ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΣΦΑΛΗ ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΠΡΑΚΤΟΡΩΝ

Διδακτορική Διατριβή

Κοτζανικολάου Παναγιώτη

Πειραιάς, Ιανουάριος 2003

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τριμελής Συμβουλευτική Επιτροπή

Επιβλέπων:
Νικόλαος Αλεξανδρής
Καθηγητής
Πανεπιστημίου Πειραιώς

Μέλη:

Βασίλειος Χρυσικόπουλος
Καθηγητής
Ιονίου Πανεπιστημίου

Χρήστος Δουληγέρης
Αναπληρωτής Καθηγητής
Πανεπιστημίου Πειραιώς

Πανεπιστήμιο Πειραιώς

Τμήμα Πληροφορικής

Διατριβή
Για την απόκτηση Διδακτορικού Διπλώματος
του Τμήματος Πληροφορικής

Κοτζανικολάου Ι. Παναγιώτη

«ΑΣΦΑΛΗ ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΠΡΑΚΤΟΡΩΝ»

Επταμελής Εξεταστική Επιτροπή

Πρόεδρος:
Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη:

Σωκράτης Κάτσικας
Καθηγητής Πανεπιστημίου Αιγαίου

Ευάγγελος Κιουντούζης
Καθηγητής Οικονομικού Πανεπιστημίου Αθηνών

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Παναγιώτης Γεωργιάδης
Αναπληρωτής Καθηγητής Πανεπιστημίου Αθηνών

Χρήστος Δουληγέρης
Αναπληρωτής Καθηγητής Πανεπιστημίου Πειραιώς

Θεμιστοκλής Παναγιωτόπουλος
Επίκουρος Καθηγητής Πανεπιστημίου Πειραιώς

Στην οικογένειά μου.

Πίνακας Περιεχομένων

Περίληψη

Με την εξέλιξη της επιστήμης της πληροφορικής έχουν προταθεί διάφορες τεχνολογίες απομακρυσμένης επικοινωνίας και υπολογισμού για την υποστήριξη των κατανεμημένων συστημάτων: από κλήσεις απομακρυσμένων διαδικασιών, μετανάστευση διαδικασιών και απομακρυσμένη εκτέλεση, μέχρι τον κινητό κώδικα και πιο πρόσφατα τους κινητούς πράκτορες. Σκοπός αυτών των τεχνολογιών είναι η βέλτιστη χρήση απομακρυσμένων υπολογιστικών πόρων, η ελάττωση του κόστους δικτύου και η ευελιξία των εφαρμογών.

Οι κινητοί πράκτορες αποτελούν μία πρόσφατη τεχνολογία κατανεμημένου υπολογισμού και απομακρυσμένης εκτέλεσης που συνδυάζει πολλά από τα πλεονεκτήματα των προηγούμενων τεχνολογιών, όπως ασύγχρονη επικοινωνία, μεταφορά κώδικα και απομακρυσμένη εκτέλεση ενώ προσφέρει και νέες προγραμματιστικές δυνατότητες όπως δυναμική συνέχιση της εκτέλεσης του κώδικα και μεταφορά της κατάστασης εκτέλεσης.

Λόγω των αυξημένων δυνατοτήτων τους, οι κινητοί πράκτορες έχουν χρησιμοποιηθεί σε διάφορα συστήματα, όπως εφαρμογές ηλεκτρονικών αγορών, δημοπρασιών και διαχείρισης δικτύων. Όμως, ο κατανεμημένος χαρακτήρας και οι αυξημένες δυνατότητές τους, καθώς και η χρήση ανοικτών δικτύων για την επικοινωνία συστημάτων κινητών πρακτόρων όπως είναι το διαδίκτυο, δημιουργούν διάφορες απειλές ασφάλειας. Οι απειλές αυτές αφορούν τόσο το περιβάλλον εκτέλεσης των κινητών πρακτόρων, όσο και τους ίδιους τους πράκτορες. Έχει συνεπώς δημιουργηθεί η ανάγκη για την ανάπτυξη συστημάτων κινητών πρακτόρων τα οποία θα παρέχουν ικανοποιητική προστασία και ασφάλεια απέναντι σε αυτές τις απειλές.

Η ερευνητική προσπάθεια που παρουσιάζεται στην παρούσα διατριβή επικεντρώθηκε σε τρία κύρια ζητήματα:

1. Την αναγνώριση των απειλών ασφάλειας των συστημάτων κινητών πρακτόρων, καθώς και των αντίστοιχων υφισταμένων λύσεων.

2. Την ανάπτυξη κρυπτογραφικών πρωτοκόλλων για την αντιμετώπιση ορισμένων από τις απειλές ασφάλειας των συστημάτων κινητών πρακτόρων, που αφορούν κυρίως την εξουσιοδότηση και τον καταλογισμό ευθύνης των κινητών πρακτόρων.

3. Την ανάπτυξη αρχιτεκτονικών ασφάλειας και μηχανισμών για την αντιμετώπιση απειλών ασφάλειας σε διάφορες ειδικές εφαρμογές χρήσης κινητών πρακτόρων.

Η έρευνα που παρουσιάζεται στην παρούσα διατριβή, φιλοδοξεί να συμβάλλει στην αντιμετώπιση των παραπάνω ζητημάτων, ενώ παράλληλα, αναλύοντας και οριοθετώντας τα ζητήματα, δημιουργεί προοπτικές για περαιτέρω έρευνα στον ίδιο ή σε συναφείς τομείς.

Ευχαριστίες

Η παρούσα διατριβή είναι το προϊόν της ερευνητικής μου προσπάθειας που πραγματοποιήθηκε στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς από το Νοέμβριο του 1998 έως σήμερα. Στην προσπάθεια αυτή συνέβαλαν αρκετοί άνθρωποι, χωρίς τη βοήθεια των οποίων δεν θα ήταν δυνατή η ολοκλήρωση της διατριβής αυτής και για αυτό το λόγο θα ήθελα να τους ευχαριστήσω.

Αρχικά θα ήθελα να ευχαριστήσω την Τριμελή Επιτροπή που είχε την εποπτεία της διατριβής μου:

Τον Καθηγητή Βασίλειο Χρυσικόπουλο, ο οποίος υπήρξε Επιβλέπων Καθηγητής τα δύο πρώτα χρόνια εκπόνησης της διατριβής. Τον ευχαριστώ για την ερευνητική καθοδήγηση που μου προσέφερε από τα πρώτα βήματα εκπόνησης της διατριβής και για τη συνεχή του βοήθεια.

Τον Επιβλέποντα Καθηγητή της διατριβής Νικόλαο Αλεξανδρή, για τη συνεχή και ουσιαστική υποστήριξή του σε όλη μου την προσπάθεια, καθώς και για τις πολύτιμες συμβουλές του ως επιστήμονας και δάσκαλος.

Τον Αναπληρωτή Καθηγητή Χρήστο Δουληγέρη, για τη συμπαράσταση και τις συμβουλές του. Η συνεργασία μαζί του με βοήθησε ουσιαστικά στη διεύρυνση της ερευνητικής μου προσπάθειας σε πολλούς νέους τομείς.

Επίσης, θα ήθελα να ευχαριστήσω ιδιαίτερα τον Καθηγητή Mike Burmester για την πολύτιμη επιστημονική συμβολή, τη βοήθεια και τις συμβουλές του καθ' όλη τη διάρκεια εκπόνησης της διατριβής. Η συνεργασία μαζί του τόσο σε ερευνητικό όσο και σε γενικότερο επίπεδο μου προσέφερε πάντα ιδιαίτερη χαρά.

Επίσης, θα ήθελα να ευχαριστήσω την Εξεταστική Επιτροπή της διατριβής η οποία αποτελείται, πέραν από τα μέλη της Συμβουλευτικής Επιτροπής, από τους Καθηγητές Σωκράτη Κάτσικα και Ευάγγελο Κιουντούζη και τους Αναπληρωτές Καθηγητές Παναγιώτη Γεωργιάδη και Θεμιστοκλή Παναγιωτόπουλο. Τους ευχαριστώ για την τιμή που

μου κάνουν με τη συμμετοχή τους, καθώς και για τη διάθεση της πολύτιμης εμπειρίας και του χρόνου τους για την επιστημονική κρίση και εξέταση της διατριβής.

Ακόμα, θα ήθελα να ευχαριστήσω τους κριτές των επιστημονικών συνεδρίων και περιοδικών στα οποία συμμετείχα μέσω της υποβολής ερευνητικών εργασιών για τα πολύτιμα σχόλια και τις παρατηρήσεις τους, οι οποίες ήταν πολύ χρήσιμες για τη βελτίωση της προσπάθειάς μου.

Πολλοί άλλοι άνθρωποι προσέφεραν σημαντική βοήθεια στην προσπάθεια εκπόνησης αυτής της διατριβής. Θα ήθελα να ευχαριστήσω την αδελφή μου Έλσα και τη φίλη και συνάδελφο Μαριλένα Παρασκευά για τις ουσιώδεις παρατηρήσεις τους στο κείμενο της διατριβής. Επίσης τον φίλο Γιάννη Τασούλα για την βοήθειά του στην επιμέλεια της ηλεκτρονικής επεξεργασίας της διατριβής.

Ευχαριστώ επίσης τους φίλους και συναδέλφους υποψήφιους διδάκτορες Γιάννη Παπαδάκη, Εμμανουήλ Μάγκο, Ρόζα Μαυροπόδη, Σπύρο Βοσινάκη, Κατερίνα Μητροκώτσα, Βικτώρια Τσιρίγκα, Μαρία Μουντρίδου, Κατερίνα Καμπάση, Γιάννη Καλλιγκάτση και Γιάννη Ανδρέου για τις ευχάριστες στιγμές που περάσαμε κατά τη διάρκεια της παρουσίας μας στο Τμήμα. Τέλος, θα ήθελα να ευχαριστήσω όλους όσοι βοήθησαν άμεσα ή έμμεσα στη δημιουργία των κατάλληλων συνθηκών για την ολοκλήρωση της διατριβής.

Παναγιώτης Κοτζανικολάου

Πειραιάς, Ιανουάριος, 2003

Κεφάλαιο 1

Εισαγωγή

Στο κεφάλαιο αυτό περιγράφονται εισαγωγικές έννοιες σχετικά με την τεχνολογία των κινητών πρακτόρων, τα βασικά χαρακτηριστικά τους καθώς επίσης και τα προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων. Στη συνέχεια αναφέρονται το αντικείμενο και οι στόχοι που διαπραγματεύεται η παρούσα διατριβή. Τέλος, παρουσιάζεται η δομή της διατριβής και περιγράφεται συνοπτικά η συνεισφορά της στο ερευνητικό πεδίο της ασφάλειας των κινητών πρακτόρων.

1.1 Επικοινωνία σε κατανεμημένα συστήματα

Πρώιμες Τεχνολογίες. Τα πρώτα κατανεμημένα συστήματα βασίζονταν σε *στατικές διεργασίες* οι οποίες εκτελούνταν σε απομακρυσμένους εξυπηρετητές και επικοινωνούσαν με σύγχρονες ή ασύγχρονες μεθόδους επικοινωνίας, π.χ. μέσω κλήσεων απομακρυσμένων διαδικασιών (RPC – Remote Procedure Calls). Όμως, οι συχνές κλήσεις απομακρυσμένων διαδικασιών κοστίζουν σε εύρος ζώνης δικτύου, το οποίο κόστος γίνεται μεγαλύτερο όσο αυξάνει και το πλήθος των απομακρυσμένων κλήσεων.

Για την ελάττωση αυτού του κόστους, τα πρώτα κατανεμημένα συστήματα υιοθέτησαν μία μέθοδο γνωστή ως *μετανάστευση διαδικασίας* (process migration), κατά την οποία μία διαδικασία μπορούσε να μεταφερθεί από έναν υπολογιστή σε έναν άλλο

ώστε να εκτελεστεί εκεί τοπικά, χωρίς απομακρυσμένες κλήσεις. Η μετανάστευση διαδικασιών παρόλο που βοήθησε στην ελάττωση του κόστους επικοινωνίας, δεν επέτρεπε την εύκολη επιστροφή δεδομένων, όπως αποτελέσματα υπολογισμών, χωρίς την επιστροφή ολόκληρης της διαδικασίας.

Η δυνατότητα αυτή έγινε δυνατή με τη χρήση της μεθόδου *απομακρυσμένης αποτίμησης* (remote evaluation), σύμφωνα με την οποία αιτήσεις εκτέλεσης αποστέλλονται με τη μορφή προγραμμάτων. Μετά τη λήψη μιας τέτοιας αίτησης, ο υπολογιστής εκτελεί το πρόγραμμα χρησιμοποιώντας τους τοπικούς πόρους του (μνήμη, επεξεργαστή κ.τ.λ.) και τελικά επιστρέφει τα αποτελέσματα στον αποστολέα.

Κινητός Κώδικας. Οι τεχνολογίες *κινητού κώδικα* (mobile code), στηριζόμενες σε τεχνικές αντικειμενοστρεφούς προγραμματισμού, επέκτειναν τη μέθοδο απομακρυσμένης αποτίμησης. Οι κινητοί κώδικες μπορούν να μεταναστεύσουν από έναν υπολογιστή σε έναν άλλο μεταφέροντας εκτελέσιμο κώδικα, δεδομένα με τη μορφή ιδιοτήτων αντικειμένων και πιθανώς άλλα, ενσωματωμένα εκτελέσιμα αντικείμενα. Διακρίνονται δύο κατηγορίες τεχνολογιών κινητού κώδικα: *ασθενείς* και *ισχυρές* [109].

Οι ασθενείς τεχνολογίες κινητού κώδικα παρέχουν την υποδομή για απομακρυσμένη εκτέλεση κώδικα. Επιτρέπουν σε εφαρμογές να στέλνουν κώδικα σε ένα απομακρυσμένο υπολογιστή ώστε να εκτελεστεί εκεί τοπικά, ή να ανακτήσουν και να συνδέσουν δυναμικά κώδικα από μία απομακρυσμένη τοποθεσία, ώστε να τον εκτελέσουν τοπικά. Ο μεταφερόμενος κώδικας μπορεί να περιλαμβάνει κάποια δεδομένα εκκίνησης αλλά όχι την κατάσταση εκτέλεσης. Παραδείγματα τέτοιων τεχνολογιών είναι τα Java applets [89], τα ActiveX controls [88] και η πλατφόρμα Aglets [57]. Από την άλλη πλευρά, οι ισχυρές τεχνολογίες κινητού κώδικα παρέχουν την υποδομή για την εκτέλεση κινητών πρακτόρων.

Κινητοί Πράκτορες. Οι *κινητοί πράκτορες* (mobile agents), εκτός από το τμήμα κώδικα και τα δεδομένα, τα οποία αποτελούν τη στατική περιγραφή της συμπεριφοράς ενός υπολογισμού, χαρακτηρίζονται από την *κατάσταση εκτέλεσης* (execution state), η οποία περιλαμβάνει πληροφορία σχετικά με την κατάσταση του υπολογισμού όπως είναι η στοίβα κλήσεων και ο δείκτης εντολών. Συγκεκριμένα, ένας κινητός πράκτορας ο οποίος εκτελείται σε έναν δικτυακό υπολογιστή μπορεί να σταματήσει την εκτέλεσή του, να μετατραπεί σε μορφή κατάλληλη για μετανάστευση μέσω του δικτύου (serialization) και να συνεχίσει την εκτέλεσή του μετά τη μεταφορά του σε κάποιον άλλο υπολογιστή. Από αυτή την άποψη, οι κινητοί πράκτορες διαφέρουν από τον κινητό κώδικα στο γεγονός ότι έχουν τη δυνατότητα μεταφοράς και διατήρησης της κατάστασης εκτέλεσης κατά τη μεταφορά τους από υπολογιστή σε υπολογιστή [112]. Ο παραλήπτης υπολογιστής, συνεχίζει την εκτέλεση του πράκτορα από την εντολή η οποία ακολουθεί την κλήση της διαδικασίας μετανάστευσης. Αυτό επιτρέπει στους κινητούς πράκτορες να μεταναστεύουν και να εκτελούνται διαδοχικά σε διάφορους υπολογιστές μέχρις ότου να ολοκληρώσουν έναν κατανεμημένο υπολογισμό. Με αυτόν τον τρόπο μπορούν να εκμεταλλευτούν αποδοτικότερα κατανεμημένους πόρους και τεχνολογίες. Παραδείγματα ισχυρών κινητών τεχνολογιών αποτελούν μεταξύ άλλων οι πλατφόρμες Grasshopper [58] και Voyager [95].

Οι *ευφυείς πράκτορες* μπορούν να κάνουν χρήση "έξυπνων" αλγορίθμων και μεθόδων της τεχνολογίας γνώσης, οι οποίες τους επιτρέπουν να παίρνουν αποφάσεις σχετικά με την εκτέλεσή τους μέσα από την αλληλεπίδρασή τους με το περιβάλλον εκτέλεσης. Ένας ευφυής πράκτορας μπορεί για παράδειγμα να αποφασίζει δυναμικά για τη διαδρομή που θα ακολουθήσει, ανάλογα με δυναμικά δημιουργούμενες απαιτήσεις της εφαρμογής. Είναι προφανές ότι η δυνατότητα μεταφοράς και η ευφυΐα

ενός πράκτορα είναι ορθογώνια ζητήματα. Συνεπώς οι εφαρμογές πρακτόρων μπορούν να συνδυάζουν αυτές τις δύο ιδιότητες σε μικρότερο ή μεγαλύτερο βαθμό. Η παρούσα διατριβή ασχολείται με το χαρακτηριστικό της μεταφερσιμότητας των πρακτόρων και των προβλημάτων ασφάλειας που δημιουργούνται από αυτή την ιδιότητα σε εφαρμογές κινητών πρακτόρων που αφορούν κυρίως το Ηλεκτρονικό Εμπόριο.

