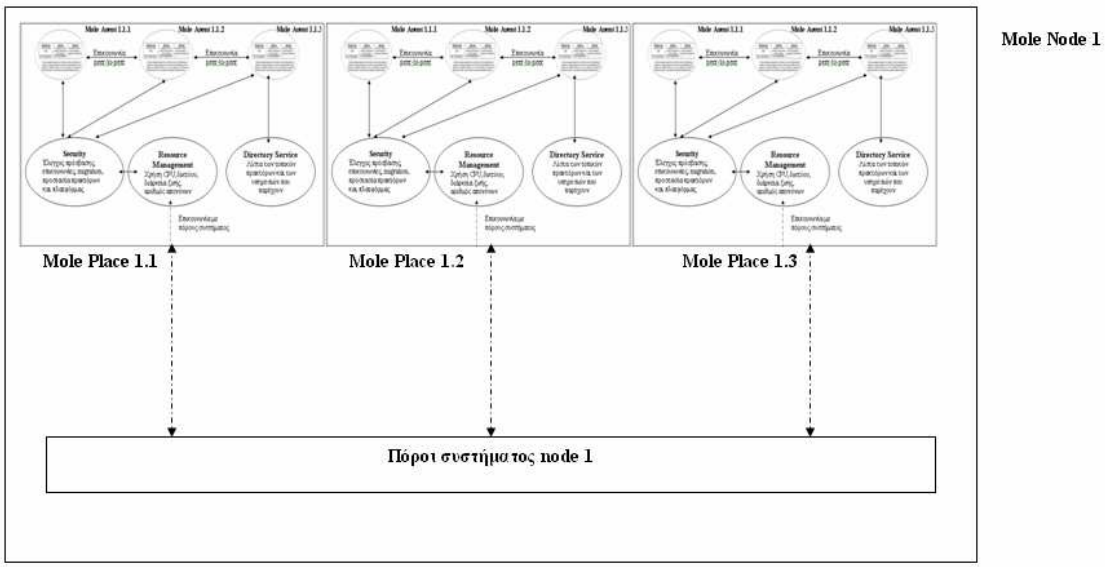
Ο πράκτορας Mole αποτελείται από τον κώδικα, τα δεδομένα του και την κατάστασή του. Ο κώδικας και τα δεδομένα υπογράφονται ψηφιακά από τον ιδιοκτήτη για λόγους αυθεντικοποίησης ενώ δεν γίνεται διαχωρισμός με τον προγραμματιστή – δημιουργό. Ο σχεδιασμός του πράκτορα παραμένει και εδώ απλός, όπως οι περισσότεροι πράκτορες σε Java, αλλά περιλαμβάνει μέσα στον πράκτορα και την κατάσταση εκτέλεσής του, κάτι που χρειάζεται στη λειτουργία της μετανάστευσης. Όλες τις υπηρεσίες που χρειάζεται τις λαμβάνει εξωτερικά.



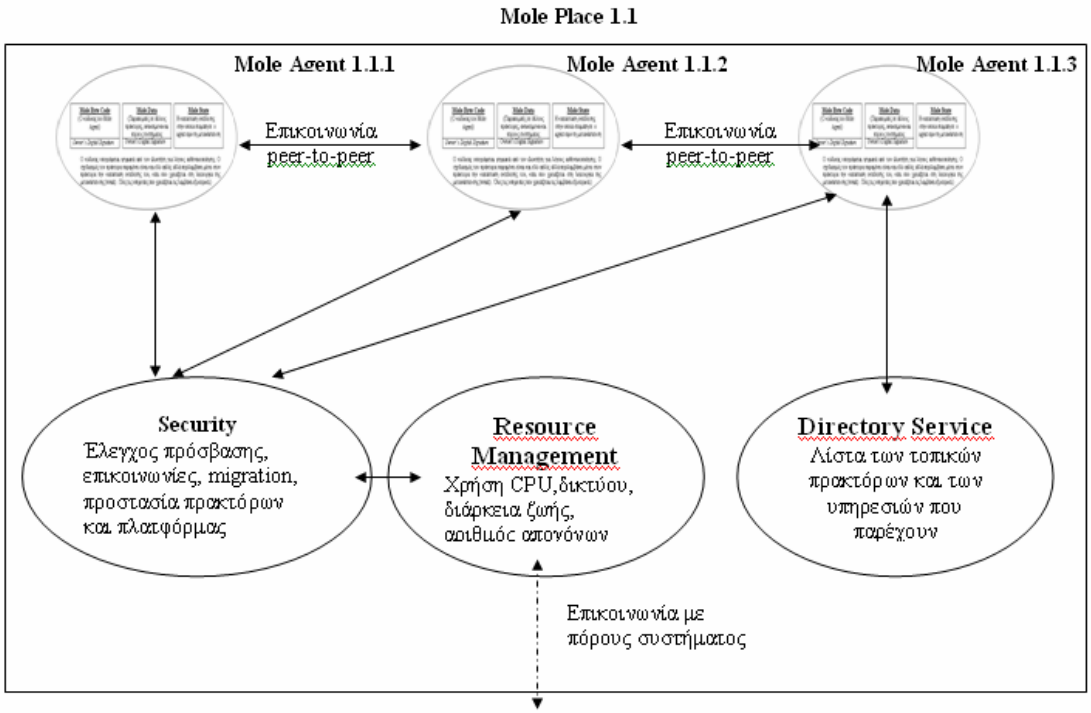
Εικόνα 37 – Διάγραμμα επιπέδου 4: Ένας πράκτορας Mole.

Το μηχάνημα εκτέλεσης των Mole ονομάζεται Mole Node (Εικόνα 38). Υποστηρίζονται ομαδοποιήσεις πρακτόρων μέσα σε ένα Node που ονομάζονται Mole Places (Εικόνα 39). Όλες οι υπηρεσίες της πλατφόρμας υλοποιούνται σε επίπεδο place του οποίου και αποτελούν μέρος και μόνο οι πόροι του συστήματος ανήκουν στο Node. Έτσι διατηρεί απλούστατο σχεδιασμό αλλά μεταφέρει την πολυπλοκότητα στο επίπεδο της επιμέρους ομαδοποίησης. Από τα places παρέχεται έλεγχος πρόσβασης, επικοινωνίες, ασθενής μετανάστευση, προστασία πρακτόρων

και πλατφόρμας, χρήση CPU, δικτύου, καταγράφετε η διάρκεια ζωής και ο αριθμός απογόνων, ενώ παρέχονται υπηρεσίες καταλόγου και επικοινωνία peer-to-peer μεταξύ πρακτόρων του ίδιου place. Οι υπηρεσίες και σε αυτό το σύστημα κινητών πρακτόρων θεωρούνται ως στατικοί πράκτορες.

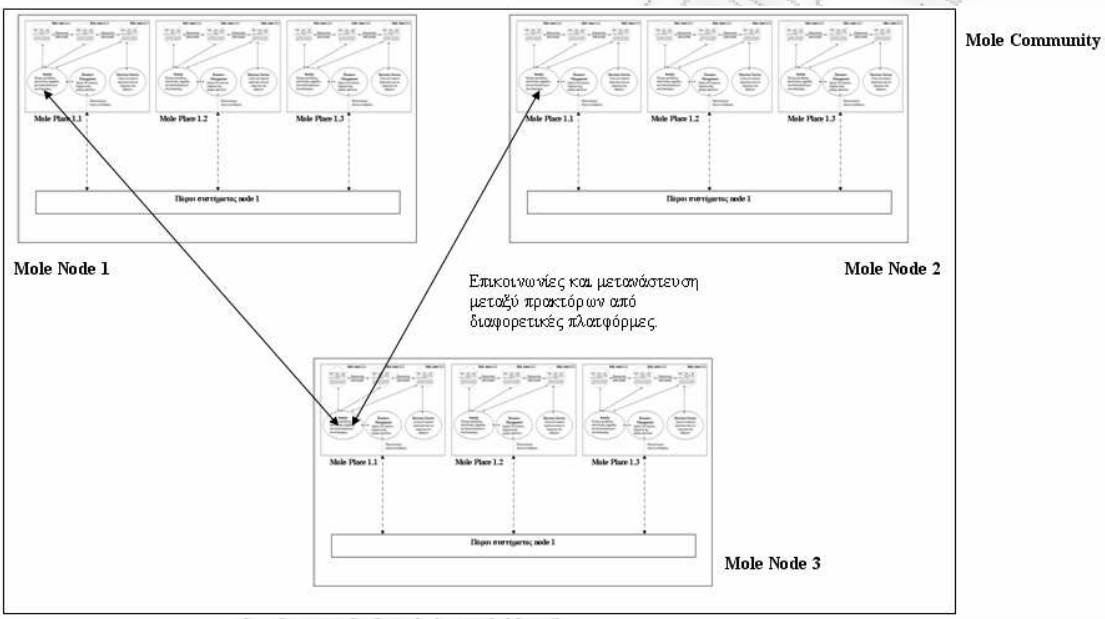


Εικόνα 38 – Διάγραμμα επιπέδου 2: Η πλατφόρμα εκτέλεσης Mole (Mole Node) και τα places που περιλαμβάνει.



Εικόνα 39 – Διάγραμμα επιπέδου 3: Ένα Mole Place.

Στο Mole η ανώτερη οντότητα είναι η Mole Community (Εικόνα 40). Αν και ορίζεται η Community έχει περισσότερο θεωρητική υπόσταση, καθώς δεν υπάρχει κεντρική διαχειριστική οντότητα. Βεβαίως, είναι δυνατή η επικοινωνία και η μετανάστευση μεταξύ διαφορετικών node μέσω ενός δικτύου, οπότε και με αυτόν τον τρόπο υπονοείται ότι υπάρχει κάποιος κοινός διαχειριστής σε όλους τους Node. Αυτό όμως δεν αρκεί για να διαφοροποιήσει το Mole από τα συστήματα χωρίς ανώτερη επικράτεια.

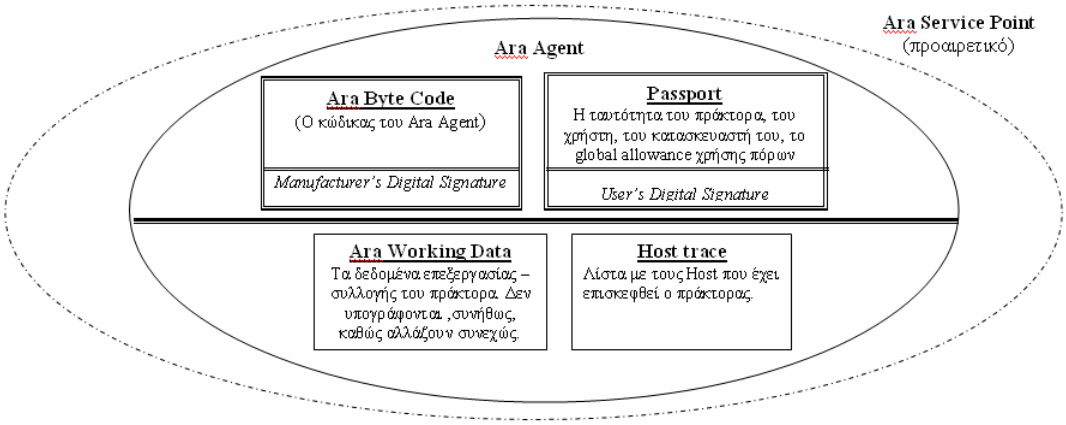


Εικόνα 40 – Διάγραμμα Πλαίσιο: Μια Mole Community. Είναι δυνατή η επικοινωνία και μετανάστευση μεταξύ διαφορετικών node μέσω ενός δικτύου.

3.3.8.4 Ara

Το σύστημα κινητών πρακτόρων Ara αναπτύχθηκε από το Πανεπιστήμιο Kaiserslauern της Γερμανίας. Αποσκοπεί στην ταυτόχρονη χρήση μεγάλου αριθμού γλωσσών προγραμματισμού [85], [86], [87].

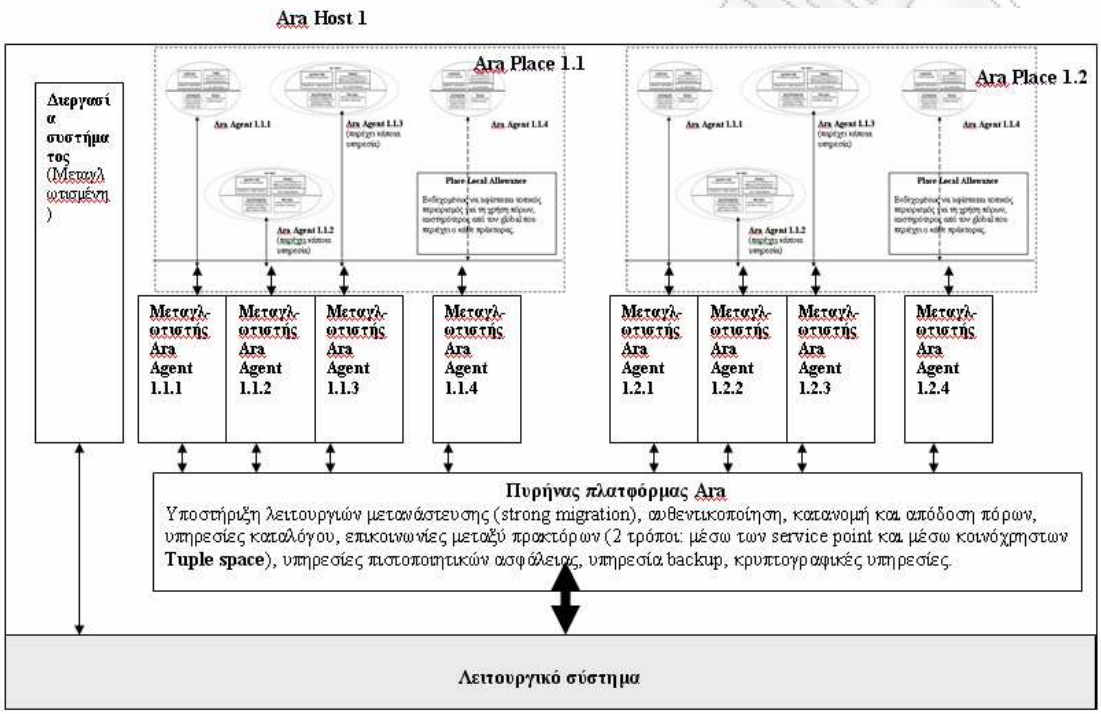
Ο πράκτορας Ara αποτελείται από το κώδικα, τα δεδομένα του, το "διαβατήριο" με τα στοιχεία του και το ιστορικό των host που έχει επισκεφθεί (Εικόνα 41). Ο κώδικας υπογράφεται ψηφιακά από τον κατασκευαστή και το διαβατήριο από τον χρήστη. Ο σχεδιασμός του πράκτορα περιλαμβάνει τα στατικά μέρη, τα οποία και υπογράφονται ψηφιακά και τα μεταβλητά όπου δεν είναι δυνατό να υπογραφούν. Υποστηρίζεται ισχυρή μετανάστευση. Ένας πράκτορας παροχής υπηρεσιών δημιουργεί προαιρετικά ένα service point μέσω του οποίου παρέχει τις υπηρεσίες αυτές (στην Εικόνα 41απεικονίζεται με διακεκομμένη έλλειψη).



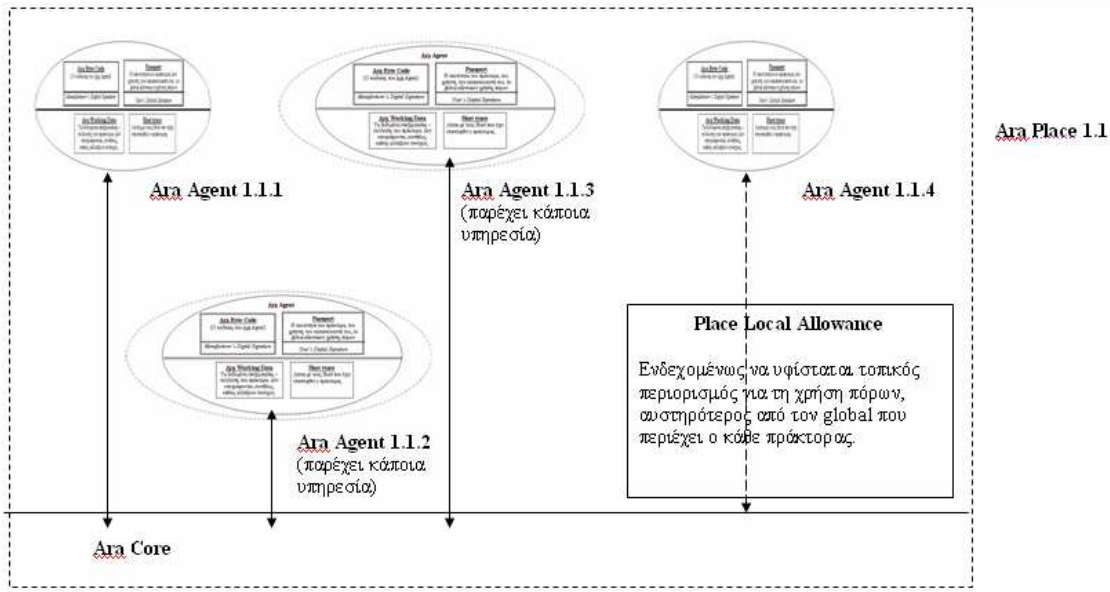
Εικόνα 41 – Διάγραμμα επιπέδου 4: Ένας πράκτορας Ara.

Το μηχάνημα εκτέλεσης των Ara ονομάζεται Ara Host (Εικόνα 42). Υποστηρίζεται ομαδοποίηση πρακτόρων μέσα σε ένα Host που ονομάζονται Ara Place. Ένας πράκτορας μπορεί να δημιουργήσει ένα δικό του Place, το οποίο δεν περιλαμβάνει λειτουργικά μέρη, παρά μόνο τα service points που είναι πράκτορες παροχής υπηρεσιών ή υπηρεσίες του συστήματος. Οι υπόλοιπες υπηρεσίες της πλατφόρμας υλοποιούνται σε επίπεδο Host. Από το Host παρέχεται υποστήριξη

λειτουργιών ισχυρής μετανάστευσης, αυθεντικοποίησης, κατανομής και απόδοσης πόρων, υπηρεσίες καταλόγου, επικοινωνίες μεταξύ πρακτόρων, υπηρεσίες πιστοποιητικών ασφάλειας, υπηρεσία αντιγράφων ασφαλείας και κρυπτογραφικές υπηρεσίες. Υποστηρίζονται, θεωρητικά, πράκτορες όλων των γλωσσών, και ο μεταγλωττιστής λειτουργεί ως διακομιστής μεσολάβησης μεταξύ του πράκτορα και των υπηρεσιών συστήματος.

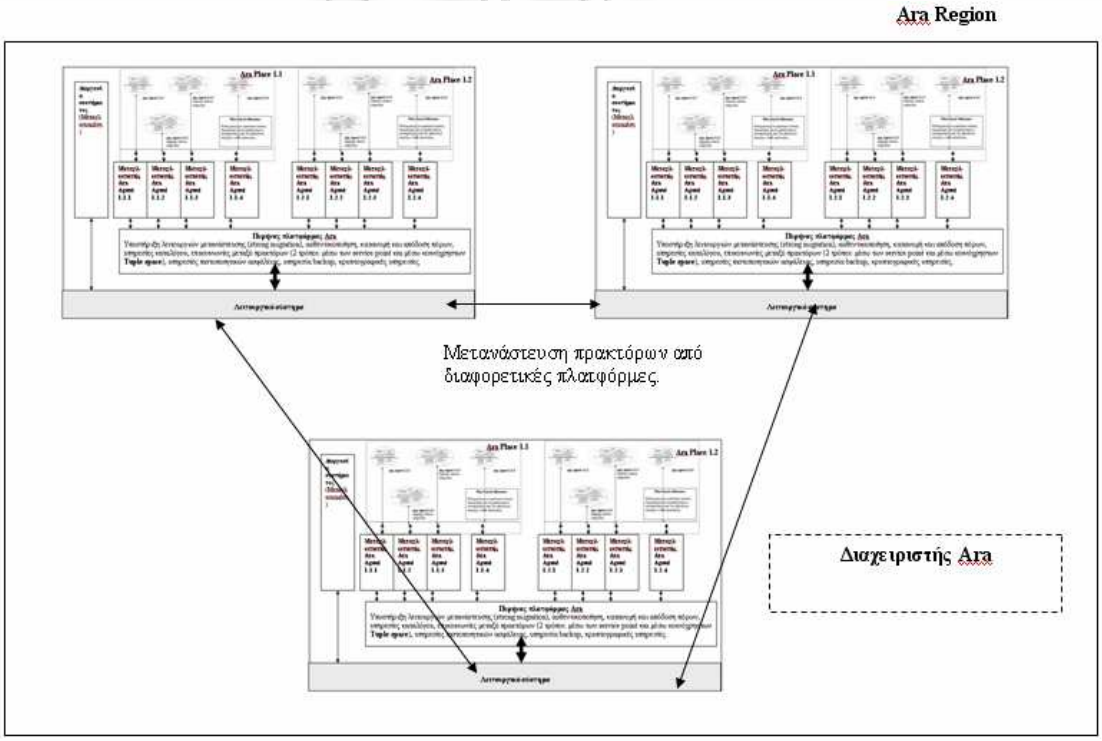


Εικόνα 42 – Διάγραμμα επιπέδου 1: Ένας Ara Host.



Εικόνα 43 – Διάγραμμα επιπέδου 3: Μια τοποθεσία (place) στο Ara.

Στο Ara ανώτερη οντότητα Επικράτειας ορίζεται το Region (Εικόνα 44). Αν και μπορεί να έχει κάποια κοινή διαχείριση, αυτή παραμένει μια θεωρητική έννοια γιατί δεν επιτρέπεται επικοινωνία σε ένα Region. Επιτρέπεται μονάχα μετανάστευση, η οποία συχνά χρησιμοποιείται σαν υποκατάστατο της επικοινωνίας μεταξύ πρακτόρων.



Εικόνα 44 – Διάγραμμα πλαίσιο: Ένα Ara Region.

3.4 Αποτελέσματα Σύγκρισης Αρχιτεκτονικής Ανά Επίπεδο

Σε αυτό τη σημείο γίνεται σύγκριση της αρχιτεκτονική των συστημάτων ανά επίπεδο. Αρχικά παραθέτουμε (Πίνακας 1) τις οντότητες που απαρτίζουν τα συστήματα πρακτόρων που εξετάσαμε και στη συνέχεια ακολουθεί η αντιπαραβολή των εξεταζόμενων συστημάτων ανά επίπεδο. Εκεί γίνεται χρήση μόνον των τριών κυριοτέρων επιπέδων τα οποία και υιοθετούν τα περισσότερα συστήματα (επίπεδο πράκτορα, επίπεδο μηχανήματος εκτέλεσης και ανώτερο επίπεδο, όπου απεικονίζεται ολόκληρος ο κόσμος του συστήματος πρακτόρων).

Όπως βλέπουμε και στον Πίνακα 1, είναι δυνατόν, ανάλογα με τη πολυπλοκότητα της αρχιτεκτονικής του κάθε συστήματος, ορισμένες από τις οντότητες να απουσιάζουν ή να ταυτίζονται με άλλες. Οι οντότητες στον πίνακα παρουσιάζονται ανά στήλες και με σειρά από την ευρύτερη στην αριστερή πλευρά του πίνακα προς τη μικρότερη στη δεξιά. Κάθε εξεταζόμενο σύστημα αποτελεί μια γραμμή του πίνακα. Κρίνουμε ότι αυτό ακριβώς το σύστημα επιτρέπει τη σχηματική παρουσίαση των πλατφορμών κινητών πρακτόρων και την άμεση αντιπαραβολή τους.

Πίνακας 1: Αντιστοιχίες οντοτήτων συστημάτων πρακτόρων

Οντότητα *Σύστημα Πρακτόρων*	**Επικράτεια (Domain)**	**Κατανεμημένη πλατφόρμα εκτέλεσης**	**Πλατφόρμα εκτέλεσης (Agent System)**	**Τοποθεσία πλατφόρμας (Place)**	**Πράκτορας (Agent)**
Aglets	**Domain**	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	**Tahiti Server**	**Context** Υποστηρί-ζεται μια τοποθεσία ανά Server και επομένως ταυτίζονται	**Aglet**
Grasshopper	**Region**	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	**Agency**	**Place**	**Grasshopper Agent – Service** (ο πράκτορας εξομοιώνεται με την υπηρεσία που

					παρέχει)
Concordia	Δεν ορίζεται. Απλά υπάρχουν συνεργαζόμενοι server σε δίκτυο.	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	**Concordia Server**	Δεν ορίζεται.	**Concordia Agent**
Cougaar (DARPA)	**Society** (μια κοινότητα χαρακτηρίζεται από έναν κοινό στόχο → στρατιωτικές εφαρμογές)	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	**Node** (ένα μηχάνημα που τρέχει Java Virtual Machine)	**Community - Enclave** Ορίζεται ως μια ομαδοποί-ηση πρακτόρων με κοινή αντιμετώ-πιση η οποία όμως μπορεί να επεκτείνεται σε πάνω από ένα host. Κοινές υπηρεσίες.	**Cougaar Agent**
JADE	Δεν ορίζεται. Απλά υπάρχουν συνεργαζόμενες πλατφόρμες σε περιβάλλον δικτύου.	**JADE Agent Platform** Τα διάφορα μέρη της (container) εκτελούνται σε διαφορετικά host, σε διαφορετική Java Virtual Machine.	**JADE Container** Υπάρχουν δύο είδη, το front-end container και τα κανονικά	Δεν ορίζεται.	**JADE Agent**
D'Agents	Δεν ορίζεται. Απλά υπάρχουν συνεργαζόμενοι server σε δίκτυο.	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	**D'Agent Server**	Δεν ορίζεται συγκεκρι-μένη οντότητα για την ομαδοποί-ηση πρακτόρων.	**D'Agent** (Java, Tcl, Scheme)
Mole	**Community**	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	**Node**	**Place** Επιτρέπεται η ύπαρξη πολλών places σε ένα node.	**Mole Agent**
Ara	**Region** Host με κοινή	Θεωρητικά δεν αποκλείεται.	**Host** Είναι δυνατόν	**Ara Place** Συνήθως	**Ara Agent** Μπορεί να

	διαχείριση. **Δεν υπάρχει επικοινωνία μεταξύ απομακρυσμένων πρακτόρων**	Στη πράξη η πλατφόρμα με τα διάφορα places εκτελείται σε ένα μηχάνημα.	να υπάρχουν πολλά places σε ένα μηχάνημα.	υπάρχει 1 σε κάθε host. Ένας πράκτορας μπορεί να δημιουργήσει ένα δικό του place.	δημιουργήσει **service point** υπηρεσιών
Mansion	**World**	**Section**	Δεν ορίζεται	**Room**	**Mansion Agent**
Nomads	Δεν ορίζεται. Απλά υπάρχουν συνεργαζόμενοι server σε δίκτυο	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	**Nomad Server – Oasis Execution Environment** Χρησιμοποιείται μια τροποποιημένη έκδοση της Java VM (Aroma)	Δεν ορίζεται συγκεκριμένη οντότητα για την ομαδοποίηση πρακτόρων.	**Nomad Agent**
Havana	**Havana Platform**	Δεν υφίσταται, η πλατφόρμα εκτελείται εξ' ολοκλήρου σε ένα μηχάνημα.	Υπάρχουν δύο είδη Havana Gateway Server, Havana Business Server	Δεν ορίζεται συγκεκριμένη οντότητα για την ομαδοποίηση πρακτόρων.	**Havana Agent**

3.4.1 Κατώτερο Επίπεδο

Στο επίπεδο αυτό παρατηρούμε ότι στις περισσότερες υλοποιήσεις πρακτόρων χρησιμοποιείται η Java. Ως αποτέλεσμα, ο σχεδιασμός παραμένει απλός και ακολουθεί "έτοιμες" λύσεις της συγκεκριμένης πλατφόρμας. Στις περιπτώσεις των Mole, Mansion και Nomads τροποποιείται το συνηθισμένο μοντέλο προκειμένου να υποστηριχθεί η λειτουργία της μετανάστευσης εν γένει μέσα από το πράκτορα. Από τις υλοποιήσεις σε Java τα Ara, Grasshopper, JADE, Cougaar, Aglets, Nomads, Mansion και Havana υποστηρίζουν ολοκληρωμένη ισχυρή μετανάστευση. Η περίπτωση του Cougaar είναι ιδιαίτερη. Δεν μπορεί να συγκριθεί ευθέως με τα υπόλοιπα συστήματα, αφού έχει δημιουργηθεί για αμυντικούς σκοπούς, για χρήση σε δίκτυα υπό επίθεση – κατάρρευση σε συνθήκες πολέμου. Υλοποιεί ασύγκριτα περισσότερες λειτουργίες εντός του πράκτορα, ενώ μπορεί να δεχθεί και τροποποιήσεις - επεκτάσεις με προσθήκες προσθέτων λογισμικού. Είναι ένα ασφαλές σύστημα με πολύ συγκεκριμένο προσανατολισμό, αντίθετα με τα γενικότερης χρηστικότητας υπόλοιπα συστήματα. Στα περισσότερα γίνεται χρήση ψηφιακών υπογραφών για λόγους ακεραιότητας τμημάτων του πράκτορα. Σε κάθε περίπτωση, όμως, μπορούν να υπογραφούν τα τμήματα που δεν αλλάζουν με τη λειτουργία του πράκτορα εκτός από συγκεκριμένες περιπτώσεις, κάτι που αποτελεί περιορισμό της τεχνολογίας. Σε τρία από τα συστήματα (Aglet, Ara και Mansion) γίνεται διαχωρισμός μεταξύ ιδιοκτήτη και δημιουργού του πράκτορα και απαιτείται αντίστοιχα διαφορετική ψηφιακή υπογραφή. Αυτή η πρακτική επιτρέπει την εφαρμογή καλύτερης αλλά περισσότερο σύνθετης πολιτικής εμπιστοσύνης.

