Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«Διδακτικής της Τεχνολογίας & Ψηφιακών Συστημάτων»

Μεταπτυχιακή Εργασία

Μελέτη Ανάλυση Μέτρων Ασφαλείας σε Πλατφόρμες Κινητού Κώδικα

Λαμπριανάκης Λάμπρος - ΜΕ/0679

Επιβλέπων: Ξενάκης Χρήστος, Λέκτορας

Περιεχόμενα

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Περίληψη

Οι ευφυείς πράκτορες λογισμικού είναι προγράμματα λογισμικού που εκτελούν συγκεκριμένα καθήκοντα για λογαριασμό του χρήστη και κατέχουν ένα βαθμό ευφυΐας που τους δίνει τη δυνατότητα να εκτελούν αυτόνομα τμήματα των καθηκόντων τους και να αλληλεπιδρούν με το περιβάλλον τους επαρκώς και με χρήσιμο τρόπο

Η ανάπτυξη όμως των πρακτόρων αντιμετωπίζεται δύσπιστα λόγω των θεμάτων ασφαλείας που προκύπτουν από τη χρήση τους. Η χρήση των agents αυξάνει τη πολυπλοκότητα με αποτέλεσμα να αυξάνεται και η διακύμανση των απειλών άρα και οι επιθέσεις . Μια πλατφόρμα agent πρέπει να έχει πρόσβαση στη δομή, το περιεχόμενα και στα δεδομένα των mobile agents.

Η εργασία αυτή χωρίζεται σε δυο κεφάλαια-μέρη. Το πρώτο μέρος δίνει έναν ορισμό των πρακτόρων(κινητών και ακίνητων), γίνεται αναφορά στις χρήσεις των πρακτόρων, ενώ περιγράφονται και οι βασικές γλώσσες συγγραφής πρακτόρων Στο δεύτερο κεφάλαιο γίνεται μελέτη για την ασφάλεια των mobile agents. Περιγράφονται οι απαιτήσεις ασφάλειας που υπάρχουν για τη προστασία των πόρων, παρουσιάζονται και οι απειλές – επιθέσεις που σχετίζονται με συστήματα.

ΜΕΡΟΣ 1^{Ο}

1. Εισαγωγή

1.1 Ιστορική αναδρομή

Οι πράκτορες λογισμικού είναι μετεξέλιξη των ανθρωποειδών, ρομπότ, cyborgs, και των ανδροειδών που σκοπό είχαν την πλήρωση ενεργειών για λογαριασμό των ανθρώπων. Οι πιο κοντινοί πρόγονοι των ευφυών πρακτόρων είναι οι σερβομηχανισμοί (servomechanisms) και διάφορες συσκευές ελέγχου.

Όμως, στη σημερινή εποχή οι πράκτορες που χρησιμοποιούνται διαφέρουν κατά πολύ από τις πρωταρχικές ιδέες. Η τάση έχει μεταφερθεί από το υλισμικό στο λογισμικό, σύμφωνα με τον Bradshaw [Bradshaw, 1997], τα άτομα που συνθέτουν ένα μηχανικό ρομπότ έχουν αντικατασταθεί από bits που συνθέτουν ένα ψηφιακό πράκτορα.

Οι πρώτοι οραματιστές ήταν ο Nicolas Negreponte [Negreponte, 1970] [Negreponte, 1989] και ο Alan Kay [Kay 1984] οι οποίοι μίλησαν για την χρήση πρακτόρων για την υλοποίηση συγκεκριμένων καθηκόντων στην καθημερινή και μη χρήση των υπολογιστών. Σύμφωνα με τον Kay [Kay, 1984], η ιδέα των πρακτόρων δημιουργήθηκε από τον John McCarthy στα μέσα της δεκαετίας του 50 και κατοχυρώθηκε από τον Oliver G. Selfridge λίγα χρόνια μετά, όταν δούλευαν και οι δύο στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης ή MIT, είχαν κατά νου ένα σύστημα, που όταν του δινόταν ένας στόχος, μπορούσε να εκτελέσει τις κατάλληλες υπολογιστικές λειτουργίες, ζητώντας και παίρνοντας συμβουλές σε φυσική γλώσσα όταν η διαδικασία εμφάνιζε προβλήματα. Ένας πράκτορας θα είναι ένα ρομπότ λογισμικού που θα ζει και εκτελεί τις λειτουργίες του μέσα στον υπολογιστή.

Οι πράκτορες λογισμικού εξελίχθηκαν σε δύο φάσεις:

- Η πρώτη φάση ξεκίνησε το 1977 στο χώρο της κατανεμημένης τεχνητής νοημοσύνης (Distributed Artificial Intelligence – DAI). Σκοπός των πρώτων ερευνών ήταν η μελέτη και αναπαράσταση των πρακτόρων με συμβολικά εσωτερικά μοντέλα. Οι πρώτες απόπειρες συνέβαλαν στην κατανόηση θεμάτων που αφορούσαν την αλληλεπίδραση και επικοινωνία των πρακτόρων, την αποσύνθεση και κατανομή των καθηκόντων τους, το συντονισμός και τη συνεργασία τους κ.α.

- Η δεύτερη φάση διαπραγματεύεται τη μελέτη περισσότερων τύπων ευφυών πρακτόρων από τους πιο απλούς έως τους πιο έξυπνους. Δίδεται έμφαση στην ταχύτατη ανάπτυξη εφαρμογών και στην δυνατότητα λειτουργίας των πρακτόρων μακριά από το αρχικό τους περιβάλλον.

Σήμερα, πολλές μεγάλες εταιρίες κατασκευής υπολογιστών χρησιμοποιούν τις παραπάνω ιδέες για να παρουσιάσουν το όραμα τους για τις διεπιφάνειες του μέλλοντος.

1.2 Ορισμός των Intelligent Software Agents

Οι ευφυείς πράκτορες λογισμικού είναι προγράμματα λογισμικού που εκτελούν συγκεκριμένα καθήκοντα για λογαριασμό του χρήστη και κατέχουν ένα βαθμό ευφυΐας που τους δίνει τη δυνατότητα να εκτελούν αυτόνομα τμήματα των καθηκόντων τους και να αλληλεπιδρούν με το περιβάλλον τους επαρκώς και με χρήσιμο τρόπο.

Ο παραπάνω ορισμός είναι γενικός και προέκυψε από μια σειρά παραδοχών που αναλύονται παρακάτω:

Η φύση των ευφυών πρακτόρων είναι πολύπλευρη και εμπλέκει διάφορα επιστημονικά πεδία, γεγονός που καθιστά δύσκολη την περιγραφή τους. Ανάλογα με την οπτική γωνία προσέγγισης της κάθε επιστήμης μπορεί να προκύψει και ένας διαφορετικός ορισμός. Για το λόγο αυτό, καθίσταται αναγκαίο να συνδυαστούν τα παραγόμενα οφέλη από όλα τα επιστημονικά πεδία, έτσι ώστε να εξαχθεί ένας ενιαίος ορισμός.

Οι ευφυείς πράκτορες χωρίζονται στις εξής κατηγορίες:

Εικόνα 1: Κατηγορίες Ευφυών Πρακτόρων

- Ανθρώπινοι πράκτορες (human agents): Ένα παράδειγμα είναι οι τουριστικοί πράκτορες, οι οποίοι έχουν τις απαραίτητες γνώσεις και τη δυνατότητα να παρέχουν ολοκληρωμένες υπηρεσίες στους ενδιαφερόμενους.

- Πράκτορες υλισμικού (hardware agents): Ένα παράδειγμα είναι ο έλεγχος του σκληρού δίσκου, μέσω της κλήσης του προγράμματος Disk Defragmenter το οποίο ελέγχει το σκληρό δίσκο για λάθη και αναδιατάσσει τα προγράμματα στο σκληρό δίσκο.
- Πράκτορες λογισμικού (software agents): Ένα παράδειγμα είναι οι buyer agents (shopping bots), οι οποίοι βοηθούν τους χρήστες του διαδικτύου να βρίσκουν προϊόντα και υπηρεσίες.

Το κοινό χαρακτηριστικό των ευφυών πρακτόρων είναι ότι σε μεγάλο βαθμό είναι ανεξάρτητοι και εκτελούν καθήκοντα για τον πελάτη τους ή για τον χρήστη τους. Το ποσοστό ευφυΐας που διαθέτουν τους επιτρέπει να ολοκληρώνουν τις εργασίες τους με τη λιγότερη δυνατή αλληλεπίδραση με τον πελάτη ή χρήστη τους. Για να επιτύχουν τους στόχους τους πρέπει να αλληλεπιδρούν με το περιβάλλον τους, καθώς και με άλλους χρήστες ή πράκτορες με τη χρήση κατάλληλης γλώσσας, να συλλέγουν πληροφορίες και να κάνουν συγκεκριμένες ενέργειες κατόπιν αποφάσεων που έχουν λάβει βασιζόμενοι στις παραπάνω πληροφορίες.

1.3 Χαρακτηριστικά πρακτόρων λογισμικού

Οι πράκτορες διαφέρουν από τα απλά προγράμματα λογισμικού διότι διαθέτουν έστω και ένα από τα παρακάτω χαρακτηριστικά:

Εικόνα 2: Οι ιδιότητες ευφυών πρακτόρων

- **Αντιδραστικότητα:** Πρέπει να υποστηρίζεται από όλους τους πράκτορες. Δείχνει την ικανότητα του πράκτορα να αλληλεπιδρά με το περιβάλλον του, το οποίο μπορεί να αποτελείται από άλλους πράκτορες, χρήστες, φυσικά αντικείμενα ή εξωτερικές πηγές πληροφόρησης.
- **Προσανατολισμός στόχου:** Η δυνατότητα ενός πράκτορα να λαμβάνει πρωτοβουλίες, απαιτεί ο πράκτορας να έχει καλά καθορισμένους στόχους ή ακόμα και ένα περίπλοκο σύστημα στόχων. Μόνο τότε έχει νόημα για έναν πράκτορα να επηρεάζει το περιβάλλον και έτσι να επιτυγχάνει τους στόχους του.
- **Δυνατότητα μάθησης:** Ένας πράκτορας πρέπει να έχει ένα ποσοστό ευφυΐας για να εκτελεί ορισμένες λειτουργίες και ένα βαθμό λογικής (rationality) για να μπορεί να εξάγει συμπεράσματα βάση των οποίων μπορεί να παίρνει αποφάσεις και να έρχεται πιο κοντά στο στόχο του. Η ικανότητα μάθησης και η προσαρμογή στο περιβάλλον συμβάλουν στη ολοκλήρωση της ευφυούς συμπεριφοράς, έτσι ώστε οι ενέργειες του, να προσαρμόζονται στα χαρακτηριστικά του κάθε χρήστη. Με το πέρας του χρόνου, δημιουργείται ένα προφίλ χρήστη βασιζόμενο στα ενδιαφέροντα του χρήστη.
- **Αυτονομία:** Ο πράκτορας δεν είναι ένα παραδοσιακό πρόγραμμα το οποίο πρέπει να παίρνει συνεχώς εντολές από το χρήστη ή από κάποιο άλλο πράκτορα, άρα λειτουργεί αυτόνομα με σκοπό την περάτωση του στόχου του. Η αυτονομία έχει ως αποτέλεσμα να απαλλάσσεται ο χρήστης από συνεχή λήψη αποφάσεων. Για να ισχύουν τα παραπάνω, θα πρέπει να είναι διαθέσιμοι όλοι οι πόροι που χρειάζεται ο πράκτορας για να ενεργήσει. Η αυτονομία προϋποθέτει την ύπαρξη της ικανότητας μάθησης και του προσανατολισμού του στόχου, εξαρτάται όμως κυρίως από τις δικαιοδοσίες που δίνει ο χρήστης στον πράκτορα.
- **Η δυνατότητα μεταφοράς:** Οι πράκτορες μπορούν να χωριστούν σε στατικούς (stationary) και κινητούς (mobile). Οι στατικοί πράκτορες περιορίζονται μέσα σε ένα υπολογιστή ενώ οι κινητοί μεταφέρονται μέσω δικτύου από υπολογιστή σε υπολογιστή. Η ύπαρξη των κινητών πρακτόρων παρόλο που προκαλεί διάφορα θέματα ασφαλείας, προστασίας δεδομένων και διαχείρισης, έχει πολλά πλεονεκτήματα, κυρίως γιατί η συγκέντρωση της απαιτούμενης πληροφορίας γίνεται χωρίς τη συνεχή ανταλλαγή μηνυμάτων μέσω δικτύου.
- **Επικοινωνία / Συνεργασία:** Επικοινωνία είναι η διαδικασία κατά την οποία οι πράκτορες μιλούν μεταξύ τους. Κάθε πράκτορας διαθέτει προκαθορισμένες ερωτήσεις και λαμβάνει προκαθορισμένες αποκρίσεις (responses). Η συνεργασία είναι η διαδικασία κατά την οποία δυο ή περισσότεροι πράκτορες συνεργάζονται για την ταχύτερη επίλυση κοινών στόχων. Τόσο η συνεργασία όσο και η επικοινωνία, απαιτούν την ύπαρξη κοινής γλώσσας.

- **Χαρακτήρας:** Ο πράκτορας είναι ένας συνεργάτης του χρήστη. Για την καλύτερη συνεργασία μεταξύ τους, είναι επιθυμητό οι πράκτορες να διαθέτουν χαρακτηριστικά που προσομοιώνουν την ανθρώπινη συμπεριφορά. Για παράδειγμα, να εκφράζουν συναισθηματικές διαθέσεις, όπως χαρά, λύπη κλπ., τα οποία τους κάνουν να μοιάζουν με ιδεατά πρόσωπα (virtual persons).

Στη πραγματικότητα, ελάχιστοι πράκτορες διαθέτουν όλα τα παραπάνω χαρακτηριστικά. Ειδικότερα, η ιδιότητα της προσομοίωσης του ανθρώπινου χαρακτήρα και της εκτέλεσης ευφυών πράξεων, βρίσκονται σε θεωρητικό επίπεδο.

1.4 Πεδία Επιρροής

Όπως αναφέρεται προηγουμένως, η φύση των ευφυών πρακτόρων είναι πολύπλευρη και εμπλέκει πολλά επιστημονικά πεδία με αποτέλεσμα να μην είναι απόλυτα κατανοητοί. Στο παρακάτω σχήμα γίνεται μια προσπάθεια να ομαδοποιηθούν τα χαρακτηριστικά των πρακτόρων με τα ομοειδή επιστημονικά πεδία.

Εικόνα 3: Πεδία Επιρροής

Είναι εμφανές ότι η αυτονομία εμπλέκεται στη θεωρία των αποφάσεων, η δυνατότητα μάθησης και ο προσανατολισμός στόχου στη τεχνητή νοημοσύνη, ενώ η αντιδραστικότητα συνυπάρχει και στη τεχνητή νοημοσύνη και στη ψυχολογία. Στην τελευταία εμπλέκεται και ο χαρακτήρας. Η επικοινωνία είναι κοινό χαρακτηριστικό στην επικοινωνία των δικτύων και στην κατανεμημένη τεχνητή νοημοσύνη, όπου η δυνατότητα μεταφοράς σχετίζεται με τη πρώτη και η συνεργασία με τη δεύτερη.

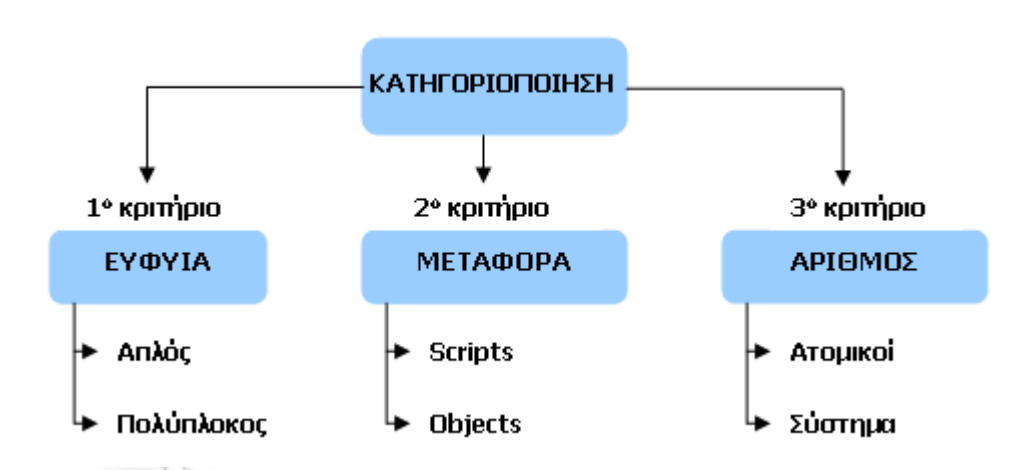
1.5 Κατηγοριοποίηση

Οι ευφυείς πράκτορες κατηγοριοποιούνται με βάση τρία κριτήρια:

- την ευφυΐα
- τη δυνατότητα μεταφοράς και
- τον αριθμό πρακτόρων

Ανάλογα με την ευφυΐα, ένας πράκτορας μπορεί να χαρακτηρισθεί απλός ή πολύπλοκος. Απλός πράκτορας είναι αυτός που έχει περιορισμένο βαθμό ευφυΐας, ενώ ο πολύπλοκος διαθέτει υψηλή ευφυΐα.

Όσον αφορά τη δυνατότητα μεταφοράς, διαχωρίζεται σε μεταφερόμενα προγράμματα και μεταφερόμενα αντικείμενα. Τα μεταφερόμενα προγράμματα στέλνονται σε κάποιον άλλον υπολογιστή πριν την εκτέλεσή τους, ενώ τα μεταφερόμενα αντικείμενα μεταφέρονται ανά πάσα στιγμή κατά τη διάρκεια της εκτέλεσής τους και απαιτούν μεγαλύτερη υπολογιστική ισχύ.



Εικόνα 4: Κατηγορίες Συστημάτων Πρακτόρων

Τέλος, όσον αφορά τον αριθμό τους, χωρίζονται σε ατομικούς πράκτορες και σε σύστημα πρακτόρων. Οι ατομικοί πράκτορες δεν είναι ικανοί να επικοινωνήσουν με άλλους πράκτορες ακόμα και αν υπάρχουν στο ίδιο περιβάλλον και επικοινωνούν μόνο με τους χρήστες. Στα συστήματα πρακτόρων, οι πράκτορες επικοινωνούν ή και συνεργάζονται μεταξύ τους.

1.6 Γλώσσες και εργαλεία συγγραφής πρακτόρων

1.6.1 Εισαγωγή

Οι ευφυείς πράκτορες, είναι προγράμματα λογισμικού, στα οποία όμως, λόγω της φύσης τους, η επιλογή της γλώσσας ανάπτυξής τους είναι πολύ σημαντική. Βασιζόμενοι στη βιβλιογραφία [Hohl 1995], [Knabe 1996], η γλώσσα που επιλέγεται πρέπει να έχει τις παρακάτω προδιαγραφές:

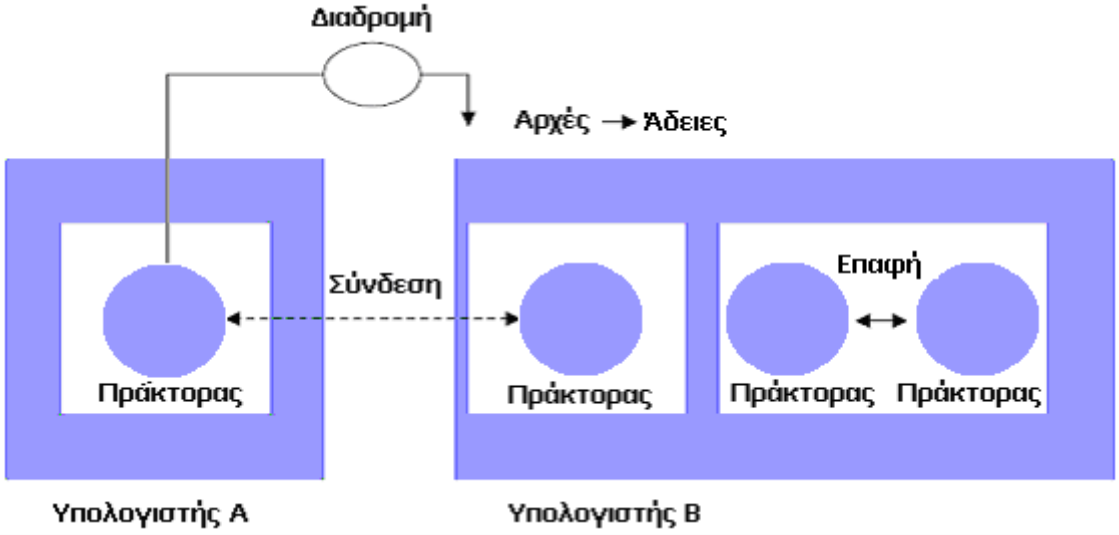
- **Δυνατότητες Επικοινωνίας:** Η γλώσσα πρέπει να επιτρέπει τη δυνατότητα δημιουργίας modules για να είναι εφικτή η επικοινωνία είτε μεταξύ των πρακτόρων είτε μεταξύ πρακτόρων και περιβάλλοντος.
- **Ανεξαρτησία πλατφόρμας:** Είναι σημαντικό ο κάθε πράκτορας να μπορεί να λειτουργεί ανεξάρτητα από το λογισμικό ή το υλισμικό στο οποίο βρίσκεται. Για το λόγο αυτό η γλώσσα που επιλέγεται πρέπει να έχει υψηλό βαθμό ανεξαρτησίας.
- **Αντικειμενοστραφικότητα:** Οι πράκτορες είναι αντικείμενα. Η γλώσσα λοιπόν θα πρέπει να υποστηρίζει το αντικειμενοστραφές μοντέλο προγραμματισμού.
- **Ασφάλεια:** Οι κινητοί πράκτορες όπως αναφέρθηκε και παραπάνω δημιουργούν πολλά θέματα ασφάλειας. Η γλώσσα υλοποίησης θα πρέπει λοιπόν να παρέχει μοντέλα ασφάλειας.
- **Διαχείριση κώδικα:** Η γλώσσα πρακτόρων θα πρέπει να μπορεί να λαμβάνει και να εκτελεί κώδικα από άλλες εφαρμογές, λόγω του ότι πολλές φορές η μεταφορά του κώδικα μέσω του διαδικτύου είναι απαραίτητη.

1.6.2 Κυριότερες Γλώσσες

1.6.2.1 Telescript

Η τεχνολογία Telescript είναι από τις πρώτες εμπορικές πλατφόρμες που χρησιμοποιήθηκε για την κατασκευή συστημάτων πρακτόρων. Περιλαμβάνει κριτήρια όπως αντικειμενοστραφικότητα, ικανότητα μεταφοράς κώδικα, δυνατότητες επικοινωνίας, και αυξημένες δυνατότητες ασφάλειας. Βασίζεται στις εξής γενικές ιδέες:

- **Μονάδα:** Μονάδα είναι ένα τμήμα του δικτύου, η οποία παρέχει μια υπηρεσία. Ένα δίκτυο ή ένας υπολογιστής μπορεί να έχει μια ή περισσότερες μονάδες. Οι μονάδες χρησιμοποιούνται κυρίως για την αποστολή και λήψη των πρακτόρων .
- **Πράκτορες:** Σε κάθε μονάδα ανατίθεται κάποιος πράκτορας, ο οποίος κάνει χρήση των υπηρεσιών της. Οι πράκτορες μπορούν να μετακινούνται από μονάδα σε μονάδα κατά τη διάρκεια μιας τυπικής εργασίας.
- **Διαδρομή:** Η εντολή *Go* της Telescript, χρησιμοποιείται από κάθε πράκτορα για τον καθορισμό σειράς επίσκεψης κάθε μονάδας, ενώ παράλληλα παρέχει ένα εισιτήριο που εμφανίζει τις παραμέτρους της διαδρομής, χωρίς να τον ενδιαφέρει ο τρόπος μετακίνησης.
- **Επαφή:** Με τη χρήση της εντολής *Meet*, δύο πράκτορες καθορίζουν τις παραμέτρους συνάντησης μεταξύ τους.
- **Σύνδεση:** Με τη χρήση της εντολής Connect, δύο πράκτορες, ένας στατικός και ένας κινητός, που δεν βρίσκονται στην ίδια μονάδα αλλά ανήκουν στον ίδιο χρήστη, μπορούν να επικοινωνήσουν μεταξύ τους.
- **Αρχές:** Με την εντολή Name, οι αρχές καθορίζουν την ταυτότητα του χρήστη ενός πράκτορα, καθώς επίσης και αν το σύστημα επιτρέπει ή όχι στον πράκτορα να εκτελέσει μια λειτουργία.
- **Άδειες:** Με τη χρήση των αδειών, ορίζονται συγκεκριμένα δικαιώματα για τους πράκτορες ή τις μονάδες, τα οποία χρησιμοποιούν οι αρχές.



Εικόνα 5: Telescript

1.6.2.2 Java

Η Java είναι μια δωρεάν αντικειμενοστρεφής γλώσσα προγραμματισμού η οποία είναι προσανατολισμένη για δικτυακή χρήση και είναι ανεξάρτητη πλατφόρμας. Ο Java κώδικας μπορεί να εκτελεστεί χωρίς καμία μετατροπή σε όλες τις πλατφόρμες που υποστηρίζουν Java με τη χρήση του Java Virtual Machine. Τα αντικείμενα της Java τα οποία παράγονται κάθε φορά μπορούν να μετακινούνται αλλά και να προσπελαύνονται από άλλους υπολογιστές.

Η Java αποτελεί τη βάση για πολλά συστήματα κατασκευής πρακτόρων, μερικά από τα οποία αποτελούν και τα πιο δημοφιλή.

1.6.2.3 Agent Tcl

Η Agent Tcl αφορά την ανάπτυξη μετακινούμενων πρακτόρων και βασίζεται στη γλώσσα προγραμματισμού Tcl. Η Agent Tcl παρέχει τα παρακάτω :

- Απλή script γλώσσα σαν κεντρική γλώσσα πρακτόρων.
- Συναρτήσεις για την διάφανη επικοινωνία μεταξύ πρακτόρων.
- Συναρτήσεις που επιτρέπουν σε πράκτορες να μεταναστεύουν από έναν υπολογιστή σε άλλον.
- Μηχανισμούς ασφάλειας σε ένα σύστημα πρακτόρων.

Η αρχιτεκτονική της αποτελείται από τα παρακάτω επίπεδα:

- **Κατώτερο επίπεδο:** Παρέχει διεπιφάνειες για όλα τα υποστηριζόμενα πρωτόκολλα επικοινωνίας.
- **Δεύτερο επίπεδο:** Διαθέτει το Server Engine ο οποίος είναι εγκατεστημένος σε όλα τα μηχανήματα. Είναι υπεύθυνος για τη διαχείριση των πρακτόρων.
- **Τρίτο επίπεδο:** Απαρτίζεται από τους interpreters των υποστηριζόμενων γλωσσών προγραμματισμού. Κάθε γλώσσα έχει το δικό της interpreter.
- **Ανώτατο επίπεδο:** Αποτελείται από πράκτορες οι οποίοι υλοποιούν τις λειτουργίες που δεν παρέχει ο Server Engine.

1.7 Οικονομικές Δυνατότητες

Η χρήση των ευφυών πρακτόρων προβλέπεται ότι θα προσφέρει σημαντικές οικονομικές δυνατότητες τόσο για τους χρήστες όσο και για τις επιχειρήσεις. Η χρήση των ευφυών πρακτόρων οδηγεί σε:

- **Βελτίωση της αποδοτικότητας:** Ο χρήστης ενημερώνει τον πράκτορα για τις επιθυμίες του κι έτσι αναλαμβάνει ο πράκτορας την επίλυση του προβλήματος, ανεξάρτητα, απαλλάσσοντας το χρήστη από φόρτο εργασίας και κατανάλωση πολύτιμου χρόνου. Έτσι ο χρόνος απόκτησης πληροφορίας και η μη επιθυμητή πληροφορία μειώνονται σημαντικά.
- **Βελτίωση της αποτελεσματικότητας:** Η χρήση πρακτόρων καθιστά πιο εύκολα προσβάσιμες τις απαιτούμενες πληροφορίες κι έτσι αυξάνεται η αποτελεσματικότητα της χρήσης του διαδικτύου.
- **Αύξηση της ολοκλήρωσης της πληροφορίας:** Οι ευφυείς πράκτορες συγκρίνουν την απαιτούμενη πληροφορία από διαφορετικές πηγές κι έτσι προσφέρουν μια ολοκληρωμένη εικόνα στο χρήστη ώστε να κάνει τη βέλτιστη επιλογή.

1.8 Εφαρμογές Ευφυών Πρακτόρων

1.8.1 Εισαγωγή

Στη συγκεκριμένη ενότητα γίνεται μια συνοπτική περιγραφή και κατηγοριοποίηση μερικών εφαρμογών των ευφυών πρακτόρων.

1.8.2 Ιοί και Worms

Πρόκειται για δυο διαφορετικές και επιβλαβείς οντότητες, οι οποίες συχνά προκαλούν τα ίδια συμπτώματα στους υπολογιστές που μολύνουν. Πρόκειται για προγράμματα που χρησιμοποιούν υπολογιστικούς πόρους για να αναπαράγονται. Κύριο μέσο της μετάδοσης τους αποτελεί το διαδίκτυο. Η διαφορά τους είναι ότι οι ιοί δεν είναι ολοκληρωμένα προγράμματα αλλά

μέρη προγραμμάτων, ενώ τα worms είναι ολοκληρωμένα προγράμματα τα οποία προκαλούν συνήθως υπερφόρτωση δικτύου και επιτίθονται εντοπίζοντας host υπολογιστές με χαμηλά επίπεδα ασφάλειας.

Οι ιοί κατηγοριοποιούνται ως εξής:

- **Boot-sector infectors:** Μολύνουν εκτελέσιμο κώδικα που βρίσκεται σε συγκεκριμένες περιοχές συστήματος ενός δίσκου που δεν είναι συνήθη αρχεία, όπως το master boot record στους σκληρούς δίσκους.
- **File infectors:** Επισυνάπτουν τον εαυτό τους σε συνηθισμένα προγράμματα, συνήθως σε αρχεία με καταλήξεις COM και EXE, αλλά και σε άλλα που μπορεί να γίνουν εκτελέσιμα. Η ενεργοποίηση τους γίνεται είτε άμεσα από το χρήστη ή έμμεσα από το σύστημα που εκτελεί κώδικα ενός καθήκοντος διαχείρισης υποβάθρου.

Για την αντιμετώπιση των ιών και των worms, έχουν αναπτυχθεί εφαρμογές από εξειδικευμένες εταιρίες οι οποίες σήμερα χρησιμοποιούνται ευρέως από τους χρήστες των υπολογιστών.

1.8.3 Πράκτορες Λειτουργικών Συστημάτων

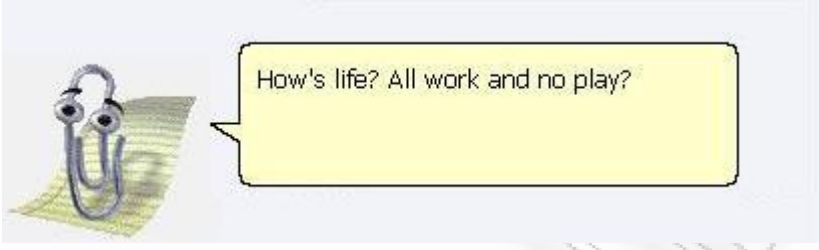
Οι πράκτορες λειτουργικών συστημάτων, καθώς και οι πράκτορες εφαρμογών, αποτελούν υποκατηγορία μιας ευρύτερης ομάδας εφαρμογών με την ονομασία desktop πράκτορες. Ένας dektop πράκτορας εκτελείται τοπικά σε έναν υπολογιστή ή σταθμό εργασίας και αποτελείται από:

- **Έξυπνες βοηθητικές εφαρμογές:** Η λειτουργία τους ορίζεται από το χρήστη. Παρακολουθούν τα γεγονότα σε επίπεδο λειτουργικού συστήματος και εκτελούν καθήκοντα συντήρησης, πχ πράκτορας συμπίεσης δίσκου, πράκτορας σύνδεσης με το διαδίκτυο.
- **Πράκτορες διεπιφάνειας:** Αλληλεπιδρούν με τη διεπιφάνεια του λειτουργικού συστήματος, αποθηκεύουν τις συνήθειες του χρήστη μέσω κάποιου μηχανισμού εξαγωγής συμπερασμάτων και δρούν για λογαριασμό του, πχ το Open Sesame, ενός πράκτορα διεπιφάνειας για περιβάλλοντα MacOS.