Χαρακτηριστικά κινητών πρακτόρων. Οι κινητοί πράκτορες μπορούν να μειώσουν το κόστος στο εύρος ζώνης δικτύου συγκρινόμενοι με τις παλαιότερες μεθόδους κατανεμημένης επικοινωνίας. Για παράδειγμα, οι κινητοί πράκτορες ελαττώνουν την κίνηση του δικτύου σε εφαρμογές που επεξεργάζονται μεγάλες ποσότητες δεδομένων. Στις εφαρμογές που στηρίζονται στο μοντέλο *πελάτη-εξυπηρετητή* (client-server) για τη μεταφορά εργασίας σε ένα απομακρυσμένο υπολογιστή, επικρατεί η άποψη ότι είναι σημαντικότερο να μεταφέρονται τα δεδομένα στο εκτελέσιμο πρόγραμμα. Η τεχνολογία των κινητών πρακτόρων επεκτείνει το μοντέλο αυτό, παρέχοντας κατά περίπτωση τη δυνατότητα αποστολής του προγράμματος στα δεδομένα. Αυτό επιτρέπει τη σχεδίαση αποδοτικότερων εφαρμογών μεγάλης κλίμακας (scalability). Ανάλογα με τις ανάγκες κάθε συγκεκριμένης εφαρμογής μπορεί να επιλέγεται η μεταφορά του κώδικα στα δεδομένα ή αντίστροφα.

Οι κινητοί πράκτορες αυξάνουν την *αυτονομία* των εφαρμογών (autonomy), αφού μπορούν να αποφασίσουν μόνοι τους για το χρόνο και τον τόπο μετανάστευσής τους, βασιζόμενοι σε *μετα-δεδομένα μετακίνησης* (mobility metadata). Το χαρακτηριστικό της αυτονομίας συμβάλλει και στην βελτίωση του κόστους δικτύου, εφόσον η αλληλεπίδραση ενός πράκτορα με την πηγή προέλευσής του ελαττώνεται στην απολύτως απαραίτητη.

Οι τεχνολογίες κινητών πρακτόρων, παρέχουν επίσης τη δυνατότητα για ασύγχρονη επικοινωνία. Για πρόσβαση σε απομακρυσμένες εφαρμογές, ένας χρήστης μπορεί να

αποστείλει ένα κινητό πράκτορα στον απομακρυσμένο υπολογιστή όπου βρίσκεται ο κώδικας και στη συνέχεια να αποσυνδεθεί από το δίκτυο. Για την υποστήριξη αυτής της συμπεριφοράς χρησιμοποιείται ένας μηχανισμός αποθήκευσης και προώθησης του πράκτορα.

1.2 Εφαρμογές κινητών πρακτόρων

Ανεκτικότητα σε λάθη. Λόγω των χαρακτηριστικών της μεταφοράς, της αυτονομίας και της ασύγχρονης επικοινωνίας, οι κινητοί πράκτορες μπορούν να χρησιμοποιηθούν για να παρέχουν *ανεκτικότητα σε λάθη δικτύου* (network fault tolerance). Οι κινητοί πράκτορες μπορούν να προσαρμόζονται ταχύτατα σε αλλαγές τόσο της κατάστασης προγράμματος όσο και του περιβάλλοντος του δικτύου – όπως είναι η κατάτμηση του δικτύου και οι αποσυνδεδεμένοι υπολογιστές, για να τροποποιήσουν τη διαδρομή τους. Αυτό το χαρακτηριστικό κάνει την τεχνολογία των κινητών πρακτόρων κατάλληλη για την προστασία κρίσιμων εφαρμογών από σφάλματα που προέρχονται από αναξιόπιστα δίκτυα.

Απομακρυσμένη ανανέωση. Οι κινητοί πράκτορες μπορούν να χρησιμοποιηθούν επίσης για την αποδοτική ανανέωση απομακρυσμένων υπηρεσιών σε κατανεμημένες εφαρμογές. Για παράδειγμα, ένας κινητός πράκτορας μπορεί να σταλεί από ένα κεντρικό σημείο ελέγχου για την ανανέωση των λειτουργιών των κόμβων ενός δικτύου.

Διαλειτουργικότητα. Οι κινητοί πράκτορες επεκτείνουν τη διαλειτουργικότητα σε κατανεμημένα περιβάλλοντα. Εφαρμογές μπορούν να εκτελούνται σε διαφορετικές πλατφόρμες και λειτουργικά συστήματα και να επικοινωνούν μέσω κινητών πρακτόρων.

Συμπαγής επικοινωνία και συνδέσεις χαμηλού εύρους. Οι κινητοί πράκτορες είναι κατάλληλοι για εφαρμογές που απαιτούν *συμπαγή επικοινωνία* (robustness) μέσα από μη αξιόπιστα δίκτυα και συνδέσεις χαμηλού εύρους ζώνης δικτύου [112]. Παραδείγματα εφαρμογών τους περιλαμβάνουν μεταξύ άλλων, διαχείριση δικτύων [18, 26], εφαρμογές ηλεκτρονικού εμπορίου [93] και ηλεκτρονικές δημοπρασίες [84].

1.3 Προβλήματα και απειλές ασφάλειας

Παρόλο που η τεχνολογία κινητού πράκτορα επεκτείνει τις δυνατότητες των παραδοσιακών μεθόδων απομακρυσμένης επικοινωνίας και κατανεμημένου υπολογισμού, δημιουργεί προβλήματα ασφάλειας. Τα συστήματα εκείνα τα οποία χρησιμοποιούν κινητούς πράκτορες, είναι εκτεθειμένα σε διάφορες *απειλές ασφάλειας*.

Σημείωση 1.3.1. *Στη συνέχεια της παρούσας διατριβής, οι έννοιες υπολογιστής εκτέλεσης, περιβάλλον εκτέλεσης, διακομιστής και εξυπηρετητής θα χρησιμοποιούνται εναλλακτικά για να περιγράψουν υπολογιστές που παρέχουν περιβάλλον εκτέλεσης σε κινητούς πράκτορες, εκτός εάν δηλώνεται διαφορετικά κατηγορηματικά.*

Οι απειλές ασφάλειας μπορούν να ομαδοποιηθούν σε τρεις κατηγορίες: απειλές από κακόβουλους πράκτορες, απειλές από κακόβουλους υπολογιστές εκτέλεσης και απειλές κατά τη διάρκεια της μετανάστευσης των πρακτόρων. Παρακάτω περιγράφονται αναλυτικά αυτές οι απειλές.

1. **Απειλές από κακόβουλους πράκτορες.**

   Όπως αναφέρθηκε στην ενότητα 1.1, οι κινητοί πράκτορες μεταφέρουν δεδομένα και εκτελέσιμο κώδικα. Συνεπώς, κακόβουλοι πράκτορες μπορεί να χρησιμοποιηθούν για να προκαλέσουν διάφορες επιθέσεις στους υπολογιστές που

εκτελούνται. Για παράδειγμα, άρνηση εξυπηρέτησης, μη-εξουσιοδοτημένη προσπέλαση / τροποποίηση δεδομένων και μεταφορά ιών και Δούρειων ίππων. Αναλυτικότερα, οι επιθέσεις αυτές περιλαμβάνουν:

- *Πλαστοπροσωπία* (impersonation) και *μεταμφίεση* (masquerading). Σε περίπτωση έλλειψης μεθόδων αυθεντικοποίησης, κακόβουλοι πράκτορες μπορούν να προσποιηθούν ότι προέρχονται από έμπιστες πηγές, ώστε να αποκτήσουν πρόσβαση στο περιβάλλον εκτέλεσης. Επίσης, σε περίπτωση έλλειψης μεθόδων ελέγχου προσπέλασης, κακόβουλοι πράκτορες μπορεί να εκτελεστούν με περισσότερα από τα αναμενόμενα δικαιώματα, ώστε να αποκτήσουν μη-εξουσιοδοτημένη πρόσβαση σε εμπιστευτικά δεδομένα, προγράμματα ή άλλους πόρους του συστήματος, ή να προκαλέσουν μη-εξουσιοδοτημένη τροποποίησή τους.
- *Άρνηση εξυπηρέτησης* (denial-of-service). Τέτοιες επιθέσεις μπορεί να προκληθούν με διάφορους τρόπους, όπως για παράδειγμα με τη δέσμευση μεγάλου αριθμού υπολογιστικών πόρων. Ένας κακόβουλος πράκτορας μπορεί να εκκινήσει μεγάλο αριθμό TCP/IP συνδέσεων με άλλους απομακρυσμένους υπολογιστές, ώστε να παρεμποδίσει τη δημιουργία άλλων απομακρυσμένων συνδέσεων. Το ίδιο αποτέλεσμα μπορεί να προκληθεί από κακόβουλους πράκτορες που καταναλώνουν μεγάλη ποσότητα της μνήμης του υπολογιστή στον οποίο εκτελούνται, ή από επιθέσεις μέσω ιών.
- *Παρακολούθηση* (eavesdropping). Κακόβουλοι πράκτορες ενεργώντας ως Δούρειοι ίπποι, μπορεί να λειτουργήσουν ως παθητικοί ωτακουστές, είτε παρακολουθώντας την επικοινωνία του υπολογιστή εκτέλεσης με άλλους

υπολογιστές και προγράμματα, είτε προσπαθώντας να προσπελάσουν εμπιστευτική πληροφορία, αποθηκευμένη στον υπολογιστή εκτέλεσης. Επίσης μπορεί να λειτουργήσουν ως ενεργοί ωτακουστές, προσπαθώντας να αποστείλουν αυτή την πληροφορία σε έναν απομακρυσμένο προορισμό.

2. **Απειλές από κακόβουλους υπολογιστές εκτέλεσης.**

Οι κινητοί πράκτορες στηρίζονται για την εκτέλεσή τους, στους πόρους των υπολογιστών στους οποίους μεταναστεύουν. Για αυτό το λόγο, οι κινητοί πράκτορες είναι ευάλωτοι σε διάφορες επιθέσεις που μπορεί να προέρχονται από ένα κακόβουλο υπολογιστή εκτέλεσης.

- *Πλαστοπροσωπία* (impersonation) και *μεταμφίεση* (masquerading). Σε περίπτωση έλλειψης μεθόδων αυθεντικοποίησης πριν την μετανάστευση ενός πράκτορα σε έναν υπολογιστή, ένας εχθρικός υπολογιστής μπορεί να προσποιηθεί ότι αποτελεί κάποιον έμπιστο προορισμό.
- *Άρνηση εξυπηρέτησης* (denial-of-service). Είναι φανερό ότι ένας υπολογιστής εκτέλεσης μπορεί να αρνηθεί την παροχή πόρων για την εκτέλεση ενός πράκτορα ή να αρνηθεί τη μετανάστευση ενός πράκτορα σε κάποιον άλλο υπολογιστή και να τερματίσει την εκτέλεσή του.
- *Παρακολούθηση* (eavesdropping). Ο υπολογιστής εκτέλεσης έχει πρόσβαση στον κώδικα, τα δεδομένα και τη ροή εκτέλεσης ενός πράκτορα. Συνεπώς μπορεί να προσπελάσει οποιαδήποτε πληροφορία μεταφέρει ο πράκτορας, τουλάχιστον κατά τη στιγμή που θα πρέπει να χρησιμοποιήσει την πληροφορία αυτή και ο ίδιος ο πράκτορας.
- *Τροποποίηση κώδικα* (code tampering). Ο υπολογιστής που εκτελεί ένα

πράκτορα, μπορεί να τροποποιήσει των κώδικά του, για παράδειγμα εισάγοντας ιούς ή άλλου είδους επιβλαβή κώδικα. Επίσης, μπορεί να αλλάξει τμήματα του εκτελέσιμου κώδικα ή των δεδομένων του πράκτορα με άλλα της επιλογής του.

- *Αυθαίρετος καταλογισμός ευθύνης* (arbitrary non-repudiation). Ο υπολογιστής εκτέλεσης ενός πράκτορα, μπορεί να υποκλέψει το μυστικό κλειδί υπογραφής ενός κινητού πράκτορα τη στιγμή που το χρησιμοποιεί ο ίδιος ο πράκτορας για κάποιο υπολογισμό και να το χρησιμοποιήσει για να δεσμεύσει τον πράκτορα (ή τον αποστολέα του) σε αυθαίρετες συναλλαγές της επιλογής του.

3. **Απειλές κατά τη διάρκεια της μεταφοράς.**

Σε περίπτωση που κατά τη διαδικασία μετανάστευσης δεν προστατεύεται η εμπιστευτικότητα και η ακεραιότητα των κινητών πρακτόρων, τότε οι πράκτορες είναι ευάλωτοι σε επιθέσεις παρακολούθησης και τροποποίησης από τρίτους (man-in-the-middle attacks). Επειδή η φάση της μεταφοράς αφορά τους πράκτορες, αυτή η κατηγορία απειλών ασφάλειας μπορεί να θεωρηθεί μία ειδική περίπτωση απειλών ασφάλειας κατά των κινητών πρακτόρων.

1.4 Αντικείμενο και στόχοι της διατριβής

Αν και τα πλεονεκτήματα των κινητών πρακτόρων έχουν ευρέως αναγνωριστεί, η μέχρι σήμερα χρήση τους σε πραγματικές εφαρμογές είναι σχετικά περιορισμένη. Ο βασικότερος λόγος της περιορισμένης χρήσης κινητών πρακτόρων, είναι σύμφωνα με πολλούς ερευνητές τα προβλήματα ασφάλειας που εισάγουν [27, 29, 42, 55, 63, 66, 104, 109, 114, 116].

Λόγω της μεταφοράς τους μέσω ανοικτών δικτύων, καθώς επίσης και των αυξημένων προγραμματιστικών δυνατοτήτων τους, οι κινητοί πράκτορες εισάγουν ένα μεγάλο αριθμό απειλών ασφάλειας για τους υπολογιστές εκτέλεσης. Επίσης, λόγω της εξάρτησης των κινητών πρακτόρων από τους υπολογιστές εκτέλεσης, οι κινητοί πράκτορες υπόκεινται σε διάφορες απειλές ασφάλειας που μπορεί να προέρχονται από εχθρικούς υπολογιστές εκτέλεσης. Οι υπάρχουσες λύσεις μπορούν να αντιμετωπίσουν ορισμένα από τα προβλήματα αυτά, αλλά όχι στο βαθμό εκείνο που θα καταστήσουν την τεχνολογία των κινητών πρακτόρων αρκετά ασφαλή για πραγματικές εφαρμογές ευρείας κλίμακας. Για παράδειγμα, σε ένα βασικό πεδίο εφαρμογών της τεχνολογίας κινητού πράκτορα που είναι το Ηλεκτρονικό Εμπόριο και οι ηλεκτρονικές συναλλαγές, οι υπάρχουσες λύσεις δεν επιλύουν αρκετά ζητήματα ασφάλειας όπως είναι η εξουσιοδότηση πρόσβασης, ο καταλογισμός ευθύνης και η μεταβίβαση δικαιωμάτων πρόσβασης των κινητών πρακτόρων.

Αντικείμενο της παρούσας διατριβής είναι τα προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων. Αναλυτικότερα, στους στόχους της διατριβής περιλαμβάνονται:

1. Η ανάλυση των απειλών ασφάλειας σε εφαρμογές κινητού πράκτορα και η ταξινόμηση των υφιστάμενων λύσεων.

2. Η συνεισφορά στη λύση ορισμένων από τα ανοικτά προβλήματα ασφάλειας των κινητών πρακτόρων. Για την επίλυση συγκεκριμένων προβλημάτων ασφάλειας κινητών πρακτόρων, αναπτύσσονται κρυπτογραφικά πρωτόκολλα, μηχανισμοί και αρχιτεκτονικές ασφάλειας.

3. Η παρουσίαση των προβλημάτων ασφάλειας των κινητών πρακτόρων που παραμένουν ανοικτά.

1.5 Δομή της διατριβής

Η παρούσα διατριβή αποτελείται από εννέα κεφάλαια, τα οποία είναι ταξινομημένα σε τρεις ενότητες (βλέπε Σχήμα 1.1). Η πρώτη ενότητα παρέχει στον αναγνώστη το απαραίτητο υπόβαθρο για την πληρέστερη κατανόηση των προβλημάτων ασφάλειας της τεχνολογίας των κινητών πρακτόρων. Περιλαμβάνει το παρόν κεφάλαιο στο οποίο παρουσιάζεται μία εισαγωγή στα προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων, καθώς και το δεύτερο κεφάλαιο στο οποίο γίνεται επισκόπηση στη διεθνή βιβλιογραφία, σχετικά με τις υφιστάμενες λύσεις για την αντιμετώπιση αυτών των προβλημάτων ασφάλειας.

Η δεύτερη ενότητα περιλαμβάνει κρυπτογραφικά πρωτόκολλα τα οποία αναπτύχθηκαν για την αντιμετώπιση διαφόρων προβλημάτων ασφάλειας των κινητών πρακτόρων. Αποτελείται από τα κεφάλαια 3 έως και 5. Στο τρίτο κεφάλαιο περιγράφεται το πρωτόκολλο της μη-αποσπώμενης υπογραφής RSA. Στο τέταρτο κεφάλαιο περιγράφεται το σχήμα της δυναμικής πολυ-υπογραφής, το οποίο βασίζεται στο πρόβλημα του διακριτού λογαρίθμου. Στο πέμπτο κεφάλαιο, περιγράφεται το σχήμα ισχυρής χρονικής ασφάλειας, το οποίο χρησιμοποιείται για τη χρονική προστασία μυστικών κλειδιών σε κρυπτογραφικά συστήματα δημόσιου κλειδιού.