3.4.2 Μεσαίο Επίπεδο

Και στο επίπεδο αυτό γίνεται χρήση της Java από τους περισσότερους πράκτορες, η οποία επιβάλλει κάποια ομοιογένεια στην αρχιτεκτονική σε επίπεδο μηχανήματος εκτέλεσης και στις παρεχόμενες υπηρεσίες. Η προσπάθεια όμως των προγραμματιστών να προσφέρουν δυνατότητες πέρα από εκείνες της Java διαφοροποιούν τους εκάστοτε servers σε μεγαλύτερο βαθμό από ότι σε επίπεδο πράκτορα. Όλες οι πλατφόρμες προσφέρουν τις απαραίτητες υπηρεσίες καταλόγου, αυθεντικοποίησης, ελέγχου πόρων, επικοινωνιών, κρυπτογραφίας και μετανάστευσης, αλλά συχνά διαφέρει ο τρόπος που τις παρέχουν. Στην περίπτωση της μετανάστευσης τα περισσότερα συστήματα υποστηρίζουν ισχυρή μετανάστευση (Ara, Grasshopper, JADE, Cougaar, Aglets, Nomads, Mansion και Havana). Και σε αυτό το επίπεδο το Cougaar παρουσιάζει μεγάλη διαφοροποίηση από τις άλλες υλοποιήσεις καθώς προσφέρει πολλαπλά επίπεδα πολιτικών και ελέγχου και, κυρίως, διαθέτει προσαρμοστικότητα με βάση το πώς αντιλαμβάνεται το περιβάλλον. Το συγκεκριμένο χαρακτηριστικό δεν συναντάται αλλού και υποδηλώνει τη στρατιωτική χρήση για την οποία προορίζεται. Τα JADE και Havana είναι τα μοναδικά συστήματα που, αν και βασισμένα στη JVM, διαφοροποιούνται από τα υπόλοιπα χρησιμοποιώντας δύο διαφορετικούς servers ανάλογα με τη χρήση. Τέλος, το Mansion ξεφεύγει τελείως από τη προσέγγιση server-host και την καταργεί τελείως. Αντί αυτού, κατανέμει την πλατφόρμα εκτέλεσής του σε δίκτυο υπολογιστών τοποθετώντας ορισμένες από τις λειτουργίες της σε κάθε μηχάνημα. Ομοίως και με τη χρήση ομαδοποίησης πρακτόρων, ενώ όσα συστήματα τη χρησιμοποιούν την ορίζουν ως υποσύνολο του server, το Mansion την επεκτείνει και αυτή στο δίκτυο. Το Mansion δείχνει ξεκάθαρα το δικτυοκεντρικό του προσανατολισμό αυξάνοντας με αυτό τον τρόπο την πολυπλοκότητα στο σύστημα και δημιουργώντας προβληματισμούς για την αποτελεσματική διαχείρισή του και αξιοπιστία σε περίπτωση προβλημάτων δικτύωσης.

3.4.3 Ανώτερο Επίπεδο

Στο ανώτερο επίπεδο η κατάσταση διαφοροποιείται αρκετά σε σχέση με τα κατώτερα. Η σχετική ομοιογένεια που επέβαλε η τεχνολογία της Java εδώ δεν υφίσταται. Σε αυτό το επίπεδο τα συστήματα πρακτόρων χωρίζονται σε δύο κατηγορίες: εκείνα που ορίζουν ανώτατο επίσημο domain (**Aglets** , **Grasshopper**, **Cougaar, Mole, Ara, Mansion, Havana)** με κάποιας μορφής κεντρική διαχείριση σε επίπεδο πολιτικής, τουλάχιστον, και σε εκείνα που απλά εισάγουν ένα αριθμό server στο δίκτυο (**Nomads, D'Agents, JADE, Concordia)**. Συνήθως, για να μπορεί να γίνει επικοινωνία και ακόμη περισσότερο μετανάστευση μεταξύ "ξένων" server υπονοείται η ύπαρξη κάποιας σχέσης εμπιστοσύνης μεταξύ τους, ίσως δηλαδή κοινή διαχείριση, χωρίς όμως αυτό να ορίζεται. Παραφωνία αποτελεί το Ara που, αν και ορίζει ανώτατη οντότητα, το Region, στη πράξη δεν το χρησιμοποιεί, αφού δεν του εισάγει κάποια ουσιαστική λειτουργικότητα – διαχειριστική εξουσία. Επίσης, για λόγους ασφάλειας δεν επιτρέπει την επικοινωνία μεταξύ πρακτόρων διαφορετικών hosts αλλά επιτρέπει τη μετανάστευση μεταξύ τους. Σε γενικές γραμμές η ύπαρξη ενός ανώτατου επιπέδου πέρα από τα όρια μιας πλατφόρμας σε ένα μηχάνημα διευρύνει τη λειτουργικότητα του συστήματος και προσθέτει ένα ακόμη επίπεδο ασφάλειας που επιτρέπει την εισαγωγή κάποιων ελάχιστων επιπέδων ασφάλειας.

3.4.4 Συμπεράσματα Σύγκρισης Επιπέδων

Από τη παρούσα σύγκριση διαπιστώνουμε ότι σε γενικές γραμμές υπάρχει μια ομοιομορφία στην αρχιτεκτονική των συστημάτων, τουλάχιστον στα χαμηλότερα επίπεδα, ενώ υπάρχουν κάποιες σημαντικές διαφοροποιήσεις. Η γενική ομοιομορφία απορρέει από τη χρήση της Java και των μηχανισμών ασφάλειας που παρέχει η Java Virtual Machine. Είναι γεγονός ότι παρέχει μια πλατφόρμα ανάπτυξης με πολλά έτοιμα εργαλεία, κατάλληλα για δικτυακές εφαρμογές και εκτέλεση κινητού κώδικα με σχετική ασφάλεια. Έτσι, ξεκινώντας από το επίπεδο του πράκτορα, παρατηρούμε ότι οι περισσότεροι πράκτορες έχουν απλό σχεδιασμό,

καθώς βασικά περιλαμβάνουν το κώδικα λειτουργίας και τα αρχικά δεδομένα. Ως στοιχειώδες μέτρο ασφάλειας αυτοί υπογράφονται ψηφιακά, προστατεύοντας έτσι την ακεραιότητά τους. Το μειονέκτημα όμως είναι ότι δεν είναι δυνατόν να είναι υπογεγραμμένος ολόκληρος ο πράκτορας, παρά μόνον τα τμήματά του που δεν τροποποιούνται κατά την εκτέλεσή του (ο κώδικας), αποτελώντας απειλή για την ασφάλεια. Το **Ara**, το **Mansion** και το **Havana** χρησιμοποιούν ένα πρόσθετο μέτρο ασφάλειας σε επίπεδο πράκτορα: αποθηκεύουν το ιστορικό των μεταναστεύσεων του πράκτορα για λόγους εντοπισμού εισβολών. Καθώς, λοιπόν, διατηρούν απλό σχεδιασμό, όλες οι υπηρεσίες τους παρέχονται από την πλατφόρμα εκτέλεσης. Έτσι, όμως, δημιουργείται πρόβλημα ασφάλειας στην περίπτωση κακόβουλης πλατφόρμας. Διαφορετική προσέγγιση ακολουθεί το σύστημα **Cougaar**, το οποίο λόγω του ότι προορίζεται για χρήση σε στρατιωτικές εφαρμογές, ακολουθεί ένα πιο σύνθετο σχεδιασμό με πρώτη προτεραιότητα την ασφάλεια. Περιλαμβάνει μέσα στον ίδιο τον πράκτορα πολλές από τις βασικές λειτουργίες που παρέχονται εξωτερικά στα υπόλοιπα συστήματα. Με αυτόν τον τρόπο εκτίθεται λιγότερο στην πλατφόρμα αλλά αυξάνει τη πολυπλοκότητα ενδεχομένως σε βάρος των επιδόσεων. Παρόλ' αυτά όμως ο προσανατολισμός του απαιτεί ασφαλή εκτέλεση περιορισμένων κρίσιμων λειτουργιών κάτι για το οποίο είναι καταλληλότερος από τα υπόλοιπα συστήματα.

Ομοίως και σε επίπεδο μηχανήματος εκτέλεσης διατηρείται μια σχετική ομοιομορφία και πάλι λόγω χρήσης Java. Στις περισσότερες πλατφόρμες "τρέχει" Java Virtual Machine η οποία ουσιαστικά υπαγορεύει τμήματα της αρχιτεκτονικής και των παρεχόμενων υπηρεσιών σε επίπεδο ασφάλειας. Σε αυτό οφείλεται και ο περιορισμός των συστημάτων στο είδος της μετανάστευσης που μπορούν να κάνουν (ασθενής) καθώς δεν τους επιτρέπεται να μεταφέρουν ακριβώς την κατάσταση στην οποία σταμάτησαν την εκτέλεσή τους στον προηγούμενο host. Εξαίρεση αποτελούν τα **Aglets**, **Grasshopper**, **Cougaar, Mole, Ara, Mansion, Havana**. Και εδώ το Cougaar χρησιμοποιεί διαφορετική αρχιτεκτονική, κεντρικοποιημένη και σύνθετη, με εφαρμογή πολιτικών για όλες τις παραμέτρους λειτουργίας και κάνει χρήση ενός πρωτότυπου μηχανισμού προσαρμοστικότητας. Αντίθετα, το Mansion κατανέμει τις λειτουργίες της πλατφόρμας σε δίκτυο και μάλιστα με συχνή επανάληψή τους. Η

συγκεκριμένη προσέγγιση δημιουργεί ερωτηματικά στην ευκολία και την ποιότητα λειτουργίας και διαχείρισης.

Στο ανώτερο επίπεδο η διαφοροποίηση μεγαλώνει καθώς άλλες πλατφόρμες ορίζουν ανώτερη οντότητα – διαχειριστή και άλλες όχι, αρκούμενες στην ασφάλεια που παρέχει ένα μηχάνημα – πλατφόρμα.

Σε γενικές γραμμές η κεντρικοποιημένη δομή και οργάνωση με διαφορετικά επίπεδα ασφάλειας μάλλον αποτελεί καταλληλότερο περιβάλλον ανάπτυξης για πράκτορες. Από την πλευρά της ασφάλειας είναι καλύτερο αλλά ενδεχομένως να αποδειχθεί “ακριβότερο” από πλευράς πόρων συστήματος. Είναι πάντως βέβαιο ότι με τη δημιουργία ενός γενικότερου πλαισίου λειτουργίας που διαθέτει κεντρικοποιημένη διαχείριση ασφάλειας διαμορφώνεται ένα “έμπιστο” περιβάλλον, όπου ένας πράκτορας διαφορετικής πλατφόρμας μπορεί να εκτελεστεί χωρίς σημαντικούς περιορισμούς απόδοσης πόρων.

3.5 Αποτελέσματα Ανάλυσης με Βάση τα Κριτήρια Σύγκρισης

Έχοντας εξετάσει τα χαρακτηριστικά ασφάλειας και την αρχιτεκτονική των συστημάτων πρακτόρων προχωρούμε στη σύγκρισή τους. Αρχικά, παρατίθενται ορισμένες ομοιότητες που εντοπίστηκαν στην αρχιτεκτονική τους και στη συνέχεια πραγματοποιείται η σύγκριση των συστημάτων που εξετάστηκαν, με βάση τα κριτήρια που τέθηκαν στο προηγούμενο κεφάλαιο. Επιπλέον, η σύγκρισή των συστημάτων αποτυπώνεται συνοπτικά στους Πίνακα 2 και Πίνακα 3.

Όλα τα συστήματα που εξετάζουμε βασίζονται στην Java, η οποία και χρησιμοποιείται ευρέως σε εφαρμογές κινητού κώδικα, λόγω των εξειδικευμένων λειτουργιών που παρέχει [21], [25], [92]. Πιο συγκεκριμένα, στον τομέα της ασφάλειας, η Java διαθέτει το μηχανισμό Java Sandbox που επιτρέπει την εκτέλεση κώδικα άλλων οντοτήτων. Εξαίρεση αποτελούν το Mansion και τα D' Agents που, πέρα από τη Java, υποστηρίζουν και επιπλέον γλώσσες.

Όλα τα συστήματα διαθέτουν τα δικό τους μοντέλο ασφάλειας και εμπιστοσύνης, το οποίο χρησιμοποιεί διάφορους τυποποιημένους μηχανισμούς ασφάλειας, όπως SSL, ψηφιακές υπογραφές και συστήματα ελέγχου πρόσβασης και αυθεντικοποίησης με βάση την ταυτότητα του χρήστη. Αυτοί οι μηχανισμοί, είναι δυνατόν να χρησιμοποιηθούν ή όχι, ανάλογα με τις απαιτήσεις ασφάλειας της κάθε εφαρμογής.

Η ακεραιότητα του πράκτορα επιδιώκεται με παρόμοιες μεθόδους σε όλες τις πλατφόρμες που εξετάσαμε. Συγκεκριμένα χρησιμοποιούν την ψηφιακή υπογραφή του χρήστη – ιδιοκτήτη του πράκτορα καθώς και το ασφαλές περιβάλλον που παρέχει (από απειλές άλλων πρακτόρων) η Java. Επιπλέον αυτών, το Cougaar προσφέρει τη δυνατότητα της προσθήκης χαρακτηριστικών ασφάλειας στους ίδιους τους πράκτορες με τη χρήση πρόσθετων λογισμικού. Ακόμη, τα Aglets και Mansion προσφέρουν επιπλέον χαρακτηριστικά για την προστασία των πρακτόρων τους. Τα Aglets χρησιμοποιούν στον κάθε πράκτορα ένα διακομιστή μεσολάβησης και ένα μηχανισμό εντοπισμού εισβολών, ενώ το Mansion χρησιμοποιεί την υπηρεσία Agent Management Service ως μεσάζοντα και επιπλέον χρησιμοποιεί ένα σύστημα ελέγχου. Πρέπει να σημειωθεί ότι όλοι οι παραπάνω μηχανισμοί ασφάλειας όλων

των συστημάτων που εξετάσαμε εστιάζουν στην αντιμετώπιση απειλών που προέρχονται από άλλους πράκτορες και όχι από την πλατφόρμα εκτέλεσης.

Όλα τα συστήματα επιδιώκουν την προστασία της πλατφόρμας με τη χρήση του Java Sandbox. Και σε αυτό το κριτήριο, στο Cougaar η ασφάλεια ενισχύεται με τη χρήση του ενσωματωμένου μηχανισμού εντοπισμού εισβολών. Στο Nomads, αντίθετα, η ακεραιότητα της πλατφόρμας ενισχύεται με τη χρήση του προηγμένου μηχανισμού διαχείρισης πόρων που διαθέτει και μπορεί να περιορίσει τους πόρους που έχουν ανατεθεί στην περίπτωση ενός κακόβουλου πράκτορα.

Οι επικοινωνίες διασφαλίζονται με τη χρήση τυποποιημένων κρυπτογραφικών αλγορίθμων, όπως ο SSL, και με τη χρήση πιστοποιητικών στα περισσότερα συστήματα. Οι μηχανισμοί αυτοί μπορεί να ενεργοποιηθούν ή όχι, ανάλογα με τις ανάγκες της κάθε εφαρμογής. Το Cougaar έχει τη δυνατότητα να προσαρμόζει δυναμικά το επίπεδο της ασφάλειας των επικοινωνιών, ανάλογα με τις απειλές που αντιμετωπίζονται, χρησιμοποιώντας την Security Adaptive Engine που διαθέτει. Στα Aglets, αντίθετα, χρησιμοποιούνται μονάχα τα MIC με βάση ένα μονάχα κοινό μυστικό κλειδί για όλες τις οντότητες του Κόσμου. Τέλος το Nomads δεν ορίζει κρυπτογραφικές τεχνικές και στηρίζεται σε όποια μέτρα ασφάλειας υλοποιούνται σε επίπεδο λειτουργικού συστήματος.

Στο Concordia, το JADE, το Mansion και το Havana, ο πράκτορας αυθεντικοποιείται χρησιμοποιώντας την ψηφιακή υπογραφή του χρήστη. Αντίθετα, στο JADE προσφέρεται η επιπλέον δυνατότητα της αυθεντικοποίησης με τη χρήση ενός κοινού μυστικού κλειδιού μέσω ενός συστήματος Kerberos. Παρόμοιος μηχανισμός με ένα κοινό κλειδί χρησιμοποιείται στα Aglets, που όμως αποτελεί τη μοναδική μέθοδο αυθεντικοποίησης σε αυτό στο σύστημα. Το Mansion κάνει χρήση Self-certifying Identifiers τα οποία όμως υπογράφονται μόνον από τον ιδιοκτήτη τους (self-signed) και όχι από κάποια Έμπιστη Τρίτη Όντότητα (TTP). Στο Grasshopper πραγματοποιείται αμοιβαία αυθεντικοποίηση μεταξύ χρήστη και πλατφόρμας. Στο Cougaar όλες οι οντότητες που ορίζονται (actors – χρήστες, πράκτορες ή πρόσθετα λογισμικού) και είναι δυνατόν να αλληλεπιδρούν καθώς και η πλατφόρμα μπορούν να αυθεντικοποιούνται αμοιβαία, ανάλογα με την εφαρμογή.

Και σε αυτό το κριτήριο σύγκρισης τα Nomads δεν ορίζουν την αυθεντικοποίηση άλλης οντότητας πέρα από τους χρήστες.

Όλα τα συστήματα που εξετάσαμε βασίζουν τον έλεγχο πρόσβασης στην αυθεντικοποίηση, όπως είναι αναμενόμενο, και κάνουν χρήση λιστών με χρήστες. Η διαχείριση είναι αντίστοιχη. Γίνεται ανάλογα με την ταυτότητα του χρήστη και στηρίζεται σε μηχανισμούς που παρέχονται από την Java. Στην περίπτωση του Nomads η διαχείριση πόρων διαφοροποιείται και γίνεται χρήση ενός δυναμικού συστήματος που μπορεί να θέσει λεπτομερείς περιορισμούς (ρυθμού και ποσοτικούς) για όλους τους πόρους της πλατφόρμας.

Όλα τα συστήματα παρέχουν δυνατότητα ισχυρής μετανάστευσης των πρακτόρων σε άλλες πλατφόρμες κατά την οποία μετακινείται η πιο πρόσφατη κατάσταση εκτέλεσης του πράκτορα στη νέα πλατφόρμα. Το Mansion αν και υποστηρίζει ισχυρή μετανάστευση την επιτρέπει μόνον μεταξύ προκαθορισμένων έμπιστων δωματίων, ενώ το Nomads υποστηρίζει επιπλέον και αναγκαστική μετανάστευση, διαφανή προς τον πράκτορα. Εξαίρεση στη δυνατότητα ισχυρής μετανάστευσης αποτελεί το Concordia, το οποίο παρέχει δυνατότητα μετανάστευσης μόνον σε προκαθορισμένα στάδια της εκτέλεσης του πράκτορα. Κάτι τέτοιο ενδέχεται να είναι περιοριστικό για κάποια είδη εφαρμογών

Το μοντέλο εμπιστοσύνης που υιοθετείται από όλα τα συστήματα είναι παρόμοιο αν και σε κάποια σημεία διαφοροποιείται. Πιο αναλυτικά, ο πράκτορας θεωρείται έμπιστος αν ανήκει σε τοπικό χρήστη ή σε αυθεντικοποιημένο χρήστη της ίδιας Επικράτειας (εάν αυτή ορίζεται). Σε κάθε περίπτωση, η πλατφόρμα θεωρείται εξ’ ορισμού ως έμπιστη από τους πράκτορες που εκτελούνται σε αυτή. Συγκεκριμένα στο Cougaar οι υποθέσεις εμπιστοσύνης μπορεί να διαφοροποιηθούν, ανάλογα με την εφαρμογή που υλοποιείται. Το Mansion δημιουργεί μια σύνθετη ιεραρχία εμπιστοσύνης, με βάση το κλειδί του ιδιοκτήτη του Κόσμου. Διάφορα δωμάτια και ζώνες μπορούν να συμμετέχουν στον ίδιο Κόσμο, χωρίς απαραίτητα να εμπιστεύονται μεταξύ τους. Ιδιαίτερο ενδιαφέρον παρουσιάζει το Havana το οποίο χρησιμοποιεί ένα απλό μοντέλο εμπιστοσύνης, στο οποίο όλες οι οντότητες δεσμεύονται από ένα πραγματικό εμπορικό συμβόλαιο, με ιδιαίτερες συνέπειες για

την οντότητα που θα το αθετήσει. Έτσι, όλες οι οντότητες μέσα στην Επικράτεια του Havana θεωρούνται έμπιστες.

Τέλος, όλα τα συστήματα εκτός από το Concordia υποστηρίζουν κεντρικοποιημένη πολιτική ασφάλειας, η οποία αυξάνει συνολικά το επίπεδο ασφάλειας αλλά και το επίπεδο λειτουργικότητας μέσα σε μια Επικράτεια. Το Mansion αν και ορίζει ένα κεντρικό διαχειριστή που διαχειρίζεται και θέματα ασφάλειας ενός κόσμου, ορίζει επιπλέον επιμέρους διαχειριστές στα διάφορα υποσύνολά του που μπορούν να διαμορφώσουν ανεξάρτητα τη δική τους πολιτική. Με αυτήν την προσέγγιση, όμως, η διαχείριση της πολιτικής ασφάλειας κατανέμεται μέσα στον Κόσμο του Mansion.

Πίνακας 2: Αποτελέσματα Ανάλυσης με Βάση τα Κριτήρια Σύγκρισης (1/2)

Κριτήρια	Grasshopper	Concordia	JADE	Cougaar
Ακεραιότητα πράκτορα	Ψηφιακή υπογραφή χρήστη, προστασία Java	Ψηφιακή υπογραφή χρήστη, προστασία Java	Ψηφιακή υπογραφή χρήστη, προστασία Java	Ψηφιακή υπογραφή χρήστη, προστασία Java, μπορεί να αναβαθμιστεί με τη χρήση plug-in στον πράκτορα
Ακεραιότητα πλατφόρμας εκτέλεσης	Java Sandbox	Java Sandbox	Java Sandbox	Java Sandbox, σύστημα εντοπισμού εισβολών
Ασφάλεια επικοινωνιών	Ευέλικτη, SSL, X. 509	Ευέλικτη, SSL, VeriSign	Ευέλικτη, SSL, X. 509	Ευέλικτη, προσαρμοστική, αναβαθμιζόμενη
Μοντέλο αυθεντικοποίησης	Αμοιβαία αυθεντικοποίηση με πλατφόρμα με τη χρήση υπογραφών	Αυθεντικοποίηση με βάση την ψηφιακή υπογραφή του χρήστη	Αυθεντικοποίηση με βάση την ψηφιακή υπογραφή του χρήστη ή με χρήση Kerberos	Ανάλογα με την εφαρμογή, αμοιβαία αυθεντικοποίηση actors και πλατφόρμας, χρήση συνθηματικών ή υπογραφών
Έλεγχος πρόσβασης	Λίστες ελέγχου πρόσβασης με ομαδοποιήσεις χρηστών	Λίστες ελέγχου πρόσβασης με ομαδοποιήσεις χρηστών	Λίστες ελέγχου πρόσβασης με ομαδοποιήσεις χρηστών	Λίστες ελέγχου πρόσβασης με ομαδοποιήσεις χρηστών
Διαχείριση πόρων	Java	Java	Java	Java
Δυνατότητα μετανάστευσης	Ισχυρή	Ασθενής	Ισχυρή	Ισχυρή
Μοντέλο εμπιστοσύνης	Η πλατφόρμα θεωρείται εξ ορισμού ως έμπιστη, ο πράκτορας ανάλογα με τον χρήστη του.	Η πλατφόρμα θεωρείται εξ ορισμού ως έμπιστη, ο πράκτορας ανάλογα με τον χρήστη του.	Η πλατφόρμα θεωρείται εξ ορισμού ως έμπιστη, ο πράκτορας ανάλογα με τον χρήστη του.	Ανάλογα με την εφαρμογή, οι αυθεντικοποιημένοι actors θεωρούνται έμπιστοι
Κεντρικοποιημένη διαχείριση ασφάλειας	Ναι (Region Registry)	Όχι	Ναι (Front-End Container)	Ναι (Society Authority)

Πίνακας 3: Αποτελέσματα Ανάλυσης με Βάση τα Κριτήρια Σύγκρισης (2/2)

Κριτήρια	Aglets	Nomads	Mansion	Havana
Ακεραιότητα πράκτορα	Ψηφιακή υπογραφή χρήστη, agent proxy, σύστημα εντοπισμού εισβολών	Προστασία από το περιβάλλον εκτέλεσης Oasis	Ψηφιακή υπογραφή χρήστη, Agent Management Service, audit, προστασία εικονικής μηχανής	Ψηφιακή υπογραφή χρήστη, προστασία Java
Ακεραιότητα πλατφόρμας εκτέλεσης	Java Sandbox, σύστημα εντοπισμού εισβολών	Oasis (JVM), περιορισμός πόρων εκτέλεσης	Java Sandbox	Java Sandbox
Ασφάλεια επικοινωνιών	MIC, κοινό μυστικό κλειδί κόσμου	Δεν διευκρινίζεται	SSL	SSL
Μοντέλο αυθεντικοποίησης	Αυθεντικοποίηση με βάση το κοινό μυστικό κλειδί κόσμου	Δεν διευκρινίζεται	Αμοιβαία αυθεντικοποίηση με βάση υπογραφές, Self-certifying Identifiers	Αυθεντικοποίηση οντοτήτων με βάση τις υπογραφές
Έλεγχος πρόσβασης	Λίστες ελέγχου πρόσβασης με ομαδοποιήσεις χρηστών	Λίστες ελέγχου πρόσβασης με ομαδοποιήσεις χρηστών	Λίστες ελέγχου πρόσβασης με ομαδοποιήσεις χρηστών	Λίστες ελέγχου πρόσβασης με όλες τις εγγεγραμμένες οντότητες
Διαχείριση πόρων	Java	Δυναμική, περιορισμοί ποσοτικοί και ρυθμού	VM, ο χρήστης χρησιμοποιεί μονάχα τους πόρους του δωματίου που βρίσκεται	Java
Δυνατότητα μετανάστευσης	Ισχυρή, χρησιμοποιεί http tunneling	Ισχυρή, εξαναγκασμένη	Ισχυρή, μέσω υπαρχόντων υπερσυνδέσμων, χρήση πρωτοκόλλου παράδοσης	Ισχυρή
Μοντέλο εμπιστοσύνης	Οι server ίδιου κόσμου θεωρούνται έμπιστοι, η πλατφόρμα θεωρείται έμπιστη, ο πράκτορας ανάλογα με τον χρήστη του.	Οντότητες ίδιου κόσμου θεωρούνται έμπιστες, η πλατφόρμα θεωρείται έμπιστη, ο πράκτορας ανάλογα με τον χρήστη του.	Αλυσίδα εμπιστοσύνης με βάση το κλειδί ιδιοκτήτη κόσμου, η πλατφόρμα θεωρείται έμπιστη, ο πράκτορας ανάλογα με τον χρήστη του.	Κλειστός και άρα έμπιστος κόσμος, όλες οι οντότητες δεσμεύονται από πραγματικό συμβόλαιο

Κεντρικο-ποιημένη διαχείριση ασφάλειας	Ναι (Domain Authority)	Υποδηλώνεται κοινή διαχείριση ασφάλειας στον ίδιο κόσμο	Διάφοροι τοπικοί διαχειριστές σε κάθε ζώνη και δωμάτιο	Ναι (Gateway) (κλειστό περιβάλλον)

3.6 Αποτελέσματα Ανάλυσης με Βάση Σενάρια Απειλών

Σε αυτό το σημείο προχωρούμε στη σύγκριση των συστημάτων κινητών πρακτόρων που έχουμε εξετάσει, όσον αφορά στην αντίδρασή τους στα σενάρια απειλών που θέσαμε στο δεύτερο κεφάλαιο της παρούσας διατριβής. Μετά την ανάλυση που ακολουθεί, παρατίθενται τα αποτελέσματά της συνοπτικά στον Πίνακα 4.

Όσον αφορά στην πρώτη απειλή, εκείνη του κακόβουλου πράκτορα, όλα τα συστήματα χρησιμοποιούν το Java Sandbox, το οποίο είναι σχεδιασμένο για εκτέλεση μη έμπιστου κώδικα [21]. Το περιβάλλον απομονωμένης εκτέλεσης που παρέχει μπορεί να προστατεύσει την πλατφόρμα ή άλλους πράκτορες από το να επικοινωνήσουν κατευθείαν με την κακόβουλη οντότητα, τουλάχιστον έως ενός σημείου. Παρόλ' αυτά ένας έμπιστος πράκτορας που παρουσιάζει κακόβουλη συμπεριφορά αποτελεί μια σημαντική απειλή, καθώς του έχει δοθεί πρόσβαση σε πόρους συστήματος και πληροφορίες, ακόμη και με τη χρήση του Java Sandbox. Το Cougaar, το Aglets, το Nomads, το Mansion και το Havana υλοποιούν πρόσθετους μηχανισμούς που απευθύνονται στη συγκεκριμένη απειλή. Πιο συγκεκριμένα, το Aglets, το Cougaar και το Nomads χρησιμοποιούν ενσωματωμένο σύστημα εντοπισμού εισβολών, που παρακολουθεί τις ενέργειες των πρακτόρων για ύποπτη συμπεριφορά. Στην περίπτωση του Nomads, κατά το σενάριο του κακόβουλου πράκτορα, το σύστημα θα προχωρήσει στον άμεσο περιορισμό των πόρων που έχουν αποδοθεί στον πράκτορα. Το Mansion, πέρα από τους μηχανισμούς της Java Virual Machine, εφαρμόζει ένα μηχανισμό ελέγχου και στη περίπτωση κακόβουλης συμπεριφοράς πράκτορα μειώνεται αντίστοιχα το επίπεδο εμπιστοσύνης που αποδίδεται στον ιδιοκτήτη του. Το Havana, τέλος, χρησιμοποιεί τις ισχυρές υπηρεσίες μη αποποίησης που παρέχει η Gateway για την κατανομή ευθύνης στην περίπτωση κακόβουλης συμπεριφοράς. Αν και αυτή η προσέγγιση διαφοροποιείται από τις τεχνικές προσεγγίσεις των υπολοίπων συστημάτων, μπορεί να αποδειχθεί πολύ αποτελεσματική στο εμπορικό περιβάλλον του Havana, όπου όλες οι οντότητες δεσμεύονται από ένα πραγματικό συμβόλαιο.