1.8.4 Πράκτορες Εφαρμογών

Είναι εφαρμογές που λειτουργούν στο υπόβαθρο με σκοπό να αυτοματοποιήσουν και να υποβοηθήσουν την εργασία του χρήστη. Εμφανίζονται είτε αυτόματα είτε σε προκαθορισμένες στιγμές και αλληλεπιδρούν με το χρήστη όποτε αυτό κρίνεται απαραίτητο. Οι κυριότερες υποκατηγορίες είναι:

- **Βοηθητικοί πράκτορες:** βρίσκονται συνεχώς στο παρασκήνιο μιας εφαρμογής και επεμβαίνουν αναλόγως, πχ. ο βοηθητικός πράκτορας του Office.



Εικόνα 6: Βοηθητικοί πράκτορες

- **Ειδικοί πράκτορες (wizards):** είναι διαδραστικές εφαρμογές που καθοδηγούν το χρήστη με σκοπό την ολοκλήρωση κάποιας διαδικασίας, πχ ο ειδικός πράκτορας δημιουργίας συντόμευσης.

Εικόνα 7: Ειδικοί πράκτορες (wizards)

1.8.5 Πράκτορες συζητήσεων (ChatterBots)

Οι πράκτορες συζητήσεων χρησιμοποιούν τη φυσική γλώσσα για να επικοινωνούν με τους χρήστες. Οι χρήστες τους θέτουν διάφορες ερωτήσεις και αυτοί. Εμφανίζονται στις παρακάτω περιπτώσεις:

- Σε ομάδες συζητήσεων για θέματα που αφορούν τα προϊόντα μιας επιχείρησης.
- Στη παρουσίαση διαφημίσεων.
- Σε εφαρμογές εξυπηρέτησης πελατών.

1.8.6 Πράκτορες Ανάκτησης και φιλτράρισματος πληροφορίας

Η ραγδαία ανάπτυξη του διαδικτύου και η μεγάλη ποσότητα πληροφορίας που υπάρχει σε αυτό, οδήγησε στην ανάγκη δημιουργίας εργαλείων διαχείρισης αυτής της πληροφορίας. Τα βασικότερα εργαλεία είναι:

- **Οι πλοηγοί (navigators)**, πχ. οι φυλλομετρητές (browsers)
- **Οι κατάλογοι εύρεσης πληροφοριών (search catalogs)**, πχ. www.yahoo.com
- **Οι μηχανές αναζήτησης (search engines)**, πχ. www.google.com. Οι μηχανές αναζήτησης χρησιμοποιούν πράκτορες και με βάση το βαθμό ανάπτυξής τους χωρίζονται στις εξής κατηγορίες:
    - **Απλές μηχανές αναζήτησης:** αποθηκεύουν την πληροφορία σε μια βάση δεδομένων.
    - **Ψευδομηχανές αναζήτησης:** συλλογή απλών μηχανών αναζήτησης.
    - **Μεταμηχανές αναζήτησης:** βελτιωμένη έκδοση των ψευδομηχανών, όπου φιλτράρουν τα αποτελέσματα των απλών μηχανών αναζήτησης.
    - **Εξατομικευμένες μηχανές αναζήτησης:** Η εξέλιξη των μηχανών αναζήτησης έχει να κάνει με την ιδέα της επεξεργασίας των αποτελεσμάτων από διαφορετικές αναζητήσεις για τη δημιουργία εξατομικευμένων μηχανών αναζήτησης.

1.8.6.1 Διαδικασία Λειτουργίας Μηχανών Αναζήτησης

Οι διαδικασίες που βρίσκονται πίσω από τη δημιουργία μηχανών αναζήτησης, χωρίζονται σε δυο κατηγορίες, με βάση το βαθμό πολυπλοκότητας των μηχανών αναζήτησης. Η λειτουργία των απλών μηχανών αναζήτησης βασίζεται σε τρεις κύριες διαδικασίες:

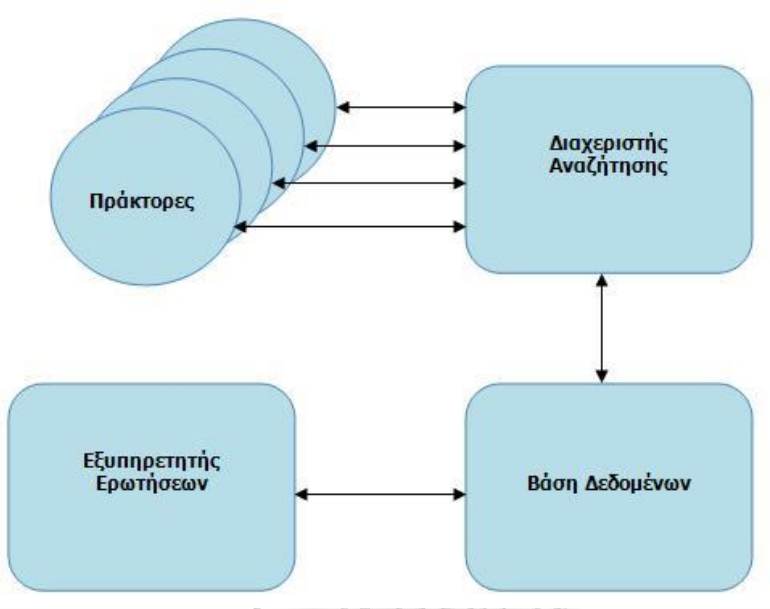
- **Είσοδος της πληροφορίας:** Ελέγχεται το περιεχόμενο των συνδέσμων, παρακολουθούνται αναδρομικά τα έγγραφα που έχουν προσπελαστεί στο παρελθόν και δίδεται στους χρήστες η δυνατότητα να προσθέσουν οι ίδιοι διευθύνσεις ιστοσελίδων στη μηχανή αναζήτησης.
- **Τοποθέτηση δεικτών και αποθήκευση πληροφορίας με βάση δεδομένων:** Συντακτική ανάλυση επιλεγμένων εγγράφων για τον καθορισμό των περιεχομένων τους και προετοιμασία αποθήκευσής τους στη ΒΔ, ώστε να είναι διαθέσιμα και με ακριβή τοποθεσία.
- **Ανάκτηση πληροφορίας βάσει ερωτήσεων:** Η ερώτηση αναζήτησης είναι αυτή που καθορίζει την εμφάνιση των κατάλληλων ιστοσελίδων, οι οποίες κατατάσσονται με βάση του βαθμού σχετικότητας τους με την ερώτηση (ranking). Ο κύριος στόχος των μεθόδων κατάταξης είναι η επίτευξη αξιοπιστίας ανάμεσα στο επιθυμητό αποτέλεσμα και στο σύνολο εγγράφων που προκύπτει από τη διαδικασία κατάταξης. Κάποιες μηχανές αναπαριστούν αυτές τις τιμές σαν ποσοστά, ενώ άλλες χρησιμοποιούν το σύστημα των φυσικών αριθμών. Σε κάθε περίπτωση πάντως, ο καθορισμός της ερώτησης αναζήτησης είναι αυτός που θα καθορίσει το τελικό σύνολο εγγραφών.

Όσον αφορά τη λειτουργία των μεταμηχανών αναζήτησης αυτές στηρίζονται σε δύο κύριες διαδικασίες:

- **Προσαρμογή της ερώτησης αναζήτησης στις διεπιφάνειες των απλών μηχανών αναζήτησης:** Οι μεταμηχανές αναζήτησης διαθέτουν ένα μηχανισμό που προσαρμόζει την ερώτηση αναζήτησης στα προκαθορισμένα κριτήρια των απλών μηχανών.
- **Ανάλυση, αξιολόγηση και παρουσίαση του επαυξημένου συνόλου αποτελεσμάτων:** Οι μεταμηχανές λαμβάνουν μεγάλο όγκο πληροφορίας από τις απλές μηχανές και γι' αυτό είναι πιθανό το σύνολο της πληροφορίας να είναι επικαλυπτόμενο και συνεπώς οι χρήστες να λαμβάνουν περιττή πληροφορία. Αυτό συνεπάγεται την περαιτέρω ανάλυση και αξιολόγηση της λαμβανόμενης πληροφορίας, ώστε να αποκλειστούν οι διπλοεγγραφές.

1.8.6.2 Αρχιτεκτονική Απλών Μηχανών Αναζήτησης

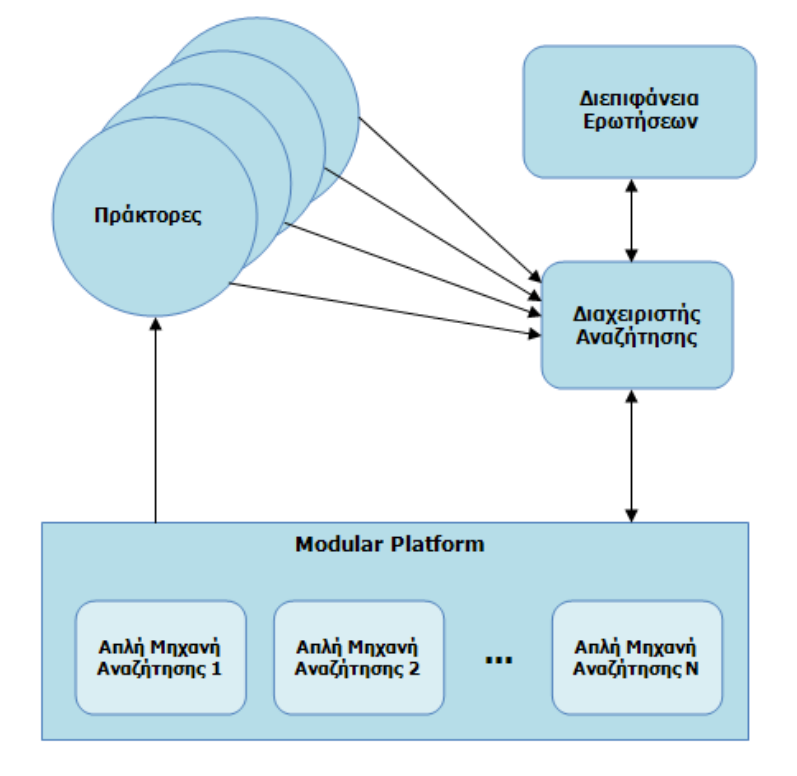
Η αρχιτεκτονική χωρίζεται σε δυο κατηγορίες. Η αρχιτεκτονική των απλών μηχανών αναζήτησης αποτελείται από τέσσερα κύρια τμήματα:



Εικόνα 8: Αρχιτεκτονική Απλών Μηχανών Αναζήτησης

- **Διαχειριστής αναζήτησης:** Τα κύρια καθήκοντά του είναι η αρχικοποίηση, ο έλεγχος απόκτησης πληροφορίας και ο έλεγχος δεικτών. Επίσης, είναι υπεύθυνος για τη συντακτική ανάλυση, την αποθήκευση και τη διαχείριση της ΒΔ. Για την έναρξη της ανάκτησης πληροφορίας, παρέχονται εντολές στους πράκτορες.
- **Πράκτορες:** Το κύριο καθήκον των πρακτόρων, είναι η ανάκτηση των εγγράφων στα οποία έχουν τοποθετηθεί δείκτες καθώς και η αναγνώριση των ανενεργών συνδέσμων. Στην ορολογία του παγκοσμίου ιστού, οι πράκτορες συχνά αναφέρονται ως **web robots, spiders** και **wanderers**. Κάποιες μηχανές χρησιμοποιούν παράλληλα αρκετούς πράκτορες ώστε να ελαττώνεται ο χρόνος ανάκτησης πληροφορίας. Λειτουργούν αποκλειστικά για τον εξυπηρετητή ερωτήσεων. Οι πράκτορες πλοηγούνται στον παγκόσμιο ιστό ακολουθώντας τους συνδέσμους που είναι ενσωματωμένοι στις σελίδες. Μιλάν τη γλώσσα (http) του παγκοσμίου ιστού και τη χρησιμοποιούν για να ανακτήσουν τα κατάλληλα έγγραφα από τους εξυπηρετητές .
- **Βάση δεδομένων:** Είναι υπεύθυνη για τη μόνιμη τοποθέτηση των δεικτών.

- **Εξυπηρετητής ερωτήσεων:** Παρέχει στο χρήστη μια διεπιφάνεια μέσω της οποίας ο χρήστης καθορίζει την ερώτησή του και επίσης, είναι υπεύθυνος για την παρουσίαση των τελικών αποτελεσμάτων.



Εικόνα 9: Εξυπηρετητής Ερωτήσεων

Όσον αφορά την αρχιτεκτονική των μεταμηχανών, όμοια και σε αυτή παρουσιάζονται τέσσερα τμήματα:

- **Διαχειριστής αναζητήσεων:** Είναι υπεύθυνος για την ανάλυση και αξιολόγηση των αποτελεσμάτων, ενώ φροντίζει και για την απόρριψη των διπλοεγγραφών. Προωθεί την ερώτηση στις απλές μηχανές και το σύνολο των αποτελεσμάτων στο χρήστη.
- **Modular platform:** Εξασφαλίζει την επικοινωνία με τις απλές μηχανές αναζήτησης και προωθεί τις αναφορές εγγράφων στους πράκτορες. Τέλος παρέχει στο χρήστη πληροφορίες κατάστασης της αναζήτησης του, όπως χρόνο απόκρισης κ.α.
- **Πράκτορες:** Είναι υπεύθυνοι για την ανάκτηση των κειμένων που γίνονται οι αναφορές, τις οποίες ανακτούν από τη modular platform. Η λειτουργία τους εξαρτάται μόνο από τα πρωτόκολλα του παγκόσμιου ιστού.

- **Διεπαφή Ερωτήσεων:** Είναι η διεπαφή που παρέχεται στο τελικό χρήστη , στην οποία καταχωρείται η ερώτηση και εμφανίζονται τα αποτελέσματα.

1.8.7 Δυνατότητα Ανάκτησης Εξειδικευμένων Πληροφοριών

Το διαδίκτυο σήμερα καλύπτει τις ανάγκες των χρηστών για την ανάκτηση εξειδικευμένης πληροφορίας. Για την καλύτερη δυνατή διαχείριση της πληροφορίας χρησιμοποιούνται πράκτορες.

1.8.7.1 Λειτουργίες Ανάκτησης Εξειδικευμένων Πληροφοριών

Οι εφαρμογές μέσω των οποίων ανακτώνται οι εξειδικευμένες πληροφορίες, χωρίζονται σε δυο κατηγορίες. Το κοινό σημείο των εφαρμογών αυτών είναι ότι εμφανίζουν τις πληροφορίες σε κανάλια (channels):

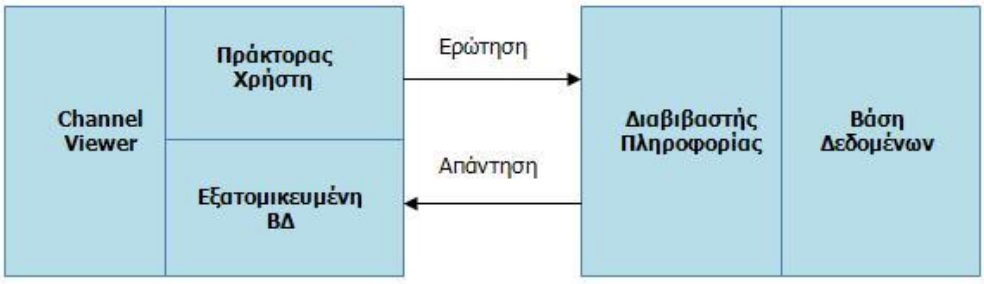
- **Εξατομίκευση καναλιών:** Φιλτράρουν και κατηγοριοποιούν την πληροφορία βάσει των προτιμήσεων του χρήστη. Προσφέρουν στο χρήστη τη δυνατότητα τροποποίησης της διεπαφής τους.
- **Ταυτοποίηση πληροφορίας:** Φροντίζει για την ανανέωση της πληροφορίας με την προϋπόθεση να έχει ορίσει ο χρήστης παραμέτρους ενημέρωσης όπως το χρόνο, τον τύπο σύνδεσης.

1.8.7.2 Αρχιτεκτονική Ανάκτησης Εξειδικευμένων Πληροφοριών

Η λειτουργία των εφαρμογών αυτών βασίζεται στην αρχιτεκτονική client-server. Τα κύρια χαρακτηριστικά της αρχιτεκτονικής είναι:

- **Channel viewer:** Οργανώνει σε κανάλια την εισερχόμενη πληροφορία και φροντίζει για τη παρουσίαση της, κάνοντας συνήθως χρήση του εγκατεστημένου browser.
- **Πράκτορας χρήστη:** Είναι υπεύθυνος για τη μετάδοση της νεότερης πληροφορίας. Θα πρέπει αρχικά να καθοριστούν παράμετροι χρόνου και διάρκειας ώστε στη συνέχεια ο πράκτορας να λειτουργεί ανεξάρτητα.
- **Εξατομικευμένη βάση δεδομένων:** Αποθηκεύει την εξειδικευμένη πληροφορία στον υπολογιστή του χρήστη, ώστε να μπορεί μέσω του channel viewer να έχει πάντα πρόσβαση στην πληροφορία. Η νεότερη πληροφορία αντικαθιστά την παλαιότερη και επίσης, ο χώρος αποθήκευσης ορίζεται δυναμικά.

- **Διαβιβαστής εξειδικευμένης πληροφορίας:** Επεξεργάζεται τις ερωτήσεις ενημέρωσης και εξασφαλίζει τη μετάδοση της απαιτούμενης πληροφορίας.
- **Βάση δεδομένων:** Παρέχει όλες τις πληροφορίες του παροχέα που είναι διαθέσιμες.



Εικόνα 10: Αρχιτεκτονική Ανάκτησης Εξειδικευμένων Πληροφοριών

1.8.8 Πράκτορες Ειδοποίησης (Notification Agents)

Οι πράκτορες ειδοποίησης, θα μπορούσαν να χαρακτηριστούν ως οι γραμματείς των χρηστών. Δηλαδή, φροντίζουν για την κοινοποίηση σημαντικών γεγονότων στους χρήστες, όπως:

- Αλλαγή περιεχομένου σε μια συγκεκριμένη σελίδα.
- Προσθήκες ερωτήσεων σε μηχανές αναζήτησης.
- Υπενθυμίσεις για προσωπικά γεγονότα.

Οι τρόποι μέσω των οποίων οι πράκτορες αντιλαμβάνονται τις αλλαγές είναι:

- Μέσω του πρωτοκόλλου HTTP, το οποίο περιέχει ένα request ("If-Modified-Since") που επιστρέφει μόνο τα έγγραφα που έχουν τροποποιηθεί από τη συγκεκριμένη ημερομηνία που συνοδεύει την αίτηση. Επίσης το HTTP προσφέρει ειδικές εντολές που ειδοποιούν τους πράκτορες για την εκτέλεση συγκεκριμένων ενεργειών.
- Οι πράκτορες ανακτούν ένα έγγραφο συγκρίνοντας το περιεχόμενο των ιστοσελίδων και επισημαίνουν τις αλλαγές .

Χαρακτηριστικό παράδειγμα τέτοιων πρακτόρων υπάρχει στο amazon.com, όπου πράκτορες ελέγχουν τις κινήσεις των χρηστών και τους προτείνουν προϊόντα που πιθανώς τους ενδιαφέρουν.

Τα κυριότερα πλεονεκτήματα των πρακτόρων ειδοποίησης συνοψίζονται στο παρακάτω πίνακα:

Χαρακτηριστικό	Πλεονέκτημα
Παρακολούθηση	Ελάττωση δουλειάς χρήστη
Παρακολούθηση χωρίς browsers	Αύξηση αποτελεσματικότητας δικτύου
Προσδιορισμός αλλαγής	Ελάττωση δουλειάς χρήστη
Υλοποίηση σε εξυπηρετητές	Εξοικονόμηση bandwidth χρήστη

Πίνακας 1: Πλεονεκτήματα Πρακτόρων Ειδοποίησης

1.8.9 Παροχή Συμβουλών Πλοήγησης και Εστίασης

Για το σκοπό αυτό υπάρχουν ειδικοί βοηθοί, οι οποίοι μαθαίνουν τον τρόπο συμπεριφοράς του χρήστη κι έτσι μπορούν να τον συμβουλεύουν και να τον πληροφορούν για το σωστότερο τρόπο πλοήγησης και εργασίας, γεγονός που συνεπάγεται να μπορεί ο χρήστης να εστιάσει στην κύρια εργασία του. Οι πράκτορες αυτής της λειτουργίας είναι στατικοί και με περιορισμένο βαθμό ευφυΐας, γι' αυτό και απαιτείται η αύξηση της ευφυΐας τους.

Οι εφαρμογές επιτρέπουν την αποδοχή και αξιολόγηση της αναζήτησης πληροφορίας, συνδυάζοντας αυτά τα καθήκοντα με την αυτοματοποίηση των λειτουργιών του χρήστη που καταναλώνουν χρόνο όταν αυτός εργάζεται με τον browser. Επίσης, μπορούν να δημιουργήσουν ένα εξατομικευμένο προφίλ χρήστη το οποίο βασίζεται στις ανάγκες του. Η πλειονότητα των καθηκόντων ανατίθεται σε πράκτορες με υψηλό βαθμό ευφυΐας και υψηλή ικανότητα μάθησης, γεγονός που σημαίνει ότι οι πράκτορες μπορούν να καταγράφουν και να μιμούνται τη συμπεριφορά του χρήστη χρησιμοποιώντας την ικανότητα επικοινωνίας με το χρήστη. Οι πράκτορες εκπαιδεύονται από το χρήστη με τη χρήση παραδειγμάτων και μπορούν να επικοινωνούν και με άλλους πράκτορες. Οι τρέχουσες εφαρμογές δίνουν βάρος κυρίως στη διαδικασία παρακολούθησης και εξαγωγής συμπερασμάτων βασιζόμενων στη συμπεριφορά του χρήστη.

1.8.10 Ψυχαγωγία

Οι εφαρμογές αυτού του πεδίου υποστηρίζουν το χρήστη στην επιλογή ψυχαγωγικών δραστηριοτήτων που ταιριάζουν με τα ενδιαφέροντά του. Συγκεκριμένα, δίδεται βοήθεια από ειδικούς πράκτορες σχετικά με διαδικτυακές αγορές, ταινίες, μουσική και τηλεόραση. Αυτό γίνεται με τη δημιουργία ενός προσωπικού προφίλ χρήστη μέσω του οποίου οι εφαρμογές παρουσιάζουν την εξατομικευμένη πληροφορία. Οι πράκτορες είναι επίσης στατικοί και με περιορισμένη ευφυΐα. Το μειονεκτήματα τους όμως είναι η περιορισμένη ικανότητα συνεργασίας, καθώς και ότι δεν υπάρχει η δυνατότητα παράλληλης συνεργασίας πρακτόρων για την επίλυση ενός προβλήματος. Για το καλύτερο δυνατό αποτέλεσμα θα πρέπει οι πράκτορες να συγκρίνουν τα προφίλ χρηστών και να επικοινωνούν και με το χρήστη.

1.8.11 Εφαρμογές Υποστήριξης Ομάδων Εργασίας

Οι εφαρμογές αυτές παρέχουν υποστήριξη για την επεξεργασία κοινών και σχετικά αδόμητων καθηκόντων. Δημιουργούν πληροφορία που ομαδοποιείται, αναλύεται και κατανέμεται σε ομάδα εργασίας. Οι κύριες μορφές των εφαρμογών αυτών περιλαμβάνουν συστήματα επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο.

Οι πράκτορες που χρησιμοποιούνται σε αυτές τις εφαρμογές υποστηρίζουν την ανάκτηση πληροφορίας και τη διαδικασία λήψης αποφάσεων κατά την επίλυση ενός προβλήματος. Επίσης, επιτρέπουν την παροχή και διαχείριση σημαντικής πληροφορίας σε όλα τα μέλη της ομάδας εργασίας και την αποδοχή δουλειάς-ρουτίνας. Και σε αυτόν τον τομέα, οι πράκτορες είναι περιορισμένης ευφυΐας, έχουν όμως τη δυνατότητα πολλαπλής παράλληλης συνεργασίας με άλλους πράκτορες.

Η διαχείριση και επεξεργασία του ηλεκτρονικού ταχυδρομείου μέσα σε μια ομάδα εργασίας αποτελεί μια ιδανική λειτουργική περιοχή για τους πράκτορες. Η χρήση τους επιτρέπει τη διαχείριση του μεγαλύτερου μέρους της δουλειάς-ρουτίνας, όπως ανάγνωση, διαγραφή, εκτύπωση και προώθηση ηλεκτρονικών μηνυμάτων.

ΜΕΡΟΣ 2ο

2. Μετρα Ασφαλείας σε Mobile Agents

2.1 Εισαγωγή

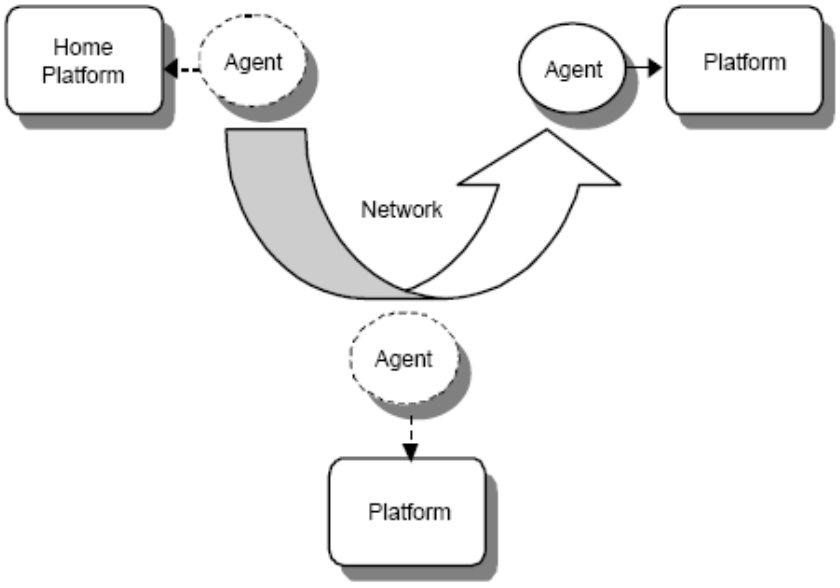
Όπως αναφέρθηκε και στο 1ο κεφάλαιο η τεχνολογία κινητών πρακτόρων (ΜΑΤ) βρίσκει εφαρμογή στις κατανεμημένες εφαρμογές. Με τη χρήση των ΜΑΤ ένα πρόγραμμα, υπό μορφή πράκτορα λογισμικού, μπορεί να αναστείλει την εκτέλεσή του σε έναν οικοδεσπότη υπολογιστή, να μεταφερθεί σε έναν άλλο στο δίκτυο, και να επαναλάβει την εκτέλεση στο νέο οικοδεσπότη. Η χρήση των κινητών πρακτόρων έχει μερικά πλεονεκτήματα σε σύγκριση με τις παραδοσιακές λύσεις client/server συστημάτων όπως

- Η μείωση της κυκλοφορίας στο δίκτυο (network traffic)
- Η διαφάνεια στην εκτέλεση και στην επικοινωνία
- Η αυτόνομη και ευφυή εκτέλεση
- Η ευελιξία προγραμματισμού και επικοινωνίας
- Η προσαρμοστικότητα σε ειδικές συνθήκες
- Η διαχείριση του κύκλου ζωής
- Η αντοχή και ανοχή σε σφάλματα και
- Η διαλειτουργικότητα.

Η ανάπτυξη όμως των πρακτόρων αντιμετωπίζεται δύσπιστα από τα θέματα ασφαλείας που προκύπτουν από τη χρήση τους. Η χρήση των agents αυξάνει τη πολυπλοκότητα με αποτέλεσμα να αυξάνεται και η διακύμανση των απειλών άρα και οι επιθέσεις . Μια πλατφόρμα agent πρέπει να έχει πρόσβαση στη δομή, το περιεχόμενα και στα δεδομένα των mobile agents. Επιπλέον ένας

agent επισκέπτης μπορεί να ενεργήσει κακόβουλα είτε στην ίδια τη πλατφόρμα, είτε στους άλλους agents που φιλοξενούνται σε αυτήν.

Η τεχνολογία των agents είναι εκτεθειμένη σε μια σειρά επιθέσεων τόσο στη πλατφόρμα agent όσο και στους mobile agents. Για να αντιμετωπιστούν αυτές οι επιθέσεις, ένα σύστημα mobile agent πρέπει να ενσωματώνει ένα πλαίσιο ασφάλειας που θα προστατεύει τόσο τη πλατφόρμα του agent όσο και τους επισκέπτες agent. Το πλαίσιο αυτό θα πρέπει να διαμορφώνεται ανάλογα με τις απαιτήσεις του κάθε συστήματος, τις εφαρμογές που υπάρχουν σε αυτό καθώς και τους πιθανούς κινδύνους που θα αντιμετωπίσει βάσει του περιβάλλοντος στο οποίο βρίσκεται.



Εικόνα 11 : Μοντέλο Mobile Agent

Στο συγκεκριμένο κεφάλαιο γίνεται μελέτη για την ασφάλεια των mobile agents. Θα περιγραφούν οι απαιτήσεις ασφάλειας που υπάρχουν για τη προστασία των πόρων ενώ θα παρουσιαστούν και οι απειλές – επιθέσεις που σχετίζονται με συστήματα. Η πλειονότητα των μέτρων ασφαλείας κατηγοριοποιούνται σε δυο κατηγορίες

- Σε εκείνα που εξασφαλίζουν τη πλατφόρμα
- Σε εκείνα που εξασφαλίζουν τον agent

Οι μηχανισμοί που προστατεύουν την πλατφόρμα δίνουν έμφασή κυρίως στη ενεργή προστασία ενώ αυτοί των agents στον εντοπισμό.

2.2 Πλαίσιο Ασφαλείας

2.2.1 Απαιτήσεις ασφαλείας

Οι απαιτήσεις ασφαλείας στο πλαίσιο των MAT δίνουν έμφαση στη προστασία του κώδικα των δεδομένων αλλά και των πόρων του συστήματος. Οι απαιτήσεις αυτές πρέπει να προσδιοριστούν χρησιμοποιώντας μερικά standard δεδομένα (όπως η εμπιστευτικότητα, η μυστικότητα, η ανωνυμία, η ακεραιότητα, η υπευθυνότητα και η διαθεσιμότητα) για να προσδιοριστεί το κατάλληλο επίπεδο ασφάλειας.