Η τρίτη ενότητα περιλαμβάνει αρχιτεκτονικές και μηχανισμούς που έχουν προταθεί για την αντιμετώπιση των προβλημάτων ασφάλειας των κινητών πρακτόρων και αποτελείται από τα κεφάλαια 6 έως και 8. Στο έκτο κεφάλαιο περιγράφεται ένα πολυπρακτορικό σύστημα για ασφαλείς συναλλαγές κινητών πρακτόρων. Στο έβδομο κεφάλαιο περιγράφεται ένας μηχανισμός για ασφαλή μεταβίβαση δικαιωμάτων πρόσβασης μεταξύ κινητών πρακτόρων. Ο μηχανισμός αυτός κάνει χρήση της μη-αποσπώμενης υπογραφής RSA (κεφάλαιο 3) και της ισχυρής χρονικής ασφάλειας (κεφάλαιο 5). Στο όγδοο κεφάλαιο περιγράφεται μία αρχιτεκτονική για ασφαλή ευφυή δίκτυα με τη

Ενότητες – Κεφάλαια	Κύριοι Στόχοι
Ενότητα Α ***Προβληματική και Εννοιολογικό Πλαίσιο*** *Κεφ.1: Εισαγωγή* Κεφ.2: Επισκόπηση Λύσεων	✓ *Παρουσίαση εισαγωγικών εννοιών* ✓ *Ταξινόμηση λύσεων για τα προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων* ✓ *Παρουσίαση ανοικτών προβλημάτων ασφάλειας* ✓ *Υποστήριξη της κύριας ερευνητικής εργασίας που παρουσιάζεται στις επόμενες ενότητες*
Ενότητα Β ***Κρυπτογραφικά Πρωτόκολλα*** *Κεφ.3: Μη-αποσπώμενη Υπογραφή* RSA *Κεφ.4: Δυναμικές Πολύ-υπογραφές για Ασφαλείς Αυτόνομους Πράκτορες* *Κεφ.5: Ισχυρή Χρονική Ασφάλεια*	✓ *Παρουσίαση πρωτοκόλλου ασφαλών ψηφιακών υπογραφών για κινητούς πράκτορες* ✓ *Παρουσίαση πρωτοκόλλου ασφαλών ψηφιακών πολύ-υπογραφών για κινητούς πράκτορες* ✓ *Παρουσίαση πρωτοκόλλου για χρονική προστασία μυστικού κλειδιού*
Ενότητα Γ ***Μηχανισμοί και Αρχιτεκτονικές Ασφάλειας*** *Κεφ.6: Το Μοντέλο Κύριου Πράκτορα – Εξαρτημένων Πρακτόρων* *Κεφ.7: Ασφαλής Μεταβίβαση Ρόλου Μεταξύ Κινητών Πρακτόρων* *Κεφ.8: Κινητοί Πράκτορες στην Ασφάλεια Ευφυών Δικτύων*	✓ *Αρχιτεκτονική ασφάλειας συναλλαγών με κινητούς πράκτορες* ✓ *Μηχανισμός ασφαλούς μεταβίβασης δικαιωμάτων πρόσβασης για κινητούς πράκτορες σε εχθρικό περιβάλλον εκτέλεσης* ✓ *Αντιμετώπιση προβλημάτων ασφάλειας σε ευφυή δίκτυα με κινητούς πράκτορες*
Κεφ.9: Συμπεράσματα και Ανοικτά Ερευνητικά Πεδία	✓ *Συμπεράσματα της διατριβής και ανοικτά προβλήματα για μελλοντική έρευνα*

Σχήμα 1.1: Δομή της Διατριβής

χρήση κινητών πρακτόρων.

Τέλος, στο ένατο κεφάλαιο παρουσιάζονται τα τελικά συμπεράσματα που απορρέουν από την παρούσα διατριβή. Γίνεται μία ανασκόπηση της διατριβής, ενώ παρουσιάζονται προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων που παραμένουν ανοικτά και πεδία περαιτέρω έρευνας.

1.6 Συνεισφορά της διατριβής και σχετικές δημοσιεύσεις

Η συνεισφορά της παρούσας διατριβής περιλαμβάνει τρεις διαφορετικές πτυχές.

1. Αρχικά, η παρούσα διατριβή ταξινομεί τα προβλήματα ασφάλειας που απορρέουν από τη χρήση της τεχνολογίας των κινητών πρακτόρων, τόσο για τους κινητούς πράκτορες, όσο και για το περιβάλλον εκτέλεσής τους, καθώς και τις υπάρχουσες λύσεις. Στο δεύτερο κεφάλαιο γίνεται μια τέτοια ταξινόμηση. Μέρος του κεφαλαίου αυτού δημοσιεύτηκε στην εργασία [73].

2. Η δεύτερη πτυχή της συνεισφοράς αυτής της διατριβής, αφορά την παρουσίαση κρυπτογραφικών πρωτοκόλλων για την ασφάλεια των κινητών πρακτόρων. Ειδικότερα:

   (α') Στο τρίτο κεφάλαιο παρουσιάζεται το σχήμα της μη-αποσπώμενης υπογραφής RSA. Αποτελεί το πρώτο σχήμα υπογραφών για κινητούς πράκτορες με αποδεδειγμένη υπολογιστική ασφάλεια. Το πρωτόκολλο αυτό δημοσιεύτηκε στην εργασία [71].

   (β') Στο τέταρτο κεφάλαιο περιγράφεται το σχήμα των δυναμικών πολυ-υπογραφών, το οποίο παρέχει δυνατότητα υπογραφής τόσο για τον πράκτορα

όσο και για τους υπολογιστές εκτέλεσης. Επίσης, επιτρέπει ασφαλή εκτέλεση του πράκτορα σε πολλαπλούς υπολογιστές, χωρίς προκαθορισμένο δρομολόγιο. Το σχήμα αυτό δημοσιεύτηκε στην εργασία [72].

(γ') Το σχήμα ισχυρής χρονικής ασφάλειας που περιγράφεται στο πέμπτο κεφάλαιο, επιτρέπει τη χρονική προστασία μυστικών κλειδιών σε κρυπτογραφικά συστήματα δημόσιου κλειδιού και έχει εφαρμογές στην προστασία κλειδιών κινητών πρακτόρων. Το σχήμα δημοσιεύτηκε στην εργασία [19].

3. Τέλος, η τρίτη πτυχή της συνεισφοράς αυτής της διατριβής αφορά την παρουσίαση αρχιτεκτονικών και μηχανισμών, οι οποίοι επιλύουν συγκεκριμένα προβλήματα ασφάλειας σε συστήματα κινητών πρακτόρων.

(α') Το πολυ-πρακτορικό σύστημα που περιγράφεται στο έκτο κεφάλαιο, παρέχει ασφαλείς δοσοληψίες κινητών πρακτόρων με μεγάλη ανθεκτικότητα σε λάθη δικτύου. Το σύστημα αυτό δημοσιεύτηκε στην εργασία [74].

(β') Ο μηχανισμός για μεταβίβαση δικαιωμάτων πρόσβασης μεταξύ κινητών πρακτόρων που περιγράφεται στο έβδομο κεφάλαιο, κάνει χρήση της μη-αποσπώμενης υπογραφής RSA [71] και της ισχυρής χρονικής ασφάλειας [19], για την αποφυγή της αυθαίρετης μεταβίβασης δικαιωμάτων μεταξύ κινητών πρακτόρων.

(γ') Τέλος, η αρχιτεκτονική ευφυών δικτύων που παρουσιάζεται στο όγδοο κεφάλαιο, επιτρέπει την ασφαλή διαχείριση ευφυών δικτύων με τη χρήση κινητών πρακτόρων και κατάλληλων μηχανισμών ασφάλειας. Η αρχιτεκτονική αυτή δημοσιεύτηκε στην εργασία [40].

1.6.1 Αναφορές άλλων ερευνητών

Αρκετές ερευνητικές δημοσιεύσεις στη διεθνή βιβλιογραφία [13, 14, 15, 16, 23, 24, 25, 68, 78, 79, 80, 83, 90, 96, 99, 107, 117, 118] έχουν χρησιμοποιήσει τα αποτελέσματα των δημοσιεύσεων που παρουσιάζονται στη διατριβή αυτή [19, 40, 71, 72, 73, 74]. Στο σχήμα 1.2 αναφέρονται συνοπτικά οι δημοσιεύσεις τα αποτελέσματα των οποίων αναπτύσσονται στα διάφορα κεφάλαια της διατριβής, καθώς επίσης και ορισμένες δημοσιεύσεις άλλων ερευνητών οι οποίες αναφέρονται ή επεκτείνουν τα αποτελέσματα των σχετικών δημοσιεύσεων της παρούσας διατριβής.

Κεφάλαιο	Σχετικές Δημοσιεύσεις	Αναφορές Άλλων Ερευνητών στις Σχετικές Δημοσιεύσεις
2	[73] Kotzanikolaou et al, *"Role Based Access Control Policies in the Mobile Agent Paradigm"*	
3	[71] Kotzanikolaou et al, *"Secure Transactions with Mobile Agents in Hostile Environments"*	[13] Borselius, *"Mobile Agent Security"* [14] Borselius et al, *"On Mobile Agent Based Transactions in Moderately Hostile Environments"* [15] Borselius et al, *"Undetachable Threshold Signatures"* [16] Borselius et al, *"A Pragmatic Alternative to Undetachable Signatures"* [23] Cartrysse and van der Lubbe, *"An Agent Digital Signature in an Untrusted Environment"* [24] Cartrysse et al, *"Privacy Incorporated Software Agents (PISA) – Cryptographic Mechanisms to be Applied"* [24] Cartrysse et al, *"Privacy Incorporated Software Agents (PISA) – Privacy Protection Software Design"* [68] Kim et al, *"Secret Computation with Secrets for Mobile Agent Using One-time Proxy Signature"* [78] Lee et al, *"Secure Mobile Agent Using Strong Non-designated Proxy Signature"* [79] Lee et al, *"Strong Proxy Signatures and its Applications"* [80] Li and Lam, *"A Secure Group Solution for Multi-agent EC System"* [83] Maamar et al, *"Moving Code vs. Inviting Code: What Strategy Should Software Agents Follow?"* [99] Onbilger et al, *"Remote Digital Signing with Mobile Agents"* [102] Shum and Wei, *"A Strong Proxy Signature Scheme with Proxy Signer Privacy Protection"*
4	[72] Kotzanikolaou et al, *"Dynamic Multi-signatures for Secure Autonomous Agents"*	[90] Mitchell and Hur, *"On the Security of a Structural Proven Signer Ordering Multisignature Scheme"*
5	[19] Burmester et al, *"Strong Forward Security"*	
6	[67] Kotzanikolaou et al, *"Mobile Agents for Secure Electronic Transactions"*	[68] Kim et al, *"Secret Computation with Secrets for Mobile Agent Using One-time Proxy Signature"* [78] Lee et al, *"Secure Mobile Agent Using Strong Non-designated Proxy Signature"* [79] Lee et al, *"Strong Proxy Signatures and its Applications"* [96] Oguara, *"Secure Transaction Between Intelligent Agents"* [117] Zhang and Karmouch, *"Adding Security Features to FIPA Agent Platforms"* [118] Zhang et al, *"Towards a Secure Agent Platform Based on FIPA"*
7	[19] Burmester et al, *"Strong Forward Security"* [71] Kotzanikolaou et al, *"Secure Transactions with Mobile Agents in Hostile Environments"*	
8	[40] Douligeris et al, *"Secure Distributed Intelligent Networks"*	

Σχήμα 1.2: Σχετικές δημοσιεύσεις και αναφορές άλλων ερευνητών

Κεφάλαιο 2

Επισκόπηση λύσεων

Στο κεφάλαιο αυτό αρχικά παρουσιάζεται μία ταξινόμηση των προτεινόμενων στη διεθνή βιβλιογραφία λύσεων για τα προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων. Στη συνέχεια παρουσιάζονται οι κρυπτογραφικοί μηχανισμοί που έχουν προταθεί για την παροχή υπηρεσιών ασφάλειας σε συστήματα κινητών πρακτόρων, ταξινομημένοι ανάλογα με τις υπηρεσίες ασφάλειας που προσφέρουν. Σημειώνεται ότι στην επισκόπηση των λύσεων περιλαμβάνονται και οι προτεινόμενες στην παρούσα διατριβή λύσεις όπως κρυπτογραφικά πρωτόκολλα, αρχιτεκτονικές και μηχανισμοί, καθώς επίσης και λύσεις που στηρίζονται στα κρυπτογραφικά πρωτόκολλα και τους μηχανισμούς που προτείνονται στη διατριβή αυτή.

2.1 Υπάρχουσες λύσεις – Ταξινόμηση λύσεων

Στη διεθνή βιβλιογραφία έχουν περιγραφεί διάφορες τεχνικές, αρχιτεκτονικές, κρυπτογραφικά πρωτόκολλα και μηχανισμοί για την αντιμετώπιση διαφόρων απειλών ασφάλειας για τα συστήματα κινητών πρακτόρων, οι οποίες διαχωρίζονται σε δύο ευρείες κατηγορίες: *α) προστασία του υπολογιστή εκτέλεσης από κακόβουλους πράκτορες* και *β) προστασία του πράκτορα από εχθρικούς υπολογιστές εκτέλεσης*.

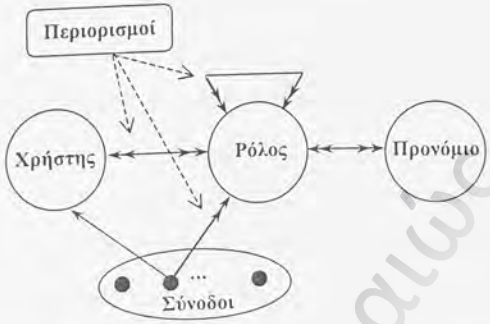
2.1.1 Προστασία από κακόβουλους πράκτορες

Η προστασία του υπολογιστή από κακόβουλους πράκτορες είναι δυνατή με τη χρήση αποτελεσματικών ελέγχων πρόσβασης (access controls), τεχνικών ασφαλούς προγραμματισμού (language safety) και sandbox μηχανισμών (π.χ. τα sandbox στοιχεία ασφάλειας της γλώσσας java) - βλέπε [63].

Οι έλεγχοι πρόσβασης αποτελούν ένα πολύ σημαντικό μηχανισμό για την προστασία κάθε κατανεμημένης εφαρμογής. Η *πολιτική πρόσβασης* καθορίζει κανόνες για την αυθεντικοποίηση (authentication) και την εξουσιοδότηση (authorization) οντοτήτων που ζητούν πρόσβαση σε συγκεκριμένους πόρους ενός συστήματος. Στην περίπτωση συστημάτων κινητών πρακτόρων η πολιτική πρόσβασης καθορίζει κανόνες για την αυθεντικοποίηση των κινητών πρακτόρων που ζητούν πρόσβαση σε κάποιον υπολογιστή εκτέλεσης. Επίσης περιλαμβάνει κανόνες που προσδιορίζουν την εξουσιοδότηση που έχει κάποιος πράκτορας για κατανάλωση συγκεκριμένων πόρων, πρόσβαση σε συγκεκριμένα αρχεία ή εφαρμογές και άλλα δικαιώματα όπως εξουσιοδότηση για την εκκίνηση σύνδεσης σε κάποιον απομακρυσμένο υπολογιστή. Πολλά από τα προτεινόμενα στη διεθνή βιβλιογραφία σχήματα ελέγχου πρόσβασης για συστήματα κινητών πρακτόρων βασίζονται σε *ρόλους*, για παράδειγμα [9, 22, 42, 44, 64, 66, 73, 92]. Τα σχήματα αυτά αναλύονται παρακάτω.

Έλεγχος πρόσβασης βασισμένος σε ρόλους

Οι παραδοσιακές πολιτικές ελέγχου πρόσβασης βασίζονται στα μοντέλα Υποχρεωτικού Ελέγχου Πρόσβασης (Mandatory Access Control - MAC) [34] και Διακριτικού Ελέγχου Πρόσβασης (Discretionary Access Control - DAC) [76]. Το μοντέλο MAC χρησιμοποιεί μια δομή ροής πληροφοριών μίας κατεύθυνσης, η οποία οδηγεί σε περισσότερο ασφαλείς αλλά αρκετά δύσκαμπτες πολιτικές πρόσβασης. Το μοντέλο DAC



Σχήμα 2.1: Το μοντέλο Ελέγχου Πρόσβασης Βασισμένου σε Ρόλους (RBAC)

χρησιμοποιείται για πολιτικές διαχείρισης δικαιωμάτων πρόσβασης οι οποίες βασίζονται στον ιδιοκτήτη των δεδομένων και για το λόγο αυτό είναι περισσότερο εύκαμπτες. Όμως, η διαχείριση των δικαιωμάτων πρόσβασης είναι πιο περίπλοκη.

Το μοντέλο Ελέγχου Πρόσβασης Βασισμένου σε Ρόλους (Role Based Access Control - RBAC) [105] συνδυάζει τα στοιχεία ασφάλειας των μοντέλων MAC με την ελαστικότητα των μοντέλων DAC και επιπλέον παρέχει αποτελεσματική διαχείριση των δικαιωμάτων πρόσβασης. Γενικά, μια πολιτική η οποία στηρίζονται στο μοντέλο RBAC βασίζεται σε τρία σύνολα σημασιολογικών δομών, δηλαδή στους *χρήστες*, τους *ρόλους* και τα *προνόμια* (ή *δικαιώματα πρόσβασης*) - βλέπε Σχήμα 2.1.