Η απειλή της κακόβουλης πλατφόρμας αντιμετωπίζεται με διάφορους τρόπους στα συστήματα που εξετάσαμε, αν και κατά βάση όλα θεωρούν ότι μια αυθεντικοποιημένη πλατφόρμα εκτέλεσης θεωρείται ως έμπιστη από πράκτορες που προέρχονται από το ίδιο διαχειριστικό περιβάλλον (π.χ. από την ίδια Επικράτεια). Κάποια από τα συστήματα δεν υλοποιούν κανένα σχετικό μηχανισμό ασφάλειας. Συγκεκριμένα το μοντέλο εμπιστοσύνης του Grasshopper στηρίζεται αποκλειστικά σε αυτή την παραδοχή για τη διασφάλιση της ακεραιότητας του πράκτορα, το οποίο μπορεί να αποδειχθεί ιδιαίτερα επικίνδυνο στην περίπτωση που μια πλατφόρμα γίνει κακόβουλη. Αντίστοιχα, τα μοντέλα εμπιστοσύνης των JADE, Nomads και Mansion στηρίζονται και αυτά μόνο στην υπόθεση ότι η πλατφόρμα εκτέλεσης είναι έμπιστη. Όμως, ο σχεδιασμός τους υποδηλώνει ότι προορίζονται για χρήση μεταξύ αλληλοσυνεργαζόμενων πλατφορμών εκτέλεσης, ή στην περίπτωση του Mansion μεταξύ αλληλοσυνεργαζόμενων υποσυνόλων του κόσμου. Η αποτελεσματικότητα αυτής της προσέγγισης ενδέχεται να είναι περιορισμένη, καθώς είναι δυνατόν μια πλατφόρμα να γίνει κακόβουλη κάτω από συγκεκριμένα σενάρια. Ομοίως το Cougaar στηρίζεται στην ίδια υπόθεση, οπότε είναι δυνατή μια επίθεση από κακόβουλη πλατφόρμα. Όμως ο κίνδυνος αυτός περιορίζεται από τη φύση του κλειστού δικτυακού περιβάλλοντος. Καθώς το Cougaar αναπτύχθηκε για στρατιωτικές εφαρμογές, βασίζεται στην αμοιβαία αυθεντικοποίηση οντοτήτων, κλειστά δίκτυα, ανθεκτικό υλικό (tamper-resistant hardware) και ιδιωτικά κανάλια επικοινωνίας. Όλα αυτά τα χαρακτηριστικά αφήνουν ελάχιστο περιθώριο για την ύπαρξη κακόβουλης πλατφόρμας. Αντίθετα, τα Aglets επιδιώκουν να αντιμετωπίσουν αυτή την απειλή με τη χρήση ενός διακομιστή μεσολάβησης, ενσωματωμένου μέσα στον πράκτορα. Και αυτή η προσέγγιση μπορεί να μην είναι ιδιαίτερα αποτελεσματική, καθώς η κακόβουλη πλατφόρμα μπορεί να επιχειρήσει να παρέμβει στη λειτουργία του διακομιστή μεσολάβησης, ο οποίος εκτελείται τοπικά στην πλατφόρμα. Τέλος, το Havana δεν χρησιμοποιεί κανένα μηχανισμό ασφάλειας για να προστατεύσει ένα πράκτορα από μια κακόβουλη πλατφόρμα, αλλά υποθέτει ότι η πλατφόρμα εκτέλεσης είναι έμπιστη. Και σε αυτό το σενάριο απειλής, η ουσιαστική προστασία του Havana προέρχεται από το ίδιο του το επιχειρηματικό μοντέλο. Διασφαλίζει ότι δεν πρόκειται να υπάρχει όφελος αν μια

πλατφόρμα επιτεθεί σε ένα πράκτορα, στη περίπτωση που υπάρχει τέτοια πρόθεση. Στην περίπτωση που μια τέτοια επίθεση όντως συμβεί, οι υπηρεσίες μη αποποίησης, σε συνδυασμό με το συμβόλαιο διασφαλίζουν την αποζημίωση της οντότητας που υπήρξε θύμα.

Σχετικά με το τρίτο σενάριο, εκείνο της λειτουργίας του πράκτορα σε ανοιχτό περιβάλλον, όλα τα συστήματα κινητών πρακτόρων ακολουθούν παρόμοια προσέγγιση. Όλα τα συστήματα είναι σχεδιασμένα για λειτουργία σε μια αυστηρά ορισμένη Επικράτεια, ή σε ένα δίκτυο συνεργαζόμενων οντοτήτων με κάποιου είδους κεντρική διαχείρισης ασφάλειας. Συγκεκριμένα, στην περίπτωση του Havana, πέρα από την πολιτική ασφάλειας που εφαρμόζεται από την Gateway, οι οντότητες του κόσμου δεσμεύονται και από ένα εμπορικό συμβόλαιο του πραγματικού κόσμου. Ενώ είναι δυνατόν τα συστήματα που εξετάσαμε να λειτουργήσουν σε ένα ανοιχτό δίκτυο όπως το Διαδίκτυο, τα μοντέλα εμπιστοσύνης τους απαιτούν την ύπαρξη κεντρικής διαχείρισης ασφάλειας, και κάνει τα συστήματα μη προσβάσιμα από τρίτες οντότητες. Αυτό σημαίνει ότι κανένα από τα συστήματα κινητών πρακτόρων που αναλύσαμε δεν υποστηρίζει, πρακτικά, λειτουργία σε ανοιχτά περιβάλλοντα στα οποία δεν διατίθεται κάποια κεντρική διαχείριση ασφάλειας.

Έτσι καταλήγουμε στο συμπέρασμα ότι με τη σημερινή τεχνολογία κινητού κώδικα η λειτουργία των συστημάτων κινητών πρακτόρων σε ανοιχτό περιβάλλον είναι, κατά πάσα πιθανότητα, αδύνατη. Γι’ αυτό και η δημιουργία κάποιου είδους “κλειστού” περιβάλλοντος κρίνεται μονόδρομος για την ασφαλή τους λειτουργία.

Πίνακας 4: Αποτελέσματα Σύγκρισης σε Σενάρια Απειλών

Συστήματα κινητών πρακτόρων	**Σενάρια Απειλών**		
	Κακόβουλος Πράκτορας	**Κακόβουλη Πλατφόρμα**	**Ανοιχτό Περιβάλλον**
JADE	Java Sandbox	Ο πράκτορας είναι εκτεθειμένος	Λειτουργεί στα όρια μιας αυστηρά ορισμένης πλατφόρμας
Nomads	Java Sandbox, σύστημα ανίχνευσης εισβολών σε συνδυασμό με διαχείριση πόρων	Ο πράκτορας είναι εκτεθειμένος	Λειτουργεί μόνο μεταξύ συνεργαζόμενων πλατφόρμων εκτέλεσης
Mansion	Java Sandbox. Audit system (AMS)	Ο πράκτορας είναι εκτεθειμένος, η μετανάστευση επιτρέπεται μεταξύ προκαθορισμένων πλατφόρμων εκτέλεσης	Λειτουργεί μόνο μεταξύ προκαθορισμένων τμημάτων του κόσμου
Havana	Πραγματικές συνέπειες λόγω παραβίασης συμβολαίου, ισχυρές υπηρεσίες μη αποποίησης από την Gateway, Java Sandbox	Η επίθεση είναι δυνατή αλλά απίθανη, λόγω πραγματικών συνεπειών λόγω παραβίασης συμβολαίου, ισχυρές υπηρεσίες μη αποποίησης από την Gateway	Λειτουργεί εντός κλειστού περιβάλλοντος για εμπορικές συναλλαγές. Όλες οι οντότητες δεσμεύονται από πραγματικό επιχειρηματικό συμβόλαιο.
Grasshopper	Java Sandbox	Ο πράκτορας είναι εκτεθειμένος	Λειτουργεί στα όρια ενός αυστηρά ορισμένου κόσμου (Region)
Cougaar	Σύστημα ανίχνευσης εισβολών (Monitor and Response), Java Sandbox	Η επίθεση είναι δυνατή αλλά απίθανη, λόγω του κλειστού δικτυακού περιβάλλοντος	Λειτουργεί στα όρια ενός αυστηρά ορισμένου κόσμου (Society).
Aglets	Σύστημα ανίχνευσης εισβολών, Java Sandbox	Proxy (περιορισμένη αποτελεσματικότητα)	Λειτουργεί στα όρια ενός αυστηρά ορισμένου κόσμου (Domain)

3.7 Συμπεράσματα

Με βάση τη σύγκριση των μοντέλων ασφάλειας και εμπιστοσύνης κινητών πρακτόρων που προηγήθηκε καταλήξαμε σε μια σειρά συμπερασμάτων σχετικά με το επίπεδο ασφάλειας που παρέχει η σημερινή τεχνολογία. Μολονότι η αρχιτεκτονική των επιλεγμένων συστημάτων δεν είναι ομοιόμορφη, οι κατευθύνσεις που ακολουθούν είναι παρόμοιες.

Όλα τα συστήματα χρησιμοποιούν μέτρα ασφάλειας για τη λειτουργία τους, αν και το καθένα επικεντρώνεται περισσότερο σε κάποιους τομείς από ό,τι σε άλλους, κάτι που ενδεχομένως να οφείλεται στη διαφορετική τους χρήση. Σε γενικές γραμμές ορισμένοι από τους τομείς ασφάλειας που εξετάσαμε θεωρούμε ότι καλύπτονται επαρκώς από τους υπάρχοντες μηχανισμούς. Συγκεκριμένα στον τομέα της ασφάλειας των επικοινωνιών η εφαρμογή του μηχανισμού SSL αποτελεί επαρκή λύση καθώς προσφέρει υψηλό βαθμό ασφάλειας και αποτελεί καθιερωμένη λύση σε κάθε είδους δικτυακές επικοινωνίες. Ομοίως, η διαχείριση πόρων βασίζεται συνήθως σε υπάρχοντες μηχανισμούς του λειτουργικού συστήματος και της εικονικής μηχανής εκτέλεσης οι οποίοι είναι σε θέση να πραγματοποιήσουν τη λειτουργία αυτή σε ικανοποιητικό βαθμό, αν και ένα από τα συστήματα που εξετάσαμε (Nomads) έχει υλοποιήσει μηχανισμό διαχείρισης πόρων με μεγαλύτερη ακρίβεια. Αντίστοιχα, η δυνατότητα μετανάστευσης του πράκτορα παρέχεται στην ισχυρή της μορφή από τα περισσότερα συστήματα που αναλύσαμε προηγουμένως. Στους υπόλοιπους τομείς ασφάλειας παύει να υπάρχει ομοιομορφία και τα διάφορα συστήματα που εξετάσαμε υλοποιούν συνδυασμό διαφορετικών μέτρων με μικρότερη ή μεγαλύτερη αποτελεσματικότητα.

Έτσι, συμπεραίνουμε ότι δεν υιοθετείται κάποιο πλήρες μοντέλο ασφάλειας και εμπιστοσύνης που να καλύπτει όλους τους τομείς λειτουργίας ενός συστήματος κινητών πρακτόρων. Αυτό συνεπάγεται ότι αν και είναι θεωρητικά δυνατή η συνεργασία μεταξύ πρακτόρων διαφόρων τύπων μέσα από πρότυπα όπως της FIPA και της OMG, δεν μπορεί να γίνει με ένα πρωτοτυποποιημένα ασφαλή τρόπο.

Μια διαφορετική παρατήρηση όσον αφορά στο μοντέλο εμπιστοσύνης αποτελεί το γεγονός ότι ένας αυθεντικοποιημένος πράκτορας που ανήκει σε έμπιστο χρήστη θεωρείται και αυτός έμπιστος, ενώ αντίστοιχα και η πλατφόρμα εκτέλεσης θεωρείται εξ ορισμού ως έμπιστη από τους πράκτορες. Οι δύο αυτές υποθέσεις μπορεί να οδηγήσουν σε σημαντικές παραβιάσεις ασφάλειας, ειδικά στην περίπτωση μιας κακόβουλης πλατφόρμας. Αν και είναι δυνατόν να υλοποιηθούν μέτρα αυτοπροστασίας μέσα σε ένα πράκτορα [1],[75], [77], [78], αυτά σε γενικές γραμμές δεν παρέχουν ολοκληρωμένη ασφάλεια, καθώς, γενικά, υπάρχουν μικρότερα περιθώρια αντίδρασης απέναντι σε αυτή την απειλή. Αυτή η ομοιομορφία στα μοντέλα εμπιστοσύνης μας οδηγεί στο συμπέρασμα ότι συμβαίνει επειδή δεν μπορεί να γίνει διαφορετικά και μας οδηγεί στο συμπέρασμα ότι τα υπάρχοντα μοντέλα εμπιστοσύνης κρίνονται ανεπαρκή για τη λειτουργία συστημάτων κινητών πρακτόρων. Οποιαδήποτε κακόβουλη συμπεριφορά συμβεί σε βάρος αυτών των παραδοχών εμπιστοσύνης θα πρέπει να αντιμετωπιστεί με νέους, διαφορετικούς τρόπους.

Για τους παραπάνω λόγους, τα υπάρχοντα συστήματα λειτουργούν με σχετική ασφάλεια μονάχα μέσα σε μια ορισμένη Επικράτεια ή σε δίκτυο στο οποίο υπάρχει κάποιου είδους κεντρική διαχείριση. Σε τέτοια περιβάλλοντα, οι απειλές από κακόβουλες οντότητες περιορίζονται σημαντικά. Βέβαια, μια τέτοιου είδους χρήση μπορεί να αποδειχθεί ιδιαίτερα περιοριστική για κάποιες εφαρμογές και δεν ευνοεί τη χρήση των κινητών πρακτόρων [34]. Αποτελεί γεγονός το ότι ένα σύστημα κινητών πρακτόρων απαιτεί ένα έμπιστο περιβάλλον. Κάτι τέτοιο μπορεί να επιτευχθεί λειτουργώντας είτε σε ένα τελείως κλειστό περιβάλλον, είτε χρησιμοποιώντας μια τρίτη αρχή διαχείρισης εμπιστοσύνης (trust authority) που θα εγγυάται για την νομιμότητα και το επίπεδο εμπιστοσύνης που μπορεί να αποδοθεί στις οντότητες μέσα σε ένα σύστημα κινητών πρακτόρων.

Συγκεκριμένα, το σύστημα Havana παρουσιάζει τον ενδιαφέροντα συνδυασμό της ύπαρξης αρχής διαχείρισης εμπιστοσύνης με τη δέσμευση των οντοτήτων με συμβόλαιο. Αυτός ο συνδυασμός διασφαλίζει ότι στην περίπτωση κακόβουλης συμπεριφοράς θα υπάρχουν συνέπειες στο χρήστη πίσω από την κακόβουλη οντότητα στον πραγματικό κόσμο.

Λόγω της ιδιαίτερης φύσης της τεχνολογίας των κινητών πρακτόρων, που αφορά εκτέλεση μη έμπιστου κώδικα σε πλατφόρμες τρίτων, ό,τι μέτρο ασφαλείας και να χρησιμοποιηθεί το μοντέλο εμπιστοσύνης θα είναι δυνατόν, κατά πάσα πιθανότητα να αποτύχει. Δεδομένης της αδυναμίας που παρατηρείται στο να αντιμετωπιστούν κάποιοι από τους κινδύνους με τεχνικούς τρόπους, καταλήγουμε στο συμπέρασμα ότι η λύση στα πρόβλημα ασφάλειας πρέπει να αναζητηθεί και εκτός των ορίων του συστήματος κινητών πρακτόρων. Προτείνουμε την εισαγωγή μιας αρχής διαχείρισης εμπιστοσύνης εντός των πλαισίων ενός καθολικού μοντέλου ασφάλειας και εμπιστοσύνης, το οποίο πρέπει να συνδυάζει τα νεότερα μέτρα ασφάλειας για κινητούς πράκτορες, μαζί με ένα επιχειρηματικό μοντέλο με βάση το οποίο θα παρέχει τις υπηρεσίες του. Αυτό αποτελεί το αντικείμενο του επόμενου κεφαλαίου, στο οποίο γίνεται η πρόταση ενός μοντέλου με βάση τις προδιαγραφές που τέθηκαν προκαταρκτικά στη διατριβή (2.3 Απαιτήσεις Ασφάλειας) και σε συνδυασμό με τα συμπεράσματα που εξαγάγαμε από την ανάλυση των αδυναμιών των υπαρχόντων συστημάτων.

4 ΠΡΟΤΕΙΝΟΜΕΝΟ ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ & ΕΜΠΙΣΤΟΣΥΝΗΣ

4.1 Εισαγωγή

Στο παρόν κεφάλαιο ορίζουμε τις προδιαγραφές που πρέπει να πληροί ένα μοντέλο-πρότυπο ασφάλειας και εμπιστοσύνης κινητών πρακτόρων. Η τελική μορφή των προδιαγραφών αυτών προέκυψε μετά από ανάλυση των σύγχρονων συστημάτων και με βάση τα συμπεράσματα που προέκυψαν από τη σύγκριση των συστημάτων αυτών, που πραγματοποιήθηκε στο προηγούμενο κεφάλαιο. Με βάση τις προδιαγραφές αυτές γίνεται ο σχεδιασμός ενός θεωρητικού καθολικού μοντέλου ασφάλειας και εμπιστοσύνης που επιτρέπει τη λειτουργία και συνεργασία των πρακτόρων κατά τρόπο ασφαλή. Το προτεινόμενο μοντέλο παρουσιάζεται κατά τομείς, που έχουν προκύψει με βάση τις κύριες οντότητες/λειτουργίες ενός συστήματος κινητών πρακτόρων.

4.2 Απαιτούμενες Προδιαγραφές

Με βάση την προηγούμενη έρευνα, έχουμε καταλήξει στο συμπέρασμα ότι ένα μοντέλο ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες οφείλει να προσφέρει τόσο μηχανισμούς ασφάλειας, όσο και πολιτικές για το τι πρέπει να συμβαίνει μετά από περιπτώσεις αποτυχίας του (επιτυχημένες επιθέσεις). Έτσι καταλήγουμε συγκεντρωτικά, και αναβαθμίζοντας τις προκαταρκτικές προδιαγραφές που τέθηκαν στο υποκεφάλαιο 2.3 Απαιτήσεις Ασφάλειας), στο ότι τέτοια μοντέλα πρέπει να πληρούν τις παρακάτω προδιαγραφές:

1. **Διαβαθμιζόμενες υπηρεσίες ασφαλείας (Scalable security services)**. Ένα πλήρες μοντέλο ασφάλειας και εμπιστοσύνης πρέπει να καλύπτει όλες τις πτυχές της λειτουργίας ενός συστήματος κινητών πρακτόρων. Αυτό συνεπάγεται τη χρήση ενός σημαντικού αριθμού μηχανισμών ασφαλείας, και η εφαρμογή του συνόλου τους θα εξασφαλίζει πλήρως τη λειτουργία του συστήματος κινητών πρακτόρων, αλλά με ανάλογη επίδραση στις επιδόσεις

του συστήματος. Οπότε, ένα μοντέλο ασφάλειας και εμπιστοσύνης οφείλει να παρέχει εναλλακτικές επιλογές για την κάθε λειτουργία. Έτσι, για μια εμπορική εφαρμογή που περιλαμβάνει χρηματικές συναλλαγές θα υλοποιείται το σύνολο των μηχανισμών και των δυνατοτήτων που προβλέπονται από το μοντέλο. Αντίθετα, για μια απλούστερη εφαρμογή μικρού κινδύνου και αξίας η υλοποίηση μηχανισμών ασφαλείας πέρα των ελάχιστων που απαιτούνται για την ορθή της λειτουργία θα αποτελεί άσκοπη επιβάρυνση των πόρων της πλατφόρμας εκτέλεσης. Το μοντέλο ασφάλειας και εμπιστοσύνης πρέπει να επιτρέπει την επιλογή επιπέδων ασφαλείας από τις εφαρμογές. Αυτή η προδιαγραφή καλύπτει την προκαταρκτική προδιαγραφή περί διεξοδικότητας (2.3 Απαιτήσεις Ασφάλειας), ενώ επιπλέον απαιτεί διαβάθμιση των παρεχόμενων υπηρεσιών ασφάλειας.

2. **Παροχή υπηρεσιών μη αποποίησης (Strong non-repudiation services)**. Είναι σημαντικό να παρέχονται υπηρεσίες μη αποποίησης για την περίπτωση περιστατικών παραβίασης της ασφάλειας. Έτσι, το μοντέλο ασφάλειας και εμπιστοσύνης πρέπει να μπορεί να παρέχει το πλήρες ιστορικό των εμπλεκομένων οντοτήτων και των ενεργειών ανά πάσα στιγμή. Αυτό απαιτεί ένα ισχυρό μηχανισμό αυθεντικοποίησης όλων των οντοτήτων σε συνδυασμό με την υπηρεσία διατήρησης ιστορικού ενεργειών. Πρόκειται να λειτουργεί αποτρεπτικά για περιπτώσεις επίθεσης, αφού ο επιτιθέμενος εντοπίζεται με τρόπο αδιαμφισβήτητο.
3. **Προσαρμοστικό μοντέλο εμπιστοσύνης (Adaptive trust model using reputation scheme)**. Το επίπεδο εμπιστοσύνης μιας οντότητας και, άρα, και τα δικαιώματα που του αποδίδονται πρέπει να αντικατοπτρίζει τις προγενέστερες ενέργειές της. Έχουμε αναλύσει την ανάγκη του να πρέπει να θεωρηθούν κάποιες οντότητες ενός συστήματος κινητών πρακτόρων ως έμπιστες, ακόμη και με τον υπαρκτό κίνδυνο οι υποθέσεις αυτές να αποδειχθούν εσφαλμένες. Το πρόβλημα αυτό αντιμετωπίζεται στον επιστημονικό χώρο της διαχείρισης εμπιστοσύνης με την έννοια της υπόληψης (reputation) [69]. Αντίστοιχα, στο χώρο των συστημάτων κινητών πρακτόρων το μοντέλο εμπιστοσύνης πρέπει να είναι προσαρμοστικό. Σε

όλους τους χρήστες που βρίσκονται πίσω από πράκτορες και πλατφόρμες πρέπει να αποδίδεται ένα επίπεδο εμπιστοσύνης. Αυτό μπορεί να μεταβάλλεται ανάλογα με την προηγούμενη συμπεριφορά των οντοτήτων. Η δυνατότητα αυτή απαιτεί την ύπαρξη κάποιας κεντρικής διαχειριστικής οντότητας, όπου θα καταγράφεται η συμπεριφορά και το επίπεδο εμπιστοσύνης θα προσαρμόζεται ανάλογα. Στην περίπτωση ενός πράκτορα που πρόκειται να μεταναστεύσει, πρέπει να του παρέχεται η δυνατότητα να διερευνήσει το επίπεδο εμπιστοσύνης που αποδίδεται σε μια πλατφόρμα και ανάλογα, να επιλέξει να την παρακάμψει για μία άλλη, πιο έμπιστη πλατφόρμα. Αντίστοιχη δυνατότητα πρέπει να έχει και η πλατφόρμα, η οποία πριν δεχθεί να φιλοξενήσει ένα πράκτορα πρέπει να μπορεί να διερευνήσει το επίπεδο εμπιστοσύνης του χρήστη πίσω από τον πράκτορα και ανάλογα να δεχθεί τη μετανάστευση του πράκτορα ή να την απορρίψει. Η συγκεκριμένη προδιαγραφή καλύπτει την προκαταρκτική προδιαγραφή, περί ύπαρξης μοντέλου εμπιστοσύνης (2.3 Απαιτήσεις Ασφάλειας), ενώ επιπλέον διαμορφώνει και τον τύπο του.

4. **Παροχή υπηρεσιών ασφάλισης (Insurance services)**. Ένα μοντέλο ασφάλειας και εμπιστοσύνης για έξυπνους πράκτορες είναι δυνατόν κάποια στιγμή να αποτύχει. Το μοντέλο πρέπει να το προβλέπει και να επεκτείνεται στον πραγματικό κόσμο, παρέχοντας προαιρετικά υπηρεσίες ασφάλισης. Καθώς οι αδυναμίες ασφάλειας της τεχνολογίας των πρακτόρων θεωρείται ότι περιορίζουν την υιοθέτησή τους [34] είναι απαραίτητο, πέρα από τους μηχανισμούς ασφάλειας, να υπάρχει πρόνοια για την περίπτωση παραβίασής τους. Για κάποιες εφαρμογές η περίπτωση παραβίασης ασφάλειας είναι απλά μη αποδεκτή. Για αυτές ειδικά τις εφαρμογές πρέπει να παρέχεται μηχανισμός ασφάλισης για απρόοπτες καταστάσεις. Η λειτουργία ενός τέτοιου μηχανισμού προϋποθέτει την προηγούμενη απαίτηση για παροχή υπηρεσιών μη αποποίησης, ώστε να είναι δυνατή η αποζημίωση της οντότητας που έπεσε θύμα επίθεσης. Η παροχή υπηρεσιών ασφάλισης μπορεί να συνδυαστεί με την προδιαγραφή για προσαρμοστικό μοντέλο εμπιστοσύνης με χρήση της έννοιας της υπόληψης, αντίστοιχα με τις

ασφαλιστικές υπηρεσίες χώρων διαφορετικών από την Πληροφορική. Για αυτή τη δυνατότητα απαιτείται μια κεντρική οντότητα του πραγματικού κόσμου να αναλαμβάνει την εγγραφή των χρηστών καθώς και την παρακολούθηση όλων των λειτουργιών ενός συστήματος κινητών πρακτόρων. Αυτός ο τύπος υπηρεσίας έχει νόημα μόνον για εφαρμογές υψηλής αξίας. Στην περίπτωση παραβίασης της ασφάλειας ο υπεύθυνος θα καθίσταται νομικά υπεύθυνος, ενώ θα είναι εγγυημένη και η αποκατάσταση του ζημιωμένου.

5. **Ανεξάρτητο συγκεκριμένης πλατφόρμας** (**Platform independence**). Ένα μοντέλο ασφάλειας και εμπιστοσύνης καθώς και οι υπηρεσίες του πρέπει να είναι γενικό (abstract) ώστε να μπορεί να υιοθετηθεί από κάθε τύπου εφαρμογή πρακτόρων. Ενδείκνυται η ενσωμάτωσή του σε πλήρες πρότυπο λειτουργίας πρακτόρων. Αντίθετα με τις προηγούμενες προδιαγραφές, η συγκεκριμένη δεν έχει λειτουργικό χαρακτήρα (non-functional requirement). Σχετίζεται με την δυνατότητα διαλειτουργικότητας, η οποία θεωρείται ιδιαίτερα σημαντική για τη λειτουργία των συστημάτων κινητών πρακτόρων [1], [34], ενώ αποτελεί τον μέχρι τώρα κύριο στόχο των υπαρχουσών προδιαγραφών για κινητούς πράκτορες (FIPA, MASIF [13], [16], [18]) οι οποίες όμως την επιδιώκουν κυρίως μέσω της συμβατότητας των επικοινωνιών [70]. Πέρα από αυτήν όμως, απαιτείται και ομοιομορφία όσον αφορά στην ασφάλεια, καθώς η έλλειψή της θεωρείται ως ιδιαίτερο πρόβλημα για την χρήση των συστημάτων κινητών πρακτόρων [34]. Για τους παραπάνω λόγους, υποστηρίζουμε ότι ένα πλήρες μοντέλο ασφάλειας και εμπιστοσύνης πρέπει να είναι γενικό και ανεξάρτητο από συγκεκριμένες πλατφόρμες κινητών πρακτόρων. Επιπρόσθετα, θεωρούμε ότι κάθε επίσημο πρότυπο που αφορά στη λειτουργία κινητών πρακτόρων πρέπει να ενσωματώνει και κοινό πρότυπο ασφάλειας, χωρίς αυτό να σημαίνει ότι όλες οι εφαρμογές κινητών πρακτόρων θα οφείλουν να χρησιμοποιούν τους ίδιους μηχανισμούς ασφάλειας (προδιαγραφή διαβαθμιζόμενων υπηρεσιών ασφάλειας). Η τελευταία αυτή προδιαγραφή αποτελεί ουσιαστικά την

προκαταρκτική προδιαγραφή, σχετικά με την αφαιρετικότητα του μοντέλου (2.3 Απαιτήσεις Ασφάλειας).

4.3 Το Προτεινόμενο Μοντέλο

Στη συνέχεια αναλύεται η λειτουργία του μοντέλου ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες που προτείνουμε στο πλαίσιο της διατριβής και το οποίο πληροί τις προδιαγραφές στις οποίες καταλήξαμε στο κεφάλαιο 4.1 Εισαγωγή. Προκειμένου να αντιμετωπιστεί η πολυπλοκότητα που συνεπάγεται η ανάπτυξη ενός πλήρους τέτοιου μοντέλου, το διαιρούμε σε τέσσερις περιοχές, που αφορούν τις κύριες οντότητες/λειτουργίες του συστήματος:

- Ασφάλεια Πράκτορα
- Ασφάλεια Πλατφόρμας
- Ασφάλεια Επικοινωνιών / Μετανάστευσης
- Μοντέλο Εμπιστοσύνης

Στις συγκεκριμένες περιοχές ομαδοποιούνται όλες οι οντότητες και λειτουργίες των κριτηρίων σύγκρισης που έχουμε θέσει (2.4 Μοντέλο Σύγκρισης). Ο λόγος που το μοντέλο μας δεν παρουσιάζεται με βάση αυτές, είναι το συμπέρασμα στο οποίο έχουμε καταλήξει ότι τα σημερινά συστήματα παρέχουν ήδη υψηλό βαθμό ασφάλειας για κάποιες από αυτές. Έτσι, η παρουσίαση γίνεται με βάση τις κυριότερες περιοχές του συστήματος, στις οποίες όμως περιλαμβάνονται όλες οι λειτουργίες στις οποίες έχουμε προηγουμένως αναφερθεί.