Ένα σύστημα mobile agent μπορεί να θέλει να κρατήσει ιδιωτικά δεδομένα αποθηκευμένα σε μια πλατφόρμα που μεταφέρονται από ένα πράκτορα ή συναλλάσσονται μεταξύ συστημάτων εμπιστευτικά. Για αυτό το λόγο τα συστήματα των agents πρέπει να είναι σίγουρα ότι οι εσωτερικές τους επικοινωνίες αλλά και οι επικοινωνίες με τις πλατφόρμες είναι εμπιστευτικές. Οι agents επίσης θέλουν να κρατήσουν μυστική τη τοποθεσία τους από τα άλλα στοιχεία του συστήματος τους. Επιπλέον ένας agent δε θέλει να κάνει γνωστό στη πλατφόρμα τους προηγούμενους σταθμούς της διαδρομής του πριν καταλήξει σε αυτήν. Στον αντίποδα βέβαια το πλαίσιο ασφάλειας των πλατφόρμων υποδοχής δεν θα πρέπει να δέχεται agent που προέρχονται από πλατφόρμες εκτός του εγκεκριμένου τομέα ασφαλείας. Τέλος τα μητρώα ελέγχου τον πρακτόρων τα οποία περιέχουν λεπτομέρειες για τις ενέργειες τους πρέπει να σταθμίζονται με την ιδιωτικότητα των πρακτόρων και η πρόσβαση σε αυτά πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένους διαχειριστές. Γενικά η συλλογή και η χρήση πληροφοριών ελέγχου πρέπει να είναι καλά ορισμένη και κατανοητή από τους agent όταν επισκέπτονται μια πλατφόρμα

Εκτός από την εμπιστευτικότητα μια πλατφόρμα agent πρέπει να έχει τη δυνατότητα να προσφέρει στους agents ανωνυμία . Θα πρέπει να κρατάει τη ταυτότητα του agent μυστική από τους άλλους agent αλλά θα πρέπει να έχει και τη δυνατότητα να εμφανίσει τη ταυτότητα του πράκτορα σε περίπτωση που αυτό κριθεί απαραίτητο. Πάραυτα υπάρχουν αρκετές περιπτώσεις όπου πραγματοποιούνται συναλλαγές ανώνυμα. Υπάρχουν αρκετοί αποδέκτες υπηρεσιών και αγαθών που θέλουν να προστατεύσουν την ιδιωτικότητα τους μένοντας ανώνυμοι , αλλά οι

πιστοληπτικοί οργανισμοί δεν εγκρίνουν πίστωση σε ανώνυμούς προτού είναι σε θέση να ελέγξουν το πιστωτικό ιστορικό τους και τη πιστοληπτική ικανότητα του δανειζομένου

Μια πλατφόρμα agent θα πρέπει να εξασφαλίσει την ακεραιότητα του agent. Θα πρέπει να προστατεύει τους agents από μη εξουσιοδοτημένη τροποποίηση του κώδικά, των δομών και των δεδομένων τους, ενώ θα πρέπει να είναι σε θέση να επιτρέπει μόνο σε εξουσιοδοτημένους agent ή διαδικασίες να μπορούν να τροποποιήσουν κοινόχρηστα δεδομένα. Επιπλέον η λειτουργία ασφαλείας των συστημάτων mobile agents εξαρτάται από την ακεραιότητα της πλατφόρμας του τοπικού και απομακρυσμένου agent. Ένας κακόβουλος host μπορεί εύκολα να επηρεάσει την ακεραιότητα των mobile agents που τον επισκέπτονται , μπορεί να αλλάξει τη ροη εκτέλεσης και να προκαλέσει αλλοιώσεις των υπολογιζόμενων αποτελεσμάτων που είναι δύσκολο να ανιχνευθούν. Μπορεί επίσης να παρέμβει σε συναλλαγές μεταξύ agent διαφορετικών οντοτήτων και να επηρεάσει το μητρώο ελέγχου αυτών.

Φυσικά δεν είναι μονό οι mobile agents εκτεθειμένοι σε επιθέσεις των πλατφορμών αλλά συμβαίνει και το αντίθετο , για αυτό το λόγο τα συστήματα ελέγχου πρόσβασης των πλατφορμών πρέπει να βρίσκονται σε θέση να προστατεύουν την ακεραιότητα της πλατφόρμας από μη εξουσιοδοτημένους χρήστες και από δικτυακά worms, Trojan horses και viruses. Οι mobile agents δεν θα πρέπει να είναι σε θέση να επηρεάζουν τους πόρους της πλατφόρμας που τους φιλοξενούν (όπως αρχεία, εκτυπωτές κ.α) και θα πρέπει να έχουν μόνο περιορισμένη πρόσβαση σε αυτούς. Οι mobile agents πρέπει να έχουν κάποιο είδος επιμονής για παράδειγμα σε περίπτωση που το μηχάνημα κολλήσει, για να συμβεί αυτό θα πρέπει να υπάρχει ένα ασφαλές στρώμα εκτέλεσης που θα μπορεί να ανταποκριθεί τόσο σε ασφαλή όσο και σε ανασφαλή περιβάλλοντα software και hardware

2.2.2 Επιθέσεις στην Τεχνολογία Κινητών Πρακτόρων (MAT)

Οι προαναφερθείσες απαιτήσεις που αφορούν στην ασφάλεια είναι σχετικά δύσκολο να πληρούνται στο βαθμό που οι MAT είναι εκτεθειμένοι στον εγγενή κίνδυνο διαφορετικών τύπων επιθέσεων. Οι εν λόγω επιθέσεις συχνά ταξινομούνται στις εξής κατηγορίες:

- Άρνηση υπηρεσίας
- Ζημιά συστήματος
- Παραβίαση ιδιωτικότητας

- Παρενόχληση
- Επιθέσεις κοινωνικής μηχανικής

Ακολούθως δίδεται μία συνοπτική περιγραφή του κάθε τύπου επίθεσης που μπορεί να λάβει χώρα σε συστήματα κινητών πρακτόρων.

- **Άρνηση υπηρεσίας (Denial of service):** Εκτελώντας πράκτορες ή διαδικασίες, ένας εισβολέας μπορεί να προκαλέσει υπερφόρτωση πόρων ή υπηρεσιών , για παράδειγμα μέσω της συνεχούς ανάλωσης των συνδέσεων του δικτύου ή της υπερφόρτωσης ενδιάμεσων μνημών για τη δημιουργία αδιεξόδων (deadlocks).
- **Ζημιά συστήματος**: Ένας κακόβουλος φορέας μπορεί να μεταλλάξει ή να καταστρέψει τα αρχεία, τις βασικές ρυθμίσεις, την πολιτική ασφαλείας, το υλισμικό ενός συστήματος-οικοδεσπότη (host) ή των κώδικα ενός κινητού πράκτορα.
- **Παραβίαση ιδιωτικότητας (Breach of privacy):** Ένας κακόβουλος πράκτορας ή μία πλατφόρμα μπορεί να εξασφαλίσει πρόσβαση και να αποκαλύψει ιδιωτικά δεδομένα.
- **Παρενόχληση (Harassment):** Ένας κακόβουλος πράκτορας ή διαδικασία μπορεί να εκτελέσει ενοχλητικές, επαναλαμβανόμενες επιθέσεις, π.χ. εμφανίζοντας ανεπιθύμητες εικόνες.
- **Κοινωνική μηχανική (Social engineering):** μία κακόβουλη οντότητα μπορεί να χειραγωγήσει ανθρώπους, κεντρικά υπολογιστικά συστήματα ή κινητούς πράκτορες χρησιμοποιώντας παραπλανητικές πληροφορίες. Για παράδειγμα, ένας κινητός πράκτορας μπορεί να ζητήσει τους κωδικούς πρόσβασης του χρήστη υποδυόμενος το διαχειριστή του συστήματος.

Επιπροσθέτως, υπάρχουν δύο σύνθετες μορφές επιθέσεων, οι οποίες περιλαμβάνουν χαρακτηριστικά των επιθέσεων που περιγράφηκαν προηγουμένως.

- **Επιθέσεις ενεργοποιούμενες από γεγονότα (Event-triggered):** η έναρξη οποιασδήποτε από τις επιθέσεις που περιγράφηκαν προηγουμένως προκαλείται από ένα συγκεκριμένο γεγονός, όπως το χρόνο, την τοποθεσία, την άφιξη ενός συγκεκριμένου ατόμου κλπ. (όπως το πρόγραμμα δούρειου ίππου).
- **Συνδυασμένες επιθέσεις (Compound attacks):** Χρησιμοποιώντας τεχνικές συνεργασίας, οι κινητοί πράκτορες μπορούν να συνεργαστούν μεταξύ τους προκειμένου να εκτελέσουν μία σειρά επιθέσεων. Για παράδειγμα, η παρενόχληση μπορεί να

χρησιμοποιηθεί ως μέρος μίας επίθεσης κοινωνικής μηχανικής με απώτερο σκοπό την ζημιά του συστήματος ή την παραβίαση της ιδιωτικότητας.

Παρακάτω αναλύονται πιθανές περιπτώσεις επιθέσεων καθώς και οι παρενέργειες κάθε μίας επίθεσης. Αναλυτικότερα οι επιθέσεις παρουσιάζονται χωρισμένες σε τέσσερις κατηγορίες:

- **Επίθεση από έναν agent σε μια πλατφόρμα**
- **Επίθεση μιας πλατφόρμας σε agent**
- **Επίθεση από έναν agent σε κάποιον άλλο agent**
- **Επίθεση άλλων οντοτήτων σε πλατφόρμα agents**

2.2.2.1 Επίθεση από έναν agent σε μια πλατφόρμα

Στη συγκεκριμένο περίπτωση επίθεσης ο agent εκμεταλλεύεται αδυναμίες ασφάλειας μιας πλατφόρμας και εξαπολύει επίθεση προς αυτή. Μπορούν να εμφανιστούν οι παρακάτω κατηγορίες επιθέσεων :

- Masquerading
- Άρνηση Υπηρεσίας (Denial of Service)
- Μη εξουσιοδοτημένη Πρόσβαση

2.2.2.1.1 Masquerading

Masquerading είναι η επίθεση κατά την οποία ένας μη εξουσιοδοτημένος agent προσποιείται ότι είναι κάποιος άλλος agent. Ο μεταμφιεσμένος agent μπορεί να εμφανιστεί ως εξουσιοδοτημένος για νε έχει πρόσβαση σε πόρους και υπηρεσίες που ειδάλλως δε θα είχε, ή να εμφανιστεί σα μη εξουσιοδοτημένος με σκοπό να μεταθέσει τις ευθύνες μιας πράξης σε κάποιον άλλο agent.Με αυτό τον τρόπο μπορεί να καταστρέψει την αξιοπιστία κάποιου άλλου agent στο σύστημα.

2.2.2.1.2. Άρνηση Υπηρεσίας

Οι κινητοί πράκτορες μπορούν να προκαλέσουν επιθέσεις άρνησης υπηρεσιών καταναλώνοντας υπερβολικό όγκο υπολογιστικών πόρων μιας πλατφόρμας από agents. Αυτό μπορεί να συμβεί είτε εσκεμμένα τρέχοντας scripts επιθέσεων ώστε να εκμεταλλευτούν τα τρωτά σημεία τους συστήματος είτε μη σκόπιμα μέσω προγραμματιστικών λαθών. Επιθέσεις ασφαλείας που προέρχονται από προγραμματίστηκα λάθη και πλήξη σε τρωτά σημεία αναφέρονται για πρώτη φορά στη βιβλιογραφία στις αρχές του 1970.

Ο έλεγχος προγραμμάτων, η διαχείριση ρυθμίσεων, οι ανεξάρτητες δοκιμές και άλλες μέθοδοι του κλάδου προγραμματισμού έχουν αναπτυχθεί ώστε να μειωθεί ο κίνδυνος κάποιος προγραμματιστής εκούσια ή ακούσια ,να εισάγει κάποιο κακόβουλο κομμάτι κώδικα σε ένα υπολογιστικό σύστημα μιας επιχείρησης

Ωστόσο, στη περίπτωση του mobile computing , απαιτείται μια πλατφόρμα agent να δεχτεί και να εκτελέσει εντολές ενός agent του οποίου ο κώδικας έχει αναπτυχθεί έξω από τον οργανισμό και δεν έχει γίνει υποκείμενο προηγούμενης επισκόπησης.

Ένας επικίνδυνος agent μπορεί να φέρει κακόβουλο κώδικα που να έχει σκοπό να καταστρέψει τις υπηρεσίες που προσφέρονται από τη πλατφόρμα των agents, να μειώσει την επίδοση της πλατφόρμας ή να εξάγει πληροφορίες στις οποίες δεν έχει εξουσιοδοτημένη πρόσβαση. Ανάλογα με το επίπεδο πρόσβασής ένας agent μπορεί ακόμα να απενεργοποιήσει ή να σταματήσει για πάντα μια πλατφόρμα

2.2.2.1.3. Μη εξουσιοδοτημένη πρόσβαση

Οι μηχανισμοί ελέγχου πρόσβασης χρησιμοποιούνται για να αποτρέψουν τη πρόσβαση μη εξουσιοδοτημένων χρηστών και διεργασιών σε υπηρεσίες και πόρους για τους οποίους δεν τους έχουν χορηγηθεί προνόμια όπως ορίζεται από την εκάστοτε πολιτική ασφαλείας. Κάθε agent που επισκέπτεται μια πλατφόρμα πρέπει να υπόκειται στη πολιτική ασφάλεια της πλατφόρμας. Για να εφαρμοστούν οι σωστοί μηχανισμοί ελέγχου πρόσβασής απαιτείται η πλατφόρμα ή ο agent , να πιστοποιήσει τη ταυτότητα του πριν αυτός αποκτήσει πρόσβαση στη πλατφόρμα. Ένας agent που έχει πρόσβαση στη πλατφόρμα και στις υπηρεσίες της χωρίς να έχει εξουσιοδότηση μπορεί να βλάψει άλλους agent ή ακόμα και την ίδια τη πλατφόρμα.

Μια πλατφόρμα, που φιλοξένει agents που εκπροσωπούν διάφορους χρήστες και οργανισμούς, πρέπει να διασφαλίζει ότι οι agents δεν έχουν δικαίωμα γραφής-ανάγνωσης

δεδομένων που δεν έχουν πιστοποίηση, καθώς επίσης και πρόσβαση σε δεδομένα που είναι αποθηκευμένα σε προσωρινά αρχεία ή στη μνήμη cache.

2.2.2.2 Επίθεση μιας πλατφόρμας σε agent

Στη συγκεκριμένη κατηγορία θα αναλυθούν οι επιθέσεις που κάποια πλατφόρμα μπορεί να κάνει πάνω σε κάποιο agent. Σε αυτή τη περίπτωση εμφανίζονται οι παρακάτω επιθέσεις

- Masquerading,
- Άρνηση Υπηρεσίας
- Eavesdropping (Λαθρακρόαση)
- Μετάλλαξη

2.2.2.2.1 Masquerade

Μια πλατφόρμα μπορεί να μεταμφιεστεί σε μία άλλη, έχοντας ως αποτέλεσμα να οδηγήσει σε αυτή έναν agent που είχε κάποιον άλλο προορισμό και να προκαλέσει θέματα ασφαλείας. Μια πλατφόρμα μεταμφιεσμένη σε κάποια άλλη μπορεί να προσελκύσει agents και να εξάγει ευαίσθητες πληροφορίες από αυτούς, ενώ μπορεί να βλάψει τόσο τους agent που προσελκύει όσο και την πλατφόρμα την οποία έχει αντιγράψει. Ένας μεταμφιεσμένος agent όπως περιγράφτηκε και στη παραπάνω ενότητα μπορεί να βλάψει κάποιον άλλο agent και κάποια πλατφόρμα με τα μηνύματα που ανταλλάσουν ή με τις ενέργειες που απορρέουν από αυτά, όμως κακόβουλες πλατφόρμες που έχουν μεταμφιεστεί ως εξουσιοδοτημένες μπορούν να δημιουργήσουν σοβαρότερο πρόβλημα στους άλλους agent. Στις επόμενες ενότητες αναλύονται οι επιπτώσεις της αλλαγής του κώδικα ή των δεδομένων ενός agent από μια πλατφόρμα

2.2.2.2.2 Άρνηση Υπηρεσίας

Όταν ένας agent φτάνει σε μία πλατφόρμα περιμένει από εκείνη να εκτελέσει τις εντολές του και να του παρέχει πόρους που προέρχονται από τις συμφωνίες ποιότητας των υπηρεσιών. Πάραυτα μια κακόβουλη πλατφόρμα μπορεί να αγνοήσει τις αιτήσεις του agent για παροχή υπηρεσιών, προκαλώντας μη αναμενόμενες καθυστερήσεις σε σοβαρές διαδικασίες. Συχνά εμφανίζεται το φαινόμενο της μη εκτέλεσης ή και της απρόσμενης διακοπής κάποιας διαδικασίας

του agent. Οι agent σε άλλες πλατφόρμες που περιμένουν τα αποτελέσματα κάποιου άλλου agent που βρίσκεται σε μια κακόβουλη πλατφόρμα πρέπει να είναι πολύ προσεκτικοί για να μη πέσουν σε deadlock. Επίσης ένας agent μπορεί να βρεθεί σε κατάσταση livelocked. Ένας agent βρίσκεται σε livelocked όταν μία κακόβουλη πλατφόρμα ή ένα προγραμματιστικό λάθος δημιουργούν μια κατάσταση στην οποία ένα στάδιο μιας διαδικασίας που έχει να εκτελέσει δε μπορεί να ολοκληρωθεί γιατί τροφοδοτείται συνέχεια με extra όγκο. Ένας agent που βρίσκεται σε Livelocked διαφέρει από έναν agent που βρίσκεται σε deadlock, ο δεύτερος έχει σταματήσει για κάποιο λόγο να ανταποκρίνεται, ενώ ο πρώτος δουλεύει συνεχώς χωρίς όμως να καταφέρνει ποτέ να επιτεύξει το στόχο του

2.2.2.2.3 Eavesdropping

Η επίθεση λαθρακρόασης (eavesdropping) περιλαμβάνει τη παρακολούθηση και των έλεγχο μυστικών επικοινωνιών. Το eavesdropping στα συστήματα κινητών πρακτόρων οξύνεται γιατί εκεί η πλατφόρμα μπορεί εκτός από τις επικοινωνίες να παρακολουθήσει και οποιαδήποτε οδηγία εκτελείται από τον agent καθώς επίσης και οποιαδήποτε δημόσιά ή μη κρυπτογραφημένη πληροφορία περιέχει ο agent. Καθώς η πλατφόρμα έχει πρόσβαση στον κώδικα του agent, στη κατάστασή του και στα δεδομένα του, κάθε agent πρέπει να είναι κατασκευασμένος ώστε να μην εκθέτει ευαίσθητες πληροφορίες όπως εμπορικά μυστικά, αποκλειστικούς αλγόριθμους, στρατηγικές διαπραγμάτευσης κ.α

Βέβαια μερικές φορές ακόμα και αν ένας agent αποκλείσει τη πρόσβαση σε κάποια από τις παραπάνω πληροφορίες, οι πλατφόρμες είναι σε θέση να καταλάβουν μερικά δεδομένα από τις υπηρεσίες που απαιτούνται αλλά και από τη ταυτότητα του agent με τον οποίον επικοινωνούν. Για παράδειγμα σε περίπτωση που κάποιος agent επικοινωνεί με μία πλατφόρμα για να κανονίσει κάποιο ταξίδι για κάποιο πελάτη (travel agent), η πλατφόρμα μπορεί να υποκλέψει το μήνυμα και να το μεταβιβάσει σε κάποιον διαφημιστικό σύμβουλο ώστε να στέλνει διαφημιστικά έντυπα με ταξιδιωτικούς προσδιορισμούς ή ακόμα στη χειρότερη περίπτωση σε κάποιο κλέφτη και να τον ενημερώσει ότι το σπίτι θα είναι άδειο εκείνες τις μέρες γιατί ο κάτοχος του θα λείπει ταξίδι

2.2.2.2.4 Μετάλλαξη

Όπως αναφέρθηκε και παραπάνω όταν ένας agent φτάνει σε μία πλατφόρμα εκθέτει το κώδικά τη κατάσταση και τα δεδομένα του σε αυτήν. Καθώς κατά τη διάρκεια της ζωής του επισκέπτεται πολλές πλατφόρμες, με διαφορετικά πλαίσια ασφαλείας , θα πρέπει να υπάρχουν

μηχανισμοί που φροντίζουν για την ακεραιότητα αυτών. Μια κακόβουλη πλατφόρμα μπορεί να τροποποίηση είτε το κώδικα, είτε τα δεδομένα, είτε ακόμα και τη κατάσταση του agent χωρίς να γίνει αντιληπτή. Η τροποποίηση του κώδικα ενός agent και κατ' επέκταση η συμπεριφορά του όταν επισκέπτεται άλλες πλατφόρμες μπορεί να ανιχνευθεί έχοντας ο ιδιοκτήτης του υπογράψει ηλεκτρονικά το κώδικά του. Η ανίχνευση κακόβουλων αλλαγών στη κατάσταση ενός agent κατά την εκτέλεση του , ή στα δεδομένα του δεν είναι πάντα εφικτή. Μια πλατφόρμα για παράδειγμα θα μπορούσε να τρέχει ένα τροποποιημένο virtual μηχάνημα, χωρίς να το γνωρίζει ο agent, το οποίο θα παράγει συνεχώς λανθασμένα αποτελέσματα

Ένας mobile agent που επισκέπτεται πολλές πλατφόρμες κατά το δρομολόγιο του, είναι εκτεθειμένος σε νέους κινδύνους τόσο κατά την μετακίνηση του αλλά και όταν φτάνει σε κάθε πλατφόρμα. Ο υπεύθυνος για την οποιοδήποτε κακόβουλη αλλαγή στη κατάσταση ή τα δεδομένα, εάν δεν ανιχνευθεί αμέσως , είναι απίθανο να εντοπιστεί αφού ο agent επισκεφτεί άλλες πλατφόρμες και τα δεδομένα και η κατάσταση υποστούν αμέτρητες αλλαγές. Η χρήση των check points και η roll back διαδικασία που δουλεύει περίφημα στα άλλα περιβάλλοντα, στα πλαίσια των κινητών πρακτόρων είναι πολύ δύσκολο να χρησιμοποιηθούν, γιατί η τελική κατάσταση και τα δεδομένα ενός πράκτορα σε μία πλατφόρμα, συχνά είναι αποτέλεσμα από μία σειρά μη ντετερμινιστικών γεγονότων που εξαρτώνται από τη συμπεριφορά αυτόνομων πρακτόρων των οποίων η συμπεριφορά δε μπορεί να ξαναδημιουργηθεί

Ο κίνδυνος ασφαλείας που υπάρχει όταν ένας agent μετακινείται από τη μητρική του πλατφόρμα σε κάποια άλλη ονομάζεται πρόβλημα "single-hop", ενώ ο κίνδυνος ασφαλείας που υπάρχει όταν ο agent επισκέπτεται διάφορες πλατφόρμες ονομάζεται πρόβλημα "multi-hop" . Οι κίνδυνοι που υπάρχουν στο πρόβλημα single-hop είναι ευκολότερο να μετριασθούν σε σχέση με τους κινδύνους που υπάρχουν στο σενάριο multi-hop καθώς οι μηχανισμοί προστασίας ανάμεσα στο έμπιστο περιβάλλον της μητρικής πλατφόρμας είναι δύσκολο να χρησιμοποιηθούν στα άλλα στάδια.

Οι πλατφόρμες μπορούν επίσης να παραποιήσουν τις επικοινωνίες με τους agents, για παράδειγμα να αλλάξουν σκόπιμα πεδία σε μια λογιστική κίνηση ή ακόμα και να αλλάξουν τη λέξη αγόρασε με πούλησε σε κάποιο μήνυμα. Η παραπάνω αλλαγή στα δεδομένα είναι πιο δύσκολη από μια απλή παραποίηση ενός μηνύματος, αλλά συχνά ο επιτιθέμενος έχει μεγαλύτερο κίνητρο και σε περίπτωση επιτυχίας και ανταμοιβή.

2.2.2.2 Επίθεση μιας πλατφόρμας σε agent

Στη συγκεκριμένη κατηγορία θα αναλυθούν οι επιθέσεις που κάποια πλατφόρμα μπορεί να κάνει πάνω σε κάποιο agent. Σε αυτή τη περίπτωση εμφανίζονται οι παρακάτω επιθέσεις

- Masquerading,
- Άρνηση Υπηρεσίας
- Eavesdropping (Λαθρακρόαση)
- Μετάλλαξη

Πολλά συστατικά πλατφόρμων agents είναι τα ίδια agents. Αυτοί οι agents παρέχουν υπηρεσίες συστήματος υψηλού επιπέδου όπως υπηρεσίες καταλόγου και υπηρεσίες επικοινωνίας μεταξύ πολλών πλατφορμών. Κάποιες πλατφόρμες agents επιτρέπουν άμεση επικοινωνία μεταξύ άλλων agents και πλατφορμών agents ενώ άλλοι απαιτούν όλα τα εισερχόμενα και εξερχόμενα μηνύματα να διέρχονται πρώτα από μια πλατφόρμα agent ασφαλείας. Αυτές οι αποφάσεις που σχετίζονται με την αρχιτεκτονική ενός συστήματος συνυφαίνονται με θέματα επιθέσεων από agent σε agent και από agent σε πλατφόρμα, όπως συζητήθηκαν στις προηγούμενες ενότητες

2.2.2.3.1 Masquerade

Επικοινωνία μεταξύ των agents γίνεται είτε άμεσα είτε έμμεσα με τη συμμετοχή μιας υποκείμενης πλατφόρμας και των υπηρεσιών agent που παρέχει. Σε κάθε περίπτωση, ένας agent μπορεί να επιχειρήσει να αποκρύψει την ταυτότητα του με σκοπό να εξαπατήσει έναν άλλον agent με τον οποίο επικοινωνεί. Ένας agent μπορεί για παράδειγμα να συστηθεί ως κάποιος πωλητής επώνυμων προϊόντων και υπηρεσιών ή να επιχειρήσει να πείσει έναν μη 'υποψιασμένο' agent να του παρέχει αριθμούς πιστωτικών καρτών, πληροφορίες τραπεζικών λογαριασμών ή άλλες ιδιωτικές πληροφορίες. Όταν ένας agent μεταμφιέζεται σε έναν άλλο agent βλάπτεται κυρίως την αξιοπιστία του δεύτερου, κάτι πολύ σημαντικό σε κοινωνίες agents που η φήμη μετράει και χρησιμοποιείται σαν εχέγγυο ώστε άλλοι agents, υπηρεσίες και συστήματα να τον εμπιστευτούν.

2.2.2.3.2 Άρνηση Υπηρεσίας

Εκτός από την περίπτωση άρνησης υπηρεσίας σε πλατφόρμες agents, υπάρχει και η περίπτωση που ένας agent πραγματοποιεί επίθεση άρνησης υπηρεσίας σε έναν ή περισσότερους agents. Για παράδειγμα, η επαναλαμβανόμενη αποστολή μηνυμάτων σε έναν agent μπορεί να

δημιουργήσει ανεπιθύμητο φόρτο στις ρουτίνες διαχείρισης μηνυμάτων του παραλήπτη agent. Οι agents που βομβαρδίζονται με υπερβολικό αριθμό μηνυμάτων μπορούν να επιλέξουν να μη λαμβάνουν μηνύματα από μη εξουσιοδοτημένους agents, αλλά ακόμα και αυτό απαιτεί κάποια διαδικασία να εκτελεστεί από τον agent ή το σύστημα εξουσιοδότησης πιστοποιητικών του.

Αν ένας agent χρεώνεται με τον αριθμό τον κύκλων επεξεργασίας σε μια πλατφόρμα, ο spammed-βομβαρδισμένος agent μπορεί να χρειαστεί να πληρώσει ένα υπέρογκο ποσό λόγω ζημίας στην απόδοση της πλατφόρμας. Η γλωσσά επικοινωνίας και διαλόγου των πολιτικών ασφαλείας μεταξύ των agents πρέπει να διασφαλίσουν ότι ένας κακόβουλος agent δε θα απασχολήσει κάποιον άλλο agent σε κάποιο τεράστιο loop , ή δε θα απασχολήσει κάποιο agent σε έναν ατέλειωτο διάλογο με αποκλειστικό σκοπό να σπαταλήσει τους πόρους του agent. Οι κακόβουλοι agents μπορούν πολλές φορές να διανείμουν μη έγκυρες ή λανθασμένες πληροφορίες σε άλλους agents με σκοπό να τους εμποδίσουν να ολοκληρώσουν κάποια εργασία σωστά ή έγκαιρα.

2.2.2.3.3 Repudiation (Απόκρουση - Απάρνηση)

Απάρνηση συμβαίνει όταν ένας agent, που συμμετέχει σε κάποια συναλλαγή ή γενικά διαδικασία επικοινωνίας, αργότερα ισχυριστεί ότι ποτέ δε συμμετείχε σε αυτή. Είτε ο σκοπός της απόρριψης αυτής είναι εσκεμμένος είτε όχι, η απάρνηση μπορεί να οδηγήσει σε σοβαρές διενέξεις μεταξύ των agents που δεν είναι εύκολο να επιλυθούν αν δεν ληφθούν τα απαραίτητα μέτρα την κατάλληλη στιγμή. Μια πλατφόρμα agent δεν μπορεί να αποτρέψει μια απάρνηση συναλλαγής από κάποιον agent. Ωστόσο μπορεί να διασφαλίσει τη διαθεσιμότητα ισχυρών αποδεικτικών στοιχείων που θα την οδηγήσει στην επίλυση των διαφωνιών που θα προκύψουν από την απάρνηση αυτή. Τα στοιχεία αυτά πιθανόν να αποτρέψουν έναν agent από το να απαρνηθεί μελλοντικές συναλλαγές ώστε να διατηρήσει τη φήμη του και την εμπιστοσύνη που οι άλλοι agents του αποδίδουν. Διαφωνίες μπορεί να προκύψουν όχι μόνο όταν ένας agent απαρνηθεί μια συναλλαγή αλλά και όταν όχι τέλεια σχεδιασμένες διεργασίες μιας επιχείρησης μπορούν να οδηγήσουν σε διαφορετικά από τα αναμενόμενα αποτελέσματα. Απάρνηση συναλλαγής μπορεί να συμβεί και σε συστήματα που δε συμμετέχουν agents ή σε πραγματικές συναλλαγές μέσα σε κάποιο οργανισμό. Πολλές φορές, έγγραφα χάνονται, πλαστογραφούνται ή αλλοιώνονται. Αφού ένας agent μπορεί να απαρνηθεί μια συναλλαγή επικαλούμενος κάποια παρεξήγηση, είναι σημαντικό οι agents και οι πλατφόρμες agent που εμπλέκονται σε συναλλαγές να διατηρούν ιστορικά στοιχεία ώστε να επιλύσουν τέτοιες μελλοντικές διαφωνίες.

2.2.2.3.4.Μη εξουσιοδοτημένη Πρόσβαση (Unauthorized Access)

Αν μια πλατφόρμα agent έχει αδύναμους ή ανύπαρκτους μηχανισμούς άμυνας, ένας agent μπορεί άμεσα να επέμβει με κάποιον άλλο agent επικαλώντας δημόσιες λειτουργίες ή αποκτώντας πρόσβαση και τροποποιώντας δεδομένα και κώδικα του agent. Αλλαγή του κώδικα ενός agent είναι μια εξαιρετικά ύπουλη μορφή επίθεσης αφού μπορεί να τροποποιήσει ριζικά τη συμπεριφορά του agent (π.χ να μετατρέψει έναν 'έμπιστο' agent σε κακόβουλο κ.α). Ένας agent μπορεί επίσης να αποκτήσει πληροφορίες για τις δραστηριότητες άλλων agents χρησιμοποιώντας τις υπηρεσίες μιας πλατφόρμας για να υποκλέψει την επικοινωνία τους.