Ένας χρήστης είναι μια οντότητα, ή ένα πρόγραμμα ελεγχόμενο από μια οντότητα. Ένας ρόλος αναφέρεται σε ένα τίτλο εργασίας ή λειτουργικότητας σε μια εφαρμογή. Ένα δικαιώματα πρόσβασης είναι η έγκριση για μία συγκεκριμένη πρόσβαση σε ένα ή περισσότερους πόρους του συστήματος. Οι πολιτικές πρόσβασης καθορίζονται από τις σχέσεις ανάμεσα στους χρήστες, τους ρόλους και τα δικαιώματα πρόσβασης, όπως υποδηλώνονται με τα διπλά βέλη στο Σχήμα 2.1. Ένας χρήστης μπορεί να είναι μέλος

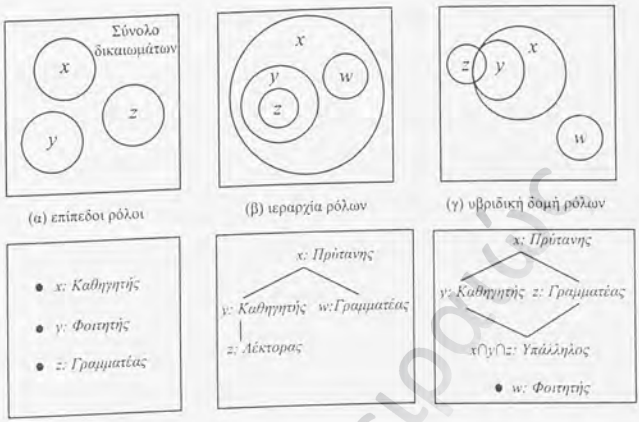
πολλαπλών ρόλων και ένας ρόλος μπορεί να ανατεθεί σε πολλούς χρήστες. Παρομοίως, ένας ρόλος μπορεί να περιλαμβάνει πολλά δικαιώματα πρόσβασης και ένα δικαίωμα πρόσβασης μπορεί να δοθεί σε πολλούς ρόλους. Για παράδειγμα, σε μια δικτυακή εφαρμογή ο ρόλος ενός τερματικού χρήστη μπορεί να έχει περιορισμένα δικαιώματα για απλές υπηρεσίες δικτύου, ενώ ο ρόλος του διαχειριστή δικτύου μπορεί να έχει την έγκριση να προσθέτει ή να διαγράφει χρήστες.

Κάθε *σύνοδος* (session) συσχετίζει ένα χρήστη με έναν ή περισσότερους ρόλους. Ανάλογα με τους *κανόνες πολιτικής* (policy rules), μπορεί να επιτραπεί στους χρήστες να ενεργοποιούν ταυτόχρονα έναν ή περισσότερους ρόλους. Τα δικαιώματα που είναι διαθέσιμα στον χρήστη είναι η ένωση των δικαιωμάτων όλων των ενεργοποιημένων ρόλων σε μια συγκεκριμένη σύνοδο. Κάθε σύνοδος συσχετίζεται με έναν μόνο χρήστη, όπως υποδηλώνεται με το μονό βέλος στο Σχήμα 2.1.

Ένα σύνολο *περιορισμών* (constraints) ορίζει τις επιτρεπόμενες εγκρίσεις για τα διάφορα στοιχεία ενός συστήματος. Για παράδειγμα, ένας περιορισμός μπορεί να απαγορεύει την ταυτόχρονη ενεργοποίηση κάποιων ρόλων από τον ίδιο χρήστη, για την επιβολή *διαχωρισμού καθηκόντων* (seperation of duties).

Οι ρόλοι μπορεί να έχουν μια *επίπεδη*, *ιεραρχική* ή *υβριδική* υποδομή - βλέπε Σχήμα 2.2. Στην πρώτη περίπτωση, οι ρόλοι δεν εμπεριέχουν κοινά δικαιώματα πρόσβασης. Στην δεύτερη περίπτωση οι ρόλοι, ως σύνολα δικαιωμάτων πρόσβασης, σχηματίζουν μια ολοκληρωμένη ιεραρχία. Στην τρίτη περίπτωση, οι ρόλοι μπορεί να έχουν κοινά και μη-κοινά δικαιώματα πρόσβασης. Παραδείγματα φαίνονται επίσης στο Σχήμα 2.2.

Η *μεταβίβαση ρόλου* (role delegation) είναι μία ιδιότητα ιδιαίτερης σπουδαιότητας για την κατασκευή RBAC πολιτικών πρόσβασης. Είναι η ιδιότητα μιας οντότητας που είναι μέλος ενός ρόλου με συγκεκριμένα δικαιώματα πρόσβασης, να εξουσιοδοτεί μια



Σχήμα 2.2: Δομές ρόλων και παραδείγματα

άλλη οντότητα ώστε να γίνει μέλος αυτού του ρόλου για μια συγκεκριμένη χρονική περίοδο.

Ένα σημαντικό χαρακτηριστικό του μοντέλου RBAC είναι ο δυναμικός του χαρακτήρας. Με τα μοντέλα MAC και DAC, οι πολιτικές πρόσβασης είναι αυστηρώς προσαρμοσμένες στην εφαρμογή. Η αναδιαμόρφωση των κανόνων πρόσβασης συνήθως απαιτεί τον ανασχεδιασμό ολόκληρης της δομής της πολιτικής. Το μοντέλο RBAC διαμορφώνει δυναμικά μια πολιτική πρόσβασης: οι πολιτικές είναι το αποτέλεσμα της διαμόρφωσης των διαφόρων στοιχείων του μοντέλου, όπως είναι οι χρήστες, οι ρόλοι, τα δικαιώματα πρόσβασης και οι μεταξύ τους σχέσεις. Συνεπώς, μπορούν εύκολα και δυναμικά να αναδιαμορφωθούν για να καλύψουν διαφορετικές ανάγκες ασφάλειας. Για μια λεπτομερή περιγραφή του μοντέλου RBAC και του δυναμικού του χαρακτήρα βλέπε [105, 100].

RBAC πολιτικές πρόσβασης για συστήματα κινητών πρακτόρων

Τα συστήματα που χρησιμοποιούν κινητούς πράκτορες για απομακρυσμένη επικοινωνία ή για κατανεμημένους υπολογισμούς χρήζουν δυναμικής προστασίας και απαιτούν ευπροσάρμοστες πολιτικές πρόσβασης. Επομένως, δεν προκαλεί έκπληξη το γεγονός ότι αρκετά σχήματα ελέγχου πρόσβασης που προτείνονται στη βιβλιογραφία για συστήματα κινητών πρακτόρων βασίζονται στο μοντέλο RBAC. Αυτά περιλαμβάνουν το σχήμα ασφάλειας των Karjoth *et al* [66], το σχήμα αυθεντικοποίησης και εξουσιοδότησης των Berkovits *et al* [9] και το σχήμα διαχείρισης δικαιωμάτων πρόσβασης του Jansen [64]. Το σχήμα των Karjoth *et al* εφαρμόζεται ειδικότερα στην πλατφόρμα πρακτόρων Aglets Workbench [57]. Το σχήμα ασφαλείας του Jansen μπορεί να εφαρμοστεί σε διάφορες πλατφόρμες βασιζόμενες σε Java, συμπεριλαμβανομένων των Aglets, Voyager [95], Grasshopper [58] και της ίδιας της Java [89]. Ένα πρωτότυπο έχει κατασκευαστεί για την πλατφόρμα Aglets. Το σχήμα των Berkovits *et al* δεν είναι εξαρτώμενο από συγκεκριμένη πλατφόρμα και ορίζεται για γενικές δομές.

Ένα κοινό γνώρισμα στα παραπάνω σχήματα είναι το ότι η πολιτική πρόσβασης βασίζεται στην αυθεντικοποίηση του πράκτορα. Ο πράκτορας αρχικά αυθεντικοποιείται, δηλαδή επιβεβαιώνεται ένας σύνδεσμος ανάμεσα στον πράκτορα και σε μια οντότητα του συστήματος. Αυτή η οντότητα μπορεί να είναι ο αποστολέας ή ο δημιουργός του πράκτορα.

Κατόπιν, η πολιτική εξουσιοδότησης εφαρμόζεται για να δοθεί συγκεκριμένη πρόσβαση στον πράκτορα, ανάλογα με τους ενεργούς ρόλους του. Οι Karjoth *et al* προσδιορίζουν επίσης μια πολιτική *επικράτειας* (domain policy). Ο ορισμός επικρατειών επιτρέπει μια περισσότερο ευπροσάρμοστη πολιτική ελέγχου πρόσβασης, μιας και είναι περισσότερο πρακτικός ο έλεγχος πρόσβασης σε μία ομάδα υπολογιστών εκτέλεσης παρά σε μεμονωμένους υπολογιστές. Στο σχήμα του Jansen δεν ορίζεται ρητά μια

πολιτική επικράτειας. Όμως, οι λεπτομέρειες υλοποίησης μπορούν να επιτρέψουν μια τέτοια πολιτική.

Η πολιτική εξουσιοδότησης στα παραπάνω σχήματα στηρίζεται σε ένα σύνολο ρόλων, κοινών σε όλα τα σχήματα. Αυτοί οι ρόλοι περιλαμβάνουν τον πράκτορα (agent), το δημιουργό του πράκτορα (agent creator), το διαχειριστή του περιβάλλοντος εκτέλεσης (host administrator) και τον υπολογιστή εκτέλεσης του πράκτορα (execution host). Οι Karjoth *et al* ορίζουν επιπλέον ρόλους. Το σχήμα του Jansen μπορεί επίσης να διαμορφωθεί ώστε να ενσωματώνει ένα επεκταμένο σύνολο ρόλων. Αυτοί οι ρόλοι διακρίνονται σε ρόλους σχετιζόμενους με τον πράκτορα (branding roles) και σε ρόλους σχετιζόμενους με το περιβάλλον εκτέλεσης (hosting roles).

Η πρώτη κατηγορία περιλαμβάνει τον κατασκευαστή του πράκτορα (agent creator) ή έναν εκτιμητή του κώδικα του πράκτορα (agent code evaluator). Η δεύτερη κατηγορία περιλαμβάνει το διαχειριστή του συστήματος (system administrator), το διαχειριστή ασφάλειας του συστήματος (system security administrator), ή το διαχειριστή επικράτειας (domain administrator). Τα προνόμια του κάθε ρόλου ορίζονται σύμφωνα με τη λειτουργικότητα του ρόλου. Για παράδειγμα, ο διαχειριστής επικράτειας έχει προνόμια πρόσβασης σε όλους τους υπολογιστές εκτέλεσης που ανήκουν στην επικράτειά του, καθώς και δικαιώματα ενημέρωσης των κανόνων πολιτικής εντός της επικράτειάς του. Τα προνόμια ενός πράκτορα συνήθως σχετίζονται με τα προνόμια του αποστολέα του πράκτορα. Για παράδειγμα ένας πράκτορας μπορεί να έχει προνόμια πρόσβασης στο προφίλ του αποστολέα του, που είναι καταχωρημένο σε έναν απομακρυσμένο υπολογιστή.

Η υποδομή των ρόλων ποικίλει επίσης μεταξύ αυτών των μοντέλων. Η πολιτική πρόσβασης στο μοντέλο των Karjoth *et al* βασίζεται σε μια προκαθορισμένη ιεραρχία ρόλων, στην οποία ο διαχειριστής επικράτειας είναι η πηγή της ιεραρχίας ρόλων. Ο

διαχειριστής επικράτειας θέτει τους βασικούς κανόνες πολιτικής ασφάλειας, οι οποίοι μπορούν να εξειδικευτούν από την ιεραρχία ρόλων. Η υποδομή των σχημάτων των Berkovits *et al* και Jansen δεν ορίζεται ρητά. Εντούτοις, στο σχήμα του Jansen αντικρουόμενοι κανόνες αντιμετωπίζονται μέσω μιας μορφής ιεραρχίας ρόλων. Πιο συγκεκριμένα, στην περίπτωση αντιφατικών κανόνων πρόσβασης, οι κανόνες πρόσβασης που θέτει ένας ρόλος σχετιζόμενος με το περιβάλλον εκτέλεσης, υπερισχύουν των κανόνων που θέτει ένας ρόλος σχετιζόμενος με τον πράκτορα. Το σχήμα των Berkovits *et al* δεν ορίζει καμία ιδιαίτερη υποδομή ρόλων.

Η πολιτική μεταβίβασης ρόλου στα παραπάνω σχήματα ασχολείται με τη μεταβίβαση από στατικούς χρήστες σε κινητούς πράκτορες ή σε υπολογιστές εκτέλεσης. Το σχήμα του Jansen ορίζει επιπλέον άμεση μεταβίβαση ρόλου σε πράκτορες και υπολογιστές εκτέλεσης από Έμπιστες Οντότητες. Με την μεταβίβαση ρόλου, οι πράκτορες και οι υπολογιστές εκτέλεσης μπορούν έμμεσα να κατέχουν ρόλους μέσω άλλων οντοτήτων και να ενεργούν εκ μέρους αυτών για περιορισμένο χρόνο. Στο Σχήμα 2.3 περιγράφονται συνοπτικά τα χαρακτηριστικά των προτεινόμενων σχημάτων για RBAC πολιτικές πρόσβασης σε συστήματα κινητών πρακτόρων.

Κινητοί πράκτορες στην εφαρμογή RBAC πολιτικών

Εκτός από την εφαρμογή RBAC πολιτικών πρόσβασης σε συστήματα πρακτόρων, οι κινητοί πράκτορες έχουν χρησιμοποιηθεί ως υποστηρικτική τεχνολογία για την υλοποίηση πολιτικών RBAC σε κατανεμημένες εφαρμογές.

Οι Demurjian *et al* [33] προτείνουν αρκετά μοντέλα τα οποία χρησιμοποιούν τεχνολογίες πρακτόρων για να υποστηρίξουν πολιτικές RBAC σε κατανεμημένες εφαρμογές. Για παράδειγμα σε μια εφαρμογή πελάτη/εξυπηρετητή, οι επιτρεπόμενες ενέργειες

Χαρακτηριστικά / Σχήμα	Karjoth *et al*	Berkovits *et al*	Jansen
• *Πλατφόρμα*	Aglets	Μη-οριζόμενη	Βασισμένη σε Java
• *Πολιτική Πρόσβασης περιλαμβάνει*			
○ *Αυθεντικοποίηση*	√	√	√
○ *Έλεγχο εξουσιοδότησης*	√	√	√
○ *Πολιτική επικράτειες*	√		√
• *Ρόλοι*			
○ *Πράκτορας*	√	√	√
○ *Κατασκευαστής πράκτορα*	√	√	√
○ *Αποστολέας πράκτορας*	√	√	√
○ *Εκτιμητής κώδικα πράκτορα*			√
○ *Υπολογιστής εκτέλεσης*	√	√	√
○ *Κατασκευαστής υπολογιστή εκτέλεσης*	√		√
○ *Ιδιοκτήτης υπολογιστή εκτέλεσης*	√		√
○ *Διαχειριστής υπολογιστή εκτέλεσης*	√		√
○ *Διαχειριστής ασφάλειας υπολογιστή εκτέλεσης*			√
○ *Διαχειριστής επικράτειας*	√		√
• *Δομή Ρόλων*			
○ *Επίπεδη*		√	
○ *Ιεραρχική*	√	√	√
○ *Υβριδική*		√	
• *Μεταβίβαση Ρόλων*			
○ *Χρήστης προς πράκτορα*	√	√	√
○ *Χρήστης προς υπολογιστή εκτέλεσης*	√	√	√
○ *Έμπιστη οντότητα προς πράκτορα*			√
○ *Έμπιστη οντότητα προς υπολογιστή εκτέλεσης*			√

Σχήμα 2.3: RBAC πολιτικές πρόσβασης σε συστήματα κινητών πρακτόρων

του αιτήματος του πελάτη σε ένα απομακρυσμένο αντικείμενο μπορούν να υπαγορευθούν από το ρόλο του πελάτη. Οι κινητοί πράκτορες χρησιμοποιούνται για να προσδιορίσουν τον πελάτη και τον ρόλο του. Οι πράκτορες περικλείουν το αίτημα και τον ρόλο του πελάτη σε ένα μήνυμα, και μεταναστεύουν σε υπολογιστικούς κόμβους για την ασφαλή πρόσβαση απομακρυσμένων αντικειμένων. Η επιτρεπόμενη πρόσβαση στο αντικείμενο βασίζεται στους ρόλους που έχουν μεταβιβαστεί στον πράκτορα από τον πελάτη.

Τέλος, οι Fayad *et al* [44] πρότειναν την έννοια των *κινητών πολιτικών* (mobile policies). Το κίνητρο πίσω από τις κινητές πολιτικές είναι περιπτώσεις στις οποίες κινητά αντικείμενα οφείλουν να ακολουθήσουν μια πολιτική πρόσβασης, ανεξάρτητα από τη θέση τους σε ένα κατανεμημένο δίκτυο. Για παράδειγμα, διάφορες ετικέτες εμπιστευτικότητας όπως η ετικέτα NOFORN του υπουργείου αμύνης των Ηνωμένων Πολιτειών, χρησιμοποιείται για να προσδιορίσει ότι η πρόσβαση σε ένα αντικείμενο με αυτή την ετικέτα απαιτεί από το χρήστη Αμερικανική ιθαγένεια. Οι κινητές πολιτικές επιτρέπουν στις πολιτικές ειδικής εφαρμογής να μετακινούνται μαζί με το αντικείμενο σε άλλα στοιχεία του συστήματος. Συνεπώς, τα κινητά αντικείμενα ενσωματώνουν την πολιτική. Ο έλεγχος πρόσβασης βασίζεται σε ρόλους, εφόσον το σύστημα προσδιορίζει ρόλους και προνόμια πρόσβασης για τις διάφορες οντότητες του συστήματος.