Στη συνέχεια, για κάθε μία από τις τέσσερις περιοχές, θα αναλύσουμε τα μέτρα ασφάλειας που αντιμετωπίζουν τις σχετικές απειλές. Καθώς όμως το προτεινόμενο μοντέλο οφείλει να παρέχει διαβαθμιζόμενες υπηρεσίες ασφάλειας (προδιαγραφή 1), ορίζουμε τρία διακριτά επίπεδα ασφάλειας μεταξύ των οποίων κυμαίνονται τα μέτρα ασφάλειας. Έτσι, οι μηχανισμοί ασφαλείας του προτεινόμενου μοντέλου παρουσιάζονται ομαδοποιημένοι σε υποομάδες ανάλογα με την περιοχή που αφορούν και ανά επίπεδο ασφάλειας που έχει επιλεγεί (Πίνακας

5). Τα επίπεδα ασφάλειας που προβλέπονται από το προτεινόμενο μοντέλο και μεταξύ των οποίων θα μπορούν να επιλέξουν οι εφαρμογές κινητών πρακτόρων είναι τα παρακάτω:

1. **Βασικό (Basic Operation)**. Εδώ παρέχονται τα ελάχιστα μέτρα ασφάλειας για να λειτουργήσουν αποτελεσματικά εφαρμογές μικρού κινδύνου. Αποσκοπεί περισσότερο στην ορθή, παρά στην ασφαλή λειτουργία της εφαρμογής ενώ είναι κατάλληλο μονάχα για εφαρμογές με μικρές απαιτήσεις ασφάλειας, όπως απλά δίκτυα αισθητήρων με βάση πράκτορες ή μικρές εφαρμογές σε κλειστά δίκτυα. Στο συγκεκριμένο επίπεδο δεν παρέχεται κάποια κεντρικοποιημένη διαχείριση λειτουργιών ασφάλειας.
2. **Ασφαλές (Secure Operation)**. Εδώ παρέχονται τα περισσότερα μέτρα ασφάλειας του συστήματος εκτός από τις υπηρεσίες ασφάλισης. Οι υπηρεσίες ασφάλειας ρυθμίζονται από κεντρική οντότητα που προβλέπει το μοντέλο. Αντίστοιχο επίπεδο ασφάλειας με παρόμοια αρχιτεκτονική, αν και με λιγότερους μηχανισμούς ασφάλειας, παρέχεται από υπάρχοντα συστήματα κινητών πρακτόρων (Cougaar, Havana). Είναι κατάλληλο για τις περισσότερες εφαρμογές που έχουν απαιτήσεις ασφαλούς λειτουργίας.
3. **Ασφαλές/Ασφαλισμένο (Secure – Insured Operation)**. Εδώ παρέχονται όλα τα μέτρα ασφάλειας μαζί με υπηρεσίες ασφάλισης. Και εδώ υπάρχει κεντρική οντότητα διαχείρισης ασφάλειας η οποία αναλαμβάνει ακόμη πιο ενεργό ρόλο στη λειτουργία του συστήματος. Αποτελεί πληρωμένη υπηρεσία, οπότε είναι κατάλληλο για κρίσιμες εφαρμογές όπου το ενδεχόμενο παραβίασης κάνει απαγορευτική τη χρήση έξυπνων πρακτόρων, όπως εμπορικές εφαρμογές με εγχρήματες συναλλαγές.

Το προτεινόμενο μοντέλο βασίζεται σε μια κεντρική οντότητα απόδοσης εμπιστοσύνης (Trust Granting Authority), η οποία ουσιαστικά λειτουργεί ως Έμπιστη Τρίτη Οντότητα, και την έχουμε ονομάσει Talos, από το ομώνυμο δημιούργημα-φρουρό της αρχαίας Ελληνικής μυθολογίας. Παρέχεται στα δύο υψηλότερα επίπεδα ασφάλειας, ενώ η λειτουργία του και η αρχιτεκτονική του διαφοροποιείται μεταξύ των δύο επιπέδων ασφάλειας που χρησιμοποιείται (Εικόνα 45, Εικόνα 46). Η κύρια λειτουργία του είναι οι υπηρεσίες διαχείρισης

εμπιστοσύνης και ασφάλισης. Για αυτό το λόγο και θα παρουσιαστεί αναλυτικά στο κομμάτι που αφορά το μοντέλο εμπιστοσύνης.

Στη συνέχεια ακολουθεί η περιγραφή του προτεινόμενου μοντέλου ανά οντότητα/λειτουργία του συστήματος.

4.3.1 Ασφάλεια Πράκτορα

Η ακεραιότητα του πράκτορα διασφαλίζεται από πιθανές επιθέσεις άλλων πρακτόρων ή πιο συχνά από επιθέσεις από την πλατφόρμα εκτέλεσης.

- Στο **Βασικό Επίπεδο** ασφάλειας ο πράκτορας απομονώνεται και προστατεύεται από τους άλλους πράκτορες χρησιμοποιώντας τους μηχανισμούς εκτέλεσης ξένου κώδικα που παρέχει η εικονική μηχανή που τρέχει στην πλατφόρμα και στην οποία εκτελούνται οι πράκτορες. Η συγκεκριμένη μέθοδος παρέχει προστασία περισσότερο από απειλές που προέρχονται από άλλους πράκτορες ενώ είναι κάτι που ήδη παρέχεται από τα υπάρχοντα συστήματα, λόγω της καθιερωμένης χρήσης της Java ([1], [2]). Επιπλέον, απαιτείται αμοιβαία αυθεντικοποίηση μεταξύ πράκτορα και πλατφόρμας, με βάση τις υπογραφές των ιδιοκτητών τους. Η διαδικασία κρίνεται απαραίτητη ως βάση για τον έλεγχο πρόσβασης, τη διαχείριση πόρων καθώς και ως μέρος της διαδικασίας μετανάστευσης. Αυτό αποτελεί και το μόνο πρόσθετο μέτρο ασφάλειας το οποίο δεν εφαρμόζεται ήδη καθολικά από τα υπάρχοντα συστήματα, παρά μόνο από κάποια.
- Για τις εφαρμογές που χρησιμοποιούν το **Ασφαλές Επίπεδο** προβλέπονται επιπλέον μηχανισμοί ασφάλειας. Αν και οι ψηφιακές υπογραφές προστατεύουν την ακεραιότητα του κώδικα του πράκτορα, δεν καλύπτουν τα δεδομένα που φέρει, καθώς αυτά ενημερώνονται συνεχώς κατά τη διάρκεια εκτέλεσης [1], [2], [9]. Το συγκεκριμένο πρόβλημα μπορεί να αντιμετωπιστεί με τη χρήση της Πλήρως Ομομορφικής Κρυπτογραφίας (Fully Homomorphic Encryption) [6], [74], [88], [89], [90]. Αυτή η πρόσφατη εξέλιξη στο χώρο της κρυπτογραφίας επιτρέπει την ενημέρωση κρυπτογραφημένων δεδομένων από μη έμπιστη οντότητα χωρίς να

χρειάζεται προηγουμένως αυτά να αποκρυπτογραφηθούν. Αυτή η τεχνική είναι κατάλληλη για εφαρμογές όπου ο πράκτορας μεταναστεύει σε μια πλατφόρμα εκτέλεσης για να συλλέξει δεδομένα και τα αποθηκεύσει εσωτερικά, όπως ένας πράκτορας τιμοληψίας προϊόντων από ηλεκτρονικά καταστήματα. Μια κακόβουλη πλατφόρμα που εκτελεί ένας πράκτορα με κρυπτογραφημένα δεδομένα έχει τη δυνατότητα να του προσθέσει αλλοιωμένες – ψευδείς πληροφορίες, αλλά δεν μπορεί να αποκτήσει πρόσβαση στα δεδομένα που ήδη έχει συλλέξει σε μη κρυπτογραφημένη μορφή (Plaintext). Με αυτό τον τρόπο διατηρείται η ιδιωτικότητα και η ακεραιότητα των δεδομένων του πράκτορα. Η ομομορφική κρυπτογραφία αποτελεί ιδανική λύση για την εκτέλεση κινητού κώδικα σε μη έμπιστη πλατφόρμα, αλλά συνεπάγεται αύξηση στις υπολογιστικές ανάγκες του συστήματος [6], [74] οπότε και δικαιολογείται μονάχα για εφαρμογές με υψηλές απαιτήσεις σε ασφάλεια. Παρόλ’ αυτά, με τη χρήση των νεότερων τεχνικών πλήρως ομομορφικής κρυπτογραφίας [88], [89], [90] η αύξηση σε υπολογιστικές απαιτήσεις είναι πλέον γραμμικά ανάλογη με τις πράξεις που πραγματοποιούνται και όχι εκθετικά ανάλογη, κάτι που σημαίνει ότι η υπολογιστική επιβάρυνση κυμαίνεται πλέον σε πολύ λογικότερα επίπεδα. Επιπρόσθετα, σε αυτό το επίπεδο ασφάλειας παρέχονται ισχυρές υπηρεσίες μη αποποίησης για την περίπτωση που παραβιαστεί η ακεραιότητα ενός πράκτορα. Αυτές παρέχονται από τον Talos (Εικόνα 45). Όλες οι οντότητες εγγράφονται υποχρεωτικά σε αυτόν και σε όλα τα στάδια λειτουργίας αποστέλλονται σε αυτόν αναφορές δραστηριότητας από όλες τις οντότητες. Έτσι, είναι δυνατόν να εντοπιστεί οποιαδήποτε κακόβουλη ενέργεια και να ταυτοποιηθεί η οντότητα που την προκάλεσε.

- Το **Ασφαλές/Ασφαλισμένο Επίπεδο** λειτουργίας παρέχει όλα τα μέτρα ασφάλειας του Ασφαλούς Επιπέδου, με την προσθήκη των ασφαλιστικών υπηρεσιών. Και εδώ είναι απαραίτητη η εγγραφή του χρήστη ενώ πραγματοποιείται επιπρόσθετα και εξακρίβωση πληροφοριών χρέωσης. Όλες οι υπηρεσίες πραγματοποιούνται μέσω του Talos, ο οποίος σε αυτό το επίπεδο αποκτά πιο ενεργό ρόλο και λαμβάνει μέρος στις αλληλεπιδράσεις μεταξύ των οντοτήτων. Η ουσιαστική προσθήκη στην προστασία της ακεραιότητας του πράκτορα είναι το ότι οι χρήστες (ιδιοκτήτες πρακτόρων και πλατφόρμων εκτέλεσης) προκειμένου να

χρησιμοποιήσουν το συγκεκριμένο επίπεδο προχωρούν στην σύναψη εμπορικής συμφωνίας με υπογραφή πραγματικού συμβολαίου. Αυτό, εξασφαλίζει την παροχή υπηρεσιών ασφάλειας και ασφάλισης από τον Talos και σε συνδυασμό με τις υπηρεσίες μη αποποίησης εγγυάται τον εντοπισμό της κακόβουλης οντότητας στην περίπτωση επίθεσης εναντίον πράκτορα. Στη συνέχεια επιρρίπτονται νομικές ευθύνες στον χρήστη πίσω από αυτήν και ο χρήστης που ζημιώθηκε αποζημιώνεται ανάλογα με την έκταση της επίθεσης και τις συνθήκες που προβλέπονται από το συμβόλαιο που έχει συνάψει.

Αν και η ασφάλιση δεν αποτελεί τεχνικό χαρακτηριστικό ασφάλειας για την προστασία του πράκτορα, η παροχή της ενδέχεται να ωφελήσει συγκεκριμένες εφαρμογές με υψηλές απαιτήσεις ασφάλειας [4]. Διαφορετικά αν δεν μπορεί να διασφαλιστεί με απόλυτο τρόπο η λειτουργία του συστήματος, η τεχνολογία των κινητών πρακτόρων κρίνεται ως ακατάλληλη και απλά δεν υιοθετείται στις συγκεκριμένες περιπτώσεις. Με τη χρήση του συνδυασμού ασφάλισης και υπηρεσιών μη αποποίησης η επίθεση εναντίον της ακεραιότητας ενός πράκτορα δεν είναι πλέον ελκυστική, ακόμη και σε περιπτώσεις οικονομικών συναλλαγών.

4.3.2 Ασφάλεια Πλατφόρμας

Η ακεραιότητα της πλατφόρμας εκτέλεσης ενός συστήματος κινητών πρακτόρων πρέπει να διασφαλίζεται από επιθέσεις πρακτόρων. Μια πλατφόρμα μπορεί να φιλοξενεί μεγάλο αριθμό πρακτόρων που σχετίζονται με διάφορες εφαρμογές. Έτσι, η παραβίαση της ακεραιότητάς της μπορεί να επηρεάσει πέρα από την ίδια και όλους τους πράκτορες που εκτελούνται σε αυτή. Γι’ αυτό το λόγο και θεωρούμε κρίσιμη την επαρκή προστασία της, ακόμη και για το χαμηλότερο επίπεδο ασφάλειας που προβλέπει το προτεινόμενο μοντέλο ασφάλειας και εμπιστοσύνης.

- Στο **Βασικό Επίπεδο** λειτουργίας θεωρούμε την αμοιβαία αυθεντικοποίηση των οντοτήτων ως βάση και για τους μηχανισμούς ασφάλειας που προστατεύουν την ακεραιότητα της πλατφόρμας, με βάση τις ψηφιακές υπογραφές. Η

αυθεντικοποίηση του πράκτορα και της πλατφόρμας είναι το πρώτο απαραίτητο στάδιο ώστε να είναι δυνατή η ταυτοποίηση του χρήστη που βρίσκεται πίσω από μία επίθεση. Επιπλέον, και για την προστασία της πλατφόρμας, η χρήση τεχνικών απομόνωσης κατά την εκτέλεση κινητού κώδικα είναι υποχρεωτική, αν και όπως είδαμε παρέχονται συνήθως από την εικονική μηχανή εκτέλεσης, λόγω της καθιέρωσης της Java ([1], [2]). Ο μηχανισμοί αυτοί αποσκοπούν κυρίως στην προστασία της ακεραιότητας της πλατφόρμας από απειλές που προέρχονται από τον ξένο κώδικα (foreign code) που εκτελεί.

- Για το **Ασφαλές Επίπεδο** λειτουργίας εισάγουμε περισσότερο ενεργούς μηχανισμούς προστασίας της ακεραιότητας της πλατφόρμας εκτέλεσης. Γίνεται χρήση ενός μηχανισμού ανίχνευσης εισβολών με βάση τη δραστηριότητα όλων των οντοτήτων που αλληλεπιδρούν με την πλατφόρμα. Ο μηχανισμός αυτός υλοποιείται ως στατικός πράκτορας που εκτελείται τοπικά στην πλατφόρμα, έτσι ώστε να μην απαιτείται η τροποποίηση της εικονικής μηχανής και να απλοποιείται η ανάπτυξή του. Με βάση τις πληροφορίες αυτού του μηχανισμού διαμορφώνεται και η λειτουργία του μηχανισμού διαχείρισης πόρων. Οι πόροι κατανέμονται δυναμικά στους κινητούς πράκτορες και η αναπροσαρμογή τους γίνεται σε πραγματικό χρόνο, ώστε να διασφαλίζεται η καλή λειτουργία της πλατφόρμας και κατ' επέκταση των πρακτόρων που φιλοξενεί. Στην περίπτωση που ανιχνευθεί κακόβουλη συμπεριφορά από κάποιο πράκτορα, οι πόροι που του έχουν αποδοθεί μπορεί να μειωθούν έως και να αφαιρεθούν τελείως τερματίζοντας τη λειτουργία του. Και στην περίπτωση της ακεραιότητας της πλατφόρμας οι ισχυροί μηχανισμοί μη αποποίησης που προσφέρονται από τον Talos αποτελούν ένα ισχυρό αποτρεπτικό μηχανισμό για πιθανούς εισβολείς.
- Στο **Ασφαλές/Ασφαλισμένο Επίπεδο** λειτουργίας, η προσέγγιση που ακολουθείται είναι αντίστοιχη με εκείνη της προστασίας της ακεραιότητας του πράκτορα. Παρέχονται όλοι οι μηχανισμοί του προηγούμενου επιπέδου με την προσθήκη των υπηρεσιών ασφάλισης. Ο Talos αντιμετωπίζει την πλατφόρμα με τον ίδιο τρόπο που αντιμετωπίζει ένα πράκτορα. Οπότε, ανεξάρτητα από το αν η κακόβουλη οντότητα είναι πράκτορας ή πλατφόρμα, ο Talos την εντοπίζει χρησιμοποιώντας τα αρχεία καταγραφής των υπηρεσιών μη αποποίησης και

εντοπίζει τον χρήστη πίσω από αυτήν. Και εδώ αποδίδονται νομικές ευθύνες στον υπεύθυνο, ενώ ο ζημιωμένος χρήστης αποζημιώνεται κάτι που επιτρέπει η ύπαρξη συμβολαίου σε αυτό το επίπεδο. Επομένως και για την ασφάλεια της πλατφόρμας ουσιαστική προστασία παρέχει το συγκεκριμένο σχήμα ασφάλειας/ασφάλισης, όπου καθιστά έως και ζημιογόνο την πραγματοποίηση οποιασδήποτε επίθεσης.

4.3.3 Ασφάλεια Επικοινωνιών / Μετανάστευσης

Σε ένα σύστημα κινητών πρακτόρων εμπεριέχεται μεγάλος βαθμός επικοινωνιών μεταξύ των οντοτήτων που το αποτελούν και αποτελούν κρίσιμο τμήμα της λειτουργίας του. Ανάλογα με την εφαρμογή του κάθε συστήματος, είναι δυνατόν αυτές οι επικοινωνίες να πραγματοποιούνται διαμέσου δημόσιων δικτύων χωρίς ενιαία διαχείριση ασφάλειας. Αυτό οφείλει να προβλέπεται από ένα μοντέλο ασφάλειας και εμπιστοσύνης και να λαμβάνονται μέτρα για την ασφάλεια των επικοινωνιών. Μέσα σε αυτές συμπεριλαμβάνονται και οι επικοινωνίες που πραγματοποιούνται για τη διαδικασία της μετανάστευσης ενός πράκτορα.

Στο προηγούμενο κεφάλαιο της διατριβής (3.7 Συμπεράσματα) συμπεράναμε ότι τα υπάρχοντα συστήματα αντιμετωπίζουν επαρκώς τα ζητήματα ασφάλειας στον συγκεκριμένο τομέα [1], [2]. Έχουμε όμως θέσει ως προϋπόθεση ότι ένα πλήρες μοντέλο ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες πρέπει να καλύπτει όλες τις πτυχές της λειτουργίας τους, ενώ οι υπηρεσίες του οφείλουν να είναι διαβαθμιζόμενες. Γι’αυτό ακριβώς το λόγο οφείλουμε να καλύψουμε το χώρο της ασφάλειας επικοινωνιών στο προτεινόμενο μοντέλο, ξεχωριστά για κάθε επίπεδο λειτουργίας.

- Στο **Βασικό Επίπεδο** λειτουργίας δεν υπάρχει απαίτηση για κρυπτογράφηση των επικοινωνιών. Καθώς προορίζεται για μη κρίσιμες εφαρμογές ή για χρήση σε ασφαλή περιβάλλοντα προτεραιότητα αποτελεί η ταχύτητα εκτέλεσης. Όλα τα μηνύματα μεταξύ πρακτόρων και πλατφορμών ανταλλάσσονται μη κρυπτογραφημένα, χρησιμοποιώντας απλά μια συνάρτηση κατακερματισμού (hash function) για λόγους αξιόπιστης μετάδοσης. Ο αλγόριθμος που θα χρησιμοποιηθεί

μπορεί να επιλεγεί από τις οντότητες που επικοινωνούν ανάλογα με το ποιοι υποστηρίζονται από την εικονική μηχανή (π.χ. η εικονική μηχανή της Java διαθέτει υλοποιημένες δεκάδες συναρτήσεις κατακερματισμού μεταξύ των οποίων οι MD5 και SHA [25], [71]). Ομοίως και κατά τη μετανάστευση ο πράκτορας μετακινείται μη κρυπτογραφημένος μέσω του δικτύου. Υπάρχει όμως απαίτηση να υλοποιείται μετανάστευση ισχυρού τύπου, ώστε ο πράκτορας να μπορεί να διακόπτει την εκτέλεσή του σε οποιαδήποτε σημείο και να μεταφέρει την τελευταία κατάσταση των δεδομένων του, αντί να υπάρχουν προεπιλεγμένα σημεία. Αν και η συγκεκριμένη δεν αποτελεί απαίτηση ασφάλειας, η απουσία της κάνει ένα σύστημα κινητών πρακτόρων λιγότερο εύχρηστο [1], [2]. Το προτεινόμενο επικοινωνιακό μοντέλο είναι απλό στην υλοποίηση και με μικρές απαιτήσεις πόρων για τη λειτουργία του, αν και κρίνεται ακατάλληλο για εφαρμογές υψηλού ρίσκου.

- Το **Ασφαλές Επίπεδο** λειτουργίας έχει αναπτυχθεί ώστε να καλύπτει τις ανάγκες για ασφάλεια επικοινωνιών σε εφαρμογές με υψηλές απαιτήσεις. Καθώς η υποκλοπή μηνυμάτων σε ασφαλή συστήματα είναι μη αποδεκτή, όλες οι επικοινωνίες κρυπτογραφούνται. Γίνεται χρήση του κρυπτογραφικού πρωτοκόλλου SSL/TLS, το οποίο αποτελεί καθιερωμένο μηχανισμό κρυπτογράφησης επικοινωνιών και μπορεί να υποστηρίξει τις ανάγκες ενός συστήματος κινητών πρακτόρων [1], [2]. Επιπλέον λόγος για τη χρήση του συγκεκριμένου πρωτοκόλλου είναι το ότι υποστηρίζεται εγγενώς από τις εικονικές μηχανές εκτέλεσης, και βεβαίως της Java [71] κάτι που συνεπάγεται απλούστατη υλοποίηση. Η διαδικασία της μετανάστευσης και εδώ απαιτείται να είναι ισχυρού τύπου, ενώ αντιμετωπίζεται από το προτεινόμενο μοντέλο ως ανταλλαγή μηνυμάτων μέσω δικτύου. Ο πράκτορας και τα δεδομένα του μεταδίδονται κρυπτογραφημένα, ως μία σύνοδος SSL/TLS μεταξύ της πλατφόρμας αφετηρίας και της πλατφόρμας προορισμού του πράκτορα.
- Στο **Ασφαλές/Ασφαλισμένο Επίπεδο** και για την περιοχή της ασφάλειας επικοινωνιών θεωρούμε ότι δεν απαιτούνται επιπλέον μέτρα ασφάλειας, πέρα από αυτά του προηγούμενου επίπεδου. Η ασφάλεια επικοινωνιών αποτελεί ένα ώριμο τεχνολογικά χώρο και όπως είδαμε, τα υπάρχοντα συστήματα χρησιμοποιούν επαρκείς μηχανισμούς ασφάλειας [1], [2].

4.3.4 Μοντέλο Εμπιστοσύνης

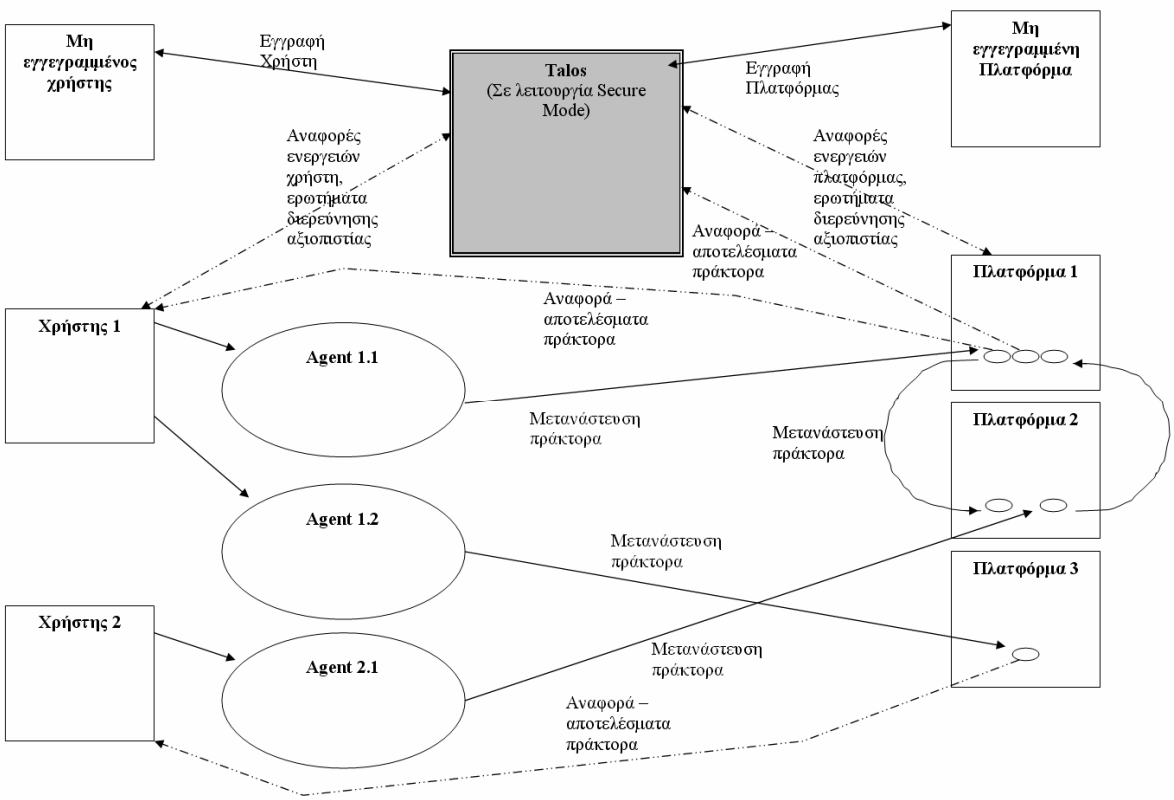
Στην πορεία της μέχρι τώρα έρευνας καταλήξαμε στο συμπέρασμα ότι τα μοντέλα εμπιστοσύνης που υιοθετούνται από τα υπάρχοντα συστήματα κινητών πρακτόρων κρίνονται ανεπαρκή για εφαρμογή σε ευρεία κλίμακα, κάτι που περιορίζει και τη χρήση τους [34]. Έτσι, το μοντέλο που προτείνουμε παρέχει μια εναλλακτική προσέγγιση, με την εισαγωγή μιας επιπλέον οντότητας στο σύστημα στα δύο υψηλότερα επίπεδα ασφάλειας.

- Το **Βασικό Επίπεδο** λειτουργίας διαμορφώνεται αντίστοιχα με τα υπάρχοντα μοντέλα εμπιστοσύνης συστημάτων κινητών πρακτόρων (Εικόνα 1), καθώς οι απαιτήσεις ασφάλειας δεν είναι μεγάλες. Σε αυτό το επίπεδο είδαμε ότι απαιτείται η αμοιβαία αυθεντικοποίηση πράκτορα και πλατφόρμας. Μετά από αυτή τη διαδικασία ο πράκτορας θεωρείται εξ ορισμού έμπιστος από την πλατφόρμα αλλά και αντίστροφα. Αναλύσαμε προηγουμένως τους κινδύνους αυτής της απλουστευτικής προσέγγισης, η οποία όμως κρίνεται επαρκής για το συγκεκριμένο επίπεδο και την αξία των εφαρμογών που το χρησιμοποιούν.
- Αντίθετα, στο **Ασφαλές Επίπεδο** λειτουργίας προβλέπονται επιπλέον μέτρα για την ενίσχυση του μοντέλου εμπιστοσύνης. Αναφέραμε προηγουμένως την ύπαρξη της οντότητας Talos, ως κεντρικού διαχειριστή εμπιστοσύνης. Η λειτουργία του προτεινόμενου μοντέλου στηρίζεται σε αυτή την οντότητα στα δύο υψηλότερα επίπεδα ασφάλειας. Στο συγκεκριμένο επίπεδο λειτουργεί ως Έμπιστη Τρίτη Οντότητα (Εικόνα 45) με αυξημένες όμως αρμοδιότητες και προσαρμοσμένη στη λειτουργία των συστημάτων κινητών πρακτόρων. Όλοι οι χρήστες που ενδιαφέρονται να χρησιμοποιήσουν το Ασφαλές Επίπεδο είναι υποχρεωτικό να εγγραφούν στον Talos προκειμένου να μπορούν να εισαχθούν στο σύστημα οι πράκτορές τους ή οι πλατφόρμες τους. Ο Talos διατηρεί ένα επίπεδο υπόληψης για τον κάθε χρήστη, το οποίο και αποδίδεται στις οντότητες που κατέχει. Όλες οι οντότητες έχουν το δικαίωμα να αναφέρουν τη δραστηριότητα άλλων οντοτήτων. Μετά από κάθε αναφορά το επίπεδο εμπιστοσύνης προσαρμόζεται αντίστοιχα. Κάθε θετική αναφορά καταμετράται ως μια θετική ψήφος, ενώ οι αρνητικές

αναφορές προσμετρώνται αρνητικά. Επιπλέον, για τις αρνητικές αναφορές αναφέρεται υποχρεωτικά το είδος της κακόβουλης ενέργειας και η σοβαρότητά της, ενώ συνοδεύονται και από τα σχετικά αρχεία καταγραφής. Παράλληλα, όλες οι οντότητες μπορούν να διερευνήσουν την υπόληψη άλλων οντοτήτων που συμμετέχουν στο σύστημα. Με βάση αυτήν την πληροφορία λαμβάνεται η απόφαση για το αν πρόκειται να προχωρήσει σε αίτηση συνεργασίας με την υπό διερεύνηση οντότητα. Αυτό το απλό προσαρμοστικό μοντέλο εμπιστοσύνης είναι καθιερωμένο σε σύγχρονες διαδικτυακές εμπορικές εφαρμογές με ιδιαίτερη εξάπλωση [72]. Έτσι, μια πλατφόρμα εκτέλεσης μπορεί να επιλέξει να απορρίψει την αίτηση μετανάστευσης ενός πράκτορα με χαμηλό επίπεδο εμπιστοσύνης, ενώ αντίστροφα ένας πράκτορας μπορεί να παρακάμψει μια πλατφόρμα εκτέλεσης με αρνητικές αναφορές. Σε αυτό το σημείο πρέπει να τονίσουμε ότι ένα υψηλό επίπεδο εμπιστοσύνης αποτελεί ένδειξη της έως τώρα δραστηριότητας μιας οντότητας και δεν αποτελεί εγγύηση μελλοντικής συμπεριφοράς. Σε κάθε περίπτωση, όμως, η προσθήκη ενός συστήματος υπόληψης, αν και όχι απολύτως αξιόπιστου, αποτελεί απαραίτητη προσθήκη για την ασφαλή λειτουργία ενός συστήματος κινητών πρακτόρων. Όλες οι δραστηριότητες αναφέρονται υποχρεωτικά στον Talos, ο οποίος και διατηρεί αρχείο με όλες τις αναφορές αποτελεσμάτων πρακτόρων, τις μεταναστεύσεις και τη δραστηριότητα της κάθε πλατφόρμας. Σε συνδυασμό με την υποχρεωτική εγγραφή των χρηστών επιτρέπει την προσφορά ισχυρών υπηρεσιών μη αποποίησης από τον Talos. Στην περίπτωση που πραγματοποιηθεί επίθεση σε πράκτορα ή πλατφόρμα ο Talos προχωρά στην ταυτοποίηση της κακόβουλης οντότητας, μειώνει το επίπεδο εμπιστοσύνης που της αποδίδεται και ενημερώνει τον χρήστη-θύμα σχετικά με το περιστατικό. Με τη χρήση αυτού του μηχανισμού μια οντότητα μπορεί να βελτιώσει την εγκυρότητα των υποθέσεων εμπιστοσύνης που κάνει.