2.2.2.4 Επίθεση άλλων οντοτήτων σε πλατφόρμες agent

Στη συγκεκριμένη κατηγορία ανήκουν οι επιθέσεις κατά τις οποίες εξωτερικές οντότητες συμπεριλαμβανομένων και των agents και τις πλατφόρμες τους απειλούν την ασφάλεια μιας πλατφόρμας

- Masquerading
- Άρνηση Υπηρεσίας
- Μη εξουσιοδοτημένη Πρόσβαση
- Αντιγραφή και Αναπαραγωγή

2.2.2.4.1 Masquerade

Οι agents μπορούν να αιτηθούν τις υπηρεσίες μιας πλατφόρμας τόσο από απόσταση όσο και τοπικά. Ένας agent σε μια απομακρυσμένη πλατφόρμα μπορεί να μεταμφιεστεί ως κάποιος άλλος agent και να αιτηθεί υπηρεσίες και πόρους τους οποίος δεν δικαιούται και δεν είναι εξουσιοδοτημένος να έχει . Μεταμφιεσμένοι agents μπορούν να ενεργούν σε συνδυασμό με κάποια κακόβουλη πλατφόρμα για να παραπλανήσουν κάποια άλλη απομακρυσμένη πλατφόρμα

ή και μόνοι τους. Μια απομακρυσμένη πλατφόρμα μπορεί επίσης να μεταμφιεστεί και να εμφανίζεται σαν κάποια άλλη πλατφόρμα και να παραπλανεί άλλες πλατφόρμας ή και agents

2.2.2.4.2 Μη εξουσιοδοτημένη Πρόσβαση.

Απομακρυσμένοι χρήστες, διαδικασίες και agents μπορούν να αιτηθούν υπηρεσίες για τις οποίες δεν είναι εξουσιοδοτημένοι. Η απομακρυσμένη πρόσβαση σε μια πλατφόρμα και στον οικείο υπολογιστή από μόνη της πρέπει να είναι προσεκτικά προστατευμένη, αφού συμβατικά scripts επίθεσης που υπάρχουν δωρεάν στο διαδίκτυο μπορούν να χρησιμοποιηθούν για να καταστρατηγήσουν το λειτουργικό σύστημα και να αποκτήσουν κατευθείαν πρόσβαση σε όλες τις πηγές του συστήματος. Απομακρυσμένη διαχείριση των χαρακτηριστικών της πλατφόρμας και των πολιτικών ασφαλείας μπορεί να είναι επιθυμητή από κάποιον διαχειριστή που είναι υπεύθυνος για διασκορπισμένες πλατφόρμες , αλλά επιτρέποντας την απομακρυσμένη διαχείριση μπορεί να κάνει το σύστημα ευάλωτο σε επιθέσεις.

2.2.2.4.3 Άρνηση Υπηρεσίας.

Μια πλατφόρμα από agents μπορεί να είναι προσβάσιμη τόσο τοπικά όσο και απομακρυσμένα. Οι υπηρεσίες των agents που προσφέρονται από τη πλατφόρμα καθώς και οι ενδοπλατφορμικές επικοινωνίες μπορεί να επηρεαστούν από τις συνηθισμένες επιθέσεις άρνησης υπηρεσίας. Οι πλατφόρμες των agents είναι εκτεθειμένες σε όλες τις επιθέσεις άρνησης υπηρεσίας που είναι εκτεθειμένα τα λειτουργικά συστήματα και τα πρωτόκολλα επικοινωνίας. Αυτές οι επιθέσεις παρακολουθούνται από οργανισμούς όπως τον Computer Emergency Response Team (CERT) στο Carnegie Mellon University και τον Federal Computer Incident Response Capability (FedCIRC)

2.2.2.4.4 Αντιγραφή και Αναπαραγωγή

Κάθε φορά που κάποιος κινητός πράκτορας μετακινείται από μια πλατφόρμα σε κάποια άλλη μεγαλώνει τη πιθανότητα να εκτεθεί σε κάποιο κίνδυνοι ασφαλείας. Ένα μέρος που παρακολουθεί ένα agent , ή τα μηνύματα του κατά τη μετάδοση, μπορεί να αντιγράψει τον agent

ή το μήνυμα του και να κλωνοποιήσει τον agent ή να αναμεταδώσει το μήνυμα του. Εάν για παράδειγμα κάποιος κακόβουλος agent αντιγράψει ένα μήνυμα <<αγόρασε>> και το επαναλάβει αρκετές φορές, θα οδηγηθούμε στο αποτέλεσμα ο αρχικός agent να αγοράσει πολλαπλές φορές κάτι που τελικά ήθελε να το αγοράσει μόνο μια

2.3 Μέτρα ασφαλείας

Για την κατανίκηση των επιθέσεων κατά της ασφαλείας που αναλύθηκαν και την ικανοποίηση των προηγμένων απαιτήσεων ασφαλείας των συστημάτων κινητών πρακτόρων, εφαρμόζεται ένα σύνολο διαφορετικών μέτρων ασφαλείας. Τα μέτρα αυτά βασίζονται είτε σε συμβατικές τεχνικές ασφαλείας που χρησιμοποιούνται στις εφαρμογές των τρεχουσών διανομών (με τις απαραίτητες βελτιώσεις για την εφαρμογή τους σε συστήματα κινητών πρακτόρων), είτε σε ειδικά επινοημένες τεχνικές για τον έλεγχο κινητού κώδικα και εκτελέσιμων περιεχομένων (π.χ. Java applets). Ακολούθως, τα μέτρα ασφαλείας που έχουν αναπτυχθεί με σκοπό την προστασία των συστημάτων κινητών πρακτόρων παρουσιάζονται και αξιολογούνται εν συντομία

Τα εν λόγω μέτρα ασφαλείας ταξινομούνται σε δύο κατηγορίες:

- σε αυτά που εστιάζουν σε πλατφόρμες πρακτόρων και
- σε εκείνα που εστιάζουν σε κινητούς πράκτορες.

2.3.1 Πλατφόρμες πρακτόρων

Μια από τις κυρίες ανησυχίες κατά τη κατασκευή ενός συστήματος agent είναι να μπορέσει να σιγουρέψει ότι ο agent δε θα βρεθεί σε σύγκρουση με κάποιον άλλο agent ή με τη πλατφόρμα που το φιλοξενεί. Μια συνηθισμένη λύση στο συγκεκριμένο πρόβλημα είναι η δημιουργία χωριστών απομονωμένων τομέων για κάθε agent και πλατφόρμα και έλεγχο αυτών με πρόσβαση μέσα στο τομέα Γενικότερα η έννοια αυτή αναφέρεται ως μια εφαρμογή αναφοράς θέσης (monitoring). Μια εφαρμογή αναφοράς θέσης έχει τα ακόλουθα χαρακτηριστικά:

- Καλείται πάντα και δεν μπορεί να παραληφθεί, διευθετώντας όλες τις προσβάσεις
- Είναι απαραβίαστη

- Είναι αρκετά μικρή ώστε να μπορεί να αναλυθεί και να δοκιμαστεί

Εφαρμογές του μοντέλου αναφοράς θέσης υπάρχουν από τις αρχές της δεκαετίας του 1980 , χρησιμοποιώντας ένα μεγάλο αριθμό των συμβατικών τεχνικών ασφάλειας που μπορούν να βρουν χρήση και στα περιβάλλοντα κινητών πρακτόρων. Μερικές τεχνικές περιλαμβάνουν τα παρακάτω:

- Μηχανισμούς για να απομονώσουν τη μια διεργασία από την άλλη και από τις διαδικασίες ελέγχου
- Μηχανισμοί που ελέγχουν τη πρόσβαση στις υπολογιστικές διεργασίες
- Κρυπτογραφικούς μεθόδους που κρυπτογραφούν τις συναλλασσόμενες πληροφορίες
- Κρυπτογραφικές μεθόδους για να αναγνωρίσουν και να αυθεντικοποιήσουν χρήστες, agents, πλατφόρμες
- Μηχανισμούς για να ελέγχουν τα γεγονότα που είναι σχετικά με την ασφάλεια και συμβαίνουν στη πλατφόρμα

Οι πιο πρόσφατες τεχνικές που αποσκοπούν στην ασφάλεια του κινητού κώδικα και των κινητών πρακτόρων έχουν εξελιχθεί σύμφωνα με αυτές τις παραδοσιακές γραμμές. Τεχνολογίες που αποσκοπούν να προστατέψουν τις πλατφόρμες agent περιλαμβάνουν τα παρακάτω:

- Απομόνωση κρίσιμων δεδομένων
- Ασφάλιση κινητού κώδικα
- Υπογεγραμμένο κώδικα
- Πιστοποιητικά δικαιωμάτων και ιδιοτήτων
- Αξιολόγηση Κατάστασης
- Ιστορικό διαδρομών
- Proof Carrying Code.

Η εν λόγω ενότητα παρουσιάζει τα μέτρα ασφαλείας που προστατεύουν τις πλατφόρμες πρακτόρων, αναλύοντας κάθε ένα από τα παραπάνω. Η παρουσίαση γίνεται από δυο διαφορετικές προσεγγίσεις:

- Απομόνωση των κρίσιμων δεδομένων.
- Ασφάλιση κινητού κώδικα.

2.3.1.1 Απομόνωση των κρίσιμων δεδομένων.

Η προσέγγιση απομόνωσης των κρίσιμων δεδομένων απομονώνει τη μνήμη και περιορίζει την προσπέλαση σε αυτή, προκειμένου να διατηρεί αποκλειστικά περιβάλλοντα εκτέλεσης. Οι πιο γνωστές τεχνικές που χρησιμοποιούν αυτήν την προσέγγιση είναι η Λογισμική Απομόνωση Σφαλμάτων (Software-Based Fault Isolation) και η Ασφαλής Διερμήνευση Κώδικα (Safe Code Interpretation), που ακολουθούν το μοντέλο ασφαλείας της Java, το επονομαζόμενο αμμοδοχείο (sandbox).

Η Λογισμική Απομόνωση Σφαλμάτων, όπως υποδηλώνει και η ονομασία, συνιστά ένα μέτρο που απομονώνει τα δομοστοιχεία της εφαρμογής σε διακριτούς τομείς σφαλμάτων. Χρησιμοποιεί μία τεχνική λογισμικού που ονομάζεται sandboxing, η οποία διασφαλίζει την εκτέλεση μη έμπιστων δομοστοιχειών κώδικα και μη ασφαλών εντολών σε περιοχές σφαλμάτων με εικονικές διευθύνσεις. Για να επιτευχθεί αυτό, τροποποιεί λογισμικό στο επίπεδο των εντολών αποτρέποντας την πρόσβαση στους κρίσιμους πόρους του συστήματος (π.χ. μνήμη) εκτός του sandbox. Η πρόσβαση σε αυτό ελέγχεται μέσω ενός μοναδικού αναγνωριστικού συνδεόμενου με τον κάθε τομέα. Αναφορικά με την ταξινόμηση των εντολών (π.χ. σε ασφαλείς και μη-ασφαλείς), οι Wahbe et. al θεωρούν τις εντολές εγγραφής και άλματος (write and jump) ως μη-ασφαλείς. Οι Small and Seltzer θεωρούν επίσης την εντολή ανάγνωσης (read) ως μη-ασφαλή, αφού ορισμένες συσκευές αλλάζουν κατάσταση όταν πραγματοποιούν ανάγνωση. Τέλος, εντολές όπως η επαναφορά (reset), οι οποίες τροποποιούν τα προνόμια προσπέλασης της μνήμης και απενεργοποιούν τις διακοπές (interrupts), πρέπει να απαγορεύονται.

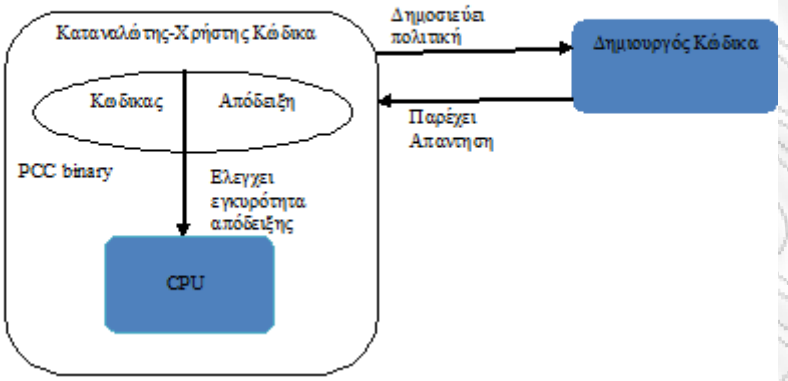
Ενώ η κεντρική ιδέα της τεχνικής της Ασφαλούς Διερμήνευσης Κώδικα έχει να κάνει με την ασφαλή εκτέλεση εντολών. Ειδικά μέτρα ασφαλείας εφαρμόζονται προκειμένου οι επιβλαβείς εντολές να μετατρέπονται σε ασφαλείς, διαφορετικά οι εντολές δεν επιτρέπεται να χρησιμοποιηθούν από τους πράκτορες. Τα εφαρμοζόμενα μέτρα ασφαλείας είναι είτε στατικά είτε δυναμικά. Ο έλεγχος στατικού τύπου υπό τη μορφή επαλήθευσης ενδιάμεσου κώδικα (bytecode) χρησιμοποιείται για τον έλεγχο συνθηκών, όπως η ορθότητα τύπου, η απουσία υπερ- ή υποχείλισης στοίβας, ο κώδικας περιορισμού, η αρχικοποίηση μητρώου, η αρχικοποίηση αντικειμένου, κλπ. Η στατική ανάλυση του ενδιάμεσου κώδικα κατά το χρόνο φόρτωσης εξασφαλίζει την ασφάλεια του λαμβανόμενου κώδικα. Από την άλλη πλευρά, ένας άλλος τρόπος εξασφάλισης των συγκεκριμένων συνθηκών είναι ο δυναμικός έλεγχος τους (π.χ. δοκιμές ορίων πίνακα), κατά την εκτέλεση του ενδιάμεσου κώδικα. Όμως, ο έλεγχος των συνθηκών κατά το χρόνο εκτέλεσης μπορεί να συνεπάγεται μεγάλο κόστος και επιβραδύνει σημαντικά την εκτέλεση.

2.3.1.2 Ασφάλιση κινητού κώδικα

Η δεύτερη προσέγγιση προστατεύει τις πλατφόρμες πρακτόρων ασφαλίζοντας τον κώδικα των κινητών πρακτόρων που τις επισκέπτονται. Περιλαμβάνει μέτρα που διασφαλίζει την αυθεντικότητα του κινητού κωδικού και των πρακτόρων, την ύπαρξη των κατάλληλων ιδιοτήτων ασφαλείας σε κινητούς πράκτορες, τον εντοπισμό οποιωνδήποτε κακόβουλων τροποποιήσεων έχουν πραγματοποιηθεί από μη έμπιστη πλατφόρμα στον κινητό πράκτορα και την εγγραφή του ιστορικού του πράκτορα.

Η αυθεντικότητα του κινητού κώδικα και των πρακτόρων επιτυγχάνεται με χρήση υπογραφής κώδικα (code signing), η οποία προϋποθέτει κρυπτογραφία δημόσιου κλειδιού (public key) και παρέχει ψηφιακές υπογραφές. Μία ψηφιακή υπογραφή χρησιμεύει ως μέσο επιβεβαίωσης της αυθεντικότητας ενός πράκτορα, της προέλευσης και της ακεραιότητας του . Επιτρέπει στην πλατφόρμα να εξακριβώσει ότι ο κώδικας δεν έχει τροποποιηθεί από την στιγμή υπογραφής του πράκτορα από το δημιουργό ή τον χρήστη (η υπογραφή από το χρήστη δηλώνει την αρχή υπό την οποία λειτουργεί ο πράκτορας). Επίσης επιτρέπει την ταυτοποίηση της υπογράφουσας οντότητας, αλλά δεν παρέχει εγγυήσεις ως προς την αξιοπιστία της. Για να το επιτύχει αυτό, κάθε πλατφόρμα που εκτελεί κινητό κώδικα πρέπει να τηρεί μία λίστα έμπιστων οντοτήτων. Εάν η υπογράφουσα οντότητα περιλαμβάνεται στη λίστα, θεωρείται πως είναι αξιόπιστη και ότι ο κώδικας της είναι ασφαλής. Σε αυτή την περίπτωση, στον κινητό κώδικα παρέχονται πλήρη προνόμια, ενώ στην αντίθετη περίπτωση ο κινητός κώδικας δε θα εκτελεστεί (π.χ. πολιτική ασφαλείας "black-and-white").

Η ύπαρξη κατάλληλων ιδιοτήτων ασφαλείας σε κινητούς πράκτορες διασφαλίζεται από τον Proof Carrying Code (PCC) . Το μέτρο αυτό υποχρεώνει τον κατασκευαστή ενός κινητού κώδικα (π.χ. το δημιουργό ενός πράκτορα) να αποδείξει τυπικά ότι το πρόγραμμα, που έχει γραφεί σε μία αυστηρού τύπου (type-safe) γλώσσα προγραμματισμού (π.χ. Java, C) διαθέτει τις απαιτούμενες ιδιότητες ασφαλείας όπως έχουν προηγουμένως ορισθεί από μία πλατφόρμα πράκτορα. Η πλατφόρμα ορίζει μία συγκεκριμένη πολιτική ασφαλείας που περιέχει τούς όρους, υπό τους οποίους η εκτέλεση ενός ξένου προγράμματος θεωρείται ασφαλής. Βασιζόμενος σε αυτή την πολιτική, ο δημιουργός κατασκευάζει μία απόδειξη ασφαλείας (εικόνα 12) από το μικρότερο δυνατό σύνολο αξιωμάτων και κανόνων συμπερασμάτων, με τέτοιο τρόπο ώστε να καθιστά εύκολη την ταυτοποίηση της χωρίς χρήση κρυπτογραφικών τεχνικών ή εξωτερικής βοήθειας. Ο κινητός κώδικας και η τυπική απόδειξη ασφαλείας συγκροτούν το PCC binary, που αποστέλλεται στην πλατφόρμα πρακτόρων, όπου η ύπαρξη ιδιοτήτων ασφαλείας μπορεί εύκολα να εξακριβωθεί.



Εικόνα 12: Proof Carrying Code (PCC)

Με την λήψη του κινητού κώδικα, ένα κατηγόρημα ασφαλείας το οποίο αντιπροσωπεύει τη σημασιολογία του προγράμματος, δημιουργείται απευθείας από τον πηγαίο κώδικα χρησιμοποιώντας μία κατηγορηματική λογική πρώτης τάξης. Αυτό διασφαλίζει ότι η συνοδεύουσα απόδειξη στην πραγματικότητα δεν αντιστοιχεί στον κώδικα (π.χ. πιστοποίηση κώδικα). Μετά, η πλατφόρμα πρακτόρων (δηλαδή ο καταναλωτής του κώδικα) χρησιμοποιεί έναν γρήγορο ελεγκτή-επαληθευτή εγκυρότητας απόδειξης (proof validator-checker), ο οποίος διενεργεί ελέγχους τύπου και ελέγχους της εγκυρότητας της απόδειξης ασφαλείας του εισερχόμενου κώδικα. Οποιαδήποτε προσπάθεια επέμβασης στον κώδικα ή στην απόδειξη ασφαλείας έχει ως συνέπεια ένα σφάλμα ελέγχου εγκυρότητας και την απόρριψη του κώδικα. Εάν ο έλεγχος εγκυρότητας είναι επιτυχής, ο κώδικας θεωρείται ασφαλής και εκτελείται χωρίς κανέναν περαιτέρω έλεγχο .

Όταν οι κινητοί πράκτορες περιπλανώνται σε πλατφόρμες, μεταφέρουν στατικά δεδομένα, συλλεγμένα δεδομένα και κατάσταση εκτέλεσης. Τα τελευταία είναι δυναμικά δεδομένα (π.χ. μετρητές προγραμμάτων, καταλόγους, κλπ.) που έχουν δημιουργηθεί και τροποποιηθεί κατά την εκτέλεση ενός πράκτορα σε μία πλατφόρμα, και έχουν χρησιμοποιηθεί ως εισροή στους υπολογισμούς που εκτελούνται στην επόμενη πλατφόρμα που επισκέπτεται ο πράκτορας. Ένα μέτρο ασφαλείας που προστατεύει μία πλατφόρμα πρακτόρων και εστιάζει στην κατάσταση εκτέλεσης των πρακτόρων που την επισκέπτονται ονομάζεται αξιολόγηση κατάστασης (state appraisal). Το μέτρο αυτό διασφαλίζει πως ο πράκτορας δεν έχει καταστεί κακόβουλος ή τροποποιηθεί ως επακόλουθο αλλαγών της κατάστασης του σε μία μη έμπιστη πλατφόρμα . Η επιτυχία του εν λόγω μέτρου εξαρτάται από το βαθμό στον οποίο είναι δυνατή η πρόβλεψη τέτοιων επιβλαβών τροποποιήσεων της κατάστασης του πράκτορα και η προετοιμασία αντιμέτρων υπό τη μορφή λειτουργιών αξιολόγησης, πριν ο πράκτορας χρησιμοποιηθεί.

Η οντότητα που δημιουργεί έναν κινητό πράκτορα παράγει μία λειτουργία αξιολόγησης της κατάστασης, η οποία υπολογίζει το μέγιστο σύνολο προνομίων, τα οποία ένας πράκτορας θα μπορούσε να ζητήσει από μία πλατφόρμα κεντρικού συστήματος. Τα εν λόγω προνόμια εξαρτώνται από την τρέχουσα κατάσταση του πράκτορα, που χαρακτηρίζεται από υπό συνθήκη συντελεστές και σταθερές κατάστασης. Οι κακόβουλες καταστάσεις ορίζονται μέσω αυθαίρετα πολύπλοκων σχέσεων μεταξύ δυναμικών μεταβλητών κατάστασης του πράκτορα. Η συνάρτηση αξιολόγησης της κατάστασης συνιστά στην πραγματικότητα ένα σύνολο συνθηκών που πρέπει να ικανοποιούνται μετά από μία σύνοδο εκτέλεσης. Επιπλέον, μπορεί να περιλαμβάνει κάποιες σταθερές κατάστασης. Βασιζόμενη σε προκαθορισμένους, υπό συνθήκη συντελεστές και στο εάν οι διαπιστωθείσες σταθερές κατάστασης τηρούνται, η συνάρτηση αξιολόγησης χρησιμοποιείται για τον καθορισμό των προνομιών που θα παραχωρηθούν στο πράκτορα.

Όπως και ο δημιουργός, έτσι και ο χρήστης, ο οποίος αποστέλλει τον πράκτορα να ενεργήσει για λογαριασμό του, παράγει μία άλλη συνάρτηση αξιολόγησης κατάστασης η οποία εξαρτάται από την τρέχουσα κατάσταση του πράκτορα και των ενεργειών προς εκτέλεση. Ο χρήστης δημιουργεί πακέτο του κινητού κώδικα με τις παρεχόμενες συναρτήσεις αξιολόγησης κατάστασης και το στέλνει στην πλατφόρμα πρακτόρων - προορισμό. Με την λήψη του, η πλατφόρμα αρχίζει τη διαδικασία ελέγχου εγκυρότητας. Ανάλογα με τα αποτελέσματα του ελέγχου εγκυρότητας, η πλατφόρμα ορίζει τα προνόμια που θα παραχωρήσει στο πράκτορα. Σε περίπτωση παραβίασης μιας σταθεράς από τον πράκτορα, αυτός μπορεί να γίνει δεκτός χωρίς προνόμια. Από την άλλη πλευρά, εάν ο πράκτορας αποτύχει να ικανοποιήσει ορισμένους υπό συνθήκη συντελεστές, μπορεί να γίνει δεκτός με περιορισμένο σύνολο προνομίων.

Τέλος, το χαρακτηριστικό ασφαλείας του ιστορικού διαδρομής (path history) τηρεί για κάθε πράκτορα ένα αρχείο πιστοποιήσιμης αυθεντικότητας για τις πλατφόρμες που επισκέφθηκε προηγουμένως. Χρησιμοποιώντας αυτό το αρχείο, η επόμενη πλατφόρμα μπορεί να ορίσει εάν θα επεξεργαστεί έναν πράκτορα και ποιο επίπεδο εμπιστοσύνης, υπηρεσιών, πόρων και προνομίων πρέπει να του παραχωρήσει. Αυτά τα επίπεδα υπολογίζονται με απλή εξέταση της λίστας οντοτήτων που παρέχει το ιστορικό διαδρομής ή μέσω της επιμέρους πιστοποίησης αυθεντικότητας των υπογραφών σε κάθε περιεχόμενη εγγραφή. Η καταγραφή του ιστορικού διαδρομής απαιτεί την προσθήκη μίας υπογεγραμμένης εγγραφής από κάθε πλατφόρμα στο σχετικό αρχείο του πράκτορα που την επισκέπτεται, στην οποία δηλώνεται η ταυτότητα του και η ταυτότητα της επόμενης πλατφόρμας που πρόκειται να επισκεφθεί. Για την αποτροπή επεμβάσεων, η υπογραφή κάθε νέας εγγραφής ιστορικού διαδρομής περιλαμβάνει μία σύνοψη των προηγούμενων . Η υπογράφουσα πλατφόρμα στέλνει τον κινητό πράκτορα συνοδευόμενο με το πλήρες ιστορικό διαδρομής στην επόμενη πλατφόρμα. Αυτή μπορεί να αποφανθεί εάν θα

εκτελέσει το πράκτορα και τι προνόμια θα του παραχωρήσει, ανάλογα με τις πληροφορίες που περιέχονται στο ιστορικό διαδρομής.

Μια βασική τεχνική για προστασία ενός συστήματος agent είναι η σήμανση του κώδικα ή άλλων συστατικών με ψηφιακή υπογραφή. Μία ψηφιακή υπογραφή δρα ως τρόπος επιβεβαίωσης της αυθεντικότητας, καταγωγής και ακεραιότητας ενός αντικειμένου. Τυπικά, ο υπογράφον είναι και ο δημιουργός του agent, ο χρήστης του ή κάποια οντότητα που έχει επανεξετάσει τον agent. Επειδή ο agent λειτουργεί για λογαριασμό κάποιο τελικού χρήστη ή οργανισμού , τα συστήματα κινητών agents συνήθως χρησιμοποιούν την υπογραφή του χρήστη σαν αναγνωριστικό της προσωπικότητας για την οποία ο agent ενεργεί.

Η υπογραφή κώδικα περιλαμβάνει κρυπτογραφία δημόσιου κλειδιού που βασίζεται σε ένα ζευγάρι κλειδιών που είναι συναφή με κάποια οντότητα. Το ένα κλειδί κρατείται μυστικό από την οντότητα, ενώ το άλλο είναι δημόσια διαθέσιμο. Η διαδικασία της ηλεκτρονικής υπογραφής ωφελείτε από την διαθεσιμότητα των δομών του δημοσίου κλειδιού, αφού η πιστοποίηση περιλαμβάνει τη ταυτότητα της οντότητας και το δημόσιο κλειδί , μπορεί εύκολα να διαβαστεί και να αναγνωριστεί. Περνώντας το κώδικα του agent από μια μη αναστρέψιμη διαδικασία hash, που υποστηρίζει αποτύπωμα ή ένα μοναδικό μήνυμα ψηφίων από το κώδικα και μετά κρυπτογραφηθούν τα αποτελέσματα με το ιδιωτικό κλειδί του υπογράφοντος δημιουργείται μια ψηφιακή υπογραφή. Επειδή το μήνυμα με τα ψηφία του κώδικα είναι μοναδικό, η υπογραφή που επιστέφεται αποτελεί έναν ολοκληρωμένο μηχανισμό.

Ο κώδικας του agent, η υπογραφή και το δημόσιο κλειδί πιστοποίησης μπορούν να προωθηθούν σε κάποιον παραλήπτη, που μπορεί εύκολα να αναγνωρίσει τη πηγή και να αυθεντικοποιήσει το κώδικα. Θα πρέπει να σημειωθεί ότι η έννοια της κάθε υπογραφής μπορεί να είναι διαφορετική και εξαρτάται από τις πολιτικές που είναι συνδεδεμένες από το σχήμα της υπογραφής και το μέρος που δίνει την υπογραφή. Για παράδειγμα, ο συγγραφές του agent, είτε μια προσωπικότητα ή ένας οργανισμός μπορεί να χρησιμοποιήσει μια ψηφιακή υπογραφή για να δηλώσει το δημιουργό του κώδικα, όχι όμως και να πιστοποιήσει ότι ο κώδικας δουλεύει χωρίς λάθη.

Η αυθεντικοποίηση της Microsoft, μια κοινή μορφή για υπογραφή κώδικα, ενεργοποιεί τα Java applets ή τα Active X Controls να είναι υπογεγραμμένα, πιστοποιώντας στους χρήστες ότι το πρόγραμμα δεν έχει τροποποιηθεί και ότι η ταυτότητα του συγγραφέα είναι αναγνωρίσιμη. Για πολλούς χρήστες, ακόμα η υπογραφή έχει περάσει από τα όρια της γνησιότητας, επηρεάζοντας τον βαθμό εμπιστοσύνης στο λογισμικό κάτι το ποίο θα μπορούσε να είχε καταστρεπτικές συνέπειες. Αντί να στηρίζεται αποκλειστικά και μόνο για τη φήμη ενός παραγωγού κώδικα, θα ήταν φρόνιμο να έχουν μια ανεξάρτητη εξέταση και επαλήθευση του κώδικα που εκτελούν από έναν αξιόπιστο συμβαλλόμενο μέρος ή από κάποια υπηρεσία βαθμολογίας. Για παράδειγμα, η

απόφαση για την εκτέλεση ενός πράκτορα θα μπορούσε να ληθφεί μόνο μετά από έγκριση κάποιου διαχειριστή ασφαλείας , δίνοντας μια μορφή ψηφιακής υπογραφής στο κώδικα. Αν και μια τέτοια προσέγγιση μπορεί να είναι επιθυμητή, εμπειρία με αξιόπιστες περιπτώσεις δείχνει ότι η απόκτηση ασφαλών συνθήκες ποιότητας έγκαιρα είναι δύσκολο να επιτευχθεί. Πάραυτα ακόμα και αυτός ο έλεγχος είναι καλύτερος από την μη ύπαρξη ελεγχού

Μια άλλη τεχνική είναι η αξιολόγηση κατάστασης. Ο στόχος της αξιολόγησης κατάστασης είναι να εξασφαλίσει ότι ο agent δεν έχει κάπου αλλοιωθεί, λόγω τον αλλαγών στη κατάσταση του. Η επιτυχία αυτής της τεχνικής βασίζεται στο ότι επιβλαβείς αλλαγές στην κατάσταση ενός agent μπορούν να προβλεφθούν, και χρησιμοποιώντας τα αντιμετρά λειτουργιών αξιολόγησης μπορούν να προετοιμαστούν πριν γίνει χρήση του agent

Λειτουργίες αξιολόγησης χρησιμοποιούνται για να καθοριστούν τα δικαιώματα που θα έχει ο agent, τα οποία βασίζονται τόσο σε εξαρτημένους παράγοντες όσο και στη κατάσταση στην οποία βρίσκεται ο agent. Για παράδειγμα εάν η κατάσταση ενός agent είναι παραβιασμένη, τότε δεν θα του δοθεί κανένα δικαίωμα, ενώ κάποιος agent που η κατάσταση του αποτυγχάνει σε κάποιο εξαρτημένο παράγοντα, θα του δοθούν περιορισμένα δικαιώματα

Τόσο ο δημιουργός, όσο και ο ιδιοκτήτης ενός πράκτορα παράγουν λειτουργίες αξιολόγησης που γίνονται ένα μέρος του κώδικα του agent. Ο ιδιοκτήτης συνήθως εφαρμόζει περιορισμούς στη κατάσταση με σκοπό να μειώσει την ευθύνη και να ελέγξει το κόστος. Όταν ένας agent διαθέτει υπογραφή από τον ιδιοκτήτη και το συγγραφέα του , τα ειδικά του χαρακτηριστικά προστατεύονται από ανιχνεύσιμες τροποποιήσεις

Μια πλατφόρμα agent χρησιμοποίει αυτές τις λειτουργίες για να επαληθεύσει τη σωστή κατάσταση του εισερχόμενου agent και να ορίσει τα δικαιώματα που θα παραχωρήσει στον agent κατά την εκτέλεση του. Τα δικαιώματα εκδίδονται από μια πλατφόρμα βάση των αποτελεσμάτων των λειτουργιών αξιολόγησης και των πολιτικών ασφαλείας της πλατφόρμας.