2.1.2 Προστασία από εχθρικούς υπολογιστές εκτέλεσης

Η προστασία του πράκτορα από εχθρικούς υπολογιστές εκτέλεσης αποτελεί ένα πολύ δυσκολότερο και ανοικτό ερευνητικά πρόβλημα. Κατά τη διάρκεια της εκτέλεσης ενός κινητού πράκτορα, ο πράκτορας βρίσκεται σε μια πολύ ασύμμετρη σχέση με τον υπολογιστή, αφού ο υπολογιστής έχει πρόσβαση στον κώδικα, τα δεδομένα και την κατάσταση εκτέλεσής του. Οι ερευνητικές προσπάθειες για την αντιμετώπιση αυτού

του προβλήματος διαχωρίζονται σε δύο κατηγορίες:

α) Ανίχνευση επιθέσεων κατά του πράκτορα. Περιλαμβάνει λύσεις που στοχεύουν στην *εκ των υστέρων* (à posteriori) ανίχνευση της ταυτότητας και στην απόδειξη της συμπεριφοράς ενός κακόβουλου υπολογιστή εκτέλεσης.

Ο Vigna [109] πρότεινε ένα μηχανισμό ανίχνευσης ο οποίος καταγράφει την εκτέλεση ενός πράκτορα και την αλληλεπίδρασή του με το περιβάλλον εκτέλεσης. Ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί αργότερα για να εντοπίσει κακόβουλους υπολογιστές. Όμως ο μηχανισμός αυτός απαιτεί συνεχή σύνδεση του αποστολέα στο δίκτυο και αλληλεπιδραστική επικοινωνία του αποστολέα με τον πράκτορα, το οποίο συνεπάγεται μεγάλο κόστος επικοινωνίας.

Για την αποφυγή της on-line σύνδεσης του αποστολέα και της αλληλεπίδρασής του με τον πράκτορα, οι Yi *et al* [114] πρότειναν τη χρήση ενός Κέντρου Υπηρεσιών Πρακτόρων (Agent Service Center). Το κέντρο αυτό λειτουργεί ως έμπιστη οντότητα και είναι υπεύθυνο για την αποστολή πρακτόρων σε ένα δίκτυο εκ μέρους διαφόρων χρηστών. Το κέντρο παρακολουθεί το δρομολόγιο κάθε πράκτορα και συλλέγει τις απαραίτητες πληροφορίες για την αποκάλυψη κακόβουλων υπολογιστών εκτέλεσης.

Στην κατηγορία μηχανισμών ανίχνευσης επιθέσεων περιλαμβάνεται και το πολυπρακτορικό σύστημα που παρουσιάζεται αναλυτικά στο έκτο κεφάλαιο της διατριβής (βλέπε επίσης [74]). Το σύστημα αυτό χρησιμοποιεί έναν στατικό και πολλούς κινητούς πράκτορες για κάθε χρήστη. Οι κινητοί πράκτορες μπορούν να εκτελούνται ασύγχρονα σε διαφορετικούς υπολογιστές, ενώ ο στατικός πράκτορας μπορεί να εντοπίσει πιθανούς κακόβουλους υπολογιστές. Το σύστημα αυτό δεν απαιτεί on-line σύνδεση του αποστολέα κατά τη διάρκεια εκτέλεσης των πρακτόρων ή την ύπαρξη έμπιστων κέντρων.

Τα συστήματα αυτά παρέχουν ικανοποιητικές λύσεις για συγκεκριμένα προβλήματα. Παρόλα αυτά, υπάρχουν περιπτώσεις όπου η εκ των υστέρων ανίχνευση δεν παρέχει αρκετή προστασία. Για παράδειγμα, σε εφαρμογές όπου ένας κινητός πράκτορας μπορεί να μεταφέρει ηλεκτρονικά νομίσματα ή/και μυστικά κλειδιά του αποστολέα του, η ανίχνευση δεν είναι αρκετή. Σε αυτές τις περιπτώσεις το χρονικό διάστημα μεταξύ της επίθεσης κατά του πράκτορα και της ανίχνευσης της επίθεσης μπορεί να είναι πολύ κρίσιμο για την ασφάλεια του αποστολέα του πράκτορα.

β) Παρεμπόδιση επιθέσεων κατά του πράκτορα. Η φιλοσοφία αυτής της μεθόδου είναι η *εκ των προτέρων* (à priori) παρεμπόδιση επιθέσεων του περιβάλλοντος εκτέλεσης κατά του πράκτορα. Διακρίνονται δύο περιπτώσεις: *παθητική* και *ενεργητική* παρεμπόδιση.

Οι μηχανισμοί παθητικής παρεμπόδισης προστατεύουν τους κινητούς πράκτορες χρησιμοποιώντας οργανωτικές ή αρχιτεκτονικές λύσεις. Οι Farmer *et al* [42] πρότειναν ένα σχήμα στο οποίο οι πράκτορες κυκλοφορούν μόνο μέσα σε έμπιστο περιβάλλον εκτέλεσης. Οι Merwe και Sholms [87] παρουσίασαν ένα σύστημα για ηλεκτρονικές αγορές μέσω πρακτόρων, όπου οι πράκτορες υλοποιούνται ως κατανεμημένα αντικείμενα που επικοινωνούν απομακρυσμένα. Μερικοί μηχανισμοί ανίχνευσης επίσης χρησιμοποιούν παθητικούς μηχανισμούς παρεμπόδισης [74, 114]. Αυτές οι προσεγγίσεις είτε κάνουν ισχυρές υποθέσεις για την εμπιστοσύνη του περιβάλλοντος εκτέλεσης, είτε κάνουν συμβιβασμούς σε πλεονεκτήματα της τεχνολογίας των κινητών πρακτόρων όπως είναι η αυτονομία [74, 114] και η μετανάστευση [87].

Η ενεργητική παρεμπόδιση επικεντρώνεται στην ανάπτυξη λύσεων που παρέχουν προστασία σε κινητούς πράκτορες από επιθέσεις του περιβάλλοντος εκτέλεσης, χωρίς να συμβιβάζουν τα πρακτικά πλεονεκτήματα του παραδείγματος των κινητών πρακτόρων. Μία κατηγορία τέτοιων λύσεων περιλαμβάνει τη χρήση ασφαλούς υλικού (tamper

resistant hardware) [101, 110]. Όμως η εφαρμογή τέτοιων λύσεων δεν είναι μεγάλη, κυρίως λόγω του υψηλού κόστους που συνεπάγονται. Η χρήση ασφαλούς υλικού συνεπάγεται επίσης υποθέσεις για την εμπιστοσύνη του περιβάλλοντος εκτέλεσης, σε μικρότερο βέβαια βαθμό από ότι οι λύσεις της προηγούμενης κατηγορίας.

Η αναζήτηση λύσεων για ενεργητική παρεμπόδιση επιθέσεων εναντίον κινητών πρακτόρων που βασίζονται σε λογισμικό (software-based), είναι σχετικά πρόσφατο ερευνητικό πεδίο. Μια πρώτη προσέγγιση για ενεργητική προστασία βασισμένη μόνο σε λογισμικό που προτάθηκε από τον Hohl [55] είναι η χρήση τεχνικών "σύγχυσης" και ανασχηματισμού του κώδικα και της ροής εκτέλεσης ενός πράκτορα. Σκοπός αυτής της μεθόδου είναι να κάνει όσο το δυνατό δυσκολότερη και χρονοβόρα την παρακολούθηση και ανακάλυψη του πραγματικού αποτελέσματος της εκτέλεσης ενός πράκτορα. Η προσέγγιση αυτή μπορεί να είναι χρήσιμη για περιπτώσεις όπου ο χρόνος κατά τον οποίο απαιτείται προστασία του πράκτορα είναι σχετικά μικρός. Όμως το χρονικό διάστημα ασφάλειας που προσφέρεται δεν μπορεί να αποδειχθεί ή να προσδιοριστεί, αφού εξαρτάται από τις υπολογιστικές δυνατότητες του αντιπάλου. Αυτή η προσέγγιση μπορεί να θεωρηθεί ότι ανήκει στην κατηγορία που είναι γνωστή στην κρυπτογραφία ως *"ασφάλεια μέσω ασάφειας"* (security through obscurity).

Μία άλλη προσέγγιση για την προστασία κινητών πρακτόρων στηρίζεται στον Ασφαλή Υπολογισμό Συναρτήσεων (Secure Function Evaluations), μία κρυπτογραφική θεώρηση που αρχικά προτάθηκε από τους Goldreigh *et al* [50]. Σύμφωνα με αυτή τη θεώρηση δύο οντότητες, η Alice[1] (ο πράκτορας) και ο Bob (ο υπολογιστής) θέλουν να υπολογίσουν το αποτέλεσμα μίας συνάρτησης f για μία είσοδο x. Η Alice γνωρίζει τη συνάρτηση f ενώ ο Bob την είσοδο x. Οι δύο συμμετέχοντες θέλουν να υπολογίσουν το αποτέλεσμα $f(x)$ με τέτοιο τρόπο ώστε κανείς από τους δύο να μην αποκτήσει

[1] Η Alice και ο Bob είναι τα συμβατικά ονόματα που χρησιμοποιούνται για την περιγραφή κρυπτογραφικών πρωτοκόλλων δύο μερών

περισσότερη πληροφορία από όση ήδη κατέχει, πέραν του αποτελέσματος $f(x)$.

Μια ειδική περίπτωση Ασφαλούς Υπολογισμού Συναρτήσεων που προτάθηκε από τους Sander και Tschudin [104] για την προστασία των κινητών πρακτόρων, είναι ο *Υπολογισμός με Κρυπτογραφημένες Συναρτήσεις - ΥΚΣ* (Computing with Encrypted Functions - CEF). Σύμφωνα με αυτή τη μέθοδο, για την απόκρυψη μίας συνάρτησης s, η συνάρτηση αυτή κρυπτογραφείται μέσω της σύνθεσής της με μία άλλη συνάρτηση f. Ο υπολογιστής εκτελεί την κρυπτογραφημένη συνάρτηση $s \circ f$ χωρίς να έχει πρόσβαση στην s. Η ασφάλεια της μεθόδου στηρίζεται στη δυσκολία "αποσύνθεσης" της κρυπτογραφημένης συνάρτησης στις αρχικές συναρτήσεις. Επειδή το πνεύμα της τεχνολογίας των κινητών πρακτόρων είναι η αυτονομία τους, οι Sander και Tschudin πρότειναν την υλοποίηση *μη-αλληλεπιδραστικών* ΥΚΣ (non-interactive CEF) για την προστασία των κινητών πρακτόρων. Οι ίδιοι ερευνητές παρατήρησαν ότι μη-αλληλεπιδραστικοί ΥΚΣ μπορούν να υλοποιηθούν με τη χρήση αλγεβρικά ομομορφικών κρυπτογραφικών συστημάτων δημόσιου κλειδιού. Δυστυχώς όμως μέχρι στιγμής δεν υπάρχουν αποδεδειγμένα ασφαλή κρυπτοσυστήματα που είναι αλγεβρικά ομομορφικά (δηλαδή προσθετικά και πολλαπλασιαστικά ομομορφικά). Υπάρχοντα κρυπτοσυστήματα που είναι προσθετικά ομομορφικά και θεωρούνται ασφαλή (π.χ. το κρυπτοσύστημα των Naccache και Stern [94]) δεν μπορούν να χρησιμοποιηθούν γιατί για τον έλεγχο της ορθότητας των αποτελεσμάτων οι παράμετροι εισόδου θα πρέπει να είναι εκθετικά μεγάλοι [104].

Οι Cachin *et al* [21] πρότειναν μία λύση για την προστασία των κινητών πρακτόρων που βασίζεται σε κρυπτογραφημένα κυκλώματα (encrypted circuits) [113] και στη μέθοδο επιλήσμονος μεταφοράς (oblivious transfer) [17]. Αν και η μέθοδος αυτή είναι πολύ ενδιαφέρουσα αφού λύνει το πρόβλημα για την προστασία οποιασδήποτε συνάρτησης πολυωνυμικού χρόνου, έχει μόνο θεωρητική αξία αφού δεν είναι πρακτικά

εφαρμόσιμη.

Οι Loureiro και Molva [82] πρότειναν μία μέθοδο που επιτρέπει σε ένα κινητό πράκτορα να υπολογίσει μία Boolean συνάρτηση, χωρίς να αποκαλύπτει την ίδια τη συνάρτηση στο περιβάλλον εκτέλεσής του. Η ασφάλεια της μεθόδου ανάγεται στην ασφάλεια του κρυπτογραφικού συστήματος δημόσιου κλειδιού του McEliece. Η μεθοδολογία αυτή αποδεικνύει ότι υπάρχουν περιπτώσεις όπου είναι δυνατό για ένα κινητό πράκτορα να υπολογίζει συναρτήσεις χωρίς να τις αποκαλύπτει στο περιβάλλον εκτέλεσης. Πρέπει να σημειωθεί όμως ότι ο πράκτορας δεν μπορεί να χρησιμοποιήσει το αποτέλεσμα του υπολογισμού αυτού πριν επιστρέψει στον αρχικό αποστολέα του, αφού το αντίστοιχο μυστικό κλειδί του αποστολέα είναι απαραίτητο για την αποκρυπτογράφηση του αποτελέσματος.

Οι Sander και Tschudin [104] πρότειναν μία εφαρμογή της μεθόδου μη-αλληλεπιδραστικών ΥΚΣ για την προστασία συναρτήσεων υπογραφής για κινητούς πράκτορες, γνωστή και ως *μη-αποσπώμενες υπογραφές* (undetchable signatures). Με αυτές τις υπογραφές, ένας κινητός πράκτορας μπορεί με ασφάλεια να υπογράψει για μία συναλλαγή, χρησιμοποιώντας μία συνάρτηση υπογραφής του αποστολέα του σε κρυπτογραφημένη μορφή. Αν και ο πράκτορας εκτελείται σε κάποιον πιθανώς εχθρικό υπολογιστή, η συνάρτηση υπογραφής είναι κρυπτογραφημένη με τέτοιο τρόπο ώστε είναι υπολογιστικά αδύνατο για τον υπολογιστή να υποκλέψει τη συνάρτηση. Για την υλοποίηση των μη-αποσπώμενων υπογραφών, οι Sander και Tschudin πρότειναν τη χρήση ρητών συναρτήσεων, που όμως αποδείχθηκαν μη ασφαλείς, αφού υπόκεινται στην επίθεση των Coppersmith *et al* [31].

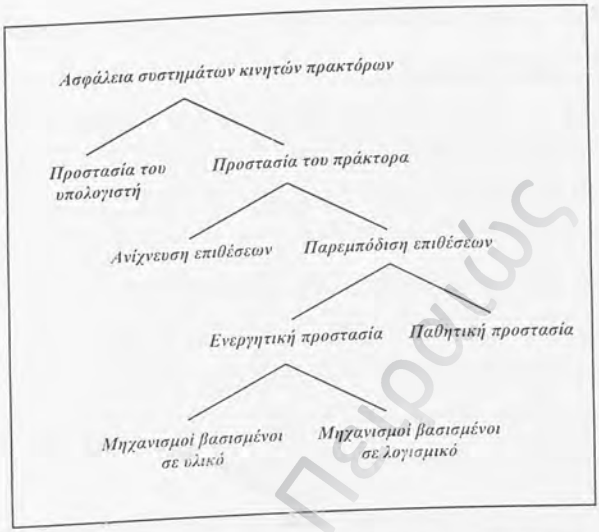
Ένα κρυπτογραφικό πρωτόκολλο ασφαλούς μη-αποσπώμενης υπογραφής παρουσιάζεται αναλυτικά στο τρίτο κεφάλαιο της διατριβής (βλέπε και [71]). Το πρωτόκολλο

αυτό συνδυάζει το σχήμα υπογραφής RSA [103] με εκθετικές συναρτήσεις. Η ασφάλεια του πρωτοκόλλου ανάγεται στην ασφάλεια της υπογραφής RSA στο μοντέλο random oracles υπό ορισμένες κρυπτογραφικές υποθέσεις. Στο τρίτο κεφάλαιο αναλύεται η ασφάλεια, οι δυνατότητες και οι περιορισμοί του.

Οι μη-αποσπώμενες υπογραφές μπορούν να χρησιμοποιηθούν από κινητούς πράκτορες για μία μόνο εκτέλεση σε κάποιον υπολογιστή, και όχι για πολλαπλές εκτελέσεις [21, 72]. Αρκετά σχήματα υπογραφής για κινητούς πράκτορες, βασίστηκαν ή επέκτειναν τις δυνατότητες του σχήματος μη-αποσπώμενης υπογραφής RSA [71]. Το σχήμα για μη-αποσπώμενες πολυ-υπογραφές το οποίο παρουσιάζεται στο τέταρτο κεφάλαιο (βλέπε και [72]), ανήκει σε αυτή την κατηγορία. Το σχήμα αυτό βασίζεται στο σχήμα πολυ-υπογραφών των Mitomi και Miyaji [91] και επιτρέπει την εκτέλεση του πράκτορα σε πολλούς υπολογιστές. Επίσης, προσφέρει καταλογισμό ευθύνης τόσο για τον πράκτορα, όσο και για το περιβάλλον εκτέλεσης.