Ο Talos μοιάζει με μια Έμπιστη Τρίτη Οντότητα στο σημείο ότι μπορεί να υποστηρίξει πολλές και διαφορετικές εφαρμογές από την ίδια πλατφόρμα. Έτσι, υποστηρίζει εγγραφή χρηστών, οι οποίοι στη συνέχεια μπορούν να δημιουργήσουν διαφορετικού τύπου πράκτορες και πλατφόρμες, ενώ το επίπεδο υπόληψης του κάθε χρήστη διαμορφώνεται συγκεντρωτικά από όλες τις δραστηριότητες των οντοτήτων

του. Ο μόνος περιορισμός είναι ότι όλες οι οντότητες οφείλουν να ακολουθούν τα καθιερωμένα πρότυπα επικοινωνίας και συνεργασίας κινητών πρακτόρων [15], [17]. Ο Talos διαφοροποιείται από μια Έμπιστη Τρίτη Οντότητα στο ότι δεν συμμετέχει μονάχα αρχικά κατά τη διαδικασία της αυθεντικοποίησης, αλλά συνεχίζει να αλληλεπιδρά με το όλο σύστημα σε όλα τα στάδια λειτουργίας του, αποτελώντας ένα κεντρικό διαχειριστή ασφάλειας.



Εικόνα 45: Ο Talos στο μεσαίο επίπεδο ασφάλειας

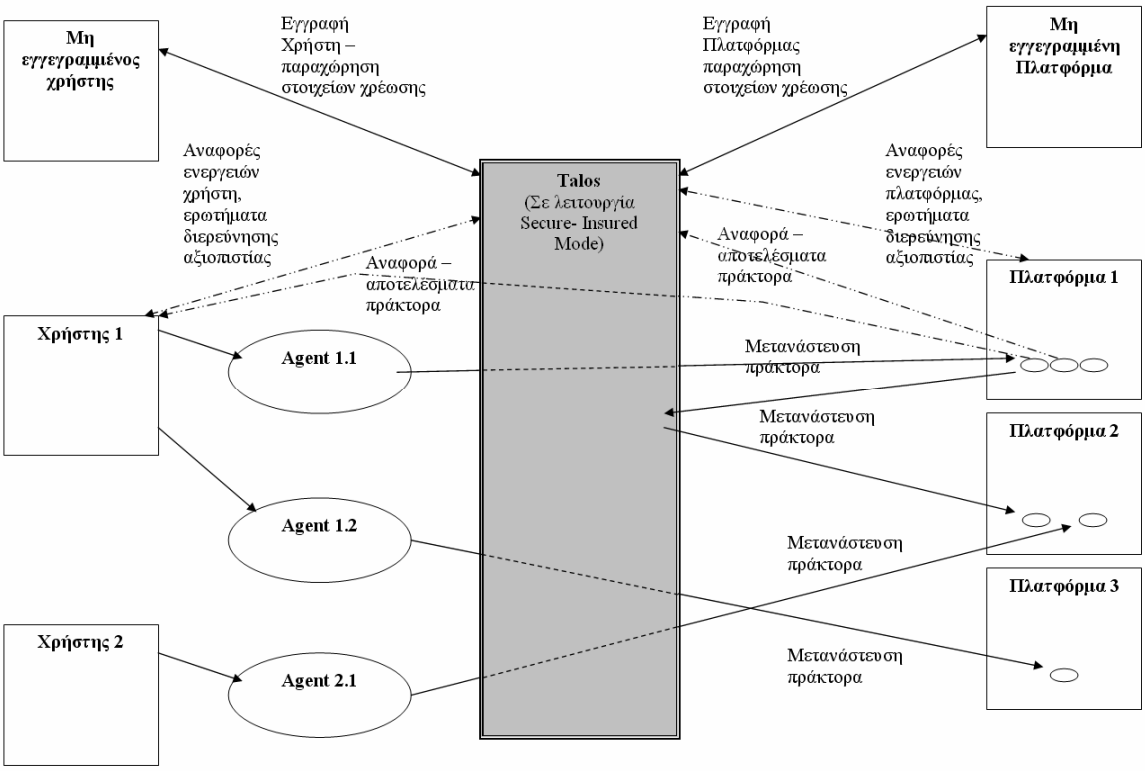
- Τέλος, στο **Ασφαλές/Ασφαλισμένο Επίπεδο** λειτουργίας χρησιμοποιούνται όλα τα χαρακτηριστικά ασφάλειας του προηγούμενου επιπέδου, ενώ ο Talos παρέχει επιπλέον λειτουργίες (Εικόνα 46). Κύρια διαφορά αποτελούν οι ασφαλιστικές υπηρεσίες που παρέχει σε αυτό το επίπεδο. Ο κάθε χρήστης δεσμεύεται με την υπογραφή συμβολαίου το οποίο προβλέπει την αξία ασφάλισης των εφαρμογών που πρόκειται να χρησιμοποιήσουν το προτεινόμενο σύστημα, ενώ προβλέπει και τις συνέπειες που θα υποστεί ο χρήστης σε περίπτωση που κάποια από τις οντότητές του πραγματοποιήσει κακόβουλες ενέργειες.

Κατά την αρχική εγγραφή στον Talos ο χρήστης εκτός του ότι πρέπει να ταυτοποιηθεί, οφείλει και να παραχωρήσει και στοιχεία χρέωσης. Η μέθοδος είναι αντίστοιχη με εκείνη που χρησιμοποιείται από το Paypal [73]. Ο χρήστης πρέπει να παρέχει μαζί με τις προσωπικές του πληροφορίες και στοιχεία χρέωσης, τα οποία επαληθεύονται με τη δέσμευση ενός μικρού χρηματικού ποσού από το λογαριασμό του χρήστη. Παράλληλα, στις πληροφορίες χρέωσης αποστέλλεται ένας τυχαίος αριθμός PIN (Personal Identification Number), τον οποίο ο χρήστης εισάγει προκειμένου να ολοκληρώσει τη διαδικασία της εγγραφής. Αυτή η διαδικασία διασφαλίζει την εγκυρότητα των στοιχείων χρέωσης, τα οποία θα χρησιμοποιηθούν για χρέωση αποζημιώσεων σε περίπτωση κακόβουλης συμπεριφοράς.

Επιπλέον, προκειμένου να ισχυροποιηθούν ακόμη περισσότερο οι υπηρεσίες μη αποποίησης ο Talos απαιτεί όλες οι δραστηριότητες να πραγματοποιούνται διαμέσω του ιδίου. Καμία οντότητα δεν επικοινωνεί κατευθείαν με κάποια άλλη, ενώ ακόμη και η διαδικασία της μετανάστευσης πραγματοποιείται μόνο μέσω του Talos, ο οποίος έτσι αποκτά λειτουργίες διακομιστή μεσολάβησης. Με αυτού του τύπου τη λειτουργία ο Talos παύει να λειτουργεί ως Έμπιστη Τρίτη Οντότητα αλλά αποκτά ενεργό ρόλο και δρα περισσότερο ως πύλη (Gateway) στο σύστημα, όπως συμβαίνει έως ενός βαθμού σε κάποια μικρά συστήματα κινητών πρακτόρων ειδικού σκοπού [58]. Στην περίπτωση παραβίασης της ασφάλειας, η κακόβουλη οντότητα μπορεί να ταυτοποιηθεί άμεσα και ο ένοχος χρήστης καθίσταται νομικά υπεύθυνος και υπόκειται σε πραγματικές συνέπειες. Καθώς έχει αθετήσει το συμβόλαιο που τον δεσμεύει, το σύστημα προχωρεί στον υπολογισμό της οικονομικής βλάβης που προκάλεσε και με τη χρήση των στοιχείων που ο χρήστης έχει παραχωρήσει κατά την εγγραφή του προχωρά στη χρέωσή του.

Το υψηλό επίπεδο ασφάλειας του προτεινόμενου μοντέλου υλοποιεί συγκεντρωτικά πολλούς μηχανισμούς ασφάλειας σε σημείο που να ξεπερνά το επίπεδο ασφάλειας που παρέχουν τα σημερινά συστήματα. Παρολ’ αυτά όμως οφείλει να προβλέπει το ενδεχόμενο αποτυχίας τους και να λαμβάνει μέτρα αντιμετώπισης. Αυτό το επιτυγχάνει με το συνδυασμό υπηρεσιών μη αποποίησης και ασφάλισης. Έτσι, καθιστά δυνατή τη χρήση συστημάτων κινητών πρακτόρων σε κρίσιμες εφαρμογές καθώς μειώνει σε ιδιαίτερα χαμηλά επίπεδα τον κίνδυνο

επίθεσης και προβλέπει δυνατότητα παροχής οικονομικής ασφάλισης και αποζημίωσης σε περίπτωση αποτυχίας των μέτρων ασφάλειας.



Εικόνα 46: Ο Talos στο υψηλό επίπεδο ασφάλειας

Πίνακας 5: Χαρακτηριστικά ασφάλειας προτεινόμενου μοντέλου ανά περιοχή και επίπεδο ασφάλειας.

	Βασικό Επίπεδο	Ασφαλές Επίπεδο	Ασφαλές/Ασφαλισμένο Επίπεδο
Ασφάλεια Πράκτορα	**- Προστασία εικονικής μηχανής** **- Αμοιβαία αυθεντικοποίηση με βάση ψηφιακές υπογραφές**	- Προστασία εικονικής μηχανής - Αμοιβαία αυθεντικοποίηση με βάση ψηφιακές υπογραφές **- Ισχυρές υπηρεσίες μη αποποίησης** **- Πλήρως Ομομορφική Κρυπτογραφία**	- Προστασία εικονικής μηχανής - Αμοιβαία αυθεντικοποίηση με βάση ψηφιακές υπογραφές - Ισχυρές υπηρεσίες μη αποποίησης - Πλήρως Ομομορφική Κρυπτογραφία **- Ασφάλιση σε περίπτωση παραβίασης ακεραιότητας πράκτορα**
Ασφάλεια Πλατφόρμας	**- Αμοιβαία αυθεντικοποίηση με βάση ψηφιακές υπογραφές** **- Τεχνικές απομονωμένης εκτέλεσης**	- Αμοιβαία αυθεντικοποίηση με βάση ψηφιακές υπογραφές - Τεχνικές απομονωμένης εκτέλεσης **- Διαχείριση πόρων πραγματικού χρόνου** **- Σύστημα εντοπισμού εισβολών** **- Ισχυρές υπηρεσίες μη αποποίησης**	- Αμοιβαία αυθεντικοποίηση με βάση ψηφιακές υπογραφές - Τεχνικές απομονωμένης εκτέλεσης - Διαχείριση πόρων πραγματικού χρόνου - Σύστημα εντοπισμού εισβολών - Ισχυρές υπηρεσίες μη αποποίησης **- Ασφάλιση σε περίπτωση παραβίασης ακεραιότητας πλατφόρμας**
Ασφάλεια Επικοινωνιών / Ματανάστευσης	**- Ανταλλαγή μη κρυπτογραφημένων μηνυμάτων** **- Δυνατότητα ισχυρής μετανάστευσης**	**- Ανταλλαγή κρυπτογραφημένων μηνυμάτων (SSL/TLS)** - Ισχυρή μετανάστευση **μέσω κρυπτογραφη-**	- Ανταλλαγή κρυπτογραφημένων μηνυμάτων (SSL/TLS) - Ισχυρή μετανάστευση μέσω κρυπτογραφημένων καναλιών

		μένων καναλιών	
Μοντέλο Εμπιστοσύνης	**- Πλατφόρμα έμπιστη εξ ορισμού** **- Αυθεντικοποιημένος χρήστης θεωρείται έμπιστος από την πλατφόρμα**	- Πλατφόρμα έμπιστη **ανάλογα με την υπόληψή της** - Αυθεντικοποιημένος χρήστης θεωρείται έμπιστος από την πλατφόρμα **ανάλογα με την υπόληψη του** **- Ισχυρές υπηρεσίες μη αποποίησης** **- Υπηρεσία Διαχείρισης Εμπιστοσύνης (Talos) – secure mode** **- Υποχρεωτική εγγραφή χρηστών στον Talos**	- Πλατφόρμα έμπιστη ανάλογα με την υπόληψή της - Αυθεντικοποιημένος χρήστης θεωρείται έμπιστος από την πλατφόρμα ανάλογα με την υπόληψη του - Ισχυρές υπηρεσίες μη αποποίησης - Υπηρεσία Διαχείρισης Εμπιστοσύνης (Talos) **- insurance mode** - Υποχρεωτική εγγραφή χρηστών στον Talos**, εξακρίβωση στοιχείων χρέωσης**

4.4 Επιχειρηματικό Μοντέλο Λειτουργίας

Είδαμε ότι το προτεινόμενο μοντέλο ασφάλειας και εμπιστοσύνης προτείνει μια σειρά τεχνικών και πολιτικών ασφάλειας, αλλά επιπλέον, για τα δύο υψηλότερα επίπεδα λειτουργίας, εισάγει τη χρήση της οντότητας Talos στο σύστημα. Καθώς όμως ο Talos λειτουργεί ως Έμπιστη Τρίτη Οντότητα στο μεσαίο επίπεδο και ως κεντρική πύλη του συστήματος στο υψηλό επίπεδο, που μάλιστα διαχειρίζεται ασφαλιστικά συμβόλαια, χρεώσεις και αποζημιώσεις η λειτουργία του συνεπάγεται πραγματικό οικονομικό κόστος. Έτσι, οφείλουμε να προτείνουμε ένα επιχειρηματικό μοντέλο (business model) που να καλύπτει τη λειτουργία του με τρόπο οικονομικά βιώσιμο. Κάτι τέτοιο, βεβαίως είναι εκτός των ορίων του αντικειμένου μελέτης της παρούσας διατριβής και θα παρουσιαστεί περισσότερο ως ενδεικτικές κατευθύνσεις όσον αφορά στην πηγή από την οποία θα πρέπει να καλυφθεί το κόστος λειτουργίας του προτεινόμενου μοντέλου ασφάλειας και εμπιστοσύνης καθώς και το φορέα από τον οποίο θα μπορούσε να το υλοποιήσει. Η επιλογή να συμπεριληφθεί ένα επιχειρηματικό μοντέλο λειτουργίας έγινε καθαρά για λόγους πληρότητας της διατριβής.

Το κόστος της λειτουργίας του Talos αναγκαστικά πρέπει να καλυφθεί από τους χρήστες που χρησιμοποιούν τις υπηρεσίες του για τις εφαρμογές τους. Έτσι, για το Βασικό επίπεδο λειτουργίας του προτεινόμενου μοντέλου δεν πρέπει να υπάρχει καμία είδους οικονομική επιβάρυνση στους χρήστες. Όλα τα μέτρα που προβλέπονται για το συγκεκριμένο επίπεδο είναι αποτελούν πολιτικές και μηχανισμούς που πρέπει να υλοποιηθούν από τα ίδια τα συστήματα κινητών πρακτόρων, ενώ το ίδιο το μοντέλο δεν παρέχει καμία ενεργή υπηρεσία, καθώς σε αυτό το επίπεδο ο Talos απουσιάζει.

Για το Ασφαλές επίπεδο λειτουργίας παρέχεται ο Talos με τις υπηρεσίες Έμπιστης Τρίτης Οντότητας, οπότε και συνεπάγεται κόστος λειτουργίας. Παρόλ' αυτά όμως δεν φτάνει στα επίπεδα του υψηλού επιπέδου, στο οποίο αναλαμβάνει πολύ πιο ενεργό ρόλο και συμμετέχει σε περισσότερες αλληλεπιδράσεις με το υπόλοιπο σύστημα. Επιπλέον, αν και το μεσαίο αυτό επίπεδο παρέχει σημαντικό βαθμό ασφάλειας σε σχέση με πολλά υπάρχοντα συστήματα, δεν κρίνεται επαρκές

για εφαρμογές κινητών πρακτόρων με χρηματικές συναλλαγές. Επομένως, είναι απίθανο να επιλεγεί από τους χρήστες το Ασφαλές επίπεδο ως πληρωμένη υπηρεσία για μια εφαρμογή κινητών πρακτόρων που δεν συνεπάγεται οικονομικό όφελος για το δημιουργό της ή τις υπόλοιπες οντότητες που αλληλεπιδρά. Έτσι, επιλέγουμε να αποτελεί ελεύθερη υπηρεσία και το όποιο κόστος αυτή συνεπάγεται να καλύπτεται από τους χρήστες που χρησιμοποιούν το υψηλότερο επίπεδο λειτουργίας.

Στο Ασφαλές/Ασφαλισμένο επίπεδο, η λειτουργία του Talos είναι πιο σύνθετη και συνεπάγεται μεγαλύτερο κόστος. Επιπλέον οι χρήστες ούτως ή άλλως πραγματοποιούν οικονομικές συναλλαγές με τον Talos στο πλαίσιο των υπηρεσιών ασφάλισης. Ακόμη, οι εφαρμογές τους είναι κατά πάσα πιθανότητα υψηλής αξίας, καθώς επιλέγουν να ενσωματώσουν τόσα μέτρα ασφάλειας και επιπλέον τη δυνατότητα της ασφάλισης. Υπό αυτές τις συνθήκες χρήσης είναι αναμενόμενο να γίνει αποδεκτή από τους υποψήφιους χρήστες μια πληρωμένη υπηρεσία, η οποία να τους εξασφαλίζει τα θέματα ασφάλειας της πολύτιμης εφαρμογής τους.

Η υλοποίηση και διαχείριση του Talos, και για τα δύο επίπεδα που χρησιμοποιείται, οφείλει να πραγματοποιηθεί από έναν οργανισμό ανεξάρτητο από κάθε σύστημα κινητών πρακτόρων και με κοινή αποδοχή. Έτσι, πλέον κατάλληλους υποψηφίους για την ανάπτυξη του προτεινόμενου μοντέλου ασφάλειας και εμπιστοσύνης αποτελούν οι οργανισμοί που ασχολούνται με την έκδοση πιστοποιητικών (Certification Authorities) και λειτουργούν ήδη ως Έμπιστες Τρίτες Οντότητες. Τέτοιοι οργανισμοί έχουν εμπειρία στη διαχείριση σχέσεων εμπιστοσύνης (Web of Trust), την υλοποίηση πληροφοριακών συστημάτων παροχής υπηρεσιών ασφάλειας με προοπτική απρόσκοπτης λειτουργίας ενώ ήδη χρεώνουν τους χρήστες για τις υπηρεσίες τους αυτές. Επιπλέον, παρέχουν τις υπηρεσίες τους παράλληλα σε πληθώρα ανεξάρτητων διαδικτυακών εφαρμογών. Έτσι, η υλοποίηση ενός συστήματος όπως το προτεινόμενο αποτελεί λογική προέκταση της επιχειρηματικής τους λειτουργίας σε ένα νέο χώρο, χρησιμοποιώντας ήδη υπάρχουσες τεχνολογίες, πρακτικές και το κυριότερο, υποδομές.

Αναλαμβάνοντας την υλοποίηση ενός τέτοιου συστήματος, ο υπεύθυνος οργανισμός μπορεί να χρεώνει τους χρήστες που χρησιμοποιούν τις υπηρεσίες του

υψηλότερου επιπέδου ασφάλειας. Κάτι αντίστοιχο υλοποιείται και στην περίπτωση του συστήματος Havana που εξετάστηκε, αν και σε μικρότερη έκταση. Σε αυτό η Gateway, χρεώνει για τις υπηρεσίες τις τους χρήστες που συμμετέχουν στο εμπορικό σχήμα που δημιουργεί. Αυτό μπορεί να γίνει κατά την εγγραφή του χρήστη και ανάλογα με το πλήθος των πρακτόρων ή πλατφορμών που εισάγει στο σύστημα και με το ύψος της ασφάλισης που επιθυμεί να ορίσει. Ως αντάλλαγμα ο οργανισμός παρέχει τις υπηρεσίες ασφάλειας και ασφάλισης που προβλέπονται από το μοντέλο, ενώ είναι σε θέση να παρέχει και στοιχεία από τα αρχεία καταγραφής, σε περίπτωση νομικής αντιδικίας μεταξύ χρηστών, μετά από κάποια παραβίαση ασφάλειας.

4.5 Συμπεράσματα

Το παραπάνω προτεινόμενο μοντέλο ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες θεωρούμε ότι είναι σε θέση να καλύψει τα κενά ασφάλειας που έχουν διαπιστωθεί και επιβραδύνουν την υιοθέτηση της τεχνολογίας. Για να το επιτύχει προβλέπει τη χρήση τόσο κλασικών όσο και πρωτότυπων τεχνικών ασφάλειας. Παράλληλα, κύριο χαρακτηριστικό του μοντέλου αποτελεί ο συνδυασμός ισχυρών υπηρεσιών μη αποποίησης μαζί με υπηρεσίες ασφάλισης. Αυτές παρέχονται προαιρετικά για τις εφαρμογές που θα επιλέξουν το υψηλό επίπεδο ασφάλειας και λειτουργούν σαν ισχυρός αποτρεπτικός παράγοντας για την πραγματοποίηση επιθέσεων.

Προκειμένου να είναι σε θέση να παρέχει τις υπηρεσίες του, το μοντέλο εισάγει μία κεντρική οντότητα στο σύστημα κινητών πρακτόρων, τον Talos, ο οποίος λειτουργεί τόσο ως κεντρικός διαχειριστής ασφάλειας, όσο και ως υπεύθυνος απόδοσης ευθυνών σε περιστατικά παραβιάσεων. Η αρχιτεκτονική του είναι τέτοια που η υλοποίησή του αναμένεται να είναι απλή από υπάρχοντες οργανισμούς που παρέχουν υπηρεσίες Έμπιστης Τρίτης Οντότητας.

Στη συνέχεια οφείλουμε να διερευνήσουμε εάν ένα τέτοιο μοντέλο επιβαρύνει τη λειτουργία ενός συστήματος κινητών πρακτόρων και σε ποιο βαθμό.

Αυτό επιδιώκεται με την πραγματοποίηση μιας προσομοίωσης, η οποία παρουσιάζεται στο επόμενο κεφάλαιο.

5 ΠΡΟΣΟΜΟΙΩΣΗ ΠΡΟΤΕΙΝΟΜΕΝΟΥ ΣΥΣΤΗΜΑΤΟΣ

5.1 Εισαγωγή

Στο τελευταίο κεφάλαιο της διατριβής εξετάζουμε την επίδραση που θα είχε στις επιδόσεις ενός συστήματος πρακτόρων η εφαρμογή του προτεινόμενου μοντέλου μας, με την πραγματοποίηση μιας προσομοίωσης σε περιβάλλον εικονικού δικτύου. Κάτι τέτοιο κρίνεται απαραίτητο για να διερευνηθεί το κατά πόσο μπορεί να είναι εφαρμόσιμο το προτεινόμενο μοντέλο και να εντοπιστούν ενδεχόμενα προβλήματα που χρήζουν βελτίωσης. Επιπλέον, αναλύονται οι λόγοι που οδήγησαν στη επιλογή της προσομοίωσης σαν μέθοδο εκτίμησης των επιδόσεων.

5.2 Επιλογή Προσομοίωσης

Μετά τη πρόταση του μοντέλου ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες στο προηγούμενο κεφάλαιο σε θεωρητικό επίπεδο, κρίνεται απαραίτητη η αξιολόγησή του όσον αφορά στη λειτουργικότητά του. Αυτό μπορεί να πραγματοποιηθεί με δύο μεθόδους:

1. Την υλοποίηση / ενσωμάτωση του προτεινόμενου μοντέλου σε κάποιο υπάρχον σύστημα πρακτόρων και την πραγματοποίηση μετρήσεων σε πραγματικές συνθήκες λειτουργίας.
2. Την προσομοίωσή του σε περιβάλλον εικονικού δικτύου.

Από τους παραπάνω τρόπους, εκείνος που επιλέχθηκε ήταν εκείνη της προσομοίωσης. Μειονέκτημα της μεθόδου της προσομοίωσης σε σχέση με την υλοποίηση του μοντέλου αποτελεί το ότι με την υλοποίηση, ενδεχομένως θα ήταν δυνατόν η λήψη επιπλέον συμπερασμάτων για τη συμπεριφορά του προτεινόμενου μοντέλου. Συγκεκριμένα, θα μπορούσαν να διαπιστωθούν τυχόν λειτουργικά προβλήματα που παρουσιάζονται σε πραγματικές συνθήκες λειτουργίας.

Παρόλ' αυτά όμως καθώς κρίθηκε ότι η μέθοδος της προσομοίωσης προσέφερε μια σειρά από πλεονεκτήματα σε σχέση με την υλοποίηση του.

- Η υλοποίηση θα απαιτούσε την εγκατάσταση του συστήματος σε αρκετούς υπολογιστές σε δίκτυο WAN, κάτι που δεν είναι δυνατόν στο τοπικό δίκτυο του Πανεπιστημίου Πειραιώς.
- Η εγκατάσταση θα απαιτούσε εύρεση ικανού αριθμού server στους οποίους θα έτρεχε το νέο σύστημα, καθώς και χρήστες που θα το χρησιμοποιούσαν συστηματικά.
- Το εγκατεστημένο σύστημα θα απαιτούσε μακρόχρονη λειτουργία όλων των υπολογιστών, προκειμένου να ληφθεί ικανό ποσό δεδομένων χρήσης. Με κάθε αλλαγή ή ενημέρωση του συστήματος θα έπρεπε να επανεκκινάται ή δειγματοληψία των δεδομένων από την αρχή.
- Με τη χρήση της προσομοίωσης δεν επηρεάζονται οι επιδόσεις του συστήματος οι παράμετροι προγραμματισμού και βελτιστοποίησης κώδικα.
- Η προσομοίωση μπορεί πολύ εύκολα να εξετάσει τις επιδόσεις του συστήματος σε κάθε σχεδόν κλίμακα που θα απαιτηθεί και κάτω από διαφορετικά σενάρια χρήσης.

Σε γενικές γραμμές η υλοποίηση του νέου μοντέλου μπορούσε να πραγματοποιηθεί μονάχα σε περιβάλλον (LAN) διαφορετικό από αυτό προορίζεται και κάτω από συνθήκες που δεν θα μπορούσαν να ελεγχθούν και να αποτιμηθούν πλήρως. Κάτι τέτοιο θα οδηγούσε σε ελλιπείς και μη ρεαλιστικές μετρήσεις. Από την άλλη πλευρά η προσομοίωση αποτελεί μια ευέλικτη λύση που μπορεί να αποτιμήσει τη λειτουργία του προτεινόμενου συστήματος κάτω από ελεγχόμενες συνθήκες, σε διάφορα σενάρια χρήσης και χωρίς ιδιαίτερες απαιτήσεις σε υλικό και δικτυακούς πόρους.

Για τις ανάγκες τις προσομοίωσης επιλέχθηκε το πρόγραμμα Comnet της εταιρίας Compuware. Ανήκει στην κατηγορία προσομοιωτών διακριτών γεγονότων, που αποτελεί την πλειοψηφία των δικτυακών προσομοιωτών (Discrete Event Simulation) [63], [64]. Διαθέτει όλες τις απαραίτητες δυνατότητες που απαιτούνταν για τις ανάγκες της έρευνας, ενώ αποτελεί ένα γρήγορο στην εκτέλεση πρόγραμμα,

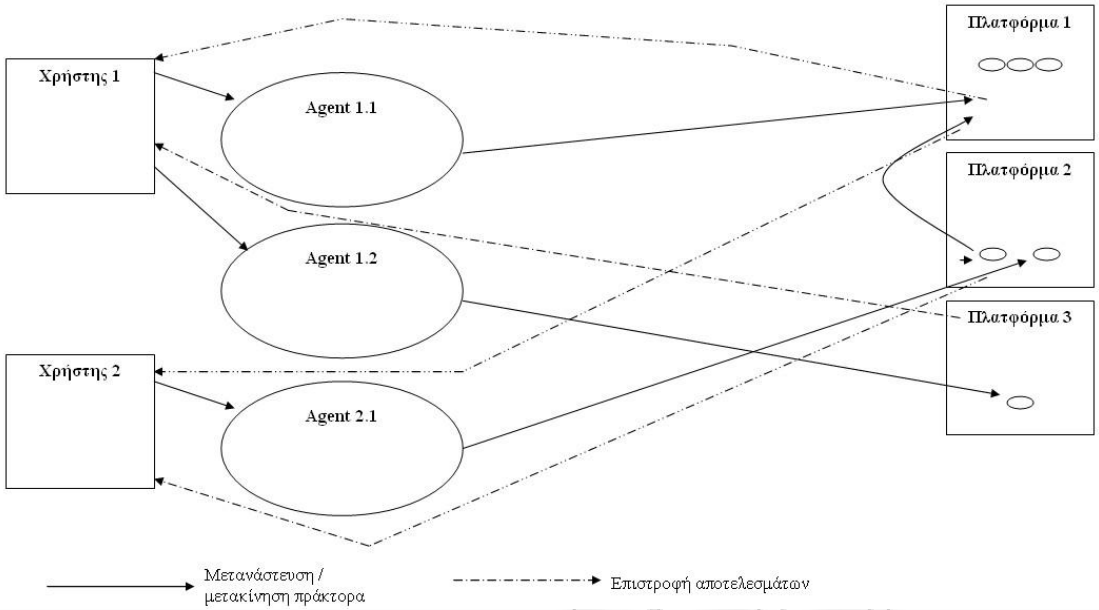
με μεγάλες δυνατότητες παραμετροποίησης του δικτύου και των πηγών κίνησης μέσα σε αυτό, κατά τρόπο μεταξύ τους ανεξάρτητο. Επιπλέον, συνοδεύεται από εκτενή βιβλιογραφία και επεξηγήσεις για τη λειτουργία του ενώ διαθέτει ιδιαιτέρως εύχρηστο γραφικό περιβάλλον. Σημαντικός παράγοντας στην επιλογή του κρίθηκε ο σημαντικός αριθμός δικτυακών προτύπων στην βιβλιοθήκη του, κάτι που μας έδωσε τη δυνατότητα κατασκευής ακριβέστερου δικτυακού μοντέλου για την προσομοίωσή μας.