2.4 Κινητοί πράκτορες

Σύμφωνα με τα όσα παρουσιάστηκαν, τα μέτρα ασφαλείας που κατευθύνονται προς την προστασία των πλατφόρμων πρακτόρων εστιάζουν στην ενεργή πρόληψη, στο μέτρο που οι κινητοί πράκτορες είναι εντελώς εκτεθειμένοι σε μία πλατφόρμα πρακτόρων. Από την άλλη πλευρά, τα μέτρα ασφαλείας που κατευθύνονται προς την προστασία των πρακτόρων εστιάζουν περισσότερο στην ανίχνευση, αφού ένας πράκτορας δεν μπορεί να αποτρέψει την εμφάνιση κακόβουλων συμπεριφορών, αλλά μπορεί να τις εντοπίσει.

Το πρόβλημα αυτό απορρέει από την αδυναμία να επεκταθεί το ασφαλές περιβάλλον της οικείας πλατφόρμας στις άλλες πλατφόρμες. Όταν ένας χρήστης υπογράφει ηλεκτρονικά έναν agent στην οικεία του πλατφόρμα πριν μετακινηθεί σε μία δεύτερη πλατφόρμα , η προστασία είναι περιορισμένη. Η δεύτερη πλατφόρμα που λαμβάνει τον agent μπορεί να επικαλεστεί την υπογραφή για να επαληθεύσει την ακεραιότητα του κώδικα, τη πληροφορία της κατάστασης και τα δεδομένα, υπό τη προϋπόθεση ότι το ιδιωτικό κλειδί του χρήστη δεν έχει παραβιαστεί.
Στα επόμενα βήματα του agent σε μια τρίτη πλατφόρμα, η αρχική υπογραφή από τη πρώτη πλατφόρμα, παραμένει έγκυρη για τον αρχικό κώδικα, τα δεδομένα και τις πληροφορίες κατάστασης, όχι όμως για οποιαδήποτε δεδομένα ή καταστάσεις έχουν προκύψουν από τη δεύτερη πλατφόρμα. Για μερικές εφαρμογές, αυτή η ελάχιστη ασφάλεια μπορεί να είναι επαρκής. Για παράδειγμα agents που δεν συσσωρεύουν τη κατάστασή τους ή μεταδίδουν αμέσως τα δεδομένα τους στην οικεία πλατφόρμα , έχουν μικρότερο κίνδυνο από τέτοιες επιθέσεις. Σε άλλες εφαρμογές, χρειάζεται κάποιο απλό σχήμα όπως για παράδειγμα σε ένα σύστημα Jumping Beans agents, χρησιμοποιεί μια αρχιτεκτονική client-server , κατά την οποία ένας πράκτορας μόνιμα επιστρέφει σε έναν ασφαλή κεντρικό οικοδεσπότη πρώτα, πριν μετακινηθεί σε κάποια άλλη πλατφόρμα.

Τα συστήματα πρακτόρων που επιτρέπουν πιο αποκεντρωμένη κινητικότητα, όπως τα IBM Aglets, εμποδίζουν τη πλατφόρμα, να υποδεχθούν agents, από κάποια άλλη πλατφόρμα που δε συμπεριλαμβάνεται στις ασφαλής πλατφόρμες όπως ορίζει το πλαίσιο ασφαλείας της πλατφόρμας. Εναλλακτικά, ο εντολέας μπορεί να περιορίσει τη διαδρομή ενός πράκτορα σε μια μόνο αξιόπιστη σειρά από πλατφόρμες γνωστές εκ των προτέρων

Οι κυριότερες τεχνικές προστασίας είναι οι παρακάτω:

- Partial Result Encapsulation
- Mutual Itinerary Recording
- Itinerary Recording with Replication and Voting
- Execution Tracing
- Environmental Key Generation
- Computing with Encrypted Functions
- Obfuscated Code (Time Limited Blackbox)

Στη συνέχεια παρουσιάζονται τα πλέον γνωστά μέτρα ασφαλείας που έχουν σχεδιαστεί για την προστασία των πρακτόρων, τα οποία επίσης ακολουθούν δύο γενικές προσεγγίσεις:

- Απομόνωση κρίσιμων δεδομένων.
- Ανίχνευση επιθέσεων – εισβολών.

2.4.1 Απομόνωση κρίσιμων δεδομένων

Η προσέγγιση απομόνωσης κρίσιμων δεδομένων μπορεί επίσης να χρησιμοποιηθεί για μέτρα ασφαλείας συσκευής που έχουν σκοπό την προστασία των κινητών πρακτόρων. Η απομόνωση των δεδομένων εφαρμόζεται κυρίως στα αποτελέσματα των ενεργειών ενός πράκτορα ενθυλακώνοντας τα στην πλατφόρμα-οικοδεσπότη ή στον ίδιο τον πράκτορα. Η απομόνωση/ενθυλάκωση των δεδομένων διενεργείται για διαφορετικούς σκοπούς με χρήση διαφορετικών μηχανισμών:

- εμπιστευτικότητα με χρήση κρυπτογράφησης,
- ακεραιότητα και δυνατότητα απόδοσης ευθύνης (accountability) με χρήση ψηφιακών υπογραφών ή
- ιδιωτικότητα με χρήση άλλων κρυπτογραφικών πρωτογενών στοιχείων (primitives) όπως κωδικών πιστοποίησης αυθεντικότητας και λειτουργιών κατακερματισμού .

Ένα κινητός πράκτορας μπορεί να κρυπτογραφήσει τα αποτελέσματα των ενεργειών του χρησιμοποιώντας υποδομή δημόσιου κλειδιού. Συγκεκριμένα, χρησιμοποιεί το δημόσιο κλειδί του δημιουργού του (δηλ. της αρχικής πλατφόρμας προέλευσης του) για να παράγει με μικρά τμήματα ένα κρυπτογράφημα, που αποκρυπτογραφείται αργότερα στην οικεία πλατφόρμα του πράκτορα με τη χρήση του ιδιωτικού κλειδιού. Για την κρυπτογράφηση ο πράκτορας χρησιμοποιεί μία ειδική μέθοδο υλοποίησης που ονομάζεται ολισθαίνουσα κρυπτογράφηση (sliding encryption) και η οποία κρυπτογραφεί ένα μικρό αριθμό δεδομένων εντός ενός μεγαλύτερου μπλοκ, ολισθαίνοντας ένα μικρό κομμάτι. Αυτό το κομμάτι συνιστά το κρυπτογράφημα, που προέρχεται από την κατάσταση όπως αυτή επηρεάζεται από όλα τα προηγούμενα κρυπτογραφικά μπλοκ. Το συγκεκριμένο μέτρο ασφαλείας δεν αποτρέπει μεν την κακόβουλη συμπεριφορά, αλλά επιτρέπει την ανίχνευση ορισμένων τύπων παράνομων τροποποιήσεων και επεμβάσεων. Το κύριο πλεονέκτημα του συγκεκριμένου μέτρου έγκειται στη δυνατότητα εφαρμογής του ανεξάρτητα από τις δυνατότητες της πλατφόρμας πρακτόρων και της υποστηρικτής υποδομής.

Ένα άλλο μέτρο ασφαλείας που επιτρέπει σε έναν πράκτορα την ενθυλάκωση των αποτελεσμάτων των ενεργειών του ονομάζεται Κωδικοί Αυθεντικοποίησης Μερικών Αποτελεσμάτων (Partial Result Authentication Codes - PRAC) . Οι PRAC παρέχουν κρυπτογραφικά αθροίσματα ελέγχου (checksums δηλ. Message Authentication Codes - MACs) χρησιμοποιώντας συμμετρική κρυπτογραφία. Για κάθε πλατφόρμα που επισκέφθηκε, ο πράκτορας χρησιμοποιεί ένα μυστικό κλειδί (σχετιζόμενο με την πλατφόρμα-οικοδεσπότη) για να υπολογίσει έναν MAC βάσει των αποτελεσμάτων της εκτέλεσης του. Ο υπολογισμένος MAC και τα παρεχόμενα αποτελέσματα

συνιστούν τους PRAC, οι οποίοι αποστέλλονται στο δημιουργό του πράκτορα. Το χρησιμοποιούμενο για τον υπολογισμό του MAC κλειδί συμπεριλαμβάνεται σε μία λίστα μυστικών κλειδιών την οποία η αρχική πλατφόρμα προέλευσης παρέχει στον πράκτορα πριν τον αποστείλει. Μετά τον υπολογισμό του MAC, το χρησιμοποιούμενο κλειδί διαγράφεται από την λίστα των μυστικών κλειδιών διασφαλίζοντας την απώτερη ακεραιότητα των παρεχόμενων αποτελεσμάτων.

Η συμμετρική κρυπτογραφία χρησιμοποιείται επίσης στο χαρακτηριστικό περιβαλλοντική δημιουργία κλειδιού (environmental key generation), το οποίο επιτρέπει σε έναν πράκτορα να εκτελεί προκαθορισμένες ενέργειες εάν είναι αληθείς ορισμένες συνθήκες περιβάλλοντος . Συγκεκριμένα, το εν λόγω χαρακτηριστικό χρησιμοποιείται σε περιπτώσεις, στις οποίες μία πλατφόρμα (π.χ. οικοδεσπότη) θέλει να επικοινωνήσει με άλλη πλατφόρμα (π.χ. στόχο) εάν ικανοποιείται μία συνθήκη περιβάλλοντος (π.χ. ενεργοποίηση μίας συγκεκριμένης διεργασίας). Η επικοινωνία επιτυγχάνεται από έναν κινητό πράκτορα που φέρει κρυπτογραφημένες (χρησιμοποιώντας κρυπτογραφία μυστικού κλειδιού) πληροφορίες (δεδομένα ή/και τμήματα εκτελέσιμου κώδικα) και μία μέθοδος δημιουργεί το χρησιμοποιούμενο μυστικό κλειδί χρησιμοποιώντας παρατηρήσεις του περιβάλλοντος. Εάν η συνθήκη περιβάλλοντος ικανοποιείται, δημιουργείται το σχετικό μυστικό κλειδί και η προστατευμένη πληροφορία μπορεί να αποκρυπτογραφηθεί. Διαφορετικά, οι φερόμενες πληροφορίες παραμένουν προστατευμένες αφού η συνθήκη περιβάλλοντος είναι κρυμμένη χρησιμοποιώντας μία λειτουργία μονόδρομου κατακερματισμού (hash). Έτσι, το χαρακτηριστικό αυτό διασφαλίζει ότι η πλατφόρμα στόχος ή ένας μεμονωμένος παρατηρητής δεν μπορεί να έχει πρόσβαση στην ενεργοποιούσα συνθήκη και στις προστατευμένες πληροφορίες διαβάζοντας απευθείας τον κώδικα του πράκτορα.

Η απομόνωση των κρίσιμων δεδομένων με χρήση κρυπτογραφίας επίσης εφαρμόζεται στον Υπολογισμό με Λειτουργίες Κρυπτογράφησης (Computing with Encrypting Functions - CEF) . Το μέτρο αυτό επιτρέπει σε ένα μη έμπιστο σύστημα-οικοδεσπότη να εκτελέσει χρήσιμους υπολογισμούς, χωρίς να είναι σε θέση να εξακριβώσει την αρχική λειτουργία και συνεπώς να καταλάβει τι σημαίνουν οι υπολογισμοί. Για να το υλοποιήσει αυτό, ο CEF διακρίνει τις λειτουργίες και τα προγράμματα του τις υλοποιούν. Ένα πρόγραμμα αποτελείται από μη κρυπτογραφημένες εντολές τις οποίες ένας επεξεργαστής κατανοεί, χωρίς όμως να μπορεί να κατανοήσει την εκτελούμενη λειτουργία από αυτές τις εντολές. Με τη χρήση CEF, ένας κινητός πράκτορας μπορεί να εκτελείται σε ένα ενδεχομένως εχθρικό περιβάλλον, αλλά το σύστημα-οικοδεσπότης δεν μπορεί να κατανοήσει τις κρυπτογραφημένες λειτουργίες του πράκτορα. Συνεπώς, ο πράκτορας μπορεί να εκτελέσει ευαίσθητες ως προς την ασφάλεια λειτουργίες (όπως λειτουργίες υπογραφής), χωρίς τον κίνδυνο παραβίασης του από το σύστημα-οικοδεσπότη, το οποίο ίσως επιχειρήσει να κατασκοπεύσει τον κώδικα του πράκτορα κατά την εκτέλεση.

Τέλος, η *συσκότιση (obfuscation)* αποσκοπεί στην προστασία του κώδικα κινητών πρακτόρων από ενδεχόμενη ανάλυση και κατανόηση του από κακόβουλα συστήματα-οικοδεσπότη,

με χρήση αλγόριθμων περίπλεξης. Η βασική ιδέα πίσω από το συγκεκριμένο μέτρο είναι απλή: περιπλέκουν τον κώδικα κατά τέτοιο τρόπο που να είναι δύσκολο για τον οποιοδήποτε να καταλάβει πλήρως τη λειτουργία του προγράμματος ή να τροποποιήσει τον περιπλεγμένο κώδικα χωρίς να εντοπιστεί. Γενικά υπάρχει μία ποικιλία από μετασχηματισμούς συσκότισης: Συσκότιση Διάταξης, Συσκότιση Δεδομένων, Συσκότιση Ελέγχου κλπ. Ως προς την απόδοση των τεχνικών αυτών, η συσκότιση διάταξης και δεδομένων μειώνουν το μέγεθος του κώδικα επιταχύνοντας έτσι την ταχύτητα εκτέλεσης του, ενώ η συσκότιση ελέγχου έχει το αντίθετο αποτέλεσμα [22].

2.4.2 Ανίχνευση επιθέσεων

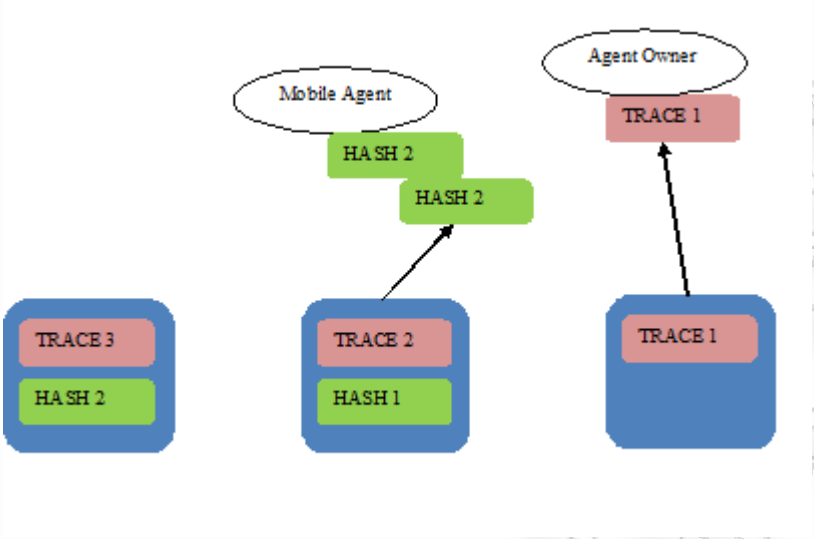
Μαζί με την προσέγγιση της απομόνωσης των κρίσιμων δεδομένων, για την προστασία κινητών πρακτόρων μπορεί επίσης να χρησιμοποιηθεί και η ανίχνευση επιθέσεων. Τα μέτρα ασφαλείας που ακολουθούν αυτή την προσέγγιση αναλύουν το ιστορικό των πρακτόρων προκειμένου να εντοπίσουν τα αποτελέσματα κακόβουλων ενεργειών, που έχουν πραγματοποιηθεί εναντίον των πρακτόρων. Στη συνέχεια, παρουσιάζονται και αναλύονται οι πλέον σημαντικές τεχνικές ανίχνευσης που μπορούν να εφαρμοστούν σε κινητούς πράκτορες.

Η τεχνική Αρχείου Αμοιβαίου Δρομολογίου (Mutual Itinerary Recording) οργανώνει τους πράκτορες σε ομάδες των δύο (δηλ. ομότιμοι), και για κάθε μία διατηρεί ένα αρχείο δρομολογίου. Οι ομότιμοι πράκτορες συνεργάζονται μεταξύ τους, ανταλλάσσουν πληροφορίες σχετικά με πλατφόρμες οικοδεσπότες και προβαίνουν στις δέουσες ενέργειες όταν καταγράφονται ασυνέπειες. Τα συστήματα-οικοδεσπότης ταξινομούνται σε κόκκινα, γκρι και λευκά σε συνάρτηση του εάν είναι κακόβουλα (κόκκινα), άγνωστα (ο πράκτορας δε διαθέτει επαρκείς πληροφορίες - γκρι) ή έμπιστα (λευκά). Όλες αυτές οι πληροφορίες συμπεριλαμβάνονται στα αρχεία δρομολογίου των πρακτόρων συγκροτώντας την αντίληψη τους για το κάθε σύστημα-οικοδεσπότη. Μετακινούμενος μεταξύ πλατφόρμων-οικοδεσπότη, ένα πράκτορας κομίζει πληροφορίες ως προς την τελευταία, την τρέχουσα και την επόμενη πλατφόρμα στον συνεργαζόμενο ομότιμο πράκτορα μέσω ενός αυθεντικοποιημένου καναλιού. Η λογική πίσω από αυτό το μέτρο ασφαλείας έγκειται στην υπόθεση ύπαρξης μικρού μόνον αριθμού κακόβουλων πλατφόρμων πρακτόρων, και ακόμα κι εάν ένας πράκτορας συναντήσει κάποια από αυτές, στη μικρή πιθανότητα συνεργασίας της πλατφόρμας με άλλη κακόβουλη πλατφόρμα την οποία έχει επισκεφθεί ο ομότιμος του πράκτορα. Ως εκ τούτου, διαμοιράζοντας τις λειτουργίες μίας εφαρμογής μεταξύ δύο πρακτόρων, είναι δυνατή η ανίχνευση της κακόβουλης συμπεριφοράς μίας πλατφόρμας πρακτόρων. Δίδεται προσοχή ώστε ο ένας πράκτορας να αποφεύγει πλατφόρμες τις οποίες έχει ήδη επισκεφθεί ο ομότιμος του.

Μία παραλλαγή της τεχνικής Mutual Itinerary Recording που υποστηρίζει δυνατότητες ανοχής σε σφάλματα είναι το Αρχείο Δρομολογίου με Αναπαραγωγή Πανομοιότυπων και

Ψηφοφορία (Itinerary Recording with Replication and Voting) . Με την εφαρμογή του συγκεκριμένου μέτρου, πολλαπλά πανομοιότυπα αντίγραφα του ίδιου πράκτορα εκτελούνται σε διαφορετικά συστήματα-οικοδεσπότη για την εκτέλεση του ίδιου υπολογισμού.. Το αποτέλεσμα που υπολογίζεται από την πλειοψηφία των συστημάτων-οικοδεσπότη γίνεται δεκτό ως το ορθό. Αυτό το μέτρο ασφαλείας χρησιμοποιείται βάσει της υπόθεσης, ότι η πλειοψηφία των συστημάτων-οικοδεσπότη δεν είναι κακόβουλα. Παρότι μία κακόβουλη πλατφόρμα μπορεί να καταστρέψει κάποια αντίγραφα του πράκτορα, ένας επαρκής αριθμός πανομοιότυπων διασφαλίζει την επιτυχή ολοκλήρωση του υπολογισμού. Συνεπώς, η εφαρμογή των δυνατοτήτων ανοχής σε σφάλματα επιτρέπει την αντιστάθμιση των συνεπειών από κακόβουλες πλατφόρμες. Για κάθε στάδιο υπολογισμού, η πλατφόρμα-οικοδεσπότης ελέγχει εάν τα συστήματα-οικοδεσπότης τα οποία ο πράκτορας επισκέφθηκε πριν είναι έμπιστα και διασφαλίζει ότι οι πράκτορες που καταφθάνουν είναι ανέπαφοι ελέγχοντας τα αρχεία δρομολογίου. Η πλατφόρμα-οικοδεσπότης συνεχίζει στο επόμενο στάδιο, μόνον εφόσον ένα υποσύνολο των πανομοιότυπων πρακτόρων θεωρηθεί έγκυρο. Επιπλέον, διαδίδουν μόνο το συγκεκριμένο υποσύνολο πανομοιότυπων πρακτόρων που βεβαιώνονται ως έγκυροι.

Η Ιχνηλάτηση Εκτέλεσης (Execution tracing) είναι ένα μέτρο ασφαλείας που εντοπίζει μη εξουσιοδοτημένες μετατροπές σε έναν πράκτορα χρησιμοποιώντας την πιστή καταγραφή της συμπεριφοράς του πράκτορα κατά την εκτέλεση του (δηλ. κώδικας πράκτορα, κατάσταση και ροή εκτέλεσης) σε κάθε πλατφόρμα πράκτορα. Το μέτρο αυτό απαιτεί τη δημιουργία και την τήρηση μη-αποποιήσιμου (non-repudiatable) ημερολογίου (log) ή ίχνους από κάθε εμπλεκόμενη πλατφόρμα-οικοδεσπότη, το οποίο περιλαμβάνει ακολουθία αναγνωριστικών ταυτότητας δηλώσεων, πληροφορίες της υπογραφής της πλατφόρμας όπως αναγνωριστικά ταυτότητας μηνύματος, ταυτότητα αποστολέα, χρονοσφραγίδα κλπ. Το τηρούμενο ημερολόγιο για ένα πράκτορα σχετίζεται με τις λειτουργίες που εκτελούνται από το διαχειριστή για όσο βρίσκεται σε ένα συγκεκριμένο σύστημα-οικοδεσπότη. Μετά την ολοκλήρωση της εκτέλεσης, το σύστημα-οικοδεσπότης δημιουργεί ένα αποτύπωμα κατακερματισμού (hash/fingerprint) του ημερολογίου εφαρμόζοντας μία κρυπτογραφική συνάρτηση κατακερματισμού, και το αποστέλλει στο έμπιστο μέρος ή στον κάτοχο του πράκτορα για έλεγχο της εγκυρότητας Το κατακερματισμένο ίχνος και η σχετιζόμενη ενδιάμεση κατάσταση υπογράφονται και προωθούνται στην επόμενη πλατφόρμα-οικοδεσπότη του δρομολογίου. Η υπογραφή της πλατφόρμας-οικοδεσπότη είναι απαραίτητη για οδηγίες που εξαρτώνται από τις διαδράσεις με το υπολογιστικό περιβάλλον που τηρείται στην πλατφόρμα. Από την άλλη πλευρά, η υπογραφή παραλείπεται σε περιπτώσεις που οι οδηγίες εξαρτώνται μόνον από τις τιμές των εσωτερικών μεταβλητών.

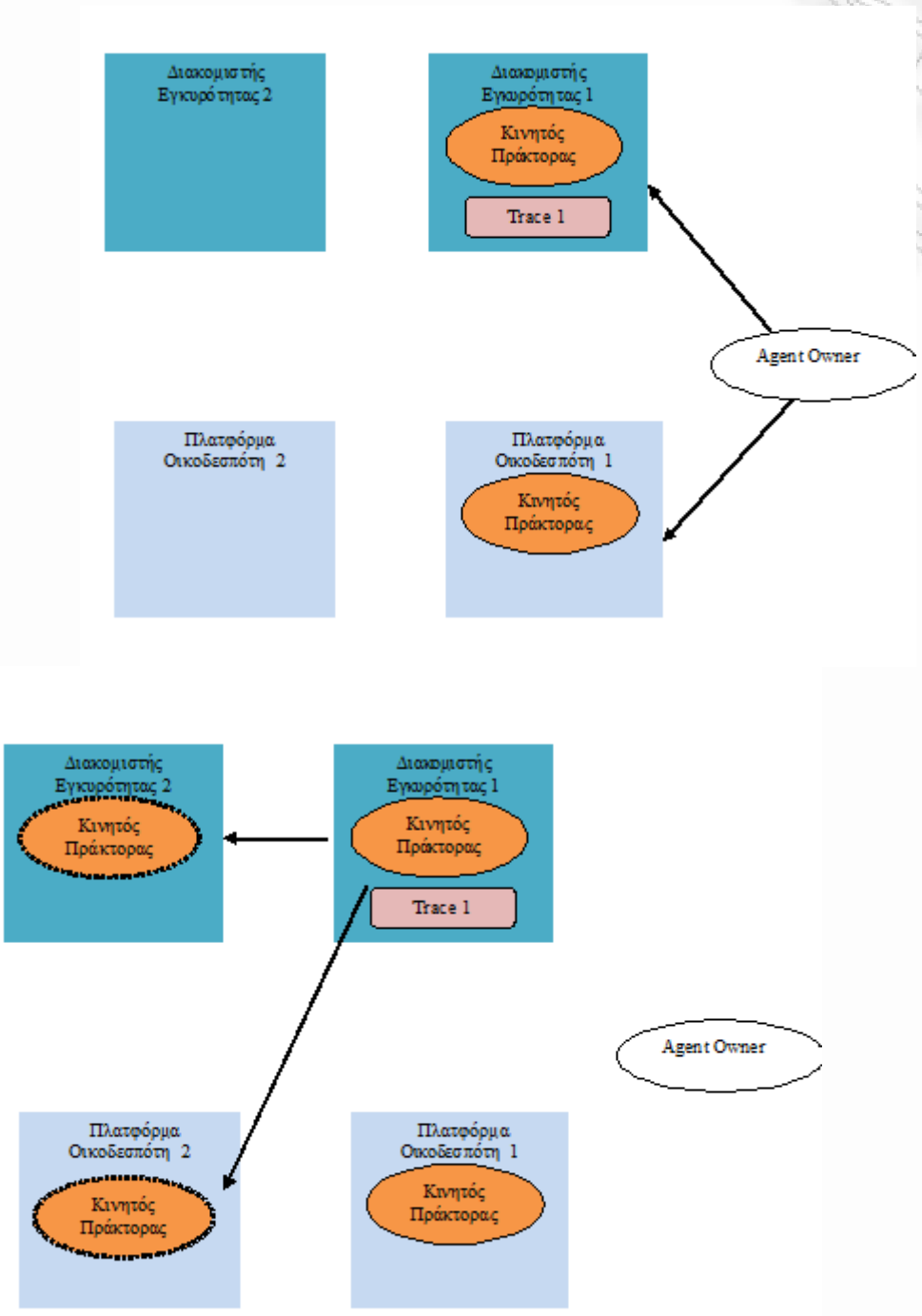


Εικόνα 13: Ανίχνευση Εκτέλεσης

Με την επιστροφή του πράκτορα στον κάτοχο του, προκαλείται μία λειτουργία ιχνηλάτησης εάν ο κάτοχος υποψιάζεται ότι μία συγκεκριμένη πλατφόρμα πραγματοποίησε εξαπάτηση, καθόσον εκτελούσε το πράκτορα (Εικόνα 13). Η λειτουργία αυτή ζητάει πρώτα από την ύποπτη πλατφόρμα να αναπαράγει το σχετικό ίχνος. Μετά, ο κάτοχος του πράκτορα εκκινεί μία προσομοίωση του ίχνους αρχίζοντας από την πρώτη πλατφόρμα οικοδεσπότη στο δρομολόγιο. Η διαδικασία αυτή θα δημιουργήσει ένα ίχνος αναγνωρίζοντας την ταυτότητα μίας ενδιάμεσης κατάστασης και την επόμενη πλατφόρμα οικοδεσπότη στο δρομολόγιο. Ο κάτοχος του πράκτορα ελέγχει την εγκυρότητα της εκτέλεσης του πράκτορα συγκρίνοντας το αναπαραγόμενο-προσομοιωμένο ίχνος με το κατακερματισμένο ίχνος και την ενδιάμεση κατάσταση που κατέχει. Η διαδικασία συνεχίζεται εντοπίζοντας οποιαδήποτε παραγωγή, εξακριβώνοντας με τον τρόπο αυτό οποιαδήποτε κακόβουλο σύστημα-οικοδεσπότη.

Μία παραλλαγή του ως άνω μέτρου ασφαλείας είναι η ιχνηλάτηση εκτέλεσης με διακομιστή επαλήθευσης εγκυρότητας (Execution Tracing with a verification server). Το μέτρο αυτό τροποποιεί το αρχικό αναθέτοντας τη διαδικασία επαλήθευσης εγκυρότητας σε ένα έμπιστο τρίτο μέρος, το διακομιστή επαλήθευσης εγκυρότητας, αντί να εξαρτάται από τον κάτοχο του πράκτορα. Όταν ένα κινητός πράκτορας μετακινείται σε μία νέα πλατφόρμα βάσει του δρομολογίου του, ένα αντίγραφο του πράκτορα και ένα ίχνος της εκτέλεσης του σε κάθε πλατφόρμα συστήματος-οικοδεσπότη υποβάλλεται στον αντίστοιχο διακομιστή επαλήθευσης εγκυρότητας πριν τη μετάβαση του πράκτορα σε μία νέα πλατφόρμα κεντρικού υπολογιστικού συστήματος. Κάθε υποβολή ίχνους πραγματοποιείται εντός ορισμένης χρονικής περιόδου που ελέγχεται από ένα χαρακτηριστικό χρονικό διάστημα λήψης (time-out) που το συγκεκριμένο μέτρο υποστηρίζει. Τα υποβληθέντα ίχνη για όλους τους πράκτορες τηρούνται στο διακομιστή

επαλήθευσης εγκυρότητας. Αυτός προσομοιώνει την εκτέλεση του πράκτορα χρησιμοποιώντας το υποβληθέν ίχνος και το αντίγραφο του πράκτορα και έτσι εντοπίζει τις οποιεσδήποτε παραβιάσεις . Ως εκ τούτου, στο συγκεκριμένο μέτρο ασφαλείας η διαδικασία επαλήθευσης της εγκυρότητας δεν προκαλείται μόνο ως επακόλουθο ύποπτων αποτελεσμάτων.



Εικόνα 14: Λειτουργία Διακομιστή Εγκυρότητας

2.5 Εφαρμογές Κινητών πρακτόρων και Σενάρια Ασφαλείας.

Η τεχνολογία κινητών πρακτόρων έχει αρχίσει να εξέρχεται δυναμικά από τα ερευνητικά κέντρα και να εισέρχεται σε πολλές εμπορικές εφαρμογές. Η παρακάτω ενότητα εστιάζει σε αυτές τις εφαρμογές και αναφέρει σχετικά θέματα ασφαλείας για τυπικά σενάρια που συναντώνται στη σημερινή πραγματικότητα.