Οι Borselius *et al* [15] επέκτειναν τις μη-αποσπώμενες υπογραφές σε threshold υπογραφές, όπου για τη δημιουργία μιας έγκυρης υπογραφής απαιτείται η συνεργασία n από k πράκτορες ($n < k$). Το σχήμα αυτό χρησιμοποιήθηκε από τους ίδιους ερευνητές για ηλεκτρονικές συναλλαγές με κινητούς πράκτορες [14].

Οι μη-αποσπώμενες υπογραφές έχουν επεκταθεί επίσης σε υπογραφές πληρεξουσιότητας (proxy signatures). Αναλυτικότερα οι Kim *et al* [68] πρότειναν ένα σχήμα για υπογραφές πληρεξουσιότητας μίας χρήσης (one-time proxy signatures), το οποίο επιτρέπει σε ένα κινητό πράκτορα να υπογράφει με ασφάλεια ένα μήνυμα. Επίσης οι Lee *et al* [78] πρότειναν ένα σχήμα για υπογραφές πληρεξουσιότητας χωρίς προκαθορισμένο αποστολέα (non-designated proxy signatures), το οποίο είναι κατάλληλο για αυτόνομους πράκτορες χωρίς προκαθορισμένο δρομολόγιο. Τέλος, οι Lee και Kim [79] πρότειναν ένα σχήμα για ισχυρές υπογραφές πληρεξουσιότητας (strong proxy



Σχήμα 2.4: Ταξινόμηση λύσεων ασφάλειας για το παράδειγμα των κινητών πρακτόρων

signatures) που προσφέρουν διπλό καταλογισμό ευθύνης.

Το Σχήμα 2.4 παρουσιάζει την ταξινόμηση των λύσεων για τα προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων.

2.2 Κρυπτογραφικοί μηχανισμοί και τεχνικές

Στην ενότητα αυτή παρουσιάζονται διάφοροι κρυπτογραφικοί μηχανισμοί και τεχνικές που μπορούν να χρησιμοποιηθούν για την προστασία εφαρμογών κινητού πράκτορα. Οι κρυπτογραφικοί μηχανισμοί είναι ταξινομημένοι ανάλογα με τις υπηρεσίες ασφάλειας που παρέχουν, δηλαδή εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση, εξουσιοδότηση και καταλογισμό ευθύνης.

2.2.1 Εμπιστευτικότητα

Συμμετρική κρυπτογραφία

Συμμετρικοί κρυπτογραφικοί αλγόριθμοι έχουν χρησιμοποιηθεί για την εμπιστευτικότητα εφαρμογών κινητού πράκτορα. Για παράδειγμα, η εκτέλεση ενός πράκτορα μπορεί να επιτραπεί μόνο σε ορισμένους υπολογιστές με τη χρήση συμμετρικής κρυπτογράφησης. Ο πράκτορας κρυπτογραφείται με ένα συμμετρικό κλειδί, το οποίο διανέμεται σε εξουσιοδοτημένους υπολογιστές. Πριν τη μετανάστευση από ένα υπολογιστή, ο πράκτορας κρυπτογραφείται με το κλειδί αυτό (μαζί με τα μερικά αποτελέσματα της εκτέλεσής του) και μόνο οι υπολογιστές που γνωρίζουν αυτό το κλειδί μπορούν να εκτελέσουν τον πράκτορα.

Υβριδική κρυπτογραφία

Για καλύτερη αποδοτικότητα μπορεί να χρησιμοποιηθεί υβριδική κρυπτογραφία. Επίσης για τον ίδιο λόγο είναι δυνατό να κρυπτογραφηθούν μόνο ορισμένα τμήματα ενός πράκτορα. Στην περίπτωση σειριακής εκτέλεσης του πράκτορα μπορούν να κρυπτογραφούνται τα μερικά αποτελέσματα της εκτέλεσης του πράκτορα με το δημόσιο κλειδί κρυπτογράφησης του αποστολέα του, ώστε να προστατεύονται από τους άλλους υπολογιστές (για παράδειγμα, στην περίπτωση που ο πράκτορας συλλέγει προσφορές για κάποια αγορά).

Κρυπτογραφία ολίσθησης

Σε πολλές περιπτώσεις η ποσότητα πληροφορίας που συλλέγεται από ένα κινητό πράκτορα, είναι σχετικά μικρή σε σχέση με το μέγεθος των κρυπτογραφικών κλειδιών που

χρησιμοποιούνται ή με το μέγεθος του τελικού κρυπτογραφήματος. Η κρυπτογράφηση ολίσθησης (sliding encryption) [115] επιτρέπει σε μικρές ποσότητες δεδομένων να κρυπτογραφούνται και να σχηματίζουν αποτελέσματα αποδοτικού μήκους. Το σενάριο για την κρυπτογράφηση ολίσθησης αφορά ένα κινητό πράκτορα ο οποίος χρησιμοποιώντας ένα δημόσιο κλειδί το οποίο φέρει, κρυπτογραφεί την πληροφορία που συγκεντρώνει από κάθε πλατφόρμα που επισκέπτεται. Αργότερα, όταν ο πράκτορας επιστρέφει στο αρχικό σημείο, η πληροφορία αποκρυπτογραφείται με το αντίστοιχο μυστικό κλειδί που διατηρείται εκεί. Αν και ο σκοπός της κρυπτογράφησης ολίσθησης είναι η εμπιστευτικότητα, ένας επιπρόσθετος έλεγχος ακεραιότητας μπορεί να πραγματοποιηθεί πριν την κρυπτογράφηση.

2.2.2 Ακεραιότητα, αυθεντικότητα, καταλογισμός ευθύνης

Άθροισμα ελέγχου ακεραιότητας και κώδικας αυθεντικοποίησης

Το άθροισμα ελέγχου ακεραιότητας είναι το αποτέλεσμα μίας συνάρτησης κατακερματισμού (hash) που χρησιμοποιείται για τον έλεγχο της ακεραιότητας μηνυμάτων. Στην περίπτωση ενός κινητού πράκτορα το άθροισμα ελέγχου ακεραιότητας είναι το αποτέλεσμα μίας συνάρτησης κατακερματισμού, με είσοδο τον εκτελέσιμο κώδικα, τα δεδομένα και την κατάσταση του πράκτορα. Το άθροισμα ελέγχου αποστέλλεται στον παραλήπτη μαζί με τον πράκτορα. Για να ελέγξει την ακεραιότητα του πράκτορα, ο παραλήπτης υπολογίζει και πάλι το αποτέλεσμα της συνάρτησης κατακερματισμού με είσοδο τον κώδικα, τα δεδομένα και την κατάσταση εκτέλεσης του πράκτορα. Εάν το αποτέλεσμα είναι ίδιο με το άθροισμα ακεραιότητας που συνοδεύει τον πράκτορα, τότε ο πράκτορας δεν έχει τροποποιηθεί.

Το άθροισμα ελέγχου ακεραιότητας μπορεί να συνδυαστεί με κρυπτογράφηση για

έλεγχο αυθεντικοποίησης. Σε αυτή την περίπτωση, το άθροισμα ελέγχου ακεραιότητας κρυπτογραφείται με ένα μυστικό συμμετρικό κλειδί το οποίο είναι γνωστό στον αποστολέα και τον παραλήπτη του πράκτορα. Το αποτέλεσμα της κρυπτογράφησης είναι γνωστό ως κώδικας αυθεντικοποίησης. Με αυτή τη μέθοδο προστατεύεται το άθροισμα ελέγχου ακεραιότητας, ενώ επιτυγχάνεται επιπλέον και ασθενής αυθεντικοποίηση, εφόσον απαιτείται γνώση του μυστικού κλειδιού για την κρυπτογράφηση του αθροίσματος ελέγχου ακεραιότητας.

Ψηφιακές υπογραφές και υπογεγραμμένος κώδικας

Όπως αναφέρθηκε προηγουμένως οι κώδικες αυθεντικοποίησης μηνύματος παρέχουν ασθενή αυθεντικοποίηση, επειδή δεν μπορούν να χρησιμοποιηθούν για να συνδέσουν μονοσήμαντα ένα πράκτορα με κάποιον αποστολέα. Οι ψηφιακές υπογραφές συνδυάζουν αλγόριθμους δημόσιου κλειδιού με συναρτήσεις κατακερματισμού και παρέχουν ακεραιότητα και ισχυρή αυθεντικοποίηση. Στην περίπτωση των κινητών πρακτόρων, ο συγγραφέας του κώδικα του πράκτορα, μπορεί να υπογράψει τον πράκτορα με το μυστικό κλειδί του για έλεγχο ακεραιότητας, ενώ ο αποστολέας του πράκτορα μπορεί να υπογράψει τον πράκτορα με το δικό του μυστικό κλειδί για έλεγχο της αυθεντικότητας του αποστολέα. Ο παραλήπτης μπορεί να ελέγξει την ακεραιότητα του πράκτορα χρησιμοποιώντας το δημόσιο κλειδί του συγγραφέα του πράκτορα και την αυθεντικότητα του αποστολέα, χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Στην περίπτωση αυτή, είναι απαραίτητη η ύπαρξη μιας Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) για να υποστηρίξει τη σύνδεση των δημοσίων κλειδιών με τις διάφορες οντότητες.

Μη-αποσπώμενες υπογραφές

Για τον καταλογισμό ευθύνης (non-repudiation), συχνά χρησιμοποιούνται ψηφιακές υπογραφές. Ένας χρήστης μπορεί να υπογράψει ψηφιακά ένα μήνυμα χρησιμοποιώντας το μυστικό κλειδί του, ενώ το αντίστοιχο δημόσιο κλειδί του χρησιμοποιείται για επαλήθευση της υπογραφής. Στην περίπτωση των κινητών πρακτόρων οι συμβατικές ψηφιακές υπογραφές δεν μπορούν να χρησιμοποιηθούν για τον καταλογισμό ευθύνης των πρακτόρων. Όπως αναφέρεθηκε προηγουμένως, ο υπολογισμός μίας ψηφιακής υπογραφής απαιτεί τη χρήση ενός μυστικού κλειδιού. Ένας κινητός πράκτορας θα πρέπει να μπορεί να χρησιμοποιήσει ένα μυστικό κλειδί υπογραφής κατά την εκτέλεσή του σε κάποιον υπολογιστή, χωρίς να αποκαλύπτει το κλειδί αυτό στο περιβάλλον εκτέλεσης.

Οι μη-αποσπώμενες υπογραφές RSA [71] μπορούν να χρησιμοποιηθούν με ασφάλεια από κινητούς πράκτορες για καταλογισμό ευθύνης. Με το σχήμα αυτό είναι υπολογιστικά αδύνατο για έναν υπολογιστή εκτέλεσης να αποσπάσει το κλειδί υπογραφής από τα στατικά δεδομένα του πράκτορα, κατά τη διάρκεια υπολογισμού της υπογραφής. Η ασφάλεια του σχήματος στηρίζεται στην ασφάλεια του κρυπτογραφικού συστήματος RSA. Επίσης, οι μη-αποσπώμενες υπογραφές δεν απαιτούν αλληλεπίδραση του πράκτορα με τον αποστολέα του για τον υπολογισμό μίας υπογραφής. Συνεπώς μπορούν να χρησιμοποιηθούν με ασφάλεια για καταλογισμό ευθύνης. Όπως αναφέρθηκε και προηγουμένως, το σχήμα αυτό παρουσιάζεται στο τρίτο κεφάλαιο της διατριβής.

Υπογραφές πληρεξουσιότητας μίας χρήσης

Οι υπογραφές πληρεξουσιότητας (proxy signatures) επιτρέπουν σε κάποιο χρήστη να μεταβιβάσει το δικαίωμα της υπογραφής του σε κάποιον πληρεξούσιό του, ο οποίος

μπορεί υπό προϋποθέσεις να υπογράφει για λογαριασμό του αρχικού χρήστη.

Οι Kim *et al* [68] πρότειναν ένα σχήμα για υπογραφές πληρεξουσιότητας μίας χρήσης (one-time proxy signatures), το οποίο επιτρέπει σε ένα κινητό πράκτορα να υπογράφει με ασφάλεια ένα μήνυμα για καταλογισμό ευθύνης. Το σχήμα αυτό μπορεί να χρησιμοποιηθεί για τον υπολογισμό μίας υπογραφής από ένα πράκτορα και προσφέρει και καταλογισμό ευθύνης τόσο για τον πράκτορα όσο και για τον υπολογιστή εκτέλεσης.

Δυναμικές πολυ-υπογραφές

Αν και οι μη-αποσπώμενες υπογραφές μπορούν να χρησιμοποιηθούν για καταλογισμό ευθύνης κινητών πρακτόρων, περιορίζουν την μεταφερσιμότητα του πράκτορα επειδή για λόγους ασφάλειας δεν μπορούν να χρησιμοποιηθούν για περισσότερες από μία υπογραφές. Το ίδιο ισχύει και για τις υπογραφές πληρεξουσιότητας μίας χρήσης. Συνεπώς δεν είναι κατάλληλες για αυτόνομους πράκτορες. Ένας αυτόνομος πράκτορας μπορεί να μεταναστεύσει και να εκτελεστεί σειριακά σε πολλαπλούς υπολογιστές οι οποίοι δεν είναι γνωστοί εκ των προτέρων. Η λίστα των υπολογιστών εκτέλεσης παράγεται δυναμικά ανάλογα με τις ανάγκες της εφαρμογής.

Επιπλέον, οι μη-αποσπώμενες υπογραφές δεν παρέχουν καταλογισμό ευθύνης για τον υπολογιστή εκτέλεσης. Για την αντιμετώπιση αυτών των προβλημάτων έχουν αναπτυχθεί διάφοροι κρυπτογραφικοί μηχανισμοί.

Για παράδειγμα, το σχήμα δυναμικών πολυ-υπογραφών [72] το οποίο παρουσιάζεται στο τέταρτο κεφάλαιο της διατριβής, βασίζεται στο σχήμα πολυ-υπογραφών των Mitomi-Miyaji [91] και κληρονομεί αρκετές ενδιαφέρουσες ιδιότητες αυτού του σχήματος όπως ευκαμψία μηνύματος (message flexibility), ευκαμψία προτεραιότητας (order

flexibility) και επιβεβαίωση προτεραιότητας (order verifiability). Επιπλέον, είναι ανθεκτικό σε επιθέσεις απομάκρυνσης, στις οποίες μία συνωνομοσία από κακόβουλους υπολογιστές εκτέλεσης προσπαθούν να απομακρύνουν από την πολυ-υπογραφή τη μερική υπογραφή ενός ή περισσοτέρων προηγούμενων υπολογιστών εκτέλεσης. Αυτό το σχήμα μπορεί να χρησιμοποιηθεί για αυτόνομους πράκτορες και παρέχει καταλογισμό ευθύνης τόσο για τον πράκτορα όσο και για τους συμμετέχοντες υπολογιστές.

Υπογραφές πληρεξουσιότητας χωρίς προκαθορισμένο αποστολέα

Αυτά τα σχήματα υπογραφής βασίζονται στις υπογραφές πληρεξουσιότητας μίας χρήσης. Οι Lee και Kim [78] πρότειναν ένα σχήμα για υπογραφές πληρεξουσιότητας χωρίς προκαθορισμένο αποστολέα (non-designated proxy signatures), το οποίο είναι κατάλληλο για αυτόνομους πράκτορες χωρίς προκαθορισμένο δρομολόγιο. Το σχήμα αυτό παρέχει καταλογισμό ευθύνης μόνο για τον πράκτορα αλλά μπορεί να χρησιμοποιηθεί από ένα πράκτορα για πολλαπλές εκτελέσεις και υπογραφές.

Οι *ισχυρές* υπογραφές πληρεξουσιότητας (strong proxy signatures) [79] παρέχουν επιπλέον καταλογισμό ευθύνης τόσο για τον πράκτορα όσο και τους υπολογιστές εκτέλεσης. Οι συγγραφείς πρότειναν δύο σχήματα ισχυρών υπογραφών πληρεξουσιότητας, βασιζόμενα στις μη-αποσπώμενες υπογραφές RSA [71] και στο κρυπτογραφικό σύστημα του Schnor [86].

Αλυσίδωτές υπογραφές και πολυ-υπογραφές

Στην περίπτωση που ένας πράκτορας πρόκειται να εκτελέσει τον κώδικά του σε πολλούς υπολογιστές, μπορούν να χρησιμοποιηθούν αλυσιδωτές υπογραφές για τον έλεγχο της ακεραιότητας τόσο του στατικού όσο και του δυναμικού μέρους του πράκτορα [108]. Με αυτές τις υπογραφές, μετά την εκτέλεση του πράκτορα, κάθε υπολογιστής υπογράφει τη νέα κατάσταση εκτέλεσης του πράκτορα. Η υπογραφή περιλαμβάνει ολόκληρη την αλυσίδα όλων των υπογραφών από προηγούμενες εκτελέσεις του πράκτορα. Όμως, η ασφάλεια των αλυσιδωτών υπογραφών δεν μπορεί να αποδειχθεί με τη χρήση συμβατικών κρυπτογραφικών υποθέσεων. Δηλαδή, η ασφάλεια των αλυσιδωτών υπογραφών δεν μπορεί να αναχθεί στην ασφάλεια του πρωτογενούς κρυπτοσυστήματος που χρησιμοποιείται. Επίσης, οι υπογραφές αυτές δεν είναι ιδιαίτερα αποδοτικές. Τέλος, οι αλυσιδωτές υπογραφές δεν είναι ανθεκτικές σε επιθέσεις απομάκρυνσης προηγούμενων υπογραφών, που μπορεί να προέρχονται από έναν ή περισσότερους κακόβουλους υπολογιστές εκτέλεσης.