5.3 Σενάριο Λειτουργίας

Το σενάριο λειτουργίας που επιλέχθηκε είναι εκείνο μιας εμπορικής εφαρμογής, μιας και το προτεινόμενο μοντέλο αποσκοπεί σε μεγάλο βαθμό στην εξασφάλιση εγχρήματων συναλλαγών με χρήση κινητών πρακτόρων και απεικονίζεται στην **Εικόνα 47.** Στο σενάριο εμπλέκονται δύο χρήστες-αγοραστές που δημιουργούν τρεις συνολικά πράκτορες (shopping agents), οι οποίοι μεταναστεύουν σε τρεις διαφορετικές πλατφόρμες καταστημάτων. Στη συνέχεια επιστρέφουν τα αποτελέσματα (αναζήτησης ή αναφορά αγορών) στους δημιουργούς τους, ενώ ο ένας από αυτούς μεταναστεύει από μια πλατφόρμα καταστήματος σε μια διαφορετική, προκειμένου να συνεχίσει τη λειτουργία του. Από εκεί αναφέρει ξανά τα νέα του αποτελέσματα στο δημιουργό του. Το σενάριο δημιουργήθηκε με βάση τη διαγραμματική λειτουργία του προτεινόμενου μοντέλου στα 2 επίπεδα ασφάλειας που διαθέτει (Εικόνα 45, Εικόνα 46).

Τα διακριτά γεγονότα που συμβαίνουν στο σενάριό της προσομοίωσης είναι τα παρακάτω:

- Ο Χρήστης 1 δημιουργεί τον Agent 1.1 → Ο Agent 1.1 μεταναστεύει στην Πλατφόρμα 1 → Αναφορά αποτελεσμάτων στον Χρήστη 1.
- Ο Χρήστης 1 δημιουργεί τον Agent 1.2 → Ο Agent 1.2 μεταναστεύει στην Πλατφόρμα 3 → Αναφορά αποτελεσμάτων στον Χρήστη 1.
- Ο Χρήστης 2 δημιουργεί τον Agent 2.1 → Ο Agent 2.1 μεταναστεύει στην Πλατφόρμα 2 → Αναφορά αποτελεσμάτων στον Χρήστη 2, Ο Agent 2.1 μεταναστεύει στην Πλατφόρμα 1 → Αναφορά αποτελεσμάτων στον Χρήστη 2.



Εικόνα 47: Γενικό σενάριο λειτουργίας που χρησιμοποιήθηκε στην προσομοίωση

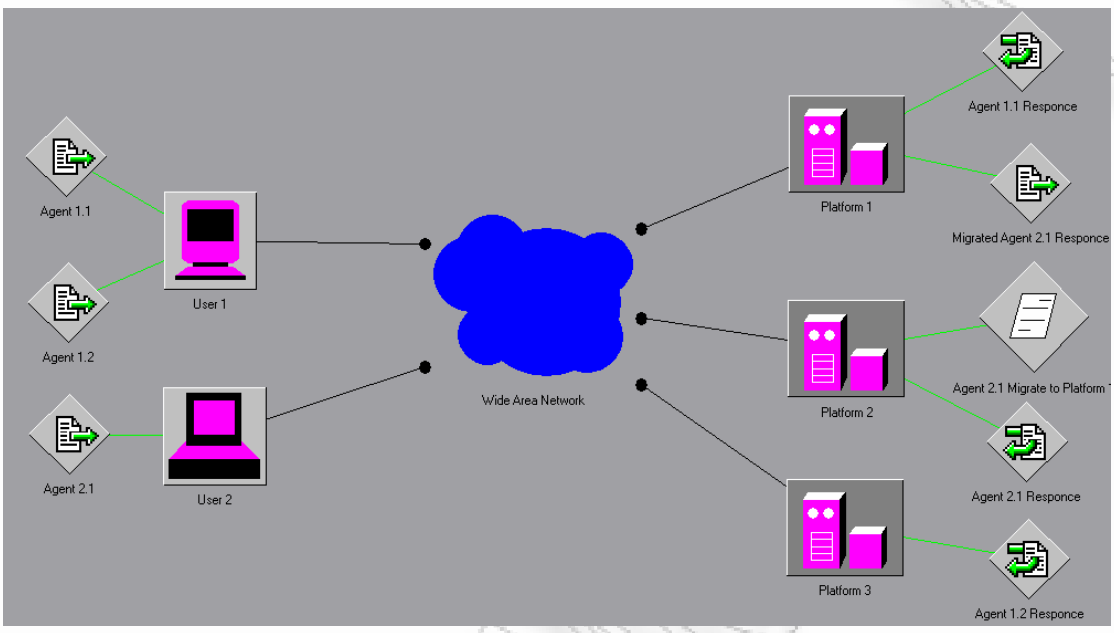
Το παραπάνω σενάριο θα εκτελεστεί τρεις συνολικά φορές. Τη πρώτη φορά θα προσομοιωθεί η λειτουργία πολλών υπαρχόντων συστημάτων που δεν διαθέτουν κεντρικοποιημένη διαχείριση. Τη δεύτερη φορά θα προσομοιωθεί το προτεινόμενο σύστημα στο πρώτο επίπεδο ασφάλειας (Secure mode) και την τρίτη θα γίνει προσομοίωση του υψηλού επιπέδου (Insured mode).

5.3.1 Προσομοίωση Υπαρχόντων Συστημάτων

Στη πρώτη επανάληψη της προσομοίωσης (Εικόνα 48) θα υλοποιηθούν ακριβώς τα βήματα του σεναρίου, καθώς δεν υπάρχει κάποια επιπλέον οντότητα στο σύστημα που να προσθέτει αλληλεπιδράσεις. Έτσι, οι ενέργειες που θα λάβουν χώρα είναι:

- Ο Χρήστης 1 δημιουργεί τον Agent 1.1 → Ο Agent 1.1 μεταναστεύει στην Πλατφόρμα 1 → Αναφορά αποτελεσμάτων στον Χρήστη 1.
- Ο Χρήστης 1 δημιουργεί τον Agent 1.2 → Ο Agent 1.2 μεταναστεύει στην Πλατφόρμα 3 → Αναφορά αποτελεσμάτων στον Χρήστη 1.
- Ο Χρήστης 2 δημιουργεί τον Agent 2.1 → Ο Agent 2.1 μεταναστεύει στην Πλατφόρμα 2 → Αναφορά αποτελεσμάτων στον Χρήστη 2, Ο Agent 2.1

μεταναστεύει στην Πλατφόρμα 1 → Αναφορά αποτελεσμάτων στον Χρήστη 2.



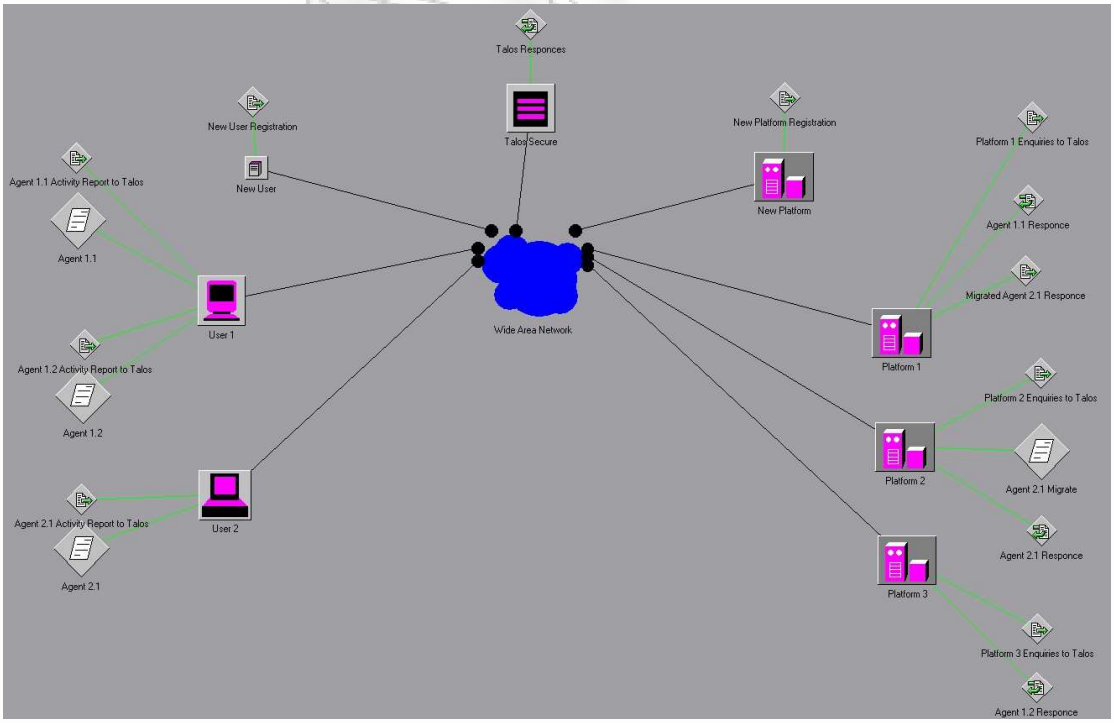
Εικόνα 48: Προσομοίωση της αρχιτεκτονικής υπαρχόντων συστημάτων στο περιβάλλον του Comnet, χωρίς κεντρικοποιημένη διαχείριση.

5.3.2 Προσομοίωση Secure Mode

Στη δεύτερη επανάληψη (**Εικόνα 49**) προσομοιώνεται η λειτουργία του προτεινόμενου συστήματος στο Secure Mode, όπως αυτή απεικονίζεται αρχιτεκτονικά στην Εικόνα 45. Σε αυτή τη προσομοίωση έχει αυξηθεί σημαντικά ο βαθμός πολυπλοκότητας του συστήματος, καθώς έχουν εισαχθεί επιπλέον οντότητες, ο Talos, νέοι χρήστες και πλατφόρμα, οι οποίες αυξάνουν τις αλληλεπιδράσεις. Εδώ υπάρχει κεντρικοποιημένη διαχείριση ασφάλειας από τον Talos, ο οποίος σε αυτό το mode λειτουργίας διαθέτει χαρακτηριστικά λειτουργίας TTP. Σύμφωνα με το μοντέλο μας, οι νέοι χρήστες και οι νέες πλατφόρμες οφείλουν να κάνουν εγγραφή στον Talos για να εισαχθούν στο σύστημα. Επιπλέον, όλες οι δραστηριότητες των πρακτόρων και των πλατφορμών αναφέρονται και καταγράφονται από τον Talos. Έτσι, οι ενέργειες που θα λάβουν χώρα είναι:

- Ο Νέος Χρήστης κάνει αίτηση εγγραφής προς τον Talos → Ο Talos απαντά στην αίτηση

- Η νέα Πλατφόρμα κάνει αίτηση εγγραφής προς τον Talos → Ο Talos απαντά στην αίτηση
- Ο Χρήστης 1 δημιουργεί τον Agent 1.1, το γεγονός αναφέρεται στον Talos → Ο Agent 1.1 μεταναστεύει στην Πλατφόρμα 1, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Χρήστη 1, το γεγονός αναφέρεται στον Talos.
- Ο Χρήστης 1 δημιουργεί τον Agent 1.2, το γεγονός αναφέρεται στον Talos → Ο Agent 1.2 μεταναστεύει στην Πλατφόρμα 3, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Χρήστη 1, το γεγονός αναφέρεται στον Talos.
- Ο Χρήστης 2 δημιουργεί τον Agent 2.1, το γεγονός αναφέρεται στον Talos → Ο Agent 2.1 μεταναστεύει στην Πλατφόρμα 2, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Χρήστη 2, το γεγονός αναφέρεται στον Talos, ο Agent 2.1 μεταναστεύει στην Πλατφόρμα 1, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Χρήστη 2, το γεγονός αναφέρεται στον Talos.



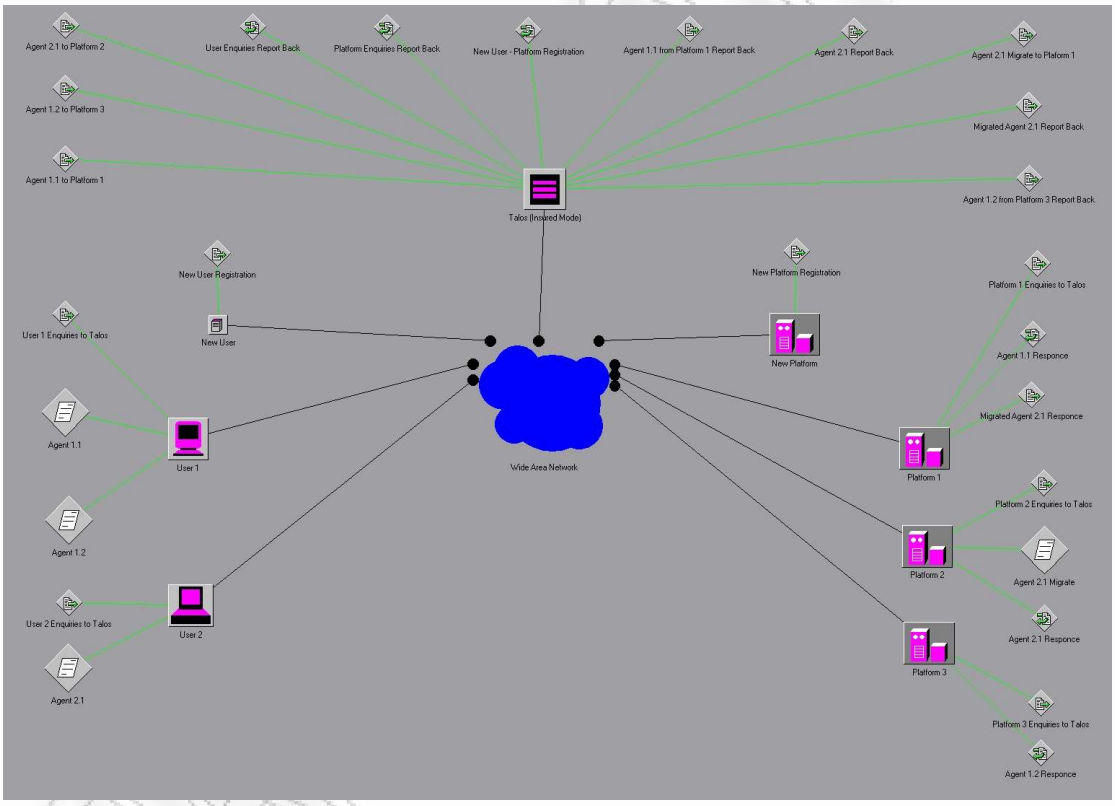
Εικόνα 49: Προσομοίωση της αρχιτεκτονικής του προτεινόμενου συστήματος (Secure Mode) στο περιβάλλον του Comnet.

5.3.3 Προσομοίωση Insured Mode

Στη τελευταία επανάληψη (**Εικόνα 50**) προσομοιώνεται η λειτουργία του προτεινόμενου συστήματος στο Insured Mode όπως αυτή απεικονίζεται αρχιτεκτονικά στην Εικόνα 46. Και σε αυτή την επανάληψη της προσομοίωσης υπάρχει κεντρικοποιημένη διαχείριση ασφάλειας από τον Talos, ο οποίος όμως εδώ λειτουργεί ως διακομιστής μεσολάβησης μεταξύ όλων των άλλων οντοτήτων. Ο βαθμός πολυπλοκότητας είναι ο πιο υψηλός, αν και ο αριθμός των οντοτήτων και των λειτουργιών που συμβαίνουν παραμένει ακριβώς ο ίδιος με το προηγούμενο επίπεδο. Αυτό συμβαίνει καθώς σύμφωνα με τα προτεινόμενο μοντέλο όλες οι αλληλεπιδράσεις δεν αναφέρονται απλά στο Talos, αλλά πραγματοποιούνται χρησιμοποιώντας τον σαν μεσάζοντα (διακομιστή μεσολάβησης). Καμιά οντότητα δεν αλληλεπιδρά με καμία άλλη άμεσα, παρά μόνο διαμέσω του Talos, ο οποίος επιπλέον τις καταγράφει. Και εδώ απαιτείται η εγγραφή νέων χρηστών και πλατφορμών στο Talos και η λειτουργία αυτή παραμένει η ίδια με το προηγούμενο επίπεδο. Έτσι, οι ενέργειες που θα λάβουν χώρα είναι:

- Ο Νέος Χρήστης κάνει αίτηση εγγραφής προς τον Talos → Ο Talos απαντά στην αίτηση
- Η νέα Πλατφόρμα κάνει αίτηση εγγραφής προς τον Talos → Ο Talos απαντά στην αίτηση
- Ο Χρήστης 1 δημιουργεί τον Agent 1.1, το γεγονός αναφέρεται στον Talos → Ο Agent 1.1 προωθείται στον Talos με αίτημα μετανάστευσης στην Πλατφόρμα 1 → Ο Agent 1.1 μεταναστεύει στην Πλατφόρμα 1, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Talos με αίτημα μεταβίβασης στον Χρήστη 1 → Αναφορά αποτελεσμάτων στον Χρήστη 1.
- Ο Χρήστης 1 δημιουργεί τον Agent 1.2, το γεγονός αναφέρεται στον Talos → Ο Agent 1.2 προωθείται στον Talos με αίτημα μετανάστευσης στην Πλατφόρμα 3 → Ο Agent 1.2 μεταναστεύει στην Πλατφόρμα 3, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Talos με αίτημα μεταβίβασης στον Χρήστη 1 → Αναφορά αποτελεσμάτων στον Χρήστη 1.

- Ο Χρήστης 2 δημιουργεί τον Agent 2.1, το γεγονός αναφέρεται στον Talos → Ο Agent 2.1 προωθείται στον Talos με αίτημα μετανάστευσης στην Πλατφόρμα 2 → Ο Agent 2.1 μεταναστεύει στην Πλατφόρμα 2, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Talos με αίτημα μεταβίβασης στον Χρήστη 2 → Αναφορά αποτελεσμάτων στον Χρήστη 2 → Ο Agent 2.1 προωθείται στον Talos με αίτημα μετανάστευσης στην Πλατφόρμα 1 → Ο Agent 2.1 μεταναστεύει στην Πλατφόρμα 1, το γεγονός αναφέρεται στον Talos → Αναφορά αποτελεσμάτων στον Talos με αίτημα μεταβίβασης στον Χρήστη 2 → Αναφορά αποτελεσμάτων στον Χρήστη 2.

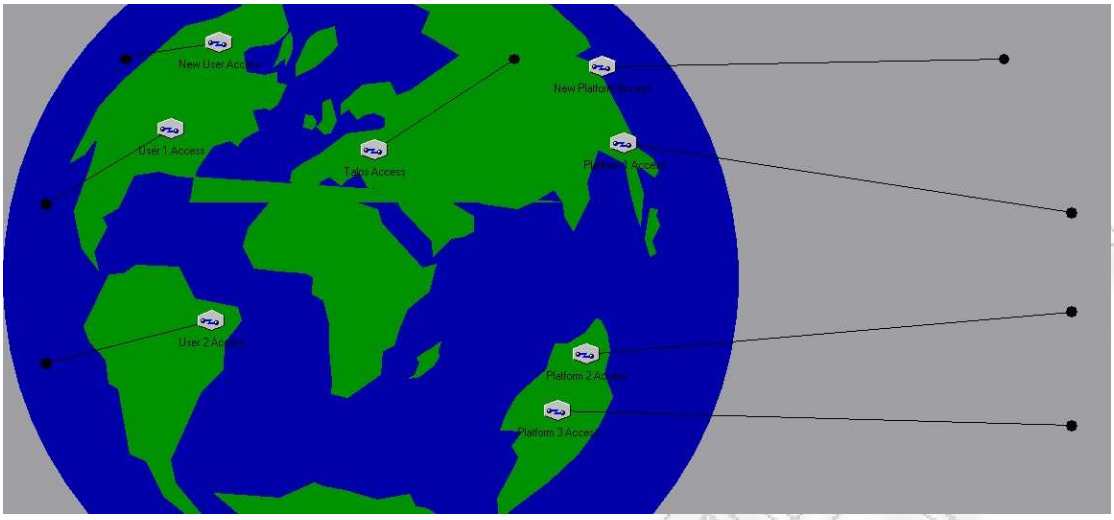


Εικόνα 50: Προσομοίωση της αρχιτεκτονικής του προτεινόμενου συστήματος (Insured Mode) στο περιβάλλον του Comnet.

5.4 Τεχνικές Λεπτομέρειες / Παραδοχές

Ο στόχος της προσομοίωσης είναι να διερευνηθεί και να απομονωθεί η επίπτωση στις επιδόσεις ενός συστήματος κινητών πρακτόρων η εφαρμογή του προτεινόμενου μοντέλου ασφάλειας και εμπιστοσύνης. Έτσι, και στις τρεις προσομοιώσεις έχουν χρησιμοποιηθεί όμοιες προδιαγραφές για τις κοινές οντότητες και τα τμήματα του δικτύου. Για τον ίδιο λόγο, έχουν γίνει κάποιες παραδοχές οι οποίες πρέπει να σημειωθούν, μαζί με τους λόγους για τους οποίους κρίθηκαν απαραίτητες. Πιο συγκεκριμένα:

- Οι υπολογιστές των χρηστών διαθέτουν έναν όμοιο επεξεργαστή των 2 Ghz.
- Οι υπολογιστές στους οποίους τρέχουν οι πλατφόρμες διαθέτουν τέσσερις όμοιους επεξεργαστές των 2 Ghz.
- Οι χρήστες διαθέτουν σύνδεση 24 Mbps Adsl, καθώς θεωρούνται οικιακοί χρήστες.
- Οι έμποροι (πλατφόρμες) διαθέτουν επαγγελματική σύνδεση 1 Gbps, συμμετρική, κατάλληλη για φιλοξενία επαγγελματικού server.
- Ο Talos και στις δύο προσομοιώσεις, διαθέτει όμοιο υλικό και σύνδεση στο Διαδίκτυο με τις πλατφόρμες. Στην πράξη οφείλει να διαθέτει ανώτερους πόρους, καθώς πρόκειται για υπηρεσία επ' αμοιβή, και οι πόροι του θα είναι ανάλογοι με το πελατολόγιό του. Η συγκεκριμένη επιλογή έγινε προκειμένου να φανεί πώς μεταφέρεται ο φόρτος από τις υπόλοιπες οντότητες στον Talos, καθώς με διαφορετικές προδιαγραφές δεν θα γινόταν αντιληπτός ο φόρτος που αναλαμβάνει.
- Η τοπολογία του Wide Area Network (**Εικόνα 51**) προέκυψε από έτοιμα μοντέλα που περιελάμβανε το Comnet στη βιβλιοθήκη του. Αποτελεί δίκτυο TCP/IP v4 στα πρότυπα του Διαδικτύου, στο οποίο τα σημεία πρόσβασης των διαφόρων οντοτήτων έχουν ενημερωθεί με βάση τις ταχύτητες των συνδέσεων που έχουν οριστεί.



Εικόνα 51: Το Wide Area Network, σε εσωτερική προβολή, που χρησιμοποιήθηκε σε όλες τις προσομοιώσεις.

- Και στις τρεις προσομοιώσεις τα κρυπτογραφικά μέσα έχουν θεωρηθεί ως υπολογιστική επιβάρυνση ορισμένου βάρους. Σύμφωνα με το μοντέλο, και στις δύο εκδοχές του, υλοποιούνται τα ίδια κρυπτογραφικά μέσα, και το μόνο που προσθέτει επιβάρυνση είναι οι επιπλέον αλληλεπιδράσεις με τον Talos στο υψηλό επίπεδο ασφάλειας. Παρόλ' αυτά, έχει χρησιμοποιηθεί καταχρηστικά ο ίδιος φόρτος και στην πρώτη προσομοίωση, αν και δεν προβλέπεται απαραίτητα υλοποίηση όλων των κρυπτογραφικών μέσων (παρόλαυτα δεν αποκλείεται για κάποια συστήματα). Ο λόγος που έγινε η επιβάρυνση αυτή στο σύστημα χαμηλής ασφάλειας είναι για να μπορεί να συγκριθεί ευθέως ο φόρτος που εισάγεται από την διαφορετική τοπολογία/αρχιτεκτονική του προτεινόμενου συστήματος. Ουσιαστικά, με αυτό τον τρόπο απομονώνεται η επιβάρυνση που εισάγει ο Talos, ως επιπλέον οντότητα και οι νέες αλληλεπιδράσεις που εισάγει.
- Όλες οι οντότητες θεωρούνται ότι έχουν up-time 100%. Δεν εξετάζονται σενάρια αποτυχίας μέρους του δικτύου, καθώς δεν είναι μέσα στους στόχους της παρούσας έρευνας.
- Δεν εξετάζεται η επίδραση των επιδόσεων των σκληρών δίσκων των υπολογιστών. Ομοίως, δεν είναι μέσα στους στόχους της παρούσας έρευνας. Αποσκοπούμε να απομονώσουμε την επιβάρυνση που εισάγει το προτεινόμενο σύστημα.

- Το μέγεθος των πρακτόρων ορίζεται στα 200 kbyte. Ανάλογα με το σύστημα, το μέγεθος του πράκτορα μπορεί να κυμαίνεται από μερικά kbyte έως να είναι μεγαλύτερο από 1 Megabyte [65], [81]. Το μέγεθος που επιλέχθηκε για την προσομοίωση αποτελεί ένα ενδεικτικό μέσο μέγεθος κινητού πράκτορα, αντιπροσωπευτικό ενός μεγάλου αριθμού συστημάτων. Ομοίως, όλες οι αναφορές (μετανάστευσης, αιτήσεις, acknowledgment κ.τ.λ) ορίζονται στο 1 kbyte. Το Comnet δίνει εκτενείς δυνατότητες διαφοροποίησης του μεγέθους, αλλά και αυτή η παραδοχή έχει γίνει προκειμένου να απομονωθεί η επιβάρυνση του προτεινόμενου συστήματος, κάτω από ελεγχόμενες συνθήκες.
- Όλες οι προσομοιώσεις έτρεξαν για 60 δευτερόλεπτα δικτυακού χρόνου (Προτεινόμενος χρόνος του Comnet).

5.4 Ανάλυση Αποτελεσμάτων

Το Comnet μπορεί να εξετάσει ένα σημαντικό αριθμό δεικτών επιδόσεων του δικτύου, η χρησιμότητα των οποίων διαφέρει ανάλογα με το είδος της προσομοίωσης. Σε κάθε κύκλο της παρούσας προσομοίωσης λήφθηκαν τιμές για το ποσοστό χρήσης του επεξεργαστή κάθε μηχανήματος, το ποσοστό χρήσης όλων των συνδέσεων και η καθυστέρηση σε msec για κάθε είδους μήνυμα που αποστέλλεται (μετανάστευση, reports, ερωτήματα, εγγραφές κ.τ.λ). Οι συγκεκριμένοι επιλέχθηκαν ως οι πιο αντιπροσωπευτικοί που μπορούν να αποδώσουν τον φόρτο στα διάφορα υποσυστήματα του δικτύου μας και πως αυτός μεταβάλλεται εισάγοντας το υπό εξέταση μοντέλο μας.

Στον Πίνακα 6 μπορούμε να συγκρίνουμε το ποσοστό χρήσης των επεξεργαστών όλων των μηχανημάτων.

Η πρώτη παρατήρηση είναι ότι με την εφαρμογή του μοντέλου μας στο Secure Mode παρατηρείται σημαντική επιβάρυνση των επεξεργαστών κατά 50 – 100%. Κάτι τέτοιο είναι αναμενόμενο, καθώς με την εφαρμογή του μοντέλου χρειάζεται να διαπραγματεύονται επιπλέον αποστολές μηνυμάτων που αφορούν επικοινωνία με τον Talos, που προηγουμένως δεν πραγματοποιούνταν. Αντίστοιχη επιβάρυνση αναμένεται να συμβαίνει σε όλα τα συστήματα με κεντρικοποιημένη διαχείριση με λειτουργίες Έμπιστης Τρίτης Οντότητας, λόγω ουσιαστικά του διπλασιασμού των αποστελομένων μηνυμάτων. Παρόλ’ αυτά και μετά την επιβάρυνση ο επεξεργαστικός φόρτος κυμαίνεται σε πολύ ανεκτά επίπεδα, στο υλικό που έχουμε ορίσει στην προσομοίωση.