2.5.1. Ηλεκτρονικό Εμπόριο – Electronic Commerce

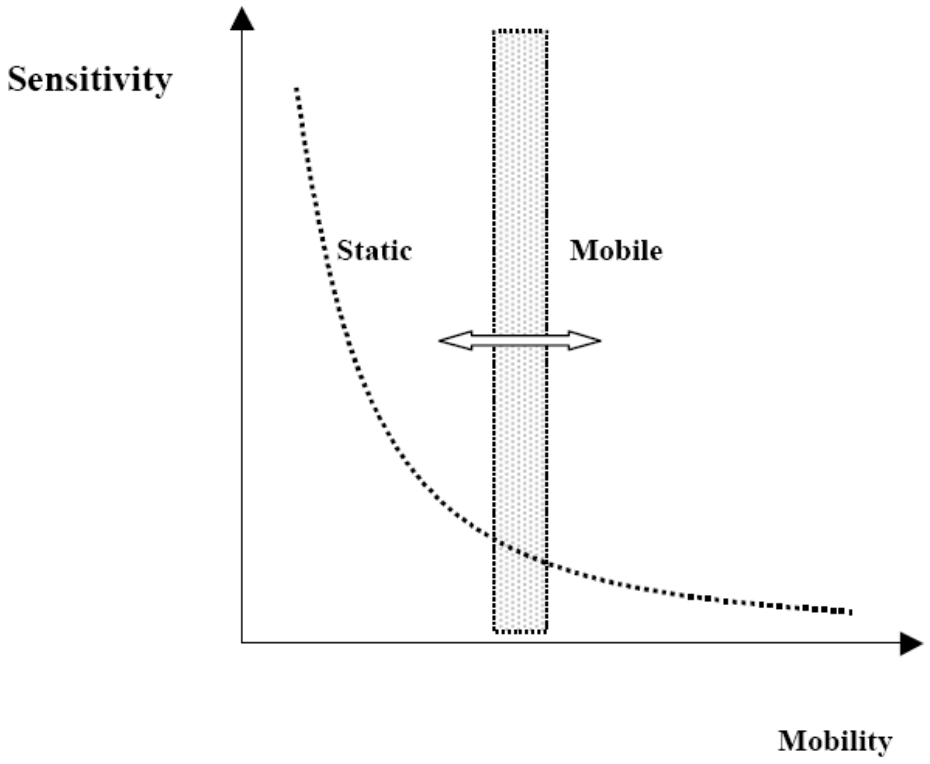
Εφαρμογές ηλεκτρονικού εμπορίου βασισμένες σε κινητούς πράκτορες έχουν προταθεί και αναπτύσσονται για ένα σύνολο διαφορετικών τομέων των επιχειρήσεων. Τέτοιοι τομείς μπορεί να είναι διαπραγματεύσεις συμβολαίων, μεσιτικές υπηρεσίες, δημοπρασίες και διακίνηση εμπορεύματος. Για παράδειγμα, οι κατασκευαστές μπορούν να διαπραγματευτούν την παραλαβή προϊόντων και υπηρεσιών μέσω εφαρμογών κινητών πρακτόρων.

Οι πράκτορες μπορεί να χρειαστεί να αποκτήσουν πρόσβαση στη βάση δεδομένων των προμηθευτών, να μεταφέρουν χρήματα για κάποια συναλλαγή και να διαπραγματευτούν όρους παράδοσης, εγγύησης και συμβολαίων υπηρεσιών. Οι κινητοί πράκτορες που εκπροσωπούν πλειοδότες αλληλεπιδρούν μεταξύ τους σε κοινή πλατφόρμα και συμμετέχουν σε δημοπρασίες εφαρμόζοντας διαφορετικές στρατηγικές και διαφορετικούς οικονομικούς περιορισμούς, ανάλογα πάντα με τις απαιτήσεις του πελάτη που εκπροσωπούν

Το επίπεδο της ασφαλείας που απαιτείται για την υλοποίηση ενός πράκτορα και την ευαισθησία του κώδικα και των δεδομένων των κινητών πρακτόρων επηρεάζει το επίπεδο κινητικότητας των κινητών πρακτόρων. Όπως φαίνεται στην εικόνα 15 **,** όσο η 'ευαισθησία' των εργασιών που έχει να επιτελέσει ένας πράκτορας αυξάνεται τόσο ο σχεδιαστής θα μειώσει την κινητικότητα του πράκτορα. Η απόφαση για το πώς τελικά θα κατασκευαστεί ο πράκτορας θα βασιστεί στους μηχανισμούς ασφαλείας, στις απαιτήσεις απόδοσης, την ευαισθησία του κώδικα και των δεδομένων του πράκτορα, στο μέγιστο αποδεκτό ρίσκο και στο επίπεδο της απαιτούμενης λειτουργικότητας.

Οι εργασίες που μπορεί να επιτελέσει ένας πράκτορας μπορούν να διαχωριστούν σε δύο κατηγορίες, οι οποίες είναι στατικές και κινητές έτσι ώστε όσο μεγαλύτερη ασφάλεια απαιτείται τόσο λιγότερη κινητικότητα θα αποκτά. Για παράδειγμα, ένας πράκτορας – πωλητής θα

επισκέπτεται ιστοσελίδες πωλητών αναζητώντας την καλύτερη τιμή και διαθεσιμότητα για ένα προϊόν ή μια υπηρεσία. Όταν βρεθεί το προϊόν ή η υπηρεσία που ταιριάζει καλύτερα στα κριτήρια που έχουν τεθεί, ένας στατικός πράκτορας σε μια πλατφόρμα εμπιστοσύνης θα αναλάβει να ολοκληρώσει την πώληση και να επιβεβαιώσει την αγορά με χρήση της τεχνικής του ιδιωτικού κλειδιού.



Εικόνα 15: Σχέση κινητικότητας - Ευαισθησίας

Η απώλεια ενός πράκτορα που δεν έχει εξουσιοδότηση να μεταφέρει χρήματα ή να ολοκληρώνει αγορές με χρήση ιδιωτικού κλειδιού μπορεί να είναι ανεκτή. Δεν ισχύει το ίδιο όμως για την απώλεια ενός πράκτορα που έχει εξουσιοδότηση να κάνει τέτοιες κινήσεις αφού μια απώλεια του από επίθεση μπορεί να καταστρέψει την αξιοπιστία του ή και ολόκληρης της πλατφόρμας.

2.5.2 Διαχείριση Δικτύου - Network Management

Οι κινητοί πράκτορες χρησιμοποιούνται επίσης σε εφαρμογές διαχείρισης δικτύου όπως διαχείριση απομακρυσμένων συνδέσεων, διανομή λογισμικού και προσαρμοσμένη ανταπόκριση σε γεγονότα δικτύου. Το λογισμικό διαχείρισης διαδικτύου βασίζεται κυρίων στο Πρωτόκολλο Απλής

Διαχείρισης Δικτύου (Simple Network Management Protocol - SNMP). Οι προγραμματιστές του Πρωτόκολλου Απλής Διαχείρισης Δικτύου το ανέπτυξαν γύρω στα μέσα της δεκαετίας του 1980 σαν ένα προσωρινό μέτρο γνωρίζοντας τα προβλήματά του και τους περιορισμούς του μέχρι η βιομηχανία να προτείνει κάποια καλύτερη λύση. Οι κινητοί πράκτορες επιτρέπουν μεγαλύτερο έλεγχο και δεν περιορίζονται από οποιαδήποτε παράμετρο επιβάλλουν οι κατασκευαστές μέσω του Πρωτόκολλου Απλής Διαχείρισης Δικτύου. Επιπλέον, οι κινητοί πράκτορες μπορούν να παρέχουν προσαρμοσμένες απαντήσεις σε γεγονότα δικτύου. Χωρίς κινητούς πράκτορες, όλο το λογισμικό που απαιτείται να υποστηρίξει και να απαντήσει σε όλα τα πιθανά σενάρια εφαρμογής τους θα έπρεπε να συντηρείται σε κάθε συσκευή τοπικά. Σε αυτή την περίπτωση, ο διαχειριστής δικτύου τότε θα πρέπει να αφιερώσει χρόνο για να απαντήσει σε κάθε γεγονός και να αλληλεπιδράσει με κάθε συσκευή ξεχωριστά. Αντιθέτως, οι κινητοί πράκτορες μπορούν αποστείλουν μια απαίτηση, να απαντήσουν σε κάποιο γεγονός και να φορτωθεί σε κάθε συσκευή μόνο το λογισμικό που απαιτείται για αυτή τη διαδικασία.

Αναβαθμίζοντας το λογισμικό δικτύου για να προστεθεί επιπλέον λειτουργικότητα απαιτεί σημαντική προσπάθεια τροχοδρόμησης εκ μέρους των διαχειριστών διαδικτύου. Εγκατάσταση νέου λογισμικού, αναβάθμιση ήδη υπάρχοντος ή και επαναρύθμιση υλικού δικτύου μπορεί να γίνει απλά εφαρμόζοντας τους πράκτορες στα απολύτως απαραίτητα μηχανήματα.

Οι πολιτικές ασφάλειας διαχειριστών δικτύου είναι απίθανο να επιτρέψουν πρόσβαση κώδικα μέσα στον οργανισμό. Μόνο εξουσιοδοτημένοι διαχειριστές δικτύου επιτρέπεται να εισάγουν κώδικα στο δίκτυο και να εφαρμόσουν αυστηρό έλεγχο πρόσβασης σε πλατφόρμες πρακτόρων. Η ανάπτυξη τέτοιων τεχνικών συμβαδίζει με σωστές μεθόδους ελέγχου ποιότητας, ώριμες αρχές σχεδίασης λογισμικού και διατήρηση και ανάλυση αρχείων log σχετικά με γεγονότα ασφάλειας δικτύου.

Απόπειρες φθοράς του πράκτορα ή της πλατφόρμας πρακτόρων εσωτερικά του οργανισμού, πιθανόν από κάποιο δυσαρεστημένο εργαζόμενο, κατά τις οποίες γίνεται προσπάθεια εκκίνησης κάποιου κακόβουλου πράκτορα είναι οι μεγαλύτερες απειλές για το σύστημα όταν κανείς ή ελάχιστοι εξωτερικοί πράκτορες έχουν την άδεια να εισέλθουν στο δίκτυο του οργανισμού. Σε αυτή την περίπτωση, μηχανισμοί αιτιολόγησης κινήσεων - λογοδότησης (Accountability) μπορούν να τοποθετηθούν ώστε να αποτρέψουν τους εργαζόμενους να εκκινούν κακόβουλους πράκτορες ηθελημένα. Ωστόσο, αυτοί οι μηχανισμοί δρουν ως αποτρεπτικός παράγοντας και δεν μπορούν να εμποδίσουν κάποιον από το να δράσει κακόβουλα. Το ρίσκο είναι το ίδιο σαν ένας εσωτερικός σε έναν οργανισμό να εισάγει trojan horses ή άλλο κακόβουλο κώδικα σε περιβάλλον μη κινητού πράκτορα αλλά η ζημιά στην περίπτωση του κινητού κώδικα θα ήταν πολύ μεγαλύτερη. Οι κινητοί πράκτορες που αναπτύσσονται εσωτερικά ή αγοράζονται από πωλητές εμπιστοσύνης υποβάλλονται σε ίδιες μεθόδους σχεδίασης και ανάπτυξης λογισμικού με τους μη κινητούς πράκτορες ώστε να διασφαλιστεί η ποιότητα του κώδικα. Δίνοντας στους

κινητούς πράκτορες την πολυπλοκότητα σχεδίασης ασφαλούς και αξιόπιστου κώδικα των μη κινητών πρακτόρων έχει νόημα αφού σχεδιαστικά και προγραμματιστικά λάθη θα συνεχίσουν να απασχολούν στους διαχειριστές συστημάτων και προγραμματιστές συστημάτων κινητών πρακτόρων.

Η δυνατότητα να κλωνοποιούν τους εαυτούς τους και η έμφυτη αυτονομία τους προσθέτει ακόμα μεγαλύτερη πολυπλοκότητα στη διαδικασία σχεδιασμού και ανάπτυξης. Προφανώς, τα εργαλεία σχεδίασης, ανάπτυξης και διαχείρισης κινητών πρακτόρων δεν έχουν αναπτυχθεί πλήρως κάτι απαραίτητο προτού πραγματοποιηθεί οποιαδήποτε ευρείας κλίμακας εφαρμογή κινητών πρακτόρων σε λειτουργικό σύστημα. Οι προγραμματιστές και οι διαχειριστές πρακτόρων θα επωφεληθούν σίγουρα από καλύτερους και πιο εύρωστους μηχανισμούς διαχείρισης πόρων σε πλατφόρμες κινητών πρακτόρων.

Σε αντίθεση με το πεδίο διαχείρισης δικτύου, η ενεργή δικτύωση και η χρήση έξυπνων πακέτων αντιπροσωπεύει την άλλη όψη του νομίσματος όπου πακέτα από οπουδήποτε μπορούν να απαιτήσουν υπολογιστικούς κύκλους και υπηρεσίες επικοινωνίας από δρομολογητές ή άλλα συστατικά του διαδικτύου. Αφού τα έξυπνα πακέτα μπορούν να εισέρχονται και απέξω από τον τομέα ασφαλείας της πλατφόρμας που φιλοξενεί τους πράκτορες, ο κώδικάς τους θα απαιτεί ισχυρότερους μηχανισμούς ασφαλείας ώστε να εγκαθιδρύσει την αξιοπιστία και θα έχουν λιγότερα προνόμια από τους κινητούς πράκτορες που προέρχονται από την πλατφόρμα που βρίσκεται εντός του τομέα ασφαλείας της πλατφόρμας που φιλοξενεί τους πράκτορες.

2.5.3. Προσωπικοί Ψηφιακοί Βοηθοί (Personal Digital Assistants -PDA)

Οι κατασκευαστές κινητών τηλεφώνων, ραδιοφώνων αυτοκινήτων και άλλων ηλεκτρονικών συσκευών εισάγουν όλο και περισσότερη λειτουργικότητα στα προϊόντα τους και εστιάζουν στην ανάπτυξη πρακτόρων σε αυτές. Η αναγνώριση φωνής μπορεί να εισαχθεί για ομιλία σε ραδιόφωνο αυτοκινήτου, για αναζήτηση και λήψη κατευθυντήριων οδηγιών, για διακανονισμό αποστολής ενός φαξ ή για σημείωση ενός σημαντικού γεγονότος στο προσωπικό ημερολόγιο. Αυτές οι συσκευές δεν είναι συνεχώς συνδεδεμένες με το ασύρματο δίκτυο και μπορούν να επωφεληθούν από την ικανότητα του πράκτορα να λειτουργεί αυτόνομα από την πλατφόρμα που το εκκίνησε.

Οι προγραμματιστές συχνά παρουσιάζουν το παράδειγμα κατά το οποίο ένας χρήστης ενώ εκκινεί μια διαδικασία για να πραγματοποιήσει κρατήσεις ταξιδιών, εστιατορίων και ξενοδοχείων διαπραγματεύονταν με άλλους πράκτορες, ως ένα χαρακτηριστικό σενάριο της τεχνολογίας των κινητών πρακτόρων.

Οι περισσότεροι χρήστες πρακτόρων δεν είναι σχεδόν ποτέ και προγραμματιστές αυτών και είτε θα έχουν κάνει λήψη αυτών από κάποιο γνωστό πωλητή είτε θα υπάρχει ήδη εγκατεστημένος στις ηλεκτρονικές συσκευές τους. Αυτά τα σενάρια χαρακτηρίζονται από συναλλαγές κατά τις οποίες ο χρήστης μοναχά στέλνει έναν πράκτορα να πραγματοποιήσει μια συναλλαγή και λαμβάνει τον ίδιο πράκτορα πίσω, ενώ σχεδόν ποτέ δε φιλοξενεί κάποιον από εξωτερική πηγή.

Επιπλέον, τα PDAs προσφέρουν λιγότερες υπηρεσίες από εμπορικές πλατφόρμες. Σε τέτοιο περιβάλλον, τα βασικά ζητήματα ασφαλείας είναι εμπιστευτικότητα, μηχανισμοί που θα απαγορεύουν την απάρνηση ενεργειών (non-repudiation) και αμοιβαία ταυτοποίηση. Πλήθος τέτοιων μηχανισμών εφαρμόζεται σε συστήματα κινητών πρακτόρων.

Η υποδομή δημόσιου κλειδιού (PKI-Public Key Infrastructure) αποτελεί τη βάση για τις υπηρεσίες ασφαλείας των κινητών πρακτόρων και συμβάλει ώστε η αμοιβαία ταυτοποίηση, η γνησιότητα των συναλλαγών και η κρυπτογράφηση να είναι άμεσα διαθέσιμες σε προγραμματιστές και χρήστες πρακτόρων.

Αν και πολλές φορές παρατηρείται αποτυχία στην επίλυση όλων των απειλών που παρουσιάζονται, υπάρχουν αρκετά παραδείγματα κατά τα οποία προσφέρουν επαρκή προστασία στους πράκτορες.

Παρόλο που συμβατικές τεχνικές κρυπτογράφησης μπορούν να εφαρμοστούν τόσο σε πράκτορες και στα μηνύματά τους, ακόμα και αν τα μηνύματα που ανταλλάσσονται με μια άλλη πλατφόρμα είναι κρυπτογραφημένα, λαθροακουστές μπορούν να εξαγάγουν συμπεράσματα σχετικά με τις προθέσεις του χρήστη, βασιζόμενοι σε στοιχεία όπως τον προορισμό των μηνυμάτων. Για παράδειγμα, αν ένας πράκτορας στέλνει μηνύματα ή επισκέπτεται πωλητές υλικού υπολογιστών, ένας πωλητής λογισμικού μπορεί να στέλνει αυτόκλητες διαφημίσεις για προγράμματα ή μέρη υπολογιστή. Εφ' όσον όταν πραγματοποιούνται συναλλαγές όταν δεν υπάρχει σύνδεση δημιουργεί περιορισμούς στην ικανότητα του πράκτορα να χρησιμοποιεί αποθηκευμένα ιδιωτικά κλειδιά στη συσκευή του και όταν τα κουβαλάει δεν είναι ασφαλές, κρίσιμες τέτοιες συναλλαγές θα πρέπει να πραγματοποιούνται σε μια τρίτη πλατφόρμα εμπιστοσύνης που είναι διαθέσιμη συνεχώς, κάτι που δεν συμβαίνει με τα PDAs. Όπως οι τράπεζες, οι εταιρίες πιστωτικών καρτών και οι ασφαλιστικές προσφέρουν ένα τεράστιο πλήθος οικονομικών και νόμιμων συναλλαγών, έτσι και παρόμοιες υπηρεσίες μπορούν να παρέχονται σε έναν πράκτορα.

2.6 Αξιολόγηση των υφιστάμενων αντίμετρων ασφαλείας

Βασιζόμενη στην προηγηθείσα ανάλυση, η παρούσα ενότητα καταπιάνεται με μία αξιολόγηση των μέτρων ασφαλείας που βρίσκουν εφαρμογή σε συστήματα κινητών πρακτόρων. Η διενεργηθείσα αξιολόγηση εστιάζει κυρίως σε συγκεκριμένα μειονεκτήματα του κάθε μέτρου ασφαλείας που αναλύθηκαν, που μπορεί να συνεπάγεται τον περιορισμό της χρήσης του ή υιοθέτηση συμβιβασμών στην ασφάλεια των συστημάτων κινητών πρακτόρων. Για την παρουσίαση των διακριβωμένων μειονεκτημάτων, ακολουθούμε την ταξινόμηση των μέτρων ασφαλείας της προηγούμενης ενότητας.

2.6.1 Μέτρα ασφαλείας για πλατφόρμες πρακτόρων

Όπως αναφέρθηκε στην παράγραφο 2.4.1, τα μέτρα ασφαλείας για την προστασία των πλατφόρμων πρακτόρων ακολουθούν κυρίως είτε την προσέγγιση απομόνωσης κρίσιμων δεδομένων είτε την προσέγγιση ασφάλισης του κινητού κώδικα. Η πρώτη προσέγγιση απομονώνει τη μνήμη και περιορίζει την πρόσβαση σε αυτήν, προκειμένου να διατηρεί περιβάλλοντα αποκλειστικής εκτέλεσης. Περιλαμβάνει τα μέτρα ασφαλείας της Λογισμικής Απομόνωσης Σφαλμάτων (SFI) και της Ασφαλούς Διερμήνευσης Κώδικα. Από την άλλη πλευρά, η δεύτερη προσέγγιση (δηλαδή ασφάλισης κινητού κώδικα) προστατεύει τις πλατφόρμες πρακτόρων ασφαλίζοντας τον κώδικα των κινητών πρακτόρων που τις επισκέπτονται. Περιλαμβάνει μέτρα που διασφαλίζουν την αυθεντικότητα του κινητού κώδικα και των πρακτόρων, την ύπαρξη των ενδεδειγμένων ιδιοτήτων ασφαλείας στους κινητούς πράκτορες, την ανίχνευση οποιασδήποτε κακόβουλης μεταβολής πραγματοποιηθεί από μία μη έμπιστη πλατφόρμα στον κώδικα ενός κινητού πράκτορα, και την τήρηση αρχείου του ιστορικού των πρακτόρων. Στη συνέχεια παρουσιάζουμε και αναλύουμε τα σημαντικότερα μειονεκτήματα που εισάγει η εφαρμογή των προαναφερθεισών μέτρων ασφαλείας. Τα συγκεκριμένα μειονεκτήματα ενδέχεται να επηρεάσουν την ασφάλεια των πλατφόρμων πρακτόρων, και συνεπώς να περιορίσουν την ανάπτυξη των συστημάτων κινητών πρακτόρων.

Η τεχνική της Λογισμικής Απομόνωσης Σφαλμάτων (SFI) διασφαλίζει ότι οι διευθύνσεις μνήμης και οι στόχοι άλματος βρίσκονται μόνο σε καθορισμένα ασφαλή δεδομένα και περιοχές κώδικα και επιτυγχάνει προστασία από ενέργειες κακόβουλου κώδικα παρόμοια με εκείνη που επιτυγχάνεται με την εκτέλεση του κώδικα σε ξεχωριστή διαδικασία λειτουργικού συστήματος ή με την απαίτηση εγγραφής του κώδικα σε γλώσσα ασφαλή για τη μνήμη. Δεν απαιτεί υποστήριξη από το λειτουργικό σύστημα ή το υλισμικό και είναι αποτελεσματική για προγράμματα που έχουν

γράφει σε οποιαδήποτε γλώσσα, συμπεριλαμβανομένων των σημαντικών, μη ασφαλών για τη μνήμη γλωσσών, όπως η C και η C++. Το κύριο μειονέκτημα του μέτρου ασφαλείας SFI σχετίζεται με το ότι μπορεί να χρειαστεί ελαφρώς περισσότερο χρόνο εκτέλεσης προκειμένου μη έμπιστα δομοστοιχεία να καταστούν διακριτά και για τον μετασχηματισμό και την εκτέλεση του κώδικα. Επίσης, ο κώδικας σε αμμοδοχείο πρέπει να ελέγχεται κατά την εισαγωγή του κώδικα, αφού δεν υπάρχει ανάγκη να εμπιστευτεί κανείς τον συνομιλητή του ως προς την ορθή εκτέλεση του sandboxing, και συνεπώς ως προς τον αποτελεσματικό περιορισμό της προσπέλαση της μνήμης σε ασφαλή δεδομένα και περιοχές κώδικα.

Στην άλλη τεχνική απομόνωσης δεδομένων, τη Διερμήνευση Ασφαλούς Κώδικα (SCI), με δεδομένη την σωστή διενέργεια του ελέγχου του τύπου και της απουσίας υπέρ- ή υποχείλισης στοίβας, οι επιβλαβείς εντολές μετασχηματίζονται σε ασφαλείς διασφαλίζοντας σε αντίθετη περίπτωση ότι οι κακόβουλες εντολές δεν εκτελούνται από πράκτορες. Το μειονέκτημα της SCI εμφανίζεται όταν εκτελεί δυναμικό έλεγχο των συνθηκών, όπως ελέγχους ορίων πίνακα (array-bound) κατά το χρόνο εκτέλεσης, που συνιστά μία 'ακριβή' σε πολυπλοκότητα διαδικασία, επιβραδύνει σημαντικά την εκτέλεση και όπως και με τη Λογισμική Απομόνωση Σφαλμάτων, η διερμήνευση και εκτέλεση του κώδικα μπορεί να απαιτήσουν μεγαλύτερο χρόνο εκτέλεσης.

Το μέτρο ασφαλείας της Υπογραφής κώδικα (Signing code) που ακολουθεί την προσέγγιση ασφάλισης του κινητού κώδικα παρουσιάζει δύο βασικά μειονεκτήματα. Τα μειονεκτήματα αυτά σχετίζονται με τη λίστα των έμπιστων οντοτήτων την οποία τηρεί η κάθε πλατφόρμα-οικοδεσπότης. Πρώτα, το συγκεκριμένο μέτρο ασφαλείας θεωρεί ότι όλες οι οντότητες που περιέχονται στη λίστα των έμπιστων είναι αξιόπιστες και άφθαρτες. Συνεπώς, οι κινητοί πράκτορες που έχουν υπογραφή στους κινητούς κώδικες και άρα προέρχονται από τέτοιες οντότητες παρέχονται πλήρη προνόμια στην εκτελούσα πλατφόρμα. Όμως, εάν μία οντότητα, η οποία έχει χαρακτηριστεί από μία εκτελούσα πλατφόρμα ως έμπιστη, είναι φθαρμένη, τότε ένας κινητός πράκτορας που δημιουργηθεί από την πρώτη μπορεί να προκαλέσει ζημιά στη δεύτερη, αφού διαθέτει πλήρη προνόμια πάνω σε αυτή. Επιπροσθέτως, ο κακόβουλος πράκτορας μπορεί να χρησιμοποιήσει τα προνόμια του επί της εκτελούσας πλατφόρμας για να ανοίξει θύρες σε άλλους κακόβουλους πράκτορες αλλάζοντας την πολιτική αποδοχής στην πλατφόρμα. Τα αποτελέσματα ενδεχόμενων επιθέσεων του κακόβουλου πράκτορα ίσως να πραγματοποιηθούν αργότερα, έτσι ώστε η σύνδεση της επίθεσης με τον επιτιθέμενο να καταστεί δύσκολη (δηλ. καθυστερημένες επιθέσεις). Από την άλλη πλευρά, το δεύτερο μειονέκτημα του μέτρου ασφαλείας της υπογραφής του κώδικα σχετίζεται με το γεγονός ότι είναι υπερβολικά περιοριστικός απέναντι σε πράκτορες που προέρχονται από μη έμπιστες οντότητες. Ένας τέτοιος πράκτορας δεν επιτρέπεται να εκτελείται στην πλατφόρμα επηρεάζοντας τις υπηρεσίες ή τις δραστηριότητες τις οποίες αυτή αντιπροσωπεύει.

Συγκριτικά με τον Υπογεγραμμένο Κώδικα (Signed Code), το μέτρο ασφαλείας PCC χρησιμοποιεί μία απλούστερη διαδικασία επαλήθευσης της εγκυρότητας στο βαθμό που δεν απαιτείται καμία κρυπτογραφία, κανένα έμπιστο τρίτο μέρος και καμία διαχείριση κλειδιών. Ένα βασικό πλεονέκτημα του συγκεκριμένου μέτρου έγκειται στη μεταβίβαση της υποχρέωσης διασφάλισης της ασφάλειας του κώδικα από τον καταναλωτή του στον κατασκευαστή του κώδικα. Συνεπώς, ο πρώτος δεν εκτελεί καμία ανάλυση του προγράμματος, σύνταξη του κώδικα και διερμηνεία εντολών. Επιπλέον, σε αυτό το μέτρο ασφαλείας η έμπιστη βάση κώδικα (trusted code base - TCB) είναι εξαιρετικά μικρή, αφού περιλαμβάνει μόνο τον ελεγκτή απόδειξης για την επαλήθευση της εγκυρότητας της απόδειξης της ασφάλειας και ο έλεγχος της απόδειξης μπορεί να είναι μία απλή μηχανική διαδικασία. Η ύπαρξη της απόδειξης επιτρέπει την off-line εκτέλεση της διαδικασίας επαλήθευσης της εγκυρότητας (δεν χρειάζεται έλεγχος κατά το χρόνο εκτέλεσης) και μόνο μία φορά για ένα δεδομένο πρόγραμμα, ανεξάρτητα από το πόσες φορές εκτελείται, γιατί το προηγούμενο στάδιο επαλήθευσης της εγκυρότητας διασφαλίζει ότι ο κώδικας τηρεί με την πολιτική ασφαλείας. Επιπλέον, εξοικονομείται χρόνος γιατί ο μη έμπιστος κώδικας έχει επαληθευτεί ως προς την εγκυρότητα του πριν να εκτελεστεί, έτσι ώστε οι επικίνδυνες λειτουργίες εντοπίζονται έγκαιρα. Οποιαδήποτε τροποποίηση στα προγράμματα PCC (κατά λάθος ή κακόβουλη) θα επιφέρει τα εξής αποτελέσματα:

- η απόδειξη θα παύσει να είναι έγκυρη και το πρόγραμμα θα απορριφθεί,
- η απόδειξη θα είναι έγκυρη αλλά θα παύσει να είναι εγγύηση ασφαλείας για το πρόγραμμα και το πρόγραμμα θα απορριφθεί ή
- η απόδειξη θα εξακολουθήσει να είναι έγκυρη και να υπάρχει απόδειξη ασφαλείας για το πρόγραμμα.

Από την άλλη πλευρά, το κύριο μειονέκτημα της PCC σχετίζεται με τη διαδικασία δημιουργίας της απόδειξης, και υπάρχει εκτενής έρευνα επάνω στους τρόπους αυτοματοποίησης της. Η δημιουργία της απόδειξης μπορεί να είναι υπολογιστικά δύσκολη και πολλές αποδείξεις εξακολουθούν να πρέπει να γίνονται χειροκίνητα, αλλά τουλάχιστον, υπάρχουν επαρκείς τυποποιημένες τεχνικές απόδειξης του θεωρήματος. Επιπροσθέτως, η προσπάθεια κωδικοποίησης των αποδείξεων των ιδιοτήτων των προγραμμάτων θα συνεπάγονταν υπερβολικά μεγάλες αποδείξεις επαλήθευσης της εγκυρότητας, μεγαλύτερες σε μέγεθος ακόμα και από καθαυτό τον κινητό κώδικα, έτσι ώστε να απαιτείται περισσότερος χρόνος και προσπάθεια. Άλλοι περιορισμοί της PCC περιλαμβάνουν το χρόνο που αναλώνεται κατά τη διαδικασία επαλήθευσης της εγκυρότητας της απόδειξης, τη μεγάλη προσπάθεια που πρέπει να καταβάλλει και τις δυσκολίες που πρέπει να αντιμετωπίσει ο κατασκευαστής του κώδικα για την εδραίωση και την τυπική απόδειξη της ασφάλειας του κινητού κώδικα, καθώς και τη συσχέτιση μίας δεδομένης απόδειξης με ένα δεδομένο πρόγραμμα, χωρίς την οποία η απόδειξη στερείται χρησιμότητας για την

επαλήθευση της εγκυρότητας της απόδειξης. Επιπροσθέτως, η PCC εγγυάται την ασφάλεια του εισερχόμενου κώδικα υπό τον όρο ότι δεν υπάρχει σφάλμα στη δημιουργία της συνθήκης επαλήθευσης της εγκυρότητας, στα λογικά αξιώματα, στους κανόνες πληκτρολόγησης, και επίσης εξαρτάται από την αξιοπιστία του ελεγκτή της απόδειξης (proof-checker).