Το σχήμα δυναμικών πολυ-υπογραφών που αναφέρθηκε προηγουμένως, μπορεί να χρησιμοποιηθεί και για τον έλεγχο της ακεραιότητας του πράκτορα πέραν του καταλογισμού ευθύνης, ενώ είναι αποδοτικότερο από το σχήμα των αλυσιδωτών υπογραφών και η ασφάλειά του μπορεί να αναχθεί στο πρόβλημα του διακριτού λογαρίθμου.

Ισχυρή χρονική ασφάλεια

Η ισχυρή χρονική ασφάλεια (strong forward security) προτείνεται ως μία μέθοδος για την ελαχιστοποίηση των συνεπειών της μη-εξουσιοδοτημένης αποκάλυψης ενός ιδιωτικού κλειδιού. Σύμφωνα με τη μέθοδο αυτή το ζεύγος μυστικού/δημόσιου κλειδιού ενός χρήστη, ανανεώνεται σε τακτά χρονικά διαστήματα. Ο μηχανισμός ανανέωσης εξασφαλίζει ότι πιθανή αποκάλυψη του μυστικού κλειδιού κατά τη διάρκεια μίας

συγκεκριμένης περιόδου, δεν θα προσβάλλει την ασφάλεια του συστήματος για τις περιόδους που προηγήθηκαν ή τις περιόδους που θα ακολουθήσουν την περίοδο κατά την οποία έγινε η αποκάλυψη.

Το πρωτόκολλο που προτείνεται στο πέμπτο κεφάλαιο της διατριβής [19], παρουσιάζει μία λύση για ισχυρή χρονική ασφάλεια, η οποία βασίζεται σε ένα μηχανισμό τυχαίας ανανέωσης κλειδιού και σε μία Αρχή Πιστοποίησης (Certifying Authority). Αρχικά κάθε χρήστης επιλέγει τυχαία ένα ζεύγος μυστικού/δημόσιου κλειδιού και το πιστοποιεί μέσω της Αρχής Πιστοποίησης, αφού αρχικά αυθεντικοποιηθεί στην Αρχή με φυσικό τρόπο (out-of-band). Στη συνέχεια, στο τέλος κάθε περιόδου επιλέγει ένα νέο τυχαίο ζεύγος μυστικού/δημόσιου κλειδιού. Το μυστικό κλειδί της τρέχουσας περιόδου χρησιμοποιείται για να υπογραφεί ψηφιακά (αυθεντικοποιηθεί) το δημόσιο κλειδί της νέας περιόδου. Αυτή η υπογραφή, μαζί με το δημόσιο κλειδί της νέας περιόδου, αποστέλλονται μαζί στην Αρχή Πιστοποίησης ώστε να πιστοποιηθεί το νέο δημόσιο κλειδί. Η Αρχή Πιστοποίησης επαληθεύει την υπογραφή καθώς και το πιστοποιητικό της τρέχουσας περιόδου και σε περίπτωση που είναι έγκυρα, εκδίδει ένα ψηφιακό πιστοποιητικό για το δημόσιο κλειδί της νέας περιόδου. Σημειώνεται ότι οι έλεγχοι για την έκδοση νέων πιστοποιητικών δεν περιλαμβάνουν εκ νέου αυθεντικοποίηση εκτός σχήματος (no out-of-band authentication). Το σχήμα αυτό προσφέρει ισχυρή χρονική ασφάλεια γιατί σε περίπτωση που το μυστικό κλειδί αποκαλυφθεί σε κάποια χρονική περίοδο χωρίς να το αντιληφθεί ο νόμιμος κάτοχος του κλειδιού, τότε για την επόμενη περίοδο δύο δημόσια κλειδιά θα υποβληθούν στην Αρχή για πιστοποίηση: ένα από τον αντίπαλο και ένα από το νόμιμο χρήστη. Και τα δύο κλειδιά θα φαίνονται σωστά υπογεγραμμένα, αφού ο αντίπαλος μπορεί να πλαστογραφεί υπογραφές του νόμιμου χρήστη. Το γεγονός αυτό θα υποδείξει στην Αρχή Πιστοποίησης ότι το κλειδί του χρήστη έχει αποκαλυφθεί και κανένα από τα δημόσια κλειδιά

δεν θα πιστοποιηθεί. Συνεπώς, η αποκάλυψη του κλειδιού μπορεί έγκαιρα να γίνει αντιληπτή.

Τα δημόσια κλειδιά που προστατεύονται με ισχυρή χρονική προστασία είναι χρονικά περιορισμένα και ελεγχόμενα από την Αρχή Πιστοποίησης. Αυτά τα συγκεκριμένα χαρακτηριστικά έχουν ειδικό ενδιαφέρον για την υλοποίηση πολιτικής πρόσβασης βασισμένης σε *μεταβίβαση ρόλων* (role delegation). Υπογραφές που προστατεύονται με ισχυρή χρονική προστασία μπορούν να χρησιμοποιηθούν για την υλοποίηση προσωρινής μεταβίβασης (temporary delegation) και χρονικά εξαρτώμενης ανάκλησης της μεταβίβασης (time-dependent revocation).

2.2.3 Εξουσιοδότηση

Αποτίμηση κατάστασης

Η *αποτίμηση κατάστασης* (state appraisal) [42] είναι ένας μηχανισμός που προτάθηκε για τον έλεγχο της κατάστασης ενός πράκτορα, πριν του παραχωρηθούν οποιαδήποτε δικαιώματα πρόσβασης. Η αποτίμηση κατάστασης επιβεβαιώνει ότι η κατάσταση ενός πράκτορα δεν έχει αλλοιωθεί κατά τη διάρκεια της μετάδοσης του πράκτορα. Σε περίπτωση αλλοίωσης μεγάλου βαθμού δεν δίδεται κανένα δικαίωμα στον πράκτορα, ενώ μικρές αλλοιώσεις μπορεί να επιτρέψουν την ανάθεση περιορισμένων δικαιωμάτων. Οι συναρτήσεις αποτίμησης κατάστασης βασίζονται τόσο σε παράγοντες που εξαρτώνται από την τρέχουσα κατάσταση, όσο και σε σταθερές της κατάστασης του πράκτορα. Οι συναρτήσεις αποτίμησης κατάστασης γίνονται μέρος του κώδικα του πράκτορα και μπορεί να δημιουργούνται είτε από το συγγραφέα είτε από τον ιδιοκτήτη του πράκτορα. Η αποτίμηση κατάστασης έχει διπλή λειτουργικότητα. Αφενός μπορεί να θεωρηθεί ως μηχανισμός εξουσιοδότησης, εφόσον χρησιμοποιείται για την παραχώρηση διαφορετικών επιπέδων πρόσβασης, ανάλογα με το αποτέλεσμα της συνάρτησης

αποτίμησης. Αφετέρου, μπορεί να θεωρηθεί ως εργαλείο ελέγχου της ακεραιότητας των πρακτόρων, εφόσον ελέγχει το βαθμό που έχει τροποποιηθεί ένας πράκτορας. Ένα πρόβλημα με το μηχανισμό αποτίμησης κατάστασης είναι ότι εάν και μπορεί εύκολα να σχεδιαστεί για να αντιμετωπίσει περισσότερο προφανείς επιθέσεις, είναι δυσκολότερο να αντιμετωπίσουν επιθέσεις που δεν έχουν προβλεφθεί ή δεν μπορούν να εντοπιστούν εύκολα.

Πιστοποιητικά χαρακτηριστικών

Μία γενική μέθοδος για τον έλεγχο της συμπεριφοράς κινητού κώδικα και κινητών πρακτόρων είναι μέσω της κατανομής χαρακτηριστικών. Τα χαρακτηριστικά αναφέρονται σε κανόνες πολιτικής, οι οποίοι ελέγχουν την πρόσβαση σε υπολογιστικούς πόρους και υπηρεσίες. Τα *πιστοποιητικά χαρακτηριστικών* (attribute certificates) έχουν χρησιμοποιηθεί για τη δυναμική αντιστοίχιση δικαιωμάτων πρόσβασης για κινητό κώδικα και κινητούς πράκτορες [44, 64]. Ένα πιστοποιητικό χαρακτηριστικών περιλαμβάνει τα δικαιώματα πρόσβασης που παραχωρούνται σε κάποια οντότητα, μαζί με άλλη πληροφορία όπως τον εκδότη του πιστοποιητικού, τον ιδιοκτήτη του πιστοποιητικού, την ημερομηνία και ώρα λήξης και μία ψηφιακή υπογραφή που αυθεντικοποιεί το πιστοποιητικό. Μια Υποδομή Δημόσιου Κλειδιού, χρησιμοποιείται συνήθως για τη διαδικασία πιστοποίησης.

Πιστοποιητικά χαρακτηριστικών μπορούν επίσης να εκδοθούν για υπολογιστές εκτέλεσης. Για παράδειγμα, ο Jansen [64] πρότεινε για το σκοπό αυτό τη χρήση *πιστοποιητικών πολιτικής* (policy certificates). Τα πιστοποιητικά αυτά έχουν την ίδια δομή με τα πιστοποιητικά χαρακτηριστικών. Όμως, αντί να εκδίδονται για έναν πράκτορα και να χρησιμοποιούνται για κανόνες πολιτικής που αφορούν τον πράκτορα αυτό,

τα πιστοποιητικά πολιτικής εκδίδονται για υπολογιστές εκτέλεσης και χρησιμοποιούνται για κανόνες πολιτικής που αφορούν όλους τους πράκτορες που θα εκτελεστούν στο συγκεκριμένο περιβάλλον. Τα πιστοποιητικά χαρακτηριστικών και τα πιστοποιητικά πολιτικής μπορούν να χρησιμοποιηθούν ως κρυπτογραφικοί μηχανισμοί για την υλοποίηση δυναμικών πολιτικών πρόσβασης βασισμένων σε ρόλους [73].

Μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων

Μεταβίβαση ρόλου (role delegation) είναι η ιδιότητα μίας ενεργής οντότητας, για παράδειγμα ενός χρήστη του συστήματος που είναι μέλος ενός ρόλου με συγκεκριμένα δικαιώματα πρόσβασης, να εξουσιοδοτήσει μία άλλη οντότητα να γίνει μέλος του ρόλου αυτού για μία συγκεκριμένη χρονική περίοδο. Υπάρχει μία φυσική αναλογία μεταξύ των εννοιών του αυτόνομου πράκτορα και της μεταβίβασης ρόλων. Η βασική χρήση των κινητών πρακτόρων είναι η μεταβίβαση εργασίας (task delegation), δηλαδή η ανάθεση σε ένα πράκτορα μίας εργασίας προς διεκπεραίωση εκ μέρους μιας άλλης οντότητας. Με τη μεταβίβαση ρόλου δικαιώματα πρόσβασης μεταβιβάζονται από μία οντότητα σε μία άλλη, ώστε να εξουσιοδοτηθεί η δεύτερη οντότητα για να πραγματοποιήσει μία εργασία. Για αυτό το λόγο, διάφορα μοντέλα μεταβίβασης ρόλου έχουν προταθεί για το σχεδιασμό πολιτικών πρόσβασης, συστημάτων βασισμένων σε κινητούς πράκτορες. Στο έβδομο κεφάλαιο της διατριβής, παρουσιάζεται ένας μηχανισμός που επιτρέπει την ασφαλή μεταβίβαση ρόλων μεταξύ κινητών πρακτόρων. Η ασφάλειά του συνίσταται τόσο στην προστασία του μηχανισμού από μη εξουσιοδοτημένη μεταβίβαση, όσο και στην ύπαρξη ελεγχόμενης διαδικασίας ανάκλησης της μεταβίβασης ρόλων. Ο κρυπτογραφικός αυτός μηχανισμός σχεδιάζεται με τη βοήθεια άλλων μηχανισμών όπως οι μη-αποσπώμενες υπογραφές, η ισχυρή χρονική ασφάλεια, καθώς και τα πιστοποιητικά χαρακτηριστικών.

Threshold μη-αποσπώμενες υπογραφές

Τα threshold κρυπτογραφικά συστήματα [36] επιτρέπουν τη διαμοίραση μίας συνάρτησης (για παράδειγμα μίας συνάρτησης υπογραφής) μεταξύ ορισμένων οντοτήτων με τέτοιο τρόπο ώστε η συνάρτηση να μπορεί να υπολογιστεί για κάποια τιμή εισόδου (για παράδειγμα για κάποιο μήνυμα που πρέπει να υπογραφεί), μόνο εάν συνεργαστεί ένα πλήθος οντοτήτων μεγαλύτερο από ένα προκαθορισμένο όριο (threshold). Ο μηχανισμός αυτός επιτρέπει την κατανομή της ασφάλειας κρυπτογραφικών συναρτήσεων μεταξύ οντοτήτων. Μπορεί να αντιμετωπίσει σφάλματα με τον ίδιο τρόπο όπως και η δημιουργία αντιγράφων κλειδιών (replication), αλλά επιτρέπει επιπλέον την αντιμετώπιση κακόβουλων σφαλμάτων. Συγκεκριμένα, ακόμα και εάν ορισμένες από τις εμπλεκόμενες οντότητες συμπεριφέρονται λανθασμένα ή είναι υπό τον έλεγχο κακόβουλων χρηστών, η κρυπτογραφική συνάρτηση θα υπολογιστεί σωστά, υπό την προϋπόθεση ότι ο αριθμός των οντοτήτων που λειτουργούν όπως απαιτεί το πρωτόκολλο είναι μεγαλύτερος από το προκαθορισμένο όριο. Η έννοια των threshold υπογραφών έχει χρησιμοποιηθεί και για την τεχνολογία των κινητών πρακτόρων, με σκοπό τη διαμοίραση της δυνατότητας υπολογισμού της υπογραφής ενός χρήστη μεταξύ πολλών κινητών πρακτόρων. Οι Borselius *et al* [15] επέκτειναν τις μη-αποσπώμενες υπογραφές σε threshold υπογραφές, όπου για τη δημιουργία μιας έγκυρης υπογραφής απαιτείται η συνεργασία n από k πράκτορες ($n < k$). Το σχήμα αυτό συνδυάζει το σχήμα RSA μη-αποσπώμενων υπογραφών [71] και το threshold σχήμα υπογραφής του Shoup [106].

Στο Σχήμα 2.5 παρουσιάζεται μία ταξινόμηση των μηχανισμών που χρησιμοποιούνται για την ασφάλεια συστημάτων κινητών πρακτόρων, ανάλογα με τις προσφερόμενες υπηρεσίες.

ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ	ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ				
	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα	Καταλογισμός Ευθύνης	Αυθεντικοποίηση/ Εξουσιοδότηση
Συμμετρική Κρυπτογραφία	△ ▭ ▱				
Υβριδική Κρυπτογραφία	△ ▭ ▱				
Κρυπτογραφία Ολίσθησης	△ ▭ ▱				
Κώδικας Αυθεντικοποίησης Μυνήματος		△ ▭			△
Ψηφιακές Υπογραφές		△ ▭			△
Μη-αποσπώμενες Υπογραφές		△ ▭		△	△
Υπογραφές Πληρεξουσιότητας Μίας Χρήσης				△	
Μη-αποσπώμενες Πολύ-υπογραφές		△ ▭		△ ▱	△
Υπογραφές Πληρεξουσιότητας Χωρίς Προκαθορισμένο Αποστολέα		△ ▭		△ ▱	△
Αλυσιδωτές Υπογραφές		△ ▭			△
Ισχυρή Χρονική Ασφάλεια					▱
Αποτίμηση Κατάστασης		△	▱		▱ △
Πιστοποιητικά Χαρακτηριστικών			▱		▱ △
Threshold Μη-αποσπώμενες Υπογραφές				△ ▱	

Χρήση Μηχανισμών για την Προστασία	
Υπολογιστή Εκτέλεσης	▱
Κινητού Πράκτορα	△
Μετανάστευσης Πράκτορα	▭

Σχήμα 2.5: Κρυπτογραφικοί μηχανισμοί για συστήματα κινητών πρακτόρων

Κεφάλαιο 3

Μη-αποσπώμενη υπογραφή RSA

Στο κεφάλαιο αυτό παρουσιάζεται το πρωτόκολλο της μη-αποσπώμενης υπογραφής RSA, το οποίο αποτελεί το πρώτο σχήμα ψηφιακών υπογραφών για καταλογισμό ευθύνης κινητών πρακτόρων, με αποδεδειγμένη υπολογιστική ασφάλεια. Αρχικά γίνεται εντοπισμός των προβλημάτων ασφάλειας που απορρέουν από τη χρήση συμβατικών ψηφιακών υπογραφών σε κινητούς πράκτορες. Στη συνέχεια παρουσιάζεται η προτεινόμενη μεθοδολογία για την επίλυση του προβλήματος και το προτεινόμενο πρωτόκολλο υπογραφής. Πρώτα εφαρμόζεται η προτεινόμενη μεθοδολογία σε ηλεκτρονικές αγορές μέσω κινητών πρακτόρων για ασφαλείς συναλλαγές και ακολουθεί η περιγραφή του γενικού σχήματος της μη-αποσπώμενης υπογραφής RSA, μαζί με την απόδειξη της ασφάλειάς του στο μοντέλο Random Oracles.