Η δεύτερη και πιο ενδιαφέρουσα παρατήρηση έχει να κάνει με τις επιδόσεις στο Insured Mode. Εδώ συμβαίνει το αντίστροφο, καθώς ο φόρτος των περισσότερων οντοτήτων μειώνεται κατά πολύ, ενώ για κάποιες αυξάνεται ελάχιστα, παρόλο της αυξημένης πολυπλοκότητας του συστήματος. Μεγάλη μείωση φόρτου παρατηρείται στους επεξεργαστές που ήταν περισσότερο επιβαρυμένοι, ενώ παρατηρείται μικρότερη μείωση σε εκείνους με μέτριο φόρτο, έως και μικρή αύξηση για εκείνους που είχαν μικρό φόρτο (Πλατφόρμα 1). Το φαινόμενο αυτό συμβαίνει διότι στο Insured Mode ο Talos λειτουργεί ως

μεσάζοντας και πέρα από την ασφάλεια που παρέχει στο σύστημα, αναλαμβάνει μέρος των λειτουργιών που κανονικά θα επιβάρυναν τις άλλες οντότητες (μεταναστεύσεις, αποστολή μηνυμάτων). Έτσι, μειώνεται ο φόρτος για το υπόλοιπο σύστημα και το επιφορτίζεται ουσιαστικά ο Talos, όπως βλέπουμε από το αυξημένο ποσοστό χρήσης του επεξεργαστή του (~3%) σε σχέση με το Secure Mode (0.0055%) όπου απλά ο Talos λειτουργεί περισσότερο εποπτικά. Σημειώνουμε, ότι στις παραδοχές έχουμε επιλέξει ο Talos να έχει το ίδιο υλικό με τις πλατφόρμες προκειμένου να φανεί ξεκάθαρα η μεταφορά του φόρτου. Σε πραγματική λειτουργία ο Talos αναμένεται να είναι εγκατεστημένος σε ισχυρό μηχάνημα, ανάλογα με τους εγγεγραμμένους χρήστες.

Πίνακας 6: Χρήση Επεξεργαστή (%)

NODE	Current	Secure	Insured
User 1	5.6494	8.1110	3.8497
User 2	3.9696	6.5371	0.7102
Platform 1	0.9570	0.9886	1.1409
Platform 2	0.9926	1.6882	0.4222
Platform 3	0.5577	1.2290	0.2398
Talos		0.0055	2.9435
New User		0.0028	0.0020
New Platform		0.0005	0.0003

Στον **Πίνακα 7** παρατίθεται το ποσοστό χρήσης των γραμμών που συνδέονται όλες οι οντότητες στο WAN. Παρατηρείται ότι οι γραμμές των χρηστών αρχίζουν να παρουσιάζουν υψηλή κίνηση στο Secure Mode και, κυρίως, όσον αφορά στην αποστολή μηνυμάτων. Αυτό εξηγείται από την επιλογή των γραμμών να είναι τύπου Asymmetric DSL, στις οποίες η αποστολή δεδομένων γίνεται σε πολύ μικρότερη ταχύτητα από τη λήψη. Το διαφορετικό ποσοστό χρήσης μεταξύ των χρηστών εξηγείται καθώς ο Χρήστης 1 παράγει περισσότερους πράκτορες. Ο πράκτορας του Χρήστη 2 μεταναστεύει κατά τη διάρκεια του κύκλου ζωής του, κάτι που προσθέτει κίνηση και στη γραμμή του χρήστη του (λόγω αναφορών), αλλά όχι τόσο όσο η παραγωγή περισσότερων πρακτόρων.

Στο συγκεκριμένο δείκτη παρατηρείται η ίδια συμπεριφορά αύξησης φόρτου στο Secure Mode και μετέπειτα μείωσης στο Insured Mode που παρατηρήθηκε στο πρώτο δείκτη που εξετάσαμε. Επαληθεύεται ότι ο Talos μειώνει το φόρτο των

υπόλοιπων οντοτήτων, αν και στον συγκεκριμένο δείκτη επιβαρύνεται ο ίδιος ελάχιστα.

Πίνακας 7: Χρήση Τηλεπικοινωνιακών Γραμμών (%)

ACCESS LINK	Current	Secure	Insured
User 2Entry	6.76	11.28	1.34
User 2 Exit	41.73	67.84	6.67
Platform 2 Entry	0.17	0.29	0.11
Platform 2 Exit	0.16	0.27	0.03
Platform 3 Entry	0.09	0.19	0.04
Platform 3 Exit	0.10	0.22	0.04
User 1 Entry	10.12	14.76	7.22
User 1 Exit	56.38	79.55	36.49
Platform 1 Entry	0.15	0.15	0.18
Platform 1 Exit	0.16	0.18	0.20
Talos Entry		0.00	0.44
Talos Exit		0.00	0.53
New User Entry		0.06	0.04
New User Exit		0.06	0.04
New Platform Entry		0.00	0.00
New Platform Exit		0.00	0.00

Τέλος, στον Πίνακα 8 και στον Πίνακα 9 παρατίθεται η καθυστέρηση στην αποστολή κάθε είδους μηνύματος (delay), ως ο τελευταίος δείκτης επιδόσεων. Σημειώνεται ότι δεν είναι δυνατό να γίνει ευθεία αντιπαράθεση των αποτελεσμάτων και των τριών προσομοιώσεων σε ένα πίνακα, καθώς δεν υπάρχει αντιστοίχηση των μηνυμάτων. Συγκεκριμένα, ενώ στις πρώτες δύο προσομοιώσεις οι οντότητες επικοινωνούν απευθείας μεταξύ τους, στο Insured Mode επικοινωνούν μονάχα με το Talos. Παρόλ’ αυτά όμως με σύγκριση των τιμών καθυστέρησης στους δύο πίνακες παρατηρούμε την ίδια συμπεριφορά με τους προηγούμενους δείκτες. Στο Secure Mode οι τιμές της καθυστέρησης αυξάνονται κατά 15-30% σε σχέση με τα υπάρχοντα συστήματα. Αντίστοιχα, οι τιμές της καθυστέρησης στο Insured Mode παρατηρούνται (κατά μέσο όρο) μειωμένες κατά 35-40% σε σχέση με το μεσαίο επίπεδο ασφάλειας αλλά και 15-20% σε σχέση με τα υπάρχοντα συστήματα που δε διαθέτουν κεντρικοποιημένη διαχείριση ασφάλειας.

Πίνακας 8: Καθυστέρηση Μηνύματος και Απάντησης Μέσος Χρόνος (ms) – Υπάρχοντα Συστήματα/Βασικό – Ασφαλές Επίπεδο

Origin / Msg Src : Destination	Current	Secure
User 1 / src Agent 1.1: Platform 1	2151.855	2778.488
User 1 / src Agent 1.2: Platform 3	2061.958	2730.289
User 1 / src Agent 1.1 Activity Report to Talos: Talos Secure		312.911
User 1 / src Agent 1.2 Activity Report to Talos: Talos Secure		320.308
User 2 / src Agent 2.1: Platform 2	1843.283	2172.420
User 2 / src Agent 2.1 Activity Report to Talos: Talos Secure		275.862
Platform 1 / src Agent 1.1 Responce: ECHO	2177.341	2729.544
Platform 1 / src Migrated Agent 2.1 Responce: User 2	1941.575	2488.262
Platform 1 / src Platform 1 Enquiries to Talos: Talos Secure		260.263
Platform 2 / src Agent 2.1 Responce: ECHO	1932.443	2315.860
Platform 2 / src Agent 2.1 Migrate: Platform 1	1642.897	1642.984
Platform 2 / src Platform 2 Enquiries to Talos: Talos Secure		260.263
Platform 3 / src Agent 1.2 Responce: ECHO	2328.831	2969.552
Platform 3 / src Platform 3 Enquiries to Talos: Talos Secure		260.263
Talos Secure / src Talos Responces: ECHO		313.744
New User / src New User Registration: Talos Secure		265.378
New Platform / src New Platform Registration: Talos Secure		260.263

Πίνακας 9: Καθυστέρηση Μηνύματος και Απάντησης Μέσος Χρόνος (ms) – Ασφαλισμένο Επίπεδο

Origin / Msg Src : Destination	Insured
User 1 / src Agent 1.1 : Talos	1910.455
User 1 / src Agent 1.2: Talos	1867.804
User 1 / src User 1 Enquiries to Talos: Talos	266.518
User 2 / src Agent 2.1: Talos	1818.836
User 2 / src User 2 Enquiries to Talos: Talos	261.377
Platform 1 / src Agent 1.1 Responce: ECHO	1642.853
Platform 1 / src Migrated Agent 2.1 Responce: Talos	1642.832
Platform 1 / src Platform 1 Enquiries to Talos: Talos	260.263
Platform 2 / src Agent 2.1 Responce: ECHO	1642.815
Platform 2 / src Agent 2.1 Migrate: Talos	1642.806
Platform 2 / src Platform 2 Enquiries to Talos: Talos	260.265
Platform 3 / src Agent 1.2 Responce: ECHO	1642.808
Platform 3 / src Platform 3 Enquiries to Talos: Talos	260.263
Talos ((Insured Mode)) / src Agent 1.1 to Platform 1: Platform 1	1642.908
Talos ((Insured Mode)) / src Agent 1.2 to Platform 3: Platform 3	1642.958
Talos ((Insured Mode)) / src Agent 2.1 to Platform 2: Platform 2	1642.991
Talos ((Insured Mode)) / src Agent 1.1 from Platform 1 Report Back: User 1	1924.235
Talos ((Insured Mode)) / src User Enquiries Report Back: ECHO	6103.359
Talos ((Insured Mode)) / src Agent 1.2 from Platform 3 Report Back: User 1	1901.516
Talos ((Insured Mode)) / src Agent 2.1 Migrate to Plaform 1: Platform 1	1642.947
Talos ((Insured Mode)) / src Migrated Agent 2.1 Report Back: User 2	1857.925
Talos ((Insured Mode)) / src Agent 2.1 Report Back: User 2	1858.126
Talos ((Insured Mode)) / src New User - Platform Registration: ECHO	1865.143
Talos ((Insured Mode)) / src Platform Enquiries Report Back: ECHO	290.500
New User / src New User Registration: Talos	265.378
New Platform / src New Platform Registration: Talos	260.263

5.5 Συμπεράσματα

Η παρούσα προσομοίωση είχε ως αποτέλεσμα την εξαγωγή μερικών πολύ χρήσιμων συμπερασμάτων σχετικά με το προτεινόμενο μοντέλο ασφάλειας και εμπιστοσύνης. Παρατηρήθηκε αύξηση των ανταλλασσόμενων μηνυμάτων μέσα στο σύστημα με την εισαγωγή μέτρων ασφάλειας, κάτι που ήταν αναμενόμενο. Ιδιαίτερη αύξηση παρατηρήθηκε στο Secure Mode, μια προσέγγιση, που έχει χρησιμοποιηθεί (σε επίπεδο αρχιτεκτονικής) και από υπάρχοντα συστήματα πρακτόρων που χρησιμοποιούν κάποιου είδους κεντρικοποιημένη διαχείριση ασφάλειας. Το ιδιαίτερο και χρησιμότερο, ίσως, συμπέρασμα της προσομοίωσης είναι ότι το προτεινόμενο μοντέλο στο υψηλό επίπεδο ασφάλειας (Insured Mode) ουσιαστικά βελτίωσε τη λειτουργία του όλου συστήματος, καθώς η οντότητα Talos που εισαγάγαμε ανέλαβε μέρος των λειτουργιών άλλων οντοτήτων, επωμιζόμενη το φόρτο τους. Αυτό συνεπάγεται ότι η εισαγωγή μια οντότητας ασφάλειας και η κεντρικοποίηση των λειτουργιών του συστήματος πρακτόρων δεν είναι καθόλου απαγορευτική από πλευράς επιδόσεων, ενώ το επιπλέον κόστος που αυτή συνεπάγεται μπορεί να καλυφθεί από την λειτουργία εφαρμογών στο Insured Mode και την πραγματοποίηση συναλλαγών υψηλού κινδύνου, που μέχρι τώρα ήταν επικίνδυνο να πραγματοποιηθούν με τη τεχνολογία των κινητών πρακτόρων.

6 ΣΥΜΠΕΡΑΣΜΑΤΑ – ΜΕΛΛΟΝΤΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ

Η παρούσα διατριβή ξεκίνησε με μια εισαγωγή στην τεχνολογία των κινητών πρακτόρων και την παρούσα κατάστασή της. Στη συνέχεια, αναπτύχθηκε ένα οργανωμένο πλαίσιο σύγκρισης για συστήματα κινητών πρακτόρων το οποίο και εφαρμόστηκε σε ένα αριθμό υπαρχόντων συστημάτων, που επιλέχθηκαν με σκοπό να απεικονίσουν κατά το δυνατόν σφαιρικότερα την πρόοδο της τεχνολογίας των μοντέλων ασφάλειας και εμπιστοσύνης. Διαπιστώθηκαν διαφορετικές προσεγγίσεις αλλά και ομοιότητες, κυρίως ανάλογα με το σκοπό λειτουργίας του κάθε συστήματος κινητών πρακτόρων.

Κύριο συμπέρασμα της σύγκρισης αποτέλεσε η έλλειψη κάποιου καθολικού προτύπου ασφάλειας και οι βασικές αδυναμίες της τεχνολογίας ειδικά στο τομέα του μοντέλου εμπιστοσύνης. Οι υπάρχουσες προσπάθειες εξασφάλισης της λειτουργίας συστημάτων κινητών πρακτόρων είναι ανάλογες με τη προοριζόμενη χρήση του κάθε συστήματος και κινούνται στην κατεύθυνση της υιοθέτησης τεχνικών μέτρων ασφάλειας και λιγότερο στην χρήση πολιτικών λειτουργίας.

Επιπλέον, καταλήξαμε στο συμπέρασμα ότι είναι πολύ δύσκολο να επιτευχθεί η εξασφαλισμένη λειτουργία των κινητών πρακτόρων χρησιμοποιώντας μονάχα τεχνικά μέσα ασφάλειας. Η ιδιαίτερη φύση τους αφορά εκτέλεση μη έμπιστου κώδικα σε πλατφόρμα τρίτου, ο οποίος μάλιστα κώδικας ενδέχεται να φέρει ευαίσθητα δεδομένα. Αν και υπάρχουν τεχνικές που επιχειρούν να διασφαλίσουν τη λειτουργία του πράκτορα ακόμη και σε κακόβουλη πλατφόρμα εκτέλεσης [7], η αποτελεσματικότητά τους δεν είναι απόλυτη έναντι όλων των ειδών επίθεσης [3], [4]. Έτσι καταλήξαμε στο συμπέρασμα ότι η λύση στο συγκεκριμένο πρόβλημα πρέπει να αναζητηθεί εκτός των στενών ορίων των μηχανισμών ασφάλειας που μπορούν να εφαρμοστούν στα διάφορα τμήματα λειτουργίας του συστήματος. Η συγκεκριμένη διαπίστωση δεν έχει διατυπωθεί ξανά στη υπάρχουσα βιβλιογραφία.

Με βάση τα συμπεράσματα που εξαγάγαμε από την ανάλυση και σύγκριση των συστημάτων πρακτόρων προχωρήσαμε στη σύνθεση των προδιαγραφών που

πρέπει να ακολουθεί ένα μοντέλο ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες, προκειμένου να είναι πλήρες. Με βάση αυτές προτείναμε ένα ολοκληρωμένο μοντέλο ασφάλειας και εμπιστοσύνης του οποίου η προσφορά εστιάζεται ακριβώς στις ελλείψεις που διαπιστώσαμε στη σημερινή τεχνολογία. Το προτεινόμενο μοντέλο συνδυάζει μια ευρεία γκάμα μηχανισμών ασφάλειας που καλύπτουν όλες τις οντότητες και τις φάσεις λειτουργίας ενός συστήματος κινητών πρακτόρων καθώς και πολιτικές που καλύπτουν το μοντέλο εμπιστοσύνης. Κάποιοι από τους μηχανισμούς που χρησιμοποιήθηκαν αποτελούν παραδοσιακές επιλογές στο χώρο της ασφάλειας των κινητών πρακτόρων. Αντίθετα, άλλοι μηχανισμοί του προτεινόμενου μοντέλου είναι πρωτότυποι και δεν έχουν ξαναπροταθεί για χρήση στο συγκεκριμένο χώρο σε επίπεδο καθολικού μοντέλου ασφάλειας και εμπιστοσύνης. Συγκεκριμένα, η υποχρεωτική χρήση της πλήρως ομομορφικής κρυπτογραφίας στα υψηλά επίπεδα ασφάλειας του μοντέλου εξασφαλίζει την ενημέρωση των κρυπτογραφημένων δεδομένων ενός κινητού πράκτορα ακόμη και σε εχθρικό περιβάλλον. Επιπλέον, ιδιαιτερότητα του μοντέλου μας αποτελεί και η ομαδοποίηση της χρήσης των διαφόρων μέτρων ασφάλειας, κλασικών και νέων, σε τρία διακριτά επίπεδα ασφάλειας που μπορούν να ακολουθήσουν οι εφαρμογές, ανάλογα με τη χρήση τους.

Δεδομένης της διαπίστωσής μας σχετικά με την αδυναμία εξασφαλισμένης λειτουργίας, προτείναμε την πρόβλεψη χρήσης υπηρεσιών ασφάλισης μαζί με υπηρεσίες μη αποποίησης μέσα στο προτεινόμενο μοντέλο ασφάλειας και εμπιστοσύνης. Οι υπηρεσίες μη αποποίησης αποτελούν ένα χαρακτηριστικό ασφάλειας που παρέχεται ήδη από κάποια υπάρχοντα συστήματα για αποτροπή παραβιάσεων. Στην πορεία της έρευνας θεωρήσαμε ότι ο συγκεκριμένος μηχανισμός μπορεί να αποτελέσει ακόμη ισχυρότερο ανασταλτικό παράγοντα για κακόβουλες συμπεριφορές αν συνδυαστεί με υπηρεσίες ασφάλισης και ο συνδυασμός αυτός παρέχεται από μια τρίτη οντότητα εκτός των ορίων του συστήματος πρακτόρων. Το συγκεκριμένο σχήμα λειτουργεί αποτρεπτικά για την πραγματοποίηση επιθέσεων, καθώς ο κακόβουλης χρήστης βρίσκεται υπόλογος κάτω μάλιστα από την εξουσία μιας τρίτης οντότητας, ενώ εξασφαλίζει και την αποζημίωση του θύματος σε περίπτωση που όντως πραγματοποιηθεί κάποια

επίθεση. Ο παραπάνω συνδυασμός και η πρόβλεψη υλοποίησής του σε επίπεδο μοντέλου ασφάλειας και εμπιστοσύνης αποτελεί νεωτερισμό στο χώρο των κινητών πρακτόρων.

Η ιδιαίτερη προσέγγιση του προτεινόμενου μοντέλου είναι δυνατή λόγω της εισαγωγής μιας Έμπιστης Τρίτης Οντότητας, του Talos στα δύο υψηλότερα επίπεδα που δρα ως κεντρικός διαχειριστής ασφάλειας. Η επιπλέον προσφορά του σε σχέση με κεντρικούς διαχειριστές ασφάλειας άλλων μοντέλων ασφάλειας και εμπιστοσύνης είναι οι πολύ περισσότερες λειτουργίες που ενσωματώνει και η διαφοροποίηση της λειτουργίας του ανά επίπεδο ασφάλειας. Η συγκέντρωση λειτουργιών του επιτρέπει την παροχή των κρίσιμων υπηρεσιών διαχείρισης υπόληψης, μη αποποίησης και ασφάλισης, οι οποίες από τη φύση τους είναι αλληλένδετες. Η εισαγωγή αυτής της οντότητας μετατρέπει τον κόσμο των κινητών πρακτόρων σε ένα κλειστό, ασφαλές περιβάλλον, με ενιαία διαχείριση ασφάλειας, περιβάλλον κατάλληλο ακόμη και για κρίσιμες διαδικτυακές εφαρμογές που μέχρι τώρα δεν υλοποιούνται με χρήση αυτής της τεχνολογίας.

Συνολικά θεωρούμε ότι το προτεινόμενο μοντέλο είναι ιδιαίτερα διεξοδικό, καλύπτει πλήρως τις προδιαγραφές στις οποίες καταλήξαμε και προσφέρει υψηλότερο επίπεδο ασφάλειας από κάθε άλλο μοντέλο που έχουμε εξετάσει. Πέρα όμως από θέματα πληρότητας κρίναμε απαραίτητο να διερευνηθεί και κατά πόσο εφικτή είναι η εφαρμογή του προτεινόμενου μοντέλου σε ένα σύστημα κινητών πρακτόρων, από πλευράς επιδόσεων. Έτσι προχωρήσαμε στην πραγματοποίηση μιας προσομοίωσης κατά την οποία προέκυψαν μερικά πολύ ενδιαφέροντα συμπεράσματα.

Συγκεκριμένα, παρατηρήθηκε αναμενόμενη επιβάρυνση της λειτουργίας του συστήματος με τη χρήση του μεσαίου (Ασφαλούς) επιπέδου λειτουργίας σε σχέση με το Βασικό, που αντιστοιχεί σε πολλά υπάρχοντα λιγότερο ασφαλή συστήματα. Παρόλ’ αυτά όμως η αύξηση του φόρτου κινήθηκε σε αποδεκτά όρια καθώς δεν είναι τέτοια που να κρίνεται απαγορευτική και δεδομένου μάλιστα του σημαντικά αυξημένου επιπέδου ασφάλειας που παρέχει.

Ιδιαίτερο ενδιαφέρον παρουσίασαν τα αποτελέσματα της προσομοίωσης του υψηλού επιπέδου λειτουργίας. Συγκεκριμένα, παρατηρήθηκε μείωση του φόρτου με

τη χρήση του Ασφαλούς / Ασφαλισμένου επιπέδου λειτουργίας, σε σχέση με το κυρίως με το μεσαίο επίπεδο αλλά ακόμη και σε σχέση με το χαμηλό επίπεδο. Αυτό δεν σημαίνει ότι στο υψηλό επίπεδο ο συνολικός φόρτος που παρατηρείται αθροιστικά στο σύστημα μειώθηκε. Για την ακρίβεια μειώθηκε ο φόρτος στις προϋπάρχουσες οντότητες, πριν την εισαγωγή του Talos. Αυτό είναι αποτέλεσμα της διαφοροποιημένης λειτουργίας του Talos στο συγκεκριμένο επίπεδο, ο οποίος αναλαμβάνει λειτουργίες που μέχρι τώρα διεκπεραιώνονταν κατανεμημένα από τις υπόλοιπες οντότητες και έτσι ουσιαστικά επωμίζεται μέρος του φόρτου του συστήματος. Κάτι τέτοιο κρίνεται αποδεκτό, από τη στιγμή που το Ασφαλές/Ασφαλισμένο επίπεδο λειτουργίας του προτεινόμενου μοντέλου αποτελεί μέρος επιχειρηματικού μοντέλου στο οποίο συμμετέχουν τα συστήματα που το χρησιμοποιούν και οι καλές επιδόσεις αποτελούν μέρος των παρεχομένων υπηρεσιών.

Ένας περιορισμός της παρούσας διατριβής αποτελεί ο ασφαλιστικός τομέας του προτεινόμενου μοντέλου καθώς και το επιχειρηματικό κομμάτι της λειτουργίας του. Οι συγκεκριμένοι τομείς είναι εκτός των στόχων της παρούσας διατριβής οπότε και ως μελλοντική επέκταση της παρούσας έρευνας προτείνουμε την επανεξέταση του προτεινόμενου μοντέλου, κάτω από το πρίσμα των αντίστοιχων επιστημονικών περιοχών. Κάτι τέτοιο κρίνουμε ότι απαιτείται για λόγους πληρότητας της πρότασης και θα επιτρέψει την ακριβέστερη διατύπωσή τους. Αυτό στη συνέχεια κατά το στάδιο της υλοποίησης θα επιτρέψει και τη βέλτιστη λειτουργία τους.

Κατόπιν προτείνουμε την αναδιατύπωση του συνολικού μοντέλου ασφάλειας και εμπιστοσύνης με τυποποιημένο τρόπο. Αυτό είναι αναγκαίο προκειμένου να είναι δυνατή και η πρότασή του στους αρμόδιους οργανισμούς FIPA και OMG, στα πλαίσια της προσπάθειάς τους παραγωγής κοινών προδιαγραφών για κινητούς πράκτορες. Η έλλειψη μοντέλου ασφάλειας και εμπιστοσύνης για κινητούς πράκτορες ως τμήμα των επίσημών τους προδιαγραφών έχει ταυτοποιηθεί ως σημαντική έλλειψη [1], [2], [34]. Έτσι, η προσθήκη ενός τέτοιου μοντέλου αναμένουμε να διευκολύνει την εξάπλωση της τεχνολογίας, και μάλιστα παρέχοντας ένα ιδανικό, ασφαλές πλαίσιο λειτουργίας.

Τέλος, το προτεινόμενο μοντέλο θα μπορούσε να ενσωματωθεί πιλοτικά σε ένα υπάρχον σύστημα κινητών πρακτόρων ανοιχτού κώδικα, προκειμένου να διερευνηθεί πέρα από τις επιδόσεις και η δυσκολία υλοποίησής του. Κάτι τέτοιο θα επιτρέψει να διαπιστωθούν τυχόν λειτουργικά προβλήματα και θα επιτρέψει την επαλήθευση των αποτελεσμάτων της προσομοίωσης, όσον αφορά τις επιπτώσεις στη λειτουργία του συστήματος.

Βιβλιογραφία

[1] M. Fragkakis, N. Alexandris, “Comparing the Trust and Security Models of Four Mobile Agent Platforms”, First International Conference in Research Challenges in Information Science ‘07, Ouarzazate, Morocco, April 2007

[2] M. Fragkakis, N. Alexandris, “Comparing the Trust and Security Models of Mobile Agents”, Third International Symposium On Information Assurance And Security, IAS 07, Manchester, UK, 29 - 31 August 2007

[3] M. Fragkakis, N. Alexandris, “Threats to the Trust Model of Mobile Agent Platforms”, 3rd International Conference on Software and Data Technologies, ICSOFT 08, Porto, Portugal, 5-8 July, 2008

[4] M. Fragkakis, N. Alexandris, “Threat Scenarios Targeting the Trust Model of Mobile Agent Platforms", International Conference on Communication Software and Networks, ICCSN 09, Macau, China, 27-28 February, 2009

[5] M. Fragkakis, N. Alexandris, "Outline of a Trust and Security Model for Multi-Agent System Platforms", Journal of Advances in Computer Science and Engineering, ISSN 0973-6999, 2011

[6] C. Gentry, “Fully Homomorphic Encryption Using Ideal Lattices”, 41st ACM Symposium on Theory of Computing (STOC), Bethesda, Maryland, USA, 2009

[7] J. Ametller, S. Robles, J. A. Ortega-Ruiz, “Self-Protected Mobile Agents”, AAMAS'04, New York, July 19-23, 2004

[8] B. Rempt, D. Mertz, “Distributing Computing Cooperative Computing with Mobile Agents”, Intel Developer Services, http://gnosis.cx/publish/programming/dc4.pdf, July 2002

[9] N. Vlassis, “A Concise Introduction to MAS and Distributed AI”, Morgan and Claypool Publishers, ISBN:1598295268 9781598295269, 2007

[10] S. Poslad, M. Calisti, P. Charlton, “Specifying Standard Security Mechanisms in Multi-Agent Systems”, Workshop on Deception, Fraud and Trust in Agent Societies, AMAS 2002, Bologna, pages 122–127, 2002

[11] M. Zhang, A. Karmough, R. Impey, “Adding Security Features to FIPA Agent Platforms”, Available: www.elec.qmul.ac.uk/staffinfo/stefan/fipa-security/rfi-responses/Karmouch-FIPA-Security-Journal.pdf, 2001

[12] C. English, P. Nixon, S. Terzis, A. McGettrick, Helen Lowe, “Dynamic Trust Models for Ubiquitous Computing Environments”, UBICOMP 2002

[13] S. Poslad, M. Calisti, “Towards Improved Trust and Security in FIPA Agent Platforms” Autonomous Agents 2000 Workshop on Deception, Fraud and Trust in Agent Societies, Spain, 2000

[14] FIPA Security Committee, http://www.fipa.org/activities/security.html

[15] FIPA, www.fipa.org

[16] M. Petsch, “Openness and Security in the FIPA Standard”, (MAI’02), (KI2002), September 2002

[17] OMG, http://www.omg.org

[18] OMG Agent Platform Special Interest Group, http://agent.omg.org/

[19] J. Altmann, F. Gruber, L. Klug, W. Stockner, E. Weippl, “Using Mobile Agents in Real World: A Survey and Evaluation of Agent Platforms”, 2nd Workshop on Infrastructure for Agents, MAS, and Scalable MAS at Autonomous Agents, Montreal, Canada, 2001

[20] S. Fischmeister, G. Vigna, R.A. Kemmerer, “Evaluating the Security Of Three Java-Based Mobile Agent Systems”, Proceedings of the 5th International Conference on Mobile Agents, Atlana, Georgia, USA, 2001

[21] N. T. Giang, D. T. Tung, “Agent Platform Evaluation and Comparison”, II-SAS, Pellucid EU 5FP IST-2001-34519 RTD, Technical report, June 2002

[22] C. Baumer, M. Breugst, S. Choy, T. Magedanz, “Grasshopper – A Universal Agent Platform Based on OMG MASIF and FIPA Standards”,

(MATA'99), Ottawa, Canada. World Scientific Publishing, pp. 1-18, October 1999

[23] F. Bellifemine, A. Poggi, G.Rimassa, "JADE – A FIPA-compliant Agent Framework", 4th International Conference and Exhibition on the Practical Application of Intelligent Agents and Multi-Agents, London, UK, 1999

[24] JADE Board, "Jade Security Guide", (Book) Copyright (C) 2004 TILAB S.p.A, JADE 3.2, last update: 26-July-2004

[25] Java Authentication and Authorization Service Web Site, http://java.sun.com/products/jaas/

[26] Mitsubish Electric Research Laboratory, http://www.merl.com/projects/concordia/

[27] N. El. Kadhi, E. Burstein, F. Barika, K. Ghedira, "Towards Agent IDS: Agent Platform Security Features Study", In Proceedings of CSC 2003, Computer Security Congress, Mexico, March 2003

[28] FIPA-OS Feature Overview, http://www.nortelnetworks.com, Feb 2000

[29] R. S. Gray, G. Cybenko, D. Kotz, R. A. Peterson, D. Rus, "D'Agents: Applications and Performance of a Mobile-Agent System," Software - Practice and Experience, 32(6):543--573, May 2002

[30] "JADE Roadmap", Jade Software Corporation Limited, September 2005

[31] R. Feiertag, J. Rho, and S. Rosset, "Engineering Security in a Multi-Agent System", Cougaar Software, 2004

[32] R. Feiertag, J. Rho, S. Rosset, "Using Security Mechanisms in Cougaar", Cougaar Software, 2004

[33] Cougaar Architecture Document, version 11.4, available at: http://www.cougaar.org, 23 December 2004

[34] V. Roth, "Obstacles to the Adoption Of Mobile Agents", MDM'04, July-2004

[35] S. Rosset, "Cougaar Security Services", Cougaar Software, 2004

[36] P. Braun, W. Rossak, Mobile Agents. Morgan Kaufmann, 2005, pp.