Το μέτρο ασφαλείας της αξιολόγησης κατάστασης αναδείχθηκε σε μία δημοφιλή τεχνική χάρη στο βαθμό δυνατότητας πρόβλεψης επιβλαβών τροποποιήσεων στην κατάσταση ενός πράκτορα και προετοιμασίας αντίμετρων, υπό τη μορφή συναρτήσεων αξιολόγησης, πριν προβεί σε χρήση του πράκτορα. Επιπροσθέτως, χρησιμοποιείται για να διασφαλίσει ότι ένα πράκτορας δεν έχει καταστεί κακόβολος κατά το δρομολόγιο του να αφοπλίζει έναν κακόβουλα τροποποιημένο πράκτορα. Ένα άλλο πλεονέκτημα της συγκεκριμένης τεχνικής έγκειται στο ότι παρέχει έναν ευέλικτο τρόπο σε έναν πράκτορα να ζητήσει άδειες αναλόγως της τρέχουσας κατάστασης του και του έργου που χρειάζεται να εκτελέσει σε μία συγκεκριμένη πλατφόρμα. Από την άλλη πλευρά, το κύριο μειονέκτημα του εν λόγω μέτρου έγκειται στη δυσκολία διατύπωσης κατάλληλων ιδιοτήτων ασφαλείας για έναν κινητό πράκτορα και επίτευξης μίας κατάστασης συνάρτησης αξιολόγησης που να εγγυάται τις ιδιότητες αυτές.

Τέλος, παρότι η χρήση του μέτρου ασφαλείας, των Ιστορικών Διαδρομής δεν εμποδίζει την κακόβουλη συμπεριφορά μίας πλατφόρμας, χρησιμεύει ωστόσο ως ισχυρό αποτρεπτικό μέσο, στο βαθμό που η υπογεγραμμένη εγγραφή διαδρομής της πλατφόρμας είναι μη-αποποιήσιμη. Ένα προφανές μειονέκτημα του συγκεκριμένου μέτρου έγκειται στην αύξηση του κόστους της επαλήθευσης της εγκυρότητας του path με την μεγέθυνση του ιστορικού του path. Αυτό γίνεται επειδή η διατήρησης εμπιστοσύνης σε πράκτορες που έχουν επισκεφθεί τεράστιο αριθμό πλατφόρμων καθίσταται δυσκολότερη. Ωστόσο, το κόστος επαλήθευσης της εγκυρότητας είναι συνάρτηση της ικανότητας της πλατφόρμας να κρίνει ορθά, εάν μπορεί να εμπιστευθεί τις εξακριβωμένες πλατφόρμες που ο πράκτορας έχει προηγουμένως επισκεφθεί. Αντίστοιχα, είναι πιο δύσκολο να εμπιστευθεί κανείς έναν πράκτορα, η διαδρομή ταξιδίου του οποίου είναι άγνωστο εκ των προτέρων, για παράδειγμα ο πράκτορας που αναζητεί νέες πληροφορίες δημιουργώντας δυναμικά τη διαδρομή ταξιδίου του.

2.6.2 Προστασία πρακτόρων

Η προστασία των πρακτόρων επίσης βασίζεται στην προσέγγιση της απομόνωσης των κρίσιμων δεδομένων και της ανίχνευσης επιθέσεων – εισβολών, οι οποίες απειλούν την εκτέλεση των πρακτόρων και των δεδομένων που φέρουν. Η απομόνωση των δεδομένων εφαρμόζεται κυρίως στα αποτελέσματα των ενεργειών του πράκτορα ενθυλακώνοντας τα είτε σε μία πλατφόρμα πρακτόρων ή σε καθαυτό το κινητό πράκτορα. Η απομόνωση υλοποιείται με την ολισθαίνουσα κρυπτογράφηση, την κωδίκων αυθεντικοποίησης μερικών αποτελεσμάτων (PRAC),

τη δημιουργία περιβαλλοντικού κλειδιού, τον υπολογισμό με κρυπτογραφικές συναρτήσεις (CEF) και το μέτρο ασφαλείας της συσκότισης. Από την άλλη, η ανίχνευση των επιθέσεων – εισβολών πραγματοποιείται με την καταγραφή του δρομολογίου ενός πράκτορα, με τη δημιουργία πανομοιότυπου αντιγράφου του πράκτορα ή με την ανίχνευση της κατάστασης του πράκτορα κατά την εκτέλεση του.

Οι παραδοσιακοί μηχανισμοί δεν είναι σχεδιασμένοι για την αντιμετώπιση απειλών, που επιτίθενται στην εφαρμογή προερχόμενες από το περιβάλλον της εκτέλεσης. Αν και αυτή η κατάσταση ενός πράκτορα που εκτελείται σε μία πλατφόρμα πρακτόρων η οποία ενδέχεται να μην είναι απολύτως έμπιστη κατέστησε επιβεβλημένη την ανάπτυξη νέων μηχανισμών αντιμετώπισης, οι τελευταίοι δεν είναι πλήρως σε θέση να παρέχουν αποτελεσματική προστασία στο πράκτορα, στο βαθμό που παρουσιάζουν ορισμένα μειονεκτήματα, τα οποία αναλύονται στην ενότητα αυτή**.**

2.6.2.1 Απομόνωση κρίσιμων δεδομένων

Το ισχυρό πλεονέκτημα της προσέγγισης της ενθυλάκωσης μερικών αποτελεσμάτων έγκειται στη δυνατότητα της να παρέχει απώτερη ακεραιότητα σε δρομολόγια πολλαπλού άλματος (multi-hop). Επιπλέον, μερικά αποτελέσματα, όπως MACs, έχουν μικρότερο κόστος υπολογισμού από εκείνο των ψηφιακών υπογραφών (αν και, προφανώς, παρέχουν διαφορετικές ιδιότητες από τις ψηφιακές υπογραφές). Από την άλλη, τα αποτελέσματα προς ενθυλάκωση ίσως να μην είναι άμεσα προφανή.

Η τεχνική PRAC υπόκειται σε μεγάλο αριθμό περιορισμών. Ο πλέον σοβαρός σημειώνεται όταν μία κακόβουλη πλατφόρμα αποκτά αντίγραφα των αυθεντικών κλειδιών της κρυπτογράφησης ή των συναρτήσεων δημιουργίας κλειδιού ενός πράκτορα. Εάν ο πράκτορας επισκεφθεί ξανά την πλατφόρμα ή επισκεφθεί άλλη πλατφόρμα η οποία συνωμοτεί με αυτήν, μία ή περισσότερες εγγραφές προηγούμενου μερικού αποτελέσματος θα μπορούσε να τροποποιηθεί χωρίς τη δυνατότητα ανίχνευσης, συνεπώς η προσέγγιση δε διασφαλίζει την ιδιωτικότητα του πράκτορα. Στο βαθμό που η PRAC προσανατολίζεται στην ακεραιότητα και όχι στην εμπιστευτικότητα, το συσσωρευμένο σύνολο των μερικών αποτελεσμάτων μπορεί επίσης να ειδωθεί από οποιαδήποτε πλατφόρμα επισκεφθεί ο πράκτορας, αν και αυτό το πρόβλημα λύνεται εύκολα με την εφαρμογή ολισθαίνοντος κλειδιού ή άλλων μορφών κρυπτογράφησης. Επιπλέον , ορισμένες φορές η συγκεκριμένη τεχνική θα μπορούσε να απαιτήσει ένα έμπιστο τρίτο μέρος για την χρονοσφράγιση ενός ψηφιακού αποτυπώματος των αποτελεσμάτων για την όποια νομική διαβεβαίωση.

Η θετική θεώρηση της προσέγγισης της Δημιουργίας Περιβαλλοντικού Κλειδιού (Environmental Key Generation) είναι ότι η απλή ανάγνωση του κώδικα του πράκτορα δεν μπορεί να αποκαλύψει το μήνυμα ενεργοποίησης. Από την άλλη πλευρά, μία αδυναμία της προσέγγισης αυτής έγκειται στο ότι εάν η πλατφόρμα λήψης είναι εχθρική, θα μπορούσε να ενεργήσει κακόβουλα κατά του εισερχόμενου πράκτορα. Όταν η περιβαλλοντική συνθήκη ικανοποιείται και δημιουργείται το κλειδί ενεργοποίησης, η πλατφόρμα, η οποία ελέγχει απόλυτα το πράκτορα θα μπορούσε απλώς να μετατρέψει το πράκτορα εξαναγκάζοντας τον να εκτελέσει διαφορετική συνάρτηση (π.χ., να εκτυπώσει αντί να εκτελέσει τον εκτελέσιμο κώδικα με την λήψη του στοιχείου ενεργοποίησης (trigger)). Επιπλέον, οι εχθρικές πλατφόρμες μπορούν να εξαναγκάσουν τον πράκτορα να εκτελεστεί δημιουργώντας τεχνηέντως το κλειδί περιβάλλοντος. Ένας πρόσθετος περιορισμός του συγκεκριμένου μέτρου έγκειται στο ότι η πλατφόρμα μπορεί να κρίνει πως δεν είναι ασφαλές να εκτελέσει έναν κρυπτογραφημένο κώδικα που είναι συνημμένος σε ένα κινητό κώδικα, γιατί θα μπορούσε να είναι π.χ. ιός. Γενικά, μία πλατφόρμα πρακτόρων κατά κανόνα περιορίζει τη δυνατότητα ενός πράκτορα να εκτελεί κώδικα που έχει δημιουργηθεί δυναμικά, αφού θεωρείται μία μη ασφαλής λειτουργία.

Ο Υπολογισμός με Κρυπτογραφημένες Συναρτήσεις (Computing with Encrypted Functions) επιτρέπει σε ένα μη έμπιστο σύστημα-οικοδεσπότη να εκτελεί χρήσιμους υπολογισμούς, χωρίς να είναι σε θέση να αναγνωρίσει τις αυθεντικές συναρτήσεις, και συνεπώς, να κατανοήσει τι σημαίνουν οι υπολογισμοί. Οι Sander και Tschudin απέδειξαν ότι ένα προσθετικά ομομορφικό σχήμα κρυπτογράφησης επιτρέπει μη διαδραστικές CEF για πολυώνυμα. Ωστόσο, τα υφιστάμενα προσθετικά ομομορφικά σχήματα κρυπτογράφησης δεν μπορούν να χρησιμοποιηθούν για CEF επειδή προκειμένου να διασφαλίζουν την ορθότητα οι παράμετροι του συστήματος πρέπει να είναι εκθετικού μεγέθους. Οι Sander και Tschudin πρότειναν επίσης τη χρήση αμφίρρητων (birational) συναρτήσεων, οι οποίες όμως αποδείχθηκαν μη ασφαλείς. Ως εκ τούτου, το κύριο πρόβλημα σε αυτό το μέτρο ασφαλείας έγκειται στην εύρεση κατάλληλων σχημάτων κρυπτογράφησης που να μπορούν να μετασχηματίσουν αυθαίρετες συναρτήσεις (χωρίς ουσιαστική απόκτηση γνώσης της συνάρτησης) κατά ένα μη διαδραστικό τρόπο. Επιπλέον, το συγκεκριμένο μέτρο εξαρτάται σημαντικά από κρυπτογραφικές ρουτίνες για την εκτέλεση και δεν αποτρέπει έναν αριθμό άλλων επιθέσεων όπως οι τροποποιήσεις σε συστήματα πρακτόρων πολλαπλού άλματος.

Αναφορικά με την συσκότιση, το κύριο πλεονέκτημα του συγκεκριμένου μέτρου σχετίζεται με το γεγονός πως θεωρείται ανθεκτική στις επιθέσεις πλαστοπροσωπίας και άρνησης υπηρεσίας , και στο ότι δεν απαιτούνται κρυπτογραφικά κλειδιά ή αλγόριθμοι. Ωστόσο ένα σοβαρό πρόβλημα με το συγκεκριμένο μέτρο έγκειται στο ότι δεν υπάρχει γνωστός αποτελεσματικός αλγόριθμος ή προσέγγιση που να παρέχει προστασία από απειλές που προέρχονται από έναν πράκτορα που αντιμετωπίζει ένα κακόβουλο σύστημα-οικοδεσπότη. Όλοι οι

γνωστοί αλγόριθμοί συσκότισης που έχουν έως σήμερα σχεδιαστεί για την προστασία των κινητών πρακτόρων αποδείχθηκαν αναποτελεσματικοί και ακόμα χειρότερα, οι υφιστάμενοι αλγόριθμοι blackbox λειτουργούν μόνο με πολυώνυμα και λογικές συναρτήσεις και δεν μπορούν να αντιμετωπίσουν δεδομένα αυθαίρετης εισαγωγής που χρησιμοποιούνται κυρίως για τον κινητό κώδικα. Ακόμα δεν υπάρχει κανένα τυπικό μοντέλο για τον προσδιορισμό της σχετικής ισχύος των αλγόριθμων περίπλεξης του κώδικα (ή για τον ποσοτικό προσδιορισμό του ευθέως ανάλογου, ωφέλιμου χρόνου προστασίας). Η κύρια αδυναμία της συσκότισης έγκειται στη δυσκολία μέτρησης του κατά πόσο αυτοί οι μετασχηματισμοί καθιστούν όντως δυσκολότερο για έναν άνθρωπο χρήστη πλήρως εξοπλισμένο με εργαλεία αποσυσκότισης να καταλάβει τον συσκοτισμένο κώδικα. Συχνά δεν είναι αναγκαίο να ανακαλύψει όλους τους κανόνες και να διασπάσει όλα τα ασαφή κατηγορήματα προκειμένου να επιτεθεί σε ένα τμήμα του κώδικα με επιτυχία. Μία προφανής αδυναμία των τεχνικών συσκότισης έγκειται στο δεν είναι αποδείξιμα ασφαλείς. Είναι πολύ πιθανό ότι για μία τεχνική συσκότισης υπάρχει μία αντίστοιχη τεχνική αποσυσκότισης. Ένα άλλο πρόβλημα ότι μόνος του ο συσκοτιστής δεν παρέχει προστασία έναντι δολιοφθοράς. Δεν είναι αναγκαίο για έναν επιτιθέμενο να ανακτήσει ολόκληρο το πρόγραμμα προκειμένου να βρει χρήσιμες πληροφορίες. Η ικανότητα να λάβει γνώση έστω και λίγων κρίσιμων πληροφοριών μπορεί να έχει ως επακόλουθο μία σημαντική απώλεια της ιδιωτικότητας. Οι D'Anna et al τονίζουν ότι η συσκότιση μπορεί να συμβάλει στην καθυστέρηση αλλά όχι στην αποτροπή επιθέσεων σε έναν πράκτορα μέσω ανάστροφης μηχανίκευσης (reverse engineering). Υποστηρίζουν επίσης ότι ένας επιτιθέμενος με επαρκείς υπολογιστικούς πόρους, όπως αρκετό χρόνο, μπορεί πάντα να αποσυσκοτίσει τον κώδικα. Ο Barak et al μελέτησε τα θεωρητικά όρια των τεχνικών συσκότισης και κατέδειξε ότι γενικά η επίτευξη μίας απόλυτα ασφαλούς συσκότισης είναι αδύνατη.

2.6.2.2 Ανίχνευση επιθέσεων – εισβολών

Στην τεχνική Mutual Itinerary Recording ένα συνεργαζόμενος πράκτορας ανιχνεύει τον πράκτορα σε μία αμοιβαία υποστηρικτική διάταξη, έτσι ώστε τα σημαντικότερα μειονεκτήματα σχετίζονται με την εδραίωση ενός ασφαλούς καναλιού για την επικοινωνία μεταξύ των πανομοιότυπων ομόλογων πρακτόρων. Μετακινούμενος ένας πράκτορας από το ένα σύστημα-οικοδεσπότη στο άλλο οι πληροφορίες για την τελευταία, την τρέχουσα και την επόμενη πλατφόρμα πρέπει να ανταλλάσσονται μέσω ενός ασφαλούς καναλιού, κάτι που συνεπάγεται κόστος για τη δημιουργία ενός αυθεντικοποιημένου καναλιού στο οποίο προστίθενται οι πρόσθετοι πόροι που καταναλώνονται από τις πανομοιότυπες οντότητες πράκτορα εξ' αιτίας του ότι οι πράκτορες πρέπει να κινούνται σε ζεύγη και να εκτελούν τις ίδιες ενέργειες σε διαφορετικές πλατφόρμες. Επιπλέον, πρέπει να αναφέρουμε την αδυναμία του ομολόγου πράκτορα να προσδιορίσει το ποια από τις δύο πλατφόρμες ευθύνεται σε περίπτωση που ένας από τους

πράκτορες σκοτωθεί. Ακόμα, σε περίπτωση που δύο πλατφόρμες, τις οποίες επισκεφθούν δύο ομόλογοι πράκτορες συνεργάζονται για την εξαπόλυση εχθρικών το σχήμα αποτυγχάνει αφού δεν μπορεί να κατανοήσει ότι θα προκαλέσει κακόβουλα αποτελέσματα. Για αυτόν ακριβώς το λόγο το σχήμα λειτουργεί μόνο υπό την υπόθεση βάσει της οποίας λίγες μόνο πλατφόρμες είναι κακόβουλες, αποφεύγοντας τη συνεργασία με τις κακόβουλες.

Αναφορικά με την παραλλαγή του προηγούμενου μέτρου ασφαλείας (δηλαδή Itinerary Recording with Replication and Voting) το κύριο μειονέκτημα σχετίζεται με τη γενική υπόθεση βάσει της οποίας η πλειοψηφία των συστημάτων-οικοδεσπότη δεν είναι κακόβουλα και το αποτέλεσμα που υπολογίζεται με αυτή γίνεται δεκτό ως το σωστό. Όπως ακριβώς και με την προηγούμενη περίπτωση, σε περίπτωση συνεργασίας πολλαπλών κακόβουλων πλατφόρμων το αποτέλεσμα που υπολογίζεται από την πλειοψηφία θα είναι επιβλαβές και το σχήμα θα αποτύχει πάλι. Αν και μία κακόβουλη πλατφόρμα μπορεί να φθείρει λίγα αντίγραφα του πράκτορα, απαιτείται τη δημιουργία πολλών πανομοιότυπων για την αποφυγή της συνάντησης και την επιτυχή ολοκλήρωση του υπολογισμού. Ένα προφανές μειονέκτημα είναι ότι οι πρόσθετοι πόροι αναλώνονται από τους πανομοιότυπους πράκτορες που απαιτούνται για την ταυτόχρονη εκτέλεση των ίδιων, για την επίτευξη του αποτελέσματος της πλειοψηφίας ή για έναν μεμονωμένο υπολογισμό.

Αν και η προσέγγιση της ιχνηλάτησης εκτέλεσης μπορεί να λειτουργήσει αποτρεπτικά έναντι κακόβουλης συμπεριφοράς μίας πλατφόρμας, παρουσιάζει μία σειρά μειονεκτημάτων. Το πλέον προφανές σχετίζεται με το γεγονός ότι το δρομολόγιο του πράκτορα μεγαλώνει ταξιδεύοντας από το ένα σύστημα-οικοδεσπότη στο άλλο, κάτι που συνεπάγεται την αύξηση του μεγέθους και του αριθμού των ιχνών συμπεριλαμβανομένων των πληροφοριών υπογραφής πλατφόρμας και αναγνωριστικών δήλωσης που πρέπει να τηρηθούν και να μεταφερθούν στην επόμενη πλατφόρμα. Η χρήση του καθίσταται εξαιρετικά δύσκολη στην περίπτωση πολυ-νηματικών (multi-threaded) πρακτόρων στο βαθμό που το ίχνος γίνεται υπέρμετρα πολύπλοκο και δυσχεραίνεται η παρακολούθηση της εκτέλεσης. Στην τεχνική αυτή, η διαδικασία επαλήθευσης της εγκυρότητας προκαλείται μόνο βάσει υποψίας τέλεσης μίας κακόβουλης επέμβασης σε ένα πράκτορα κατά το δρομολόγιο του, ένα πρόβλημα που αντιμετωπίζεται με την προσθήκη ενός διακομιστή επαλήθευσης της εγκυρότητας.

Στην τεχνική της ιχνηλάτησης εκτέλεσης με διακομιστή επαλήθευσης της εγκυρότητας η διαδικασία επαλήθευσης της εγκυρότητας δεν ενεργοποιείται μόνον από ύποπτα αποτελέσματα. Επιπροσθέτως, λήξη χρονικών ορίων (time-outs) επιτρέπουν την πρόληψη κατά επιθέσεων άρνησης υπηρεσίας που περιλαμβάνει τον τερματισμό του πράκτορα χωρίς την εκτέλεση του. Όμως η τεχνική αυτή υπόκειται στους ίδιους περιορισμούς όπως και η ιχνηλάτηση εκτέλεσης. Πρώτον, χρειάζεται η διατήρηση ενός δυνητικά μεγάλου μεγέθους και αριθμού ημερολογίων (log) και δεύτερον, κάθε πλατφόρμα μπορεί να επιλέγει το δικό της διακομιστή επαλήθευσης της

εγκυρότητας και αυτό μπορεί να ενθαρρύνει και να επιτρέψει μία ενδεχομένως κακόβουλη συνεργασία μεταξύ μίας πλατφόρμας και του διακομιστή. Για να αντιμετωπιστεί αυτό βρίσκεται σε εξέλιξη μία έρευνα της φύσης της ιχνηλάτησης εκτέλεσης και του τρόπου επίτευξης μίας πρακτικής εφαρμογής της, η οποία να μπορεί να εδραιώσει επίπεδα εμπιστοσύνης .

2.7 Θέματα ασφαλείας, σχεδιασμού και επίδοσης

Η χρήση κινητού κώδικα και κινητών πρακτόρων έχει πολλά πλεονεκτήματα όπως :

- Ξεπερνούν την αδράνεια του δικτύου
- Μειώνουν την υπερφόρτωση του δικτύου
- Εκτελούνται ασύγχρονα και αυτόνομα
- Προσαρμόζονται δυναμικά
- Λειτουργούν σε ετερογενή περιβάλλοντα
- Έχουν ισχυρή και ανεκτική σε σφάλματα συμπεριφορά

Ένα από τα βασικότερα εμπόδια για την ευρεία υιοθέτηση των κινητών πρακτόρων, είναι οι εύλογες ανησυχίες ασφαλείας των system developers, των διαχειριστών δικτύου και των υπευθύνων μηχανογράφησης. Είναι δεδομένο ότι όταν τα θέματα ασφαλείας λυθούν και αναπτυχθούν μια σειρά μηχανισμών ασφάλειας για να μειώσουν το κίνδυνο, τότε οι χρήστες της τεχνολογίας των κινητών πρακτόρων θα είναι ελεύθεροι να αναπτύξουν καινοτόμες λύσεις σε υπάρχοντα προβλήματα και να βρεθεί ένα ευρύ φάσμα τομέων εφαρμογής που θα επωφεληθούν από αυτή τη τεχνολογία.

Χρησιμοποιώντας αυτή τη συλλογή μηχανισμών ασφαλείας για να μειώνονται οι κίνδυνοι από επιθέσεις agent σε agent, agent σε πλατφόρμα και πλατφόρμας σε agent εισάγονται περιορισμοί απόδοσης που υπαγορεύουν αποφάσεις σχεδιασμού ή αναιρούν οφέλη από τη χρήση των κινητών πρακτόρων σε ορισμένες εφαρμογές .

Η συλλογή των μηχανισμών ασφαλείας που χρησιμοποιούνται για συγκεκριμένες εφαρμογές, θα πρέπει να σχεδιάζονται από την αρχική φάση σχεδιασμού ενός συστήματος agent και όχι να προστίθενται στο τέλος σαν κάποιο επιπλέον χαρακτηριστικό.

Τα ζητήματα ασφαλείας μπορούν να καθορίσουν ποιοι agents θα γίνουν κινητοί και ποιοι θα παραμείνουν στατικοί καθώς επίσης και ποιες λειτουργίες θα σχεδιαστεί ο agent να εκτελεί

και ποιες δεν θα εκτελέσει ποτέ. Παρακάτω αναλύονται οι επιπτώσεις των διαφόρων θεμάτων ασφάλειας για το σχεδιασμό και την εκτέλεση συστημάτων κινητών πρακτόρων

2.7.1. Ξεπερνώντας την αδράνεια του δικτύου

Οι λύσεις κινητών πρακτόρων αναπτύχθηκαν για κρίσιμα συστήματα που χρειάζονται να αντιδρούν σε οποιαδήποτε αλλαγή στο περιβάλλον τους σε πραγματικό χρόνο αλλαγές. Ένα παράδειγμα μιας τέτοιας εφαρμογής είναι η χρήση κινητών πρακτόρων για τον έλεγχο των robots που εργάζονται σε κατανεμημένες διαδικασίες παραγωγής. Οι κινητοί πράκτορες προσφέρονται ως λύση, επειδή μπορούν να αποσταλούν από κάποιο κεντρικό ελεγκτή να δράσουν τοπικά και να εκτελέσουν απευθείας τις οδηγίες του ελεγκτή

Αυτές οι κατανεμημένες διαδικασίες παραγωγής επιτρέπουν σε διαφορετικές εταιρίες να χρησιμοποιούν τους ειδικά σχεδιασμένους μηχανισμούς και να εκτελέσουν αλγόριθμους ανάλυσης δεδομένων. Αφού ο κινητός agent μεταφέρεται στην οικεία πλατφόρμα του ρομπότ, η διαδικασία ελέγχου δεν υπόκειται σε καθυστερήσεις δίκτυο, και δεν υπάρχουν αναξιοπιστίες που οφείλονται στα δίκτυα. Μπορεί αυτή η διαδικασία να λύνει τα προβλήματα δικτύου, προκαλεί όμως προβλήματα ασφαλείας. Για παράδειγμα ένας κινητός πράκτορας πιθανόν να θέλει να κρατήσει μυστικά από την πλατφόρμα που βρίσκεται , ενώ η πλατφόρμα θέλει να προστατεύσει τον εαυτό της από μη εξουσιοδοτημένους πράκτορες που θα τους δώσει πρόσβαση στη μηχανή .

Τα virtual μηχανήματα και οι διερμηνείς (interpreters) κάνουν την κινητικότητα σε ένα ετερογενές περιβάλλον δυνατή, αλλά ένα πρόγραμμα διερμηνέας συνήθως τρέχει αργότερα από ένα ισοδύναμο πρόγραμμα που χρησιμοποιεί τοπικό κώδικα. Επιδεινώνοντας την κατάσταση , οι μηχανισμοί ασφαλείας πρέπει να εξασφαλίσουν τον έλεγχο των πόρων , για να προστατευτεί η πλατφόρμα από κάποιον πράκτορα και να αποκρύψουν τα δεδομένα του agent από τη πλατφόρμα, ενώ μπορεί να προκληθεί και κόστος στις επιδόσεις, που μπορούν να προκαλέσουν δυσλειτουργίες κατά την εκτέλεση εφαρμογών πραγματικού χρόνου. Από τα παραπάνω φαίνεται ότι οι σχεδιαστές κινητών πρακτόρων για χρήση σε κατανεμημένες εφαρμογές πρέπει να ισορροπήσουν μεταξύ της απόδοσης και της ασφάλειας

Οι Straßer and Schwem συγκρίνουν την απόδοση των κινητών πρακτόρων με τις RPC (Remote Procedure Calls) . Μια RPC επιτρέπει σε μια διαδικασία να εκτελείται σε κάποιον απομακρυσμένο server, μεταφέροντας τον έλεγχο ροής από το client στο server μέχρι να ολοκληρωθεί η διαδικασία και να επιστραφούν τα αποτελέσματα. Οι συγγραφείς δημιούργησαν ένα μοντέλο απόδοσης για συστήματα κινητών πρακτόρων κατά το οποίο οι πράκτορες μπορούσαν εναλλακτικά να χρησιμοποιούσουν RPC ή μετακίνηση agent για να αλληλεπιδράσουν

με εφαρμογές σε άλλες πλατφόρμες. Οι συγγραφείς κατέληξαν ότι η επιλογή μεταξύ RPC και μετακίνησης agent εξαρτάται από πολλούς παράγοντες συμπεριλαμβανομένων των

- καθυστέρησης δικτύου
- όγκου
- αριθμό μηνυμάτων
- αριθμό πλατφόρμων που εμπλέκονται
- και το cache του κώδικα

Οι συγγραφείς δεν εξέτασαν όμως τις επιδράσεις της ασφάλειας στο μοντέλο απόδοσης. Η προσθήκη κρυπτογράφησης επιβαρύνει το κόστος στις επικοινωνίες και στα δύο συστήματα. Στις RPC, όσο μεγαλώνει ο αριθμός των μηνυμάτων , τόσο αυξάνεται και το κόστος από την κρυπτογράφηση τους, σε αντίθεση με ένα σύστημα κινητών πρακτόρων που πρέπει να κρυπτογραφηθεί μόνο δυο φόρες μία κατά τη διαδρομή στον host και μια στην επιστροφή.

2.7.2 Μείωση του φόρτου δικτύου

Οι κινητοί πράκτορες είναι κατάλληλοι για την έρευνα και την ανάλυση των προβλημάτων που προκύπτουν από κατανεμημένους πόρους που απαιτούν εξειδικευμένες εργασίες που δεν υποστηρίζονται από το διακομιστή δεδομένων

Μια αναζήτηση και ανάλυση δεδομένων βασισμένη σε κινητούς πράκτορες μπορεί να μειώσει την κίνηση δικτύου που προκύπτει από τη μεταφορά μεγάλων όγκων δεδομένων μέσω ενός δικτύου για τοπική επεξεργασία. Αντί να μεταφέρονται τα δεδομένα μέσα στο δίκτυο, οι κινητοί πράκτορες μπορούν να μεταφερθούν στο μηχάνημα που είναι αποδέκτης των δεδομένων, στην ουσία μεταφέροντας τον υπολογιστή στα δεδομένα και όχι τα δεδομένα στον υπολογιστή, έτσι μειώνεται το φόρτο δικτύου σε ένα τέτοιο σενάριο. Γενικά μεταφέροντας έναν agent που είναι μικρότερος σε μέγεθος από τα δεδομένα , μειώνεται ο φόρτος του δικτύου. Αυτό άλλωστε είναι και τα πλεονεκτήματα όταν γίνεται σύγκριση μεταξύ ενός ελαφριού κρυπτογραφημένου κινητού πράκτορα, έχοντας να μεταφερθούν μεγάλος όγκος δεδομένων. Τα πλεονεκτήματα βέβαια αυτά δεν μπορούν να υπάρξουν εάν δεν υπάρχουν μηχανισμοί ασφαλείας, αφού το ρίσκο να έχουν κάποιοι πρόσβαση σε δημόσια δεδομένα μέσω καλά ορισμένων διεπαφών είναι μικρό σε αντίθεση με κάποιον κινητό κώδικα που έχει πρόσβαση σε τοπικούς πόρους.

Για παράδειγμα, κάθε web site στο internet μπορεί να εκτελέσει οποιαδήποτε αναζήτηση-ερώτηση σε κάποια μηχανή αναζήτησης όπως το yahoo ή το google, ή να πάρει τις τελευταίες τιμές τρων μετοχών από το web site του NASDAQ, εάν και στη πράξη αυτό δε μπορεί να γίνει για εμπορικές χρήσεις χωρίς κάποιον μηχανισμό ασφαλείας. Αυτό είναι εφικτό γιατί οι παράμετροι που

υπάρχουν στην ερώτηση είναι καλά ορισμένες και πλήρως κατανοητές από τον διακομιστή και η ερώτηση εμπεριέχει ένα μικρό ρίσκο σε κάποιο ασφαλές περιβάλλον ή στο επιχειρηματικό περιβάλλον του παρόχου της πληροφορίας. Εάν όμως κάποιος ήθελε να κάνει μια ανάλυση μεγάλου όγκου δεδομένων σε σχέση με τις ονομαστικές μετοχές που υπάρχουν στον server NASDAQ , οι διαχειριστές θα μπορούσαν να απαγορεύσουν το κώδικα κάποιου άλλου να εκτελείται στα δικά τους μηχανήματα

Ολοκληρώνοντας θα πρέπει να αναφερθεί ότι ο υπολογισμός των πλεονεκτημάτων που αποκομίζονται από τη χρήση κινητών πρακτόρων στη μείωση του φόρτου του δικτύου θα πρέπει να γίνει σε συνδυασμό με το πλαίσιο ασφαλείας των κινητών πρακτόρων

2.7.3 Ασύγχρονη εκτέλεση και αυτονομία

Μεγάλη έμφαση έχει δοθεί στη χρήση κινητών πρακτόρων σε κινητές συσκευές όπως είναι τα κινητά τηλέφωνα, τα pda, τα ηλεκτρονικά στις αυτοκινητοβιομηχανίες καθώς και σε στρατιωτικό εξοπλισμό. Η ασύγχρονη εκτέλεση τους και η αυτονομία τους, τους κάνει χρήσιμους σε εφαρμογές που χρησιμοποιούν ασταθή ή ακριβά δίκτυα. Ένας κινητός πράκτορας μπορεί να ξεκινήσει και να συνεχίσει τη λειτουργία του ακόμα και όταν το μηχάνημα που τον έθεσε σε λειτουργία δε είναι πλέον συνδεδεμένο με το δίκτυο.

Βέβαια παρόλο που ένας κινητός πράκτορας μπορεί να έχει αυτονομία στις κινήσεις του, χωρίς να εξαρτάται από τον host που ξεκίνησε, πολλές φορές χρειάζεται το host για να του προσφέρει υπηρεσίες ασφαλείας όπως για παράδειγμα, ένα κινητός πράκτορας στο ηλεκτρονικό εμπόριο θα πρέπει για να ολοκληρώσει μια συναλλαγή του να χρησιμοποιήσει την ηλεκτρονική του υπογραφή. Οι κινητοί πράκτορες δεν μπορούν να περιέχουν με ασφάλεια το προσωπικό τους κλειδί, και πρέπει να επικοινωνούν με την οικεία πλατφόρμα τους , ή με κάποια άλλη έμπιστη πλατφόρμα για να τους παρέχει αυτή την υπηρεσία.

Εάν κάποιος κινητός πράκτορας εκτελεί κάποια συναλλαγή που επιβάλλει τη χρήση ηλεκτρονικής υπογραφής, θα πρέπει να μπορέσει να επικοινωνήσει είτε με τη πλατφόρμα του, είτε με κάποια άλλη έμπιστη πλατφόρμα. Για παράδειγμα σε μια ηλεκτρονική δημοπρασία, εάν κάποιος agent δεν μπορεί να επικοινωνήσει με την οικεία πλατφόρμα για να παρέχει μια ηλεκτρονική υπογραφή, δε μπορεί να απαιτήσει από τους άλλους agent να μην κάνουν προσφορές μέχρι να λύσει το πρόβλημα του. Στο παραπάνω παράδειγμα γίνεται φανερό ότι παρόλο που ο πράκτορας έχει αυτονομία στις κινήσεις του, η εξάρτηση του από την οικεία πλατφόρμα για λόγους ασφαλείας, μειώνει αυτή την αυτονομία.

Οι κινητοί πράκτορες, συνήθως φορτώνουν δυναμικά τα αρχεία κλάσεων που χρειάζονται από την οικεία πλατφόρμα, κάτι βέβαια που έχει συνέπειες ασφαλείας. Εάν η οικεία πλατφόρμα δεν είναι διαθέσιμη , αυτά τα αρχεία κλάσεων παρέχονται από την πλατφόρμα που φιλοξενούνται ή πρέπει να βρεθούν και να μεταφερθούν από κάποια άλλη έμπιστη απομακρυσμένη πλατφόρμα. Οι κλάσεις που φορτώνονται από μια απομακρυσμένη πλατφόρμα ή από την πλατφόρμα που φιλοξένει το πράκτορα προκαλούν πολλά ζητήματα ασφαλείας. Τα αρχεία κλάσεων μπορεί να έχουν τροποποιηθεί με τέτοιο τρόπο που να επηρεάζεται η λειτουργία του agent ή να επιτρέπουν την λαθρακρόσαη (eavesdropping) σε όλες τις συναλλαγές που πραγματοποιεί ο agent. Τέλος μπορεί να υπάρξουν προβλήματα με τις εκδόσεις των κλάσεων τα οποία μπορούν να προκαλέσουν μη προβλέψιμα αποτελέσματα

2.7.4 Δυναμική προσαρμογή

Οι κινητοί πράκτορες έχουν την ικανότητα να αντιλαμβάνονται το περιβάλλον που εκτελούνται και να μπορούν άμεσα να προσαρμοστούν στις αλλαγές. Έτσι εάν για παράδειγμα ο υπολογιστικός φόρτος σε κάποια πλατφόρμα είναι πολύ υψηλός και δεν καλύπτει τις απατήσεις του agent, ο agent μπορεί να μετακινηθεί σε κάποιον άλλο μηχανισμό που θα μπορέσει να καλύψει καλύτερα τις ανάγκες του

Οι κινητοί πράκτορες μπορούν να διανέμονται ανάμεσα στους διάφορες οικοδεσπότες μέσα στο δίκτυο με τέτοιο τρόπο ώστε να διατηρήσουν τις βέλτιστες ρυθμίσεις για την επίλυση κάποιου συγκεκριμένου προβλήματος.

Όσο διαρκεί η μετακίνηση τους στους hosts εντός του ίδιου τομέα ασφάλειας και κάθε τομέας ασφάλειας τοποθετεί τον πράκτορα κάτω από τις ίδιες πολιτικές ασφαλείας, δίνοντας του ή αποκλείοντας του τα ίδια δικαιώματα με τη προηγούμενη πλατφόρμα, τα θέματα ασφαλείας δεν επηρεάζουν την ικάνονοτητα των agent για τη δυναμική προσαρμογή στο περιβάλλον εκτέλεσης. Εάν όμως ο κινητός πράκτορας μετακινηθεί εκτός του υπάρχοντος τομέα ασφάλειας και γίνει αντικείμενο νέων πολιτικών ασφαλείας , τότε η προσαρμοστικότητα του θα επηρεαστεί και συνήθως θα περιοριστεί από τις πολιτικές ασφάλειας των άλλων πλατφόρμων.

Οι πλατφόρμες κινητών πρακτόρων, θα πρέπει να μπορούν να ενημερώνουν τους agents με τις πολιτικές ασφαλείας τους, και οι agents θα πρέπει να μπορούν να αξιολογούν διάφορες πολιτικές ασφάλειας σε σχέση με τους υπάρχοντας πόρους, πριν αποφασίσουν το επόμενο βήμα τους. Η επικοινωνία, η διαπραγμάτευση και η διαχείριση των πολιτικών ασφάλειας των κινητών πρακτόρων, απαιτεί επίσης νέο διαχειριστικό κόστος ασφάλειας για τη πλατφόρμα των agents

2.7.5 Λειτουργία σε ετερογενή περιβάλλοντα

Οι κινητοί πράκτορες είναι ανεξάρτητοι από το επίπεδο μεταφοράς και υπολογιστή και εξαρτώνται μόνο από τα περιβάλλοντα που εκτελούνται. Για τον παραπάνω λόγο αποτελούν μια πολύ καλή προσέγγιση για την ολοκλήρωση ετερογενών συστημάτων. Η δυνατότητα των κινητών πρακτόρων να λειτουργούν σε ετερογενή υπολογιστικά περιβάλλοντα καθίσταται δυνατή με εικονικά μηχανήματα ή ενδιάμεσους διερμηνείς στην host πλατφόρμα

Τα πλεονεκτήματα της ετερογένειας, όμως δημιουργούν νέα θέματα ασφάλειας. Οι σημερινές υλοποιήσεις των εικονικών μηχανημάτων ή των ενδιάμεσων διερμηνέων μπορεί να κάνουν τα ετερογενή περιβάλλοντα αξιοποιήσιμα, όμως δεν παρέχουν επαρκή υποστήριξη για διαχείριση πόρων. Η Java παραδείγματος χάριν δε παρέχει κάποιο τρόπο στον οικοδεσπότη να μειώσει τους πόρους μνήμης και επεξεργασίας που έχουν κατανεμηθεί σε κάποιο αντικείμενο ή νήμα και είναι έτσι επιρρεπές σε επιθέσεις άρνησης υπηρεσίας . Ένα σχετικό θέμα είναι η ικανότητα του agent να κατανέμει τους πόρους εξωτερικά στο πρόγραμμα για παράδειγμα ανοίγοντας αρχεία και sockets και παράγοντας παράθυρα.

Επιπλέον το υπάρχον Java VM δε προσφέρει καμία ασφάλεια από πηγές στις δημόσιες μεθόδους κάποιου αντικειμένου. Οι δημόσιοι μέθοδοι κάποιου αντικειμένου και τα δεδομένα στα οποία παρέχουν πρόσβαση, είναι διαθέσιμα σε οποιοδήποτε άλλο αντικείμενο έχει κάποια αναφορά σε αυτές. Δεν υπάρχει στη πραγματικότητα κανένας τρόπος για κάποιον πράκτορα, να γνωρίζει κατευθείαν και πολύ περισσότερο να ελέγξει ποιοι άλλοι πράκτορες έχουν πρόσβαση στις μεθόδους του

2.7.6. Ανθεκτικότητα σε σφάλματα

Η ικανότητα των κινητών πρακτόρων να αντιδρούν δυναμικά σε δυσμενής καταστάσεις και γεγονότα, βοηθάει στη δημιουργία ισχυρών και ανεκτικών σε σφάλματα κατανεμημένων συστημάτων. Εάν για παράδειγμα κάποιος οικοδεσπότης τερματίσει τη λειτουργία του, όλοι οι πράκτορες που εκτελούνται σε αυτόν, ενημερώνονται και έχουν χρόνο να αποσπαστούν και να ολοκληρώσουν την λειτουργία τους σε κάποιον άλλο οικοδεσπότη στο δίκτυο. Η δυνατότητα των κινητών πρακτόρων να κινούνται από τη μία πλατφόρμα στην άλλη σε ετερογενή περιβάλλοντα, όπως αναφέρθηκε και παραπάνω γίνεται με τη χρήση εικονικών μηχανημάτων και ενδιάμεσων διερμηνέων .

Τα εικονικά μηχανήματα και οι διερμηνείς όμως, μπορούν να προσφέρουν περιορισμένη υποστήριξη για τη διαφύλαξή ή την επανάληψη του σταδίου της εκτέλεσης σε ετερογενή

περιβάλλοντα, λόγω των διαφορετικών παραστάσεων στο υποκείμενο υλικό. Η Java για παράδειγμα δε μπορεί να γνωρίζει το στάδιο πλήρους εκτέλεσης ενός αντικειμένου και έχει περιορισμούς σε άλλες πληροφορίες .

Συμβατική ανάκαμψη από λάθη και τεχνικές σημείων επαναφοράς όπως άλλωστε έχει προαναφερθεί δε μπορούν να βρουν χρήση σε κινητούς πράκτορες. Παρόλο που υπάρχει μια πληθώρα τεχνικών που παρέχουν ασφάλεια και ανοχή σε σφάλματα, οι σχεδιαστές θα πρέπει να είναι πολύ προσεκτικοί κατά την απόφαση για χρήση κάποιου μηχανισμού και να λάβουν υπόψη τους τον πιθανό αντίκτυπο στις επιδόσεις του συστήματος και στις λειτουργίες του. Η χρήση ενός check point (σημείο ελέγχου) για παράδειγμα πριν και μετά από την άφιξη του πράκτορα, καθώς και μετά το πέρας των συναλλαγών του ή των ενεργειών του θα μπορούσε να προσφέρει μια αποδεκτή επαναφορά από κάποιο σφάλμα. Όμως με τη προσθήκη της διεργασίας για κάθε σημείο ελέγχου, καθώς επίσης και τους μηχανισμούς μη απάρνησης υπηρεσίας που χρειάζονται, αυξάνεται το φόρτο. Οι τεχνικές επαναφοράς μπορεί επίσης να χρειάζονται παραπάνω από ένα μηχάνημα κάτι που κάνει ακόμα πιο πολύπλοκη την επαναφορά.

Παρόλο που οι κινητοί πράκτορες διαθέτουν μεγάλη αυτονομία σε λειτουργίες χωρίς σύνδεση, κάποιο σφάλμα στην μητρική πλατφόρμα ή σε άλλες πλατφόρμες που ο πράκτορας αλληλεπιδρά για υπηρεσίες ασφαλείας μπορεί να μειώσει σημαντικά τις λειτουργίες του.

Οι κινητοί πράκτορες είναι πιο ανεκτικοί στα σφάλματα βάση της ικανότητας τους να μετακινούνται σε άλλη πλατφόρμα, όμως εξαρτώνται πολύ για λόγους ασφαλείας από τη μητρική πλατφόρμα ή άλλες έμπιστες πλατφόρμες. Η εξάρτηση τους αυτή συχνά, οδηγεί σε περιορισμούς στη λειτουργία τους. Οι σχεδιαστές πλατφόρμων κινητών πρακτόρων έχουν να αντιμετωπίσουν το δίλημμα μεταξύ ασφάλειας και ανοχής σε λάθη. Εάν για παράδειγμα ένα μοντέλο για να αντιμετωπίσει τους κίνδυνους από τις πολλαπλές διαδρομές των πρακτόρων, χτιστεί πάνω στο κλασσικό μοντέλο client-server, απαιτώντας από το πράκτορα πριν από κάθε νέο βήμα του να επιστρέψει στη μητρική-κεντρική πλατφόρμα, κάνει όλους τους πράκτορες να εξαρτώνται άμεσα και όχι μόνο για λόγους ασφάλειας από τη μητρική πλατφόρμα. Ένα σφάλμα ή μια δυσλειτουργία της μητρικής πλατφόρμας προκαλεί πρόβλημα σε όλους τους πράκτορες και δημιουργεί θέματα επεκτασιμότητας

2.8 Τομείς για μελλοντική έρευνα

Στις ΜΑΤ ο παραδοσιακός προσανατολισμός της κύριας υπολογιστικής μηχανής προς την ασφάλεια διατηρείται, και η εστίαση σε μηχανισμούς προστασίας εντός του παραδείγματος των κινητών πρακτόρων παραμένει. Την τρέχουσα περίοδο, υπάρχει ένας αριθμός εφαρμογών για πράκτορες όπου συμβατικοί και πρόσφατα παρουσιασθείσες τεχνικές ασφαλείας πρέπει να

αποδειχθούν επαρκείς, πριν λάβει χώρα περαιτέρω πρόοδος. Ωστόσο, πρέπει να γίνουν βελτιώσεις ασφαλείας για συστήματα πρακτόρων αφού όπως είδαμε κάθε μία από τις τεχνικές που συζητήθηκαν έχουν τα μειονεκτήματα τους και χρήζουν περαιτέρω τελειοποίησης. Οι βελτιώσεις αυτές είναι πιθανόν να εμφανιστούν από την τρέχουσα βασική γραμμή τεχνικών προστασίας, είτε μέσω αυξητικών βελτιώσεων που μειώνουν την επιβάρυνση επεξεργασίας και αποθήκευσης ή απλοποιούν τη χρήση του μηχανισμού είτε μέσω έξυπνων συνδυασμών συμπληρωματικών μηχανισμών για τη διαμόρφωση πιο αποτελεσματικών σύνθετων σχημάτων προστασίας.

Επιπροσθέτως, υπάρχουν ορισμένα θέματα που χρήζουν περαιτέρω έρευνας. Υπάρχουν πολλά άλυτα θέματα όπως η επιβάρυνση επεξεργασίας και αποθήκευσης, η παροχή ανωνυμίας, η εξακρίβωση του εάν ένας διερμηνέας δεν έχει υποστεί επέμβαση, η διασφάλιση της πλήρους εκτέλεσης του πράκτορα από το κεντρικό υπολογιστικό σύστημα και οι μηχανισμοί διάκρισης μεταξύ ενός πράκτορα και του κλώνου του. Από την ανάλυση όπως παρουσιάστηκε στην παρούσα εργασία, γίνεται αντιληπτό ότι ορισμένα πεδία μελλοντικής έρευνας στις ΜΑΤ αφορούν τα ακόλουθα:

- Η έλλειψη προηγμένων εργαλείων ανάπτυξης και μοντελοποίησης, η έλλειψη ώριμων προδιαγραφών πρακτόρων οι οποίες να επιβάλλουν διαλειτουργικότητα ή προωθούν την ολοκλήρωση των παραδοσιακών τηλεπικοινωνιών και των σύγχρονων υπολογιστικών δικτύων, και η δυσκολία βελτιστοποίησης της απόδοσης με μεταβαλλόμενα υπολογιστικά και επικοινωνιακά φορτία είναι μερικά από τα εμπόδια που περιορίζουν το σχεδιασμό και την ανάπτυξη συστημάτων κινητών πρακτόρων μεγάλης κλίμακας. Οι συγκεκριμένοι περιορισμοί επηρεάζουν επίσης το σχεδιασμό αποτελεσματικών μηχανισμών ασφαλείας και το συμβιβασμό μεταξύ λειτουργικότητας και απόδοσης.
- Απαιτείται η διενέργεια προσομοιώσεων και πειραμάτων για την αξιολόγηση των διαφορετικών μηχανισμών προστασίας που μπορούν να εφαρμοστούν σε Συστήματα Κινητών Πρακτόρων. Τα εν λόγω πειράματα (και οι προσομοιώσεις) θα μας βοηθήσουν να μετρήσουμε την ποιότητα της προστασίας που παρέχουν οι υποκείμενες λύσεις και να επιλέξουμε το βέλτιστο συνδυασμό από αυτές που θα διασφάλιζε την επίτευξη ενός επαρκούς αποτελέσματος προστασίας. Για παράδειγμα, αμφότεροι οι κρυπτογραφικοί και μη κρυπτογραφικοί μηχανισμοί ασφαλείας πρέπει να διερευνηθούν ως προς την προστασία κινητών πρακτόρων.
- Ένα άλλο ανοιχτό θέμα αφορά στη μελέτη της δυνατότητας ανίχνευσης επέμβασης στον κώδικα και στα δεδομένα του πράκτορα κατά το χρόνο εκτέλεσης. Επίσης, παραμένει εξαιρετικά ενδιαφέρον να δούμε εάν είναι δυνατή η άρση της εξάρτησης πράκτορα από διακομιστές πρακτόρων να για την εκτέλεση αλγορίθμων ελέγχου επεμβάσεων. Μία ιδέα

θα ήταν η δημιουργία ουδέτερων περιβαλλόντων εκτέλεσης κατά την επίσκεψη σε μη έμπιστους διακομιστές.

- Οι μηχανισμοί που παρέχουν ανωνυμία βρίσκονται ακόμα σε αρχικό στάδιο. Απαιτείται η πρόταση νέων και πιο αποτελεσματικών μηχανισμών προστασίας για τη διατήρηση της ανωνυμίας των χρηστών. Πρέπει να ισχύει η ανωνυμία όχι μόνο ενός αρχικού πράκτορα, αλλά και κάθε πράκτορα αποδέκτη ή των ενδιάμεσων. Οι συνήθως χρησιμοποιούμενες τεχνικές που είναι διαθέσιμες για να επιληφθεί κανείς του προβλήματος της ανωνυμίας (και πιθανώς να το επιλύσει) είναι οι επονομαζόμενες Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (Privacy-Enhancing Technologies - PETs). Μία αντιπαράθεση για τις PETs βρίσκεται σε εξέλιξη εδώ και πολλά χρόνια, αφού οι PETs χρησιμοποιούνται από εγκληματίες για να αποφεύγουν την παρακολούθηση από τους οργανισμούς αστυνόμευσης και εθνικής ασφάλειας, όμως παραμένουν μία ενδεχομένως αποτελεσματική μέθοδος για την αντιμετώπιση ζητημάτων ανωνυμίας στο βαθμό που οι αντιπαραθέσεις διευθετηθούν. Επιπλέον, από πρακτική άποψη ίσως είναι προτιμότερο να ορίζονται κεντρικά Έμπιστα Τρίτα Μέρη (Trusted Third Parties - TTPs) και μετά να καθορίζονται οι συμμετέχοντες στις τεχνικές ανωνυμίας και να ορίζονται οι μεταξύ τους σχέσεις εμπιστοσύνης, για τον προσδιορισμό των απαιτήσεων του δικτύου εμπιστοσύνης ή τη δημιουργία προτύπων εμπιστοσύνης εντός και διαμέσου κοινοτήτων πρακτόρων. Η πραγματική πρόκληση που διαφαίνεται τώρα, είναι το πως μπορεί επιτευχθεί πρακτικά η ιδιωτικότητα μέσω της ανωνυμίας, δηλαδή το πως να διατηρηθεί μία αποδεκτή καθυστέρηση και επίδοση υπό την παρουσία μηχανισμών ανωνυμίας. Ωστόσο, υπάρχει ακόμα ένα αδύνατο σημείο στις τεχνικές ανωνυμίας: το ότι εξαρτώνται από άλλους χρήστες.
- Τα θέματα εμπιστοσύνης εξακολουθούν επίσης να είναι αντικείμενο περαιτέρω έρευνας και ειδικότερα η επίσης η δυναμική εδραίωση σχέσεων εμπιστοσύνης ανάμεσα σε ενδιάμεσες πλατφόρμες και επισκεπτόμενους κόμβους. Ο δυναμικός προσδιορισμός των κόμβων εκτέλεσης απαιτεί τη δυναμική εδραίωση και επιβολή του ελέγχου πρόσβασης και την ολοκλήρωση του ελέγχου πρόσβασης με εξέταση της διαθεσιμότητας πόρων έτσι ώστε να επηρεάζει τα δρομολόγια μετανάστευσης των πρακτόρων.
- Ενώ ορισμένες εφαρμογές συστημάτων πρακτόρων ενσωματώνουν τις κατάλληλες τεχνικές ασφαλείας, συχνά δίδεται λίγη προσοχή στη διαλειτουργικότητα μεταξύ των συστημάτων πρακτόρων. Είναι σημαντικό να σχεδιαστεί ένα συνολικό πλαίσιο ασφαλείας που να ενσωματώνει συμβατές τεχνικές σε ένα αποτελεσματικό μοντέλο ασφαλείας και να παρέχει μία ομπρέλα κάτω από την οποία θα μπορούσε να υπάρξει διαλειτουργικότητα.

- Τεχνικές όπως ο συνδυασμός κρυπτογραφημένου υπολογισμού και συσκότισης για την προστασία του εκτελέσιμου κώδικα από κακόβουλους χρήστες χρήζουν βελτιστοποίησης . Ορισμένες δυνατές προσεγγίσεις για να επιτευχθεί αυτό περιλαμβάνουν: κρυπτογραφημένες συναρτήσεις συσκότισης, κρυπτογράφηση ως μέρος της διαδικασίας συσκότισης και συσκότιση ως κρυπτογράφηση. Στο βαθμό που η διάσπαση της συσκότισης είναι εφικτή, με δεδομένες ορισμένες πληροφορίες σχετικά με το αρχικό πρόγραμμα, η συσκότιση ως κρυπτογράφηση ίσως πρέπει να αποκρύπτει το στατιστικό πρότυπο του αρχικού προγράμματος. Ένας τρόπος απόκρυψης του στατιστικού προτύπου είναι η παρεμβολή διαφορετικών και ανεξάρτητων υπολογισμών. Εάν δύο τέτοιοι υπολογισμοί διαθέτουν διαφορετικά στατιστικά πρότυπα, το σύστημα-οικοδεσπότης θα μπερδευτεί. Το ερώτημα, όμως, για το εάν αυτού του είδους οι τεχνικές θα ήταν αρκετές για να καταστήσουν την συσκότιση εφικτή, ως έναν τρόπο τέλεσης κρυπτογραφημένου υπολογισμού, παραμένει ανοιχτό. Αυτό το πεδίο δείχνει ωστόσο πολλά υποσχόμενο, και συνεπώς αξίζει περαιτέρω διερεύνησης.
- Η διασφάλιση της δυνατότητας απόδοσης ευθύνης ενδεχομένως να θέσει περιορισμούς στη διαθεσιμότητα των υπηρεσιών των πλατφόρμων. Για παράδειγμα, όταν το μέσο αποθήκευσης του ημερολογίου ελέγχου (audit log) εξαντλήσει τη χωρητικότητα , πολλές πολιτικές ασφαλείας απενεργοποιούν όλες τις υπηρεσίες που δημιουργούν εγγραφές στο ημερολόγιο ελέγχου. Σε μία προσπάθεια διατήρησης της δυνατότητας απόδοσης ευθύνης, αυτή η πολιτική μπορεί ακούσια να δημιουργήσει μία ευκαιρία για επίθεση άρνησης υπηρεσίας απλώς παράγοντας ένα υπέρμετρο αριθμό ελέγξιμων γεγονότων, όπως επαναλαμβανόμενες, αποτυχημένες προσπάθειες σύνδεσης, και καταναλώνοντας το εναπομείνασα χωρητικότητα του μέσου αποθήκευσης του ημερολογίου ελέγχου. Επιπλέον, οι επιθέσεις αυτές πρέπει να αντιμετωπιστούν αποτελεσματικά με τον περιορισμό του αριθμού των εγγραφών που προέρχονται από την ίδια υπηρεσία ή με μία αποτελεσματική επέκταση της χωρητικότητας του κάθε ημερολογίου ελέγχου.
- Η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας θέτει περιορισμούς στη διαθεσιμότητα και το κόστος απόδοσης πρέπει να υπόκειται σε έλεγχο. Διερχόμενοι κρυπτογράφοντες πράκτορες και μηνύματα μπορούν να εμφανίσουν μεγάλες επεξεργαστικές επιβαρύνσεις και να επιβάλλουν μη αποδεκτές καθυστερήσεις σε περιβάλλοντα, στα οποία απαιτείται απόκριση σε σχεδόν πραγματικό χρόνο. Απαιτείται η διενέργεια μίας ποσοτικής ανάλυσης, βασισμένης σε ένα λεπτομερές μοντέλο προσομοίωσης ενός συστήματος κινητού πράκτορα για τη μέτρηση της επιρροής του ως προς την ποιότητα επικοινωνίας (προστιθέμενη καθυστέρηση για τον τελικό χρήστη) και την ανάλωση πόρων. Τα αποτελέσματα αυτής της ανάλυσης θα βοηθήσουν στην επιλογή

του ταχύτερου αλγόριθμου κρυπτογράφησης και θα αναδείξουν την ανάγκη ανάπτυξης βελτιωμένων και πιο αποτελεσματικών τρόπων κρυπτογράφησης.

3. Συμπέρασμα

Η παρούσα εργασία παρουσίασε μία αξιολόγηση των αντίμετρων ασφαλείας που εφαρμόζονται στους κινητούς πράκτορες. Τα μειονεκτήματα καθενός από τα συγκεκριμένα αντίμετρα για κινητούς πράκτορες σκιαγραφήθηκαν και σχολιάστηκαν. Γεγονός είναι ότι ο τομέας της ασφάλειας κινητών πρακτόρων είναι ανεπαρκώς ανεπτυγμένος αλλά βελτιώνεται ταχύτατα και τελευταία ιδιαίτερη έμφαση αρχίζει να δίδεται στην ανάπτυξη τεχνικών, προσανατολισμένων στην προστασία των πρακτόρων. Ενώ οι στοιχειώδεις τεχνικές ασφαλείας μπορούν να αποδειχθούν κατάλληλες για έναν αριθμό εφαρμογών που βασίζονται σε πράκτορες, πολλές νέες εφαρμογές αναμένεται να απαιτούν ένα πιο εκτενές σύνολο μηχανισμών. Προκειμένου να ανταποκριθούμε στην ανάγκη για πιο εκτενείς μηχανισμούς, είναι απαραίτητη η σχεδίαση και ανάπτυξη ενός ευέλικτου πλαισίου ασφαλείας, το οποίο θα παρέχει προηγμένες υπηρεσίες ασφαλείας. Για να επιτευχθεί αυτό απαιτείται ο καθορισμός ενός συνόλου αντίμετρων ασφαλείας το οποίο πληροί τις απαιτήσεις της φιλοσοφίας της προστασίας συστημάτων πρακτόρων και ικανοποιεί τις ανάγκες των υφιστάμενων εφαρμογών καθώς και εκείνων που θα εμφανιστούν στο μέλλον. Όμως η εδραίωση ενός τέτοιου συνόλου λύσεων ασφαλείας απαιτεί πειραματισμό και εμπειρία με εναλλακτικές επιλογές σχεδιασμού, συμπεριλαμβανομένων αυτών που προϋποθέτουν συμβιβασμούς στην απόδοση, τη δυνατότητα κλιμάκωσης και τη συμβατότητα.

Βιβλιογραφία

- Joann J. Ordille, "When Agents Roam, Who Can You Trust?" Proceedings of the First Conference on Emerging Technologies and Applications in Communications,Portland, Oregon, May 1996. <URL: http://cm.bell-labs.com/cm/cs/doc/96/5-09.ps.gz>

- Thomas Sander and Christian Tschudin, "Protecting Mobile Agents Against Malicious Hosts," in G. Vinga (Ed.), Mobile Agents and Security, Springer- Verlag, Lecture Notes in Computer Science No. 1419, 1998. <URL: http//www.icsi.berkeley.edu/~tschudin/>

- "Trusted Computer System Evaluation Criteria," Department of Defense, CSCSTD-001-83, Library No. S225 711, August 1983.

- W. Jansen, T. Karygiannis, *"NIST Special Publication 800-19: Mobile Agent Security,"* National Institute of Standards and Technology, Computer Security Division, August 1999.

- G. McGraw, E. Felten, *"Securing Java, Getting Down to Business with Mobile Code"*, Wiley, February 1999.

- M. Greenberg, J. Byington, and D. Harper, *'Mobile Agents and Security,'* IEEE Communications Magazine, July 1998, vol. 36, no. 7.

- Christopher Small and Margo Seltzer. 'A comparison of OS extension technologies', In USENIX Winter 1996.

- John Ousterhout, "Scripting: Higher-Level Programming", IEEE Computer, March 1998.

- D. Rubin and D. E. Geer, "Mobile code security," IEEE Internet Computing, 1998.

- William Farmer, Joshua Guttman, and Vipin Swarup, *"Security for Mobile Agents: Authentication and State Appraisal,"* Proceedings of the 4th European Symposium on Research in Computer Security (ESORICS '96), September 1996, pp. 118-130.

- Danny Lange and Mitsuru Oshima, Programming and Deploying Java Mobile Agents with Aglets, Addison-Wesley, 1998.

- David Chess, Benjamin Grosof, Colin Harrison, David Levine, Colin Parris, and Gene Tsudik, "Itinerant Agents for Mobile Computing," IEEE Personal Communications, vol. 2, no. 5, October 1995, pp. 34-49.

- D. Rubin and D. E. Geer, "Mobile code security," IEEE Internet Computing, 1998 Günter Karjoth, Danny B. Lange, and Mitsuru Oshima, "A Security Model For Aglets," IEEE Internet Computing, August 1997, pp. 68-77.

- Yanfeng Peng, D.J.Holding, K.J.Blow, *"A Possible Secure Solution for Mobile Agents",* Electronic Engineering, School of Engineering, Aston University, Birmingham, UK July 2004. <URL: http://www.ee.aston.ac.uk/research/acrg/papers/iawtic01.pdf >

- David Chess, Colin Harrison, and Aaron Kershenbaum, "Mobile Agents: Are They a Good Idea?" IBM Research Report RC 19887 (88465), December 1994.

- Dengfeng Gao *"Protecting Programs from Hostile Environments: Encrypted Computation, Obfuscation, and Other Techniques by Luis Sarmenta"*, October 1999

- "Trusted Computer System Evaluation Criteria," Department of Defense, CSCSTD-001-83, Library No. S225 711, August 1983.<URL: http://www.cru.fr/securite/Documents-generaux/orange.book>