[37] T. Walsh, N. Paciorek, D. Wong, "Security and Reliability in Concordia TM", Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Jan 1998.

[38] D. Wong, N. Paciorek, T. Walsh, J. DiCelie, M. Young, and B. Peet, "Concordia: An Infrastructure for Collaborating Mobile Agents", Proceedings of the First International Workshop on Mobile Agents, MA'97, LNCS 1219, pages 86-97. Springer-Verlag, 1997

[39] A. Castillo, M. Kawaguchi, N. Paciorek, D. Wong. "Concordia as Enabling Technology for Cooperative Information Gathering". Japanese Society for Artificial Intelligence Conference, Tokyo, June 17-18, 1998

[40] "Mobile Agent Computing, a White Paper", Horizon Systems Laboratory, Mitsubishi Electric ITA, 1996.

[41] S. Adnan, J. Datuin, P. Yalamanchili, "A Survey of Mobile Agent Systems," Technical report, CSE 221, 2000. Available: www.cs.ucsd.edu/classes/sp00/cse221/reports/dat-yal-adn.pdf last accessed: 24/06/2011

[42] FIPA, FIPA ACL Message Structure Specification, http://www.fipa.org/specs/fipa00061, 2001

[43] L. Ferrari "The Aglets 2.0.2 User's Manual" http://aglets.sourceforge.net/, Oct 2004

[44] M. Oshima, G. Karjoth, K. Ono "Aglets Specification 1.1 Draft", 1998 http://www.trl.ibm.com/aglets/

[45] S. Fischmeister, G. Vigna, R.A. Kemmerer, "Evaluating the Security Of Three Java-Based Mobile Agent Systems" MA 2001, 31-41 LNCS 2240, Springer-Verlag, Dec 2001

[46] G. Karjoth. D.B. Lange, M. Oshima, "A Security Model for Aglets" IBM Res. Div., Zurich, IEEE Internet Computing, Jul/Aug 1997 Vol 1, Issue: 4, pp 68-77

[47] G. Vigna, B. Cassell, D. Fayram “An Intrusion Detection System for Aglets”, MA '02 Proceedings of the 6th International Conference on Mobile Agents, Springer-Verlagn2002, ISBN:3-540-00085-2 2002

[48] N. Suri, “An Overview of the NOMADS Mobile Agent System”, 14th European Conference on Object-Oriented Programming, Sophia, Antipolis and Cannes, France, June 12 - 16, 2000

[49] M. Carvalho, T. Cowin, N. Suri “MAST – A Mobile Agent-based Security Tool”, 7th WMSCI, Florida, July 2003

[50] J.M. Bradshaw, N. Suri, A.J. Canas, R. Davis, K. Ford, R. Hoffman, R. Jeffers, T. Reichherzer, “Terraforming Cyberspace”, IEEE Computer Vol 34, July 2001, pp 48 – 56

[51] N. Suri, J.M. Bradshaw, M.R Breedy, P.T. Groth, G.A. Hill, R. Jeffers, T.S. Mitrovich, B.R. Pouliot, D.S. Smith, “NOMADS: Toward a Strong and Safe Mobile Agent System”, International Conf on Autonomous Agents, 2000

[52] P.T. Groth, N. Suri, “CPU Resource Control and Accounting in the Nomads Mobile Agent System”, ACM OOPSLA Workshop on EAMOABS, Minneapolis, 2000.

[53] G. Noordende, F.M.T. Brazier, A.S. Tanenbaum, M. van Steen, ‘‘Position Summary: Mansion, a Distributed Multi-Agent System,’’ HotOS-VIII, Schloss Elmau, Germany, pp. 151, May 2001

[54] G. Noordende, F.M.T. Brazier, A.S. Tanenbaum, “Security in a Mobile Agent System”, IEEE Symposium on Multi-Agent Security and Survivability, Philadelphia, USA, Aug 2004

[55] G. Noordende, F.M.T. Brazier, A.S. Tanenbaum "A Security Framework for a Mobile Agent System", SEMAS-2002, Bologna, Italy, July 2002. DFKI (Deutsches Forschungszentrum fur Kunstliche Intelligenz GmbH) Research Report RR-02-03 pp. 43-50

[56] Q.H. Mahmoud, L. Yu, “An Architecture and Business Model for Making Software Agents Commercially Viable”, Proceeding HICSS '05,

Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 3 - Volume 03

[57] Q.H. Mahmoud, L. Yu., “Havana: A Mobile Agent Platform for Seamless Integration with the Existing Web Infrastructure”, Canadian Conference on Electrical and Computer Engineering, Vol 3, 2-5, Ontario, Canada, May 2004 pp 1257 – 1261

[58] Q.H. Mahmoud, L. Yu, “Havana Agents for Comparison Shopping and Location-aware Advertising in Wireless Mobile Environments”, Journal on Electronic Commerce Research and Applications, Volume 5, Issue 3, Autumn 2006, Pages 220-228 5(3): 220-228, 2006

[59] N. E. Kadhi, E. Burstein, F. Barika, K. Ghedira, “Towards Agent IDS: Agent Platform Security Features Study”, Congreso de Seguridad, March 2003

[60] J. Altmann, F. Gruber, L. Klug, W. Stockner, E. Weippl, “Using Mobile Agents in Real World: A Survey and Evaluation of Agent Platforms”, Workshop on Infrastructure for Agents, MAS, and Scalable MAS at Autonomous Agents, 2001

[61] N. T. Giang, D. T. Tung, “Agent Platform Evaluation and Comparison”, II-SAS, Pellucid EU 5FP IST-2001-34519 RTD, Technical report Jun 02

[62] D. B. Lange, M. Oshima. “Seven Good Reasons for Mobile Agents”, Communications of the ACM, March 1999/Vol. 42, No. 3, pp 88-98.

[63] C. Banks, N. Nelson "Discrete Event System Simulation". 2010 Pearson

[64] S. Asmussen, P. W. Glynn, "Stochastic Simulation: Algorithms and Analysis". Springer. Series: Stochastic Modelling and Applied Probability, Vol. 57, 2007

[65] Συστήματα κινητών πρακτόρων, με το μέγεθός τους: http://koolwap.in/games_app/?search=mobileagent&ext=

[66] H.S. Nwana, “Software Agents: An Overview. Knowledge Engineering Review”, Vol.11, No.3, 205-244, Cambridge University Press, 1996

[67] W. Stallings, “Network Security Essentials: Applications and Standards 4/E”, Prentice Hall, 2011

[68] “Εμπιστοσύνη και Ασφάλεια σε Ένα Κινητό και Γρήγορο Δικτυακό Περιβάλλον” Ebusiness Forum, 2004, http://www.ebusinessforum.gr

[69] S. Jin-dian, G. He-qing, G. Yin, “An Adaptive Trust Model of Web Services”, Journal of Natural Sciences, Volume 10, Number 1, pp 21-25. Jan. 2005.

[70] D. Milojicic, M. Breugst, I. Busse, J. Campbell, S. Covaci, B. Friedman, K. Kosaka, D. Lange, K. Ono, M. Oshima, C. Tham, S. Virdhagriswaran, J. White, "MASIF The OMG Mobile Agent System Interoperability Facility", Proceedings of the International Workshop on Mobile Agents (MA'98), Stuttgart, September 1998. It also appeared as Personal Technologies, Springer Verlag, (1998), 2:117-129.

[71] Java SE Security, Oracle Technology Network, http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html

[72] Ebay Sellers Reputation System, http://pages.ebay.com/services/forum/sellerprotection.html

[73] “Pro PayPal E-Commerce” Chapter Title “Introduction to PayPal”, pp. 1 – 12, ISBN 978-1-59059-750-7, DOI - 10.1007/978-1-4302-0353-7_1, 2007

[74] P. Kotzanikolaou, C. Douligeris, R. Mavropodi, V. Chrissikopoulos: “Mobile Agent Security”. In “Network Security: Current Status and Future Directions”, IEEE Press – Wiley Interscience, ISBN 978-0-471-70355-6, pp.257-268, April 2007.

[75] P. Kotzanikolaou, M. Burmester, V. Chrissikopoulos and C. Douligeris: “Role Based Access Control Policies in the Mobile Agent

Paradigm". Informatik Forum Journal – Special Issue on Mobile Agent Technology. Vol.14, No.2, pp. 62-69, December 2002.

[76] E. Magkos, P. Kotzanikolaou, V. Chrissikopoulos: "An Asymmetric Traceabilty Scheme for Copyright Protection without Trust Assumptions". Proceedings of EC-Web 2001, LNCS Vol. 2115, Springer, pp. 186–195, Munich, Germany, September 2001.

[77] P. Kotzanikolaou, M. Burmester, V. Chrissikopoulos: "Dynamic Multi-signatures for Secure Autonomous Agents". Proceedings of DEXA 2001 Workshop, IEEE, pp. 582–586, Munich, Germany, September 2001.

[78] P. Kotzanikolaou, M. Burmester, V. Chrissikopoulos: "Secure Transactions with Mobile Agents in Hostile Environments". Information Security and Privacy, ACISP 2000, LNCS Vol. 1841, Springer-Verlag pp. 289-297, Brisbane, Australia, 2000. (Lecture Notes in Computer Science)

[79] T.M. Ahmed, K. Faisal, "Increasing Mobile Agent Performance by Using Free Areas Mechanism", Journal Of Object Technology, Vol. 6, No. 4, May-June 2007

[80] N.E. Dubrovsky "Mobile Agents Simulation with DaSSF." Technical Report TR2004-499, Dept. of Computer Science, Dartmouth College, June, 2004

[81] R.S. Gray, G. Cybenko, D. Kotz, R.A. Peterson, D. Rus, "D'Agents: Applications and Performance of a Mobile-agent System, Software", Practice & Experience, v.32 n.6, p.543-573, May 2002

[82] R.S. Gray, D. Kotz, G. Cybenko, D. Rus, "D'Agents: Security in a Multiple-Language, Mobile-Agent System", Mobile Agents and Security, volume 1419 of LNCS

[83] H. Tagra, S. Kaushik. "Mole Agents - A New Phenomenon in Auctions (from Sellers Point of View)." In Proceedings of CIMCA/IAWTIC'2005 IEEE. pp.439~443

[84] J. Himmelspach, M. Röhl, A. M Uhrmacher. "Simulation for testing software agents - an exploration based on JAMES." Winter Simulation

Conference. Ed. Stephen E Chick et al. IEEE Service Center, 2003. 799-807.

[85] H. Peine, “Application and Programming Experience with the Ara Mobile Agent System.” Software Practice Experience 32.6 (2002) : 515-541.

[86] H. Peine, “Security Concepts and Implementation for the Ara Mobile Agent System.” 7th IEEE Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises.

[87] H. Peine, “An Introduction to Mobile Agent Programming and the Ara System.” System.

[88] M. Dijk; C. Gentry, S. Halevi, V. Vaikuntanathan. "Fully Homomorphic Encryption over the Integers". International Association for Cryptologic Research, 2009-12-11.

[89] E. Levieil, D. Naccache, “Cryptographic Test Correction”, Public Key Cryptography – PKC 2008, Lecture Notes in Computer Science, 2008, Volume 4939/2008, 85-100, DOI: 10.1007/978-3-540-78440-1_6

[90] C. Gentry; S. Halevi. "A Working Implementation of Fully Homomorphic Encryption", Eurocrypt 2010

[91] G. Cabri, L. Ferrari, Letizia Leonardi, Raffaele Quitadamo, “Improving Aglets with Strong Agent Mobility through the IBM JikesRVM”, SAC '06 Proceedings of the 2006 ACM symposium on Applied computing

[92] S. Gritzalis, G. Aggelis, Security Issues Surrounding Programming Languges for Mobile Code: JAVA vs. Safe-Tcl, ACM Operating Systems Review, Vol. 32, No. 2, pp. 16-32, 1998, ACM Press

[93] OMG Security Specifications http://www.omg.org/technology/documents/security_spec_catalog.htm

ΠΑΡΑΡΤΗΜΑ - Αρχεία Καταγραφής Προσομοίωσης

Στη συνέχεια παρατίθενται ολόκληρες οι αναφορές της προσομοίωσης με επιπλέον στοιχεία από εκείνα που αναλύθηκαν στο κεφάλαιο της προσομοίωσης.

Π.1 Αναφορές Προσομοίωσης Υπαρχόντων Συστημάτων

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:38:24 2011 PAGE 1

Simulation of current models

NODES: NODE FULL UTILIZATION

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

NODES: / PORTS:	BUSY CENTRAL PROCESSORS MEAN	MAX	UTIL%	BUSY BUSES MEAN	MAX	UTIL%
User 1	.0564944	1	5.6494	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
User 2	.0396957	1	3.9696	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 1	.0382794	3	.9569840	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 2	.0397057	3	.9926424	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 3	.0223076	2	.5576888	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:38:24 2011 PAGE 2

Simulation of current models

NODES: PROCESSOR + DISK UTILIZATION

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

NODE	DISK REQSTS GRNTED	DISK USAGE (KILOBYTES) AVERAGE	MAXIMUM	STD DEV	PROCESSOR % UTIL
User 1	0	0.000	0.000	0.000	5.6494
User 2	0	0.000	0.000	0.000	3.9696
Platform 1	0	0.000	0.000	0.000	0.9570
Platform 2	0	0.000	0.000	0.000	0.9926
Platform 3	0	0.000	0.000	0.000	0.5577

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:38:24 2011 PAGE 3

Simulation of current models

WAN CLOUDS: ACCESS LINK STATS

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

CLOUD: ACCESS LINK	(ENTRY) (EXIT)	FRAMES ACCEPTED	DROPPED	BUFFER (BYTES) MAX	AVG	% UTIL STD
Wide Area Network						
User 2 Access	Entry	12232	0	N/A	N/A	6.76
	Exit	12349	0	10500	1125	1594 41.73
Platform 2 Acces	Entry	12349	0	N/A	N/A	0.17
	Exit	12232	0	1500	2	60 0.16
Platform 3 Acces	Entry	6826	0	N/A	N/A	0.09
	Exit	6981	0	1500	1	46 0.10
User 1 Access	Entry	17707	0	N/A	N/A	10.12
	Exit	17277	0	24160	2904	4002 56.38
Platform 1 Acces	Entry	11711	0	N/A	N/A	0.15
	Exit	11986	0	3000	2	60 0.16

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:38:24 2011 PAGE 4

Simulation of current models

MESSAGE + RESPONSE SOURCES: MESSAGE DELAY

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

ORIGIN / MSG SRC NAME: DESTINATION LIST	MESSAGES ASSEMBLED	MESSAGE DELAY AVERAGE	STD DEV	MAXIMUM
User 1 / src Agent 1.1:				
Platform 1	51	2151.855 MS	437.750 MS	3299.018 MS
User 1 / src Agent 1.2:				
Platform 3	34	2061.958 MS	339.088 MS	2796.507 MS
User 2 / src Agent 2.1:				
Platform 2	55	1843.283 MS	45.284 MS	2017.364 MS
Platform 1 / src Agent 1.1 Responce:				
ECHO	47	2177.341 MS	365.995 MS	3118.368 MS
Platform 1 / src Migrated Agent 2.1 Responce:				
User 2	6	1941.575 MS	110.695 MS	2108.240 MS
Platform 2 / src Agent 2.1 Responce:				
ECHO	53	1932.443 MS	72.477 MS	2120.136 MS
Platform 2 / src Agent 2.1 Migrate to Platform 1:				
Platform 1	6	1642.897 MS	0.133 MS	1643.119 MS
Platform 3 / src Agent 1.2 Responce:				
ECHO	30	2328.831 MS	481.232 MS	3276.795 MS

Π.2 Αναφορές Προσομοίωσης Προτεινόμενου Συστήματος - Secure Mode

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 00:39:59 2011 PAGE 1

Simulation with Talos Secure

NODES: NODE FULL UTILIZATION

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

NODES: / PORTS:	BUSY CENTRAL PROCESSORS MEAN	MAX	UTIL%	BUSY BUSES MEAN	MAX	UTIL%
User 1	.0811104	1	8.1110	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
User 2	.0653706	1	6.5371	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 1	.0395426	4	.9885661	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 2	.0675269	4	1.6882	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 3	.0491598	3	1.2290	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Talos Secure	.0002218	2	.0055452	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
New User	.0000283	1	.0028255	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
New Platform	.0000202	2	.0005046	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 00:39:59 2011 PAGE 2

Simulation with Talos Secure

NODES: PROCESSOR + DISK UTILIZATION

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

NODE	DISK REQSTS GRNTED	DISK USAGE (KILOBYTES) AVERAGE	MAXIMUM	STD DEV	PROCESSOR % UTIL
User 1	0	0.000	0.000	0.000	8.1110
User 2	0	0.000	0.000	0.000	6.5371
Platform 1	0	0.000	0.000	0.000	0.9886
Platform 2	0	0.000	0.000	0.000	1.6882
Platform 3	0	0.000	0.000	0.000	1.2290
Talos Secure	0	0.000	0.000	0.000	0.0055
New User	0	0.000	0.000	0.000	0.0028
New Platform	0	0.000	0.000	0.000	0.0005

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 00:39:59 2011 PAGE 3

Simulation with Talos Secure

WAN CLOUDS: ACCESS LINK STATS

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

CLOUD: ACCESS LINK		FRAMES (ENTRY)	ACCEPTED	DROPPED	BUFFER (BYTES) MAX	AVG	% UTIL STD
(EXIT)							
Wide Area Network							
User 2 Access	Entry	20270	0	N/A	N/A	N/A	11.28
	Exit	20300	0	21200	3819	4571	67.84
Platform 2 Acces	Entry	21171	0	N/A	N/A	N/A	0.29
	Exit	20715	0	1540	4	77	0.27
Platform 3 Acces	Entry	14912	0	N/A	N/A	N/A	0.19
	Exit	15565	0	1500	3	69	0.22
User 1 Access	Entry	25618	0	N/A	N/A	N/A	14.76
	Exit	24729	0	42200	8057	8742	79.55
Platform 1 Acces	Entry	11922	0	N/A	N/A	N/A	0.15
	Exit	12584	0	3000	3	63	0.18
Talos Access	Entry	328	0	N/A	N/A	N/A	0.00
	Exit	328	0	1040	0	3	0.00
New User Access	Entry	42	0	N/A	N/A	N/A	0.06
	Exit	42	0	1040	1	23	0.06
New Platform Acc	Entry	30	0	N/A	N/A	N/A	0.00
	Exit	30	0	1040	0	1	0.00

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 00:39:59 2011 PAGE 4

Simulation with Talos Secure

MESSAGE + RESPONSE SOURCES: MESSAGE DELAY

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

ORIGIN / MSG SRC NAME: DESTINATION LIST	MESSAGES ASSEMBLED	MESSAGE DELAY AVERAGE	STD DEV	MAXIMUM
User 1 / src Agent 1.1:				
Platform 1	47	2778.488 MS	1022.170 MS	4897.508 MS
User 1 / src Agent 1.2:				
Platform 3	73	2730.289 MS	918.357 MS	4975.353 MS
User 1 / src Agent 1.1 Activity Report to Talos:				
Talos Secure	5	312.911 MS	53.126 MS	407.252 MS
User 1 / src Agent 1.2 Activity Report to Talos:				
Talos Secure	8	320.308 MS	52.553 MS	435.118 MS
User 2 / src Agent 2.1:				
Platform 2	93	2172.420 MS	465.775 MS	3439.430 MS
User 2 / src Agent 2.1 Activity Report to Talos:				
Talos Secure	10	275.862 MS	22.420 MS	325.194 MS
Platform 1 / src Agent 1.1 Responce:				
ECHO	42	2729.544 MS	990.699 MS	4963.034 MS
Platform 1 / src Migrated Agent 2.1 Responce:				
User 2	8	2488.262 MS	621.771 MS	3541.481 MS
Platform 1 / src Platform 1 Enquiries to Talos:				
Talos Secure	3	260.263 MS	0.000 MS	260.263 MS
Platform 2 / src Agent 2.1 Responce:				
ECHO	85	2315.860 MS	531.172 MS	3601.464 MS
Platform 2 / src Agent 2.1 Migrate:				
Platform 1	14	1642.984 MS	0.172 MS	1643.273 MS
Platform 2 / src Platform 2 Enquiries to Talos:				
Talos Secure	10	260.263 MS	0.000 MS	260.263 MS
Platform 3 / src Agent 1.2 Responce:				
ECHO	65	2969.552 MS	992.796 MS	4993.706 MS
Platform 3 / src Platform 3 Enquiries to Talos:				
Talos Secure	6	260.263 MS	0.000 MS	260.263 MS
Talos Secure / src Talos Responces:				
ECHO	54	313.744 MS	44.358 MS	488.532 MS
New User / src New User Registration:				
Talos Secure	7	265.378 MS	0.000 MS	265.378 MS
New Platform / src New Platform Registration:				
Talos Secure	5	260.263 MS	0.000 MS	260.263 MS

Π.3 Αναφορές Προσομοίωσης Προτεινόμενου Συστήματος - Insured Mode

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:47:37 2011 PAGE 1

Simulation with Talos Insured

NODES: NODE FULL UTILIZATION

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

NODES: / PORTS:	BUSY CENTRAL PROCESSORS MEAN	MAX	UTIL%	BUSY BUSES MEAN	MAX	UTIL%
User 1	.0384975	1	3.8497	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
User 2	.0071018	1	.7101823	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 1	.0456369	4	1.1409	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 2	.0168862	3	.4221549	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Platform 3	.0095928	3	.2398210	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
Talos ((Insured Mode))	.1177405	4	2.9435	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
New User	.0000202	1	.0020182	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0
New Platform	.0000101	2	.0002523	N/A	N/A	N/A
Wide Area Network	0.0	0	0.0	0.0	0	0.0

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:47:37 2011 PAGE 2

Simulation with Talos Insured

NODES: PROCESSOR + DISK UTILIZATION

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

NODE	DISK REQSTS GRNTED	DISK USAGE (KILOBYTES) AVERAGE	MAXIMUM	STD DEV	PROCESSOR % UTIL
User 1	0	0.000	0.000	0.000	3.8497
User 2	0	0.000	0.000	0.000	0.7102
Platform 1	0	0.000	0.000	0.000	1.1409
Platform 2	0	0.000	0.000	0.000	0.4222
Platform 3	0	0.000	0.000	0.000	0.2398
Talos ((Insured Mode	0	0.000	0.000	0.000	2.9435
New User	0	0.000	0.000	0.000	0.0020
New Platform	0	0.000	0.000	0.000	0.0003

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:47:37 2011 PAGE 3

Simulation with Talos Insured

WAN CLOUDS: ACCESS LINK STATS

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

CLOUD: ACCESS LINK		FRAMES (ENTRY)	ACCEPTED	BUFFER (BYTES) DROPPED	MAX	% UTIL AVG	STD
Wide Area Network							
User 2 Access	Entry	2271	0	N/A	N/A	N/A	1.34
	Exit	2136	0	4500	146	585	6.67
Platform 2 Acces	Entry	6191	0	N/A	N/A	N/A	0.11
	Exit	4304	0	1540	0	26	0.03
Platform 3 Acces	Entry	2981	0	N/A	N/A	N/A	0.04
	Exit	2997	0	1500	1	30	0.04
User 1 Access	Entry	12271	0	N/A	N/A	N/A	7.22
	Exit	11592	0	12200	951	1480	36.49
Platform 1 Acces	Entry	13937	0	N/A	N/A	N/A	0.18
	Exit	14364	0	3000	3	66	0.20
Talos Access	Entry	35438	0	N/A	N/A	N/A	0.44
	Exit	37696	0	3000	8	109	0.53
New User Access	Entry	30	0	N/A	N/A	N/A	0.04
	Exit	30	0	1040	0	19	0.04
New Platform Acc	Entry	15	0	N/A	N/A	N/A	0.00
	Exit	15	0	40	0	0	0.00

Compuware COMNET III Release 2.5.2.814 Tue Apr 05 07:47:37 2011 PAGE 4

Simulation with Talos Insured

MESSAGE + RESPONSE SOURCES: MESSAGE DELAY

REPLICATION 1 FROM 0.0 TO 60.0 SECONDS

ORIGIN / MSG SRC NAME: DESTINATION LIST	MESSAGES ASSEMBLED	MESSAGE DELAY AVERAGE	STD DEV	MAXIMUM
User 1 / src Agent 1.1:				
Talos ((Insured Mode	45	1910.455 MS	98.819 MS	2193.330 MS
User 1 / src Agent 1.2:				
Talos ((Insured Mode	15	1867.804 MS	88.909 MS	2070.728 MS
User 1 / src User 1 Enquiries to Talos:				
Talos ((Insured Mode	6	266.518 MS	7.364 MS	281.016 MS
User 2 / src Agent 2.1:				
Talos ((Insured Mode	11	1818.836 MS	63.165 MS	1849.055 MS
User 2 / src User 2 Enquiries to Talos:				
Talos ((Insured Mode	3	261.377 MS	0.603 MS	262.230 MS
Platform 1 / src Agent 1.1 Responce:				
ECHO	38	1642.853 MS	0.228 MS	1644.227 MS
Platform 1 / src Migrated Agent 2.1 Responce:				
Talos ((Insured Mode	25	1642.832 MS	0.085 MS	1643.226 MS
Platform 1 / src Platform 1 Enquiries to Talos:				
Talos ((Insured Mode	6	260.263 MS	0.000 MS	260.263 MS
Platform 2 / src Agent 2.1 Responce:				
ECHO	10	1642.815 MS	0.033 MS	1642.914 MS
Platform 2 / src Agent 2.1 Migrate:				
Talos ((Insured Mode	28	1642.806 MS	0.006 MS	1642.830 MS
Platform 2 / src Platform 2 Enquiries to Talos:				
Talos ((Insured Mode	9	260.265 MS	0.004 MS	260.275 MS
Platform 3 / src Agent 1.2 Responce:				
ECHO	14	1642.808 MS	0.005 MS	1642.821 MS
Platform 3 / src Platform 3 Enquiries to Talos:				
Talos ((Insured Mode	8	260.263 MS	0.000 MS	260.263 MS
Talos ((Insured Mode)) / src Agent 1.1 to Platform 1:				
Platform 1	41	1642.908 MS	0.132 MS	1643.238 MS
Talos ((Insured Mode)) / src Agent 1.2 to Platform 3:				
Platform 3	14	1642.958 MS	0.170 MS	1643.362 MS
Talos ((Insured Mode)) / src Agent 2.1 to Platform 2:				
Platform 2	11	1642.991 MS	0.186 MS	1643.350 MS
Talos ((Insured Mode)) / src Agent 1.1 from Platform 1 Report Back:				
User 1	37	1924.235 MS	85.555 MS	2198.251 MS
Talos ((Insured Mode)) / src User Enquiries Report Back:				
ECHO	3	6103.359 MS	7084.348 MS	16076.940 MS
Talos ((Insured Mode)) / src Agent 1.2 from Platform 3 Report Back:				

User 1 13 1901.516 MS 63.384 MS 2080.815 MS
Talos ((Insured Mode)) / src Agent 2.1 Migrate to Plaform 1:
Platform 1 26 1642.947 MS 0.157 MS 1643.497 MS
Talos ((Insured Mode)) / src Migrated Agent 2.1 Report Back:
User 2 5 1857.925 MS 0.099 MS 1858.018 MS
Talos ((Insured Mode)) / src Agent 2.1 Report Back:
User 2 4 1858.126 MS 0.192 MS 1858.450 MS
Talos ((Insured Mode)) / src New User - Platform Registration:
ECHO 5 1865.143 MS 2015.463 MS 5197.750 MS
Talos ((Insured Mode)) / src Platform Enquiries Report Back:
ECHO 6 290.500 MS 0.000 MS 290.500 MS
New User / src New User Registration:
Talos ((Insured Mode 5 265.378 MS 0.000 MS 265.378 MS
New Platform / src New Platform Registration:
Talos ((Insured Mode 5 260.263 MS 0.000 MS 260.263 MS

Δημοσιεύσεις

1. Fragkakis, M., Alexandris N., “Comparing the Trust and Security Models of Four Mobile Agent Platforms”, RCIS’07, April 2007.
2. Fragkakis, M., Alexandris N., “Comparing the Trust and Security Models of Mobile Agents”, IAS 07, Manchester, UK, 29 - 31 August 2007
3. Fragkakis, M., Alexandris N., “Threats to the Trust Model of Mobile Agent Platforms”, ICSOFT 08, Porto, Portugal, 5-8 July, 2008
4. Fragkakis, M., Alexandris N., “Threat Scenarios Targeting the Trust Model of Mobile Agent Platforms", ICCSN 09, Macau, China, 27-28 February, 2009
5. Fragkakis, M., Alexandris N., "Outline of a Trust and Security Model for Multi-Agent System Platforms", Journal of Advances in Computer Science and Engineering, ISSN 0973-6999, 2011
6. Fragkakis, M., Alexandris N., "A Survey on the Trust and Security Models of Mobile Agent Platforms” (Εχει υποβληθεί)
7. Fragkakis, M., Alexandris N., "Simulation of a Trust and Security Model of Mobile Agent Platforms” (Εχει υποβληθεί)