3.1 Εισαγωγή

Όπως αναφέρθηκε αναλυτικά στο πρώτο κεφάλαιο, οι κινητοί πράκτορες παρέχουν συνδέσεις χαμηλού εύρους ζώνης δικτύου με αυτονομία, ασύγχρονη επικοινωνία και υποστήριξη για ετερογενή περιβάλλοντα. Τα χαρακτηριστικά αυτά καθιστούν τους κινητούς πράκτορες κατάλληλους για εφαρμογές ηλεκτρονικού εμπορίου σε ανοιχτά

δίκτυα. Ένας κινητός πράκτορας μπορεί να αναζητήσει προϊόντα ή υπηρεσίες μέσω του διαδικτύου, να διαπραγματευτεί με άλλες οντότητες για τους όρους της αγοράς και σε περίπτωση συμφωνίας να δεσμευτεί για μία αγορά για λογαριασμό του ιδιοκτήτη του. Επιπλέον οι κινητοί πράκτορες μπορούν να χρησιμοποιηθούν ως πωλητές πράκτορες. Για να δεσμευτεί ένας πράκτορας για μία συναλλαγή (αγορά ή πώληση), θα πρέπει να είναι ικανός να υπογράψει ψηφιακά για την αποδοχή της συναλλαγής αυτής, χρησιμοποιώντας ένα μυστικό κλειδί υπογραφής ή μία συνάρτηση υπογραφής του αποστολέα του.

Όμως, στα συστήματα κινητών πρακτόρων, οι κινητοί πράκτορες και οι εξυπηρετητές εκτέλεσης ανήκουν συνήθως σε οντότητες με αντικρουόμενα συμφέροντα. Για παράδειγμα ο κινητός πράκτορας μπορεί να ανήκει σε κάποιο πιθανό αγοραστή, ενώ ο εξυπηρετητής σε κάποιο ηλεκτρονικό κατάστημα (πωλητής). Κατά τη διάρκεια της εκτέλεσης ενός κινητού πράκτορα, ο πράκτορας βρίσκεται σε μια πολύ ασύμμετρη σχέση με τον εξυπηρετητή εκτέλεσης, αφού ο εξυπηρετητής πρέπει να έχει πρόσβαση στον κώδικα, τα δεδομένα και την κατάσταση εκτέλεσης του πράκτορα, έτσι ώστε να μπορεί να τον εκτελέσει.

Συνεπώς, στην περίπτωση που ένας πράκτορας επιχειρούσε να χρησιμοποιήσει ένα μυστικό κλειδί υπογραφής, ένας εχθρικός εξυπηρετητής θα μπορούσε εύκολα να το υποκλέψει και να το χρησιμοποιήσει για να υπογράφει μηνύματα της επιλογής του για λογαριασμό του ιδιοκτήτη του πράκτορα - για παράδειγμα ασύμφορες για τον ιδιοκτήτη του πράκτορα συναλλαγές.

Ένας κινητός πράκτορας μπορεί να αποκρύψει κάποια πληροφορία από τον εξυπηρετητή εκτέλεσης, με την προϋπόθεση ότι ούτε ο ίδιος ο πράκτορας θα χρησιμοποιήσει αυτή την πληροφορία κατά την εκτέλεσή του στον συγκεκριμένο εξυπηρετητή. Για παράδειγμα, ο πράκτορας μπορεί να μεταφέρει ένα μυστικό κλειδί υπογραφής (ή

μία συνάρτηση υπογραφής) κρυπτογραφημένο με κάποιο κλειδί κρυπτογράφησης. Σε περίπτωση που ο πράκτορας δεν μεταφέρει στο τμήμα των δεδομένων του το αντίστοιχο κλειδί αποκρυπτογράφησης, τότε δεν θα είναι δυνατό για κάποιο εχθρικό εξυπηρετητή να υποκλέψει το κλειδί υπογραφής, με την προϋπόθεση ότι η κρυπτογράφηση του κλειδιού υπογραφής είναι υπολογιστικά ασφαλής. Δεν είναι όμως ξεκάθαρο με ποιο τρόπο θα μπορούσε ένας πράκτορας να *χρησιμοποιήσει* ιδιωτικές πληροφορίες (όπως ένα μυστικό κλειδί) *χωρίς να αποκαλύπτονται στο περιβάλλον εκτέλεσής του.*

Μέχρι πρόσφατα, υπήρχε η γενική πεποίθηση ότι η αδυναμία των κινητών πρακτόρων μπορούσε να εμποδιστεί μόνο με λύσεις υλικού (hardware). Σύμφωνα με τους Chess *et al*: *"είναι αδύνατο να παρεμποδιστούν επιθέσεις κακόβουλων εξυπηρετητών κατά κινητών πρακτόρων, εκτός εάν χρησιμοποιηθεί ασφαλές υλικό* (tamper-resistant hardware)" [28]. Η πεποίθηση αυτή όμως αποδείχθηκε παραπλανητική και έγινε γνωστή στη βιβλιογραφία σαν *"το παράδοξο του Chess"* [104].

Οι Jakobsson και Juels [61] πρότειναν τη χρήση εκτελέσιμου κώδικα γνωστού ως X-cash, ο οποίος δεσμεύει το χρήστη σε μια δοσοληψία πληρωμής. Ο χρήστης συνδέει τον εκτελέσιμο κώδικα X-cash με ένα επονομαζόμενο *πιστοποιητικό διαπραγμάτευσης*, το οποίο μπορεί να χρησιμοποιηθεί για μια περιορισμένη αγορά. Αυτό το πρωτόκολλο είναι πρακτικό αλλά όχι πολύ ελαστικό, γιατί απαιτεί την έκδοση ενός μεγάλου αριθμού πιστοποιητικών διαπραγμάτευσης με διάφορα όρια πληρωμής, τα οποία θα χρησιμοποιηθούν για μία μόνο αγορά.

Οι Sander και Tschudin χρησιμοποιούν μια τεχνική που ονομάζεται Υπολογισμός με Κρυπτογραφικές Συναρτήσεις - ΥΚΣ (Computing with Encrypted Functions) [104]. Ο εξυπηρετητής εκτελεί μια κρυπτογραφημένη συνάρτηση $s \circ f$ όπου f είναι η συνάρτηση κρυπτογράφησης, χωρίς να έχει πρόσβαση στη συνάρτηση s. Η ασφάλεια

της μεθόδου στηρίζεται στη δυσκολία "αποσύνθεσης" της κρυπτογραφημένης συνάρτησης $s \circ f$ στις συναρτήσεις s και f. Επειδή η αυτονομία είναι βασικό χαρακτηριστικό των κινητών πρακτόρων, οι Sander και Tschudin εξερεύνησαν τις απαιτήσεις για ανάπτυξη μη-αλληλεπιδραστικών ΥΚΣ και απέδειξαν ότι για την υλοποίηση μη-αλληλεπιδραστικών ΥΚΣ θα μπορούσαν να χρησιμοποιηθούν αλγεβρικά ομοιομορφικά κρυπτογραφικά συστήματα δημόσιου κλειδιού (δηλαδή προσθετικά και πολλαπλασιαστικά ομοιομορφικά). Δυστυχώς όμως δεν υπάρχουν ασφαλή αλγεβρικά ομοιομορφικά κρυπτογραφικά συστήματα. Οπότε το πρόβλημα της προστασίας συναρτήσεων υπογραφής για κινητούς πράκτορες που εκτελούνται σε εχθρικό περιβάλλον παραμένει ανοιχτό.

3.2 Κρυπτογραφώντας μία συνάρτηση υπογραφής

Οι μη-αποσπώμενες υπογραφές προτάθηκαν αρχικά από τους Sander και Tschudin [104] και βασίζονται στην ιδέα των μη-αλληλεπιδραστικών ΥΚΣ.

Έστω ότι ένας υποψήφιος πελάτης θέλει να αποστείλει ένα κινητό πράκτορα για να αγοράσει κάποιο προϊόν από κάποιο ηλεκτρονικό κατάστημα. Ο πράκτορας θα μπορούσε αυτόνομα να αυθεντικοποιήσει τη συναλλαγή, μόνο εάν θα μπορούσε να χρησιμοποιήσει μία συνάρτηση υπογραφής s του πελάτη, η οποία θα αποτελούσε τμήμα του εκτελέσιμου κώδικα του πράκτορα. Όμως, ο πράκτορας θα εκτελεστεί σε κάποιον εξυπηρετητή άγνωστης εμπιστοσύνης. Για την προστασία της συνάρτησης υπογραφής s, ο πελάτης κρυπτογραφεί την s με μία συνάρτηση κρυπτογράφησης f, και λαμβάνει

$$f_{sig} := s \circ f \tag{3.2.1}$$

Στη συνέχεια, δίνει το ζεύγος συναρτήσεων $f(\cdot), f_{sig}(\cdot)$ στον πράκτορα, ως τμήμα

του εκτελέσιμου κώδικά του. Μετά τη μετανάστευση του πράκτορα, ο εξυπηρετητής εκτελεί το ζεύγος συναρτήσεων $f(\cdot), f_{sig}(\cdot)$ με είσοδο x για να λάβει το ζεύγος της μη-αποσπώμενης υπογραφής:

$$f(x) = m \tag{3.2.2}$$

και

$$f_{sig}(x) = s \circ f(x) = s(f(x)) = s(m) \tag{3.2.3}$$

Το ζεύγος συναρτήσεων $f(\cdot), f_{sig}(\cdot)$ επιτρέπει στον πράκτορα να υπολογίζει υπογραφές του πελάτη σε μηνύματα επιλεγμένα από τον εξυπηρετητή, χωρίς να αποκαλύπτει τη συνάρτηση υπογραφής s (ή το μυστικό κλειδί υπογραφής που περιέχεται στην s) στον εξυπηρετητή. Οι παράμετροι της συνάρτησης f είναι τέτοιες ώστε η έξοδος της f να περιέχει πάντοτε κάποιους προκαθορισμένους περιορισμούς (απαιτήσεις) του πελάτη. Συνεπώς, το μήνυμα $m = f(x)$ περικλείει τους περιορισμούς του πελάτη στην προσφορά του εξυπηρετητή. Αυτό πιστοποιείται από το αποτέλεσμα $f_{sig}(x) = s(m)$ το οποίο αποτελεί την υπογραφή του πελάτη στο μήνυμα m. Ο εξυπηρετητής δεν μπορεί να χρησιμοποιήσει το ζεύγος συναρτήσεων $f(\cdot)$, $f_{sig}(\cdot)$ για να υπογράψει *αυθαίρετα* μηνύματα, δηλαδή μηνύματα που δεν περιέχουν τους περιορισμούς του πελάτη. Οι περιορισμοί μπορεί να αφορούν λεπτομερή περιγραφή των απαιτούμενων από τον πελάτη προϊόντων, τη μέγιστη αποδεκτή τιμή και όποιες άλλες απαιτήσεις του πελάτη.

Απαιτήσεις για ασφαλείς μη-αποσπώμενες υπογραφές

Για να είναι εφαρμόσιμο και ασφαλές ένα σχήμα μη-αποσπώμενης υπογραφής, θα πρέπει να πληρεί τις παρακάτω απαιτήσεις:

1. Η εκτέλεση της κρυπτογραφημένης συνάρτησης 3.2.1 με είσοδο κάποιο μήνυμα x επιλεγμένο από τον εξυπηρετητή πρέπει να είναι εφικτή σε πολυωνυμικό χρόνο.

2. Το ζεύγος των συναρτήσεων f και s πρέπει να είναι τέτοιο ώστε να είναι υπολογιστικά αδύνατη η "αποσύνθεση" της συνάρτησης 3.2.1.

3.3 Η προτεινόμενη μεθοδολογία

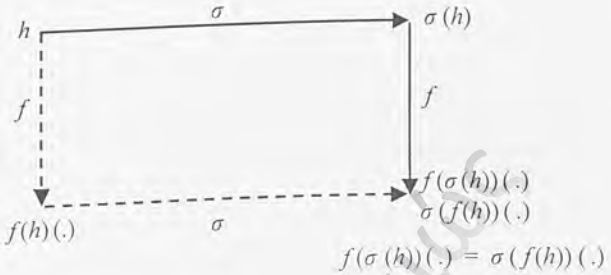
Όπως έγινε αντιληπτό, οι συναρτήσεις μη-αποσπώμενης υπογραφής χρησιμοποιούνται για να μεταβιβάσουν την ικανότητα υπογραφής ενός χρήστη σε ένα πράκτορα. Είναι ουσιαστικά υπογραφές πληρεξουσιότητας, περιορισμένες σε συγκεκριμένες απαιτήσεις εφαρμογής που έχει προκαθορίσει ο χρήστης. Μία μη-αποσπώμενη υπογραφή ενός μηνύματος m είναι έγκυρη εάν και μόνο εάν το m είναι περιορισμένο από τις απαιτήσεις εφαρμογής του χρήστη.

Ένας τρόπος να επιτευχθεί αυτό είναι με το συνδυασμό μίας συνάρτησης υπογραφής s με μία συνάρτηση περιορισμού f, η οποία χρησιμοποιείται για να συνδέσει κάθε υπογραφή στις απαιτήσεις (περιορισμούς) h του χρήστη. Η συνάρτηση μη-αποσπώμενης υπογραφής που περιορίζεται από τις απαιτήσεις h είναι: $f(s(h))(\cdot)$. Εάν οι συναρτήσεις s και f είναι *αντιμεταθετικές* τότε θα ισχύει:

$$f \circ s(h) = f(s(h))(\cdot) = s \circ f(h) = s(f(h))(\cdot) \tag{3.3.1}$$

Δηλαδή το αποτέλεσμα θα είναι και πάλι μία συνάρτηση υπογραφής — βλέπε Σχήμα 3.1.

Η προτεινόμενη μεθοδολογία για μη-αποσπώμενες υπογραφές συνδυάζει τη συνάρτηση υπογραφής RSA ($s(h) = h^d \bmod n$) με τη μονόδρομη εκθετική συνάρτηση ($f : h \to h^{(\cdot)} \bmod n$). Η αντιμεταθετικότητα των συναρτήσεων υφίσταται, αφού: $(h^d)^{(\cdot)} = h^{d(\cdot)} = (h^{(\cdot)})^d \bmod n$.



Σχήμα 3.1: Χρήση αντιμεταθετικών συναρτήσεων για μη-αποσπώμενες υπογραφές

3.4 Πρωτόκολλο για ασφαλείς δοσοληψίες με κινητούς πράκτορες

Αρχικοποίηση. Το πρωτόκολλο χρησιμοποιεί μια RSA ρύθμιση. Κάθε πελάτης επιλέγει ένα modulo n το οποίο είναι γινόμενο δύο μεγάλων πρώτων αριθμών p, q και έναν αριθμό e τέτοιο ώστε $1 < e < \phi(n) = (p-1)(q-1)$ και $gcd(e, \phi(n)) = 1$. Επίσης επιλέγει d τέτοιο ώστε $1 < d < \phi(n) = (p-1)(q-1)$ και $d \cdot e = 1 \bmod \phi(n)$, καθώς και μία κατάλληλη συνάρτηση κατακερματισμού ($hash$).

Έστω ότι C είναι ένας αναγνωριστής (identifier) για τον πελάτη, req_C οι απαιτήσεις (περιορισμοί) του πελάτη για τη συγκεκριμένη αγορά και $h = hash(C, req_C)$ μια δυαδική συμβολοσειρά η τιμή της οποίας περιορίζεται από το n. Οι περιορισμοί req_C καθορίζουν τις απαιτήσεις του πελάτη για μία συγκεκριμένη αγορά. Αυτοί μπορεί να περιλαμβάνουν την περιγραφή για ένα επιθυμητό αγαθό, τη μέγιστη τιμή που είναι αποδεκτή για τον πελάτη και μια προθεσμία για τη διανομή του προϊόντος. Περαιτέρω, μπορεί να περιέχει μία ημερομηνία λήξης και μία σφραγίδα χρόνου (timestamp). Επίσης, έστω S ένας αναγνωριστής για τον εξυπηρετητή και bid_S η προσφορά του

εξυπηρετητή η δομή της οποίας είναι αναλογική με αυτή των απαιτήσεων του πελάτη req_C.

Προετοιμάζοντας τον Πράκτορα. Ο πελάτης δίνει στον πράκτορα σαν μέρος του εκτελέσιμου κώδικά του το ζεύγος συναρτήσεων των μη-αποσπώμενων υπογραφών:

$$f(\cdot) = h^{(\cdot)} \bmod n \tag{3.4.1}$$

και

$$f_{sig}(\cdot) = k^{(\cdot)} \bmod n \tag{3.4.2}$$

όπου $k = h^d \bmod n$ είναι η RSA υπογραφή των περιορισμών του πελάτη ($h = hash(C, req_C)$). Σημειώνεται ότι η συνάρτηση f_{sig} είναι η κρυπτογράφηση $s \circ f$ της RSA συνάρτησης υπογραφής του πελάτη $s(\cdot) = (\cdot)^d \bmod n$ με την εκθετική συνάρτηση $f(\cdot) = h^{(\cdot)} \bmod n$. Δηλαδή:

$$f_{sig}(\cdot) = s \circ f(\cdot) = s(f(\cdot)) = s(h^{(\cdot)}) = (h^{(\cdot)})^d = (h^d)^{(\cdot)} = k^{(\cdot)} \bmod n \tag{3.4.3}$$

Στη συνέχεια ο πράκτορας μεταναστεύει στον εξυπηρετητή με το ζεύγος συναρτήσεων $f(\cdot)$, $f_{sig}(\cdot)$ σαν μέρος του εκτελέσιμου κώδικά του και με τα (C, req_C) σαν μέρος των δεδομένων του.

Εκτέλεση του Πράκτορα. Ο εξυπηρετητής εκτελεί το ζεύγος των συναρτήσεων του πράκτορα με είσοδο $x = hash(S, C, bid_S)$ για να αποκτήσει την RSA υπογραφή (m, z), με

$$m = f(x) = h^x \bmod n \tag{3.4.4}$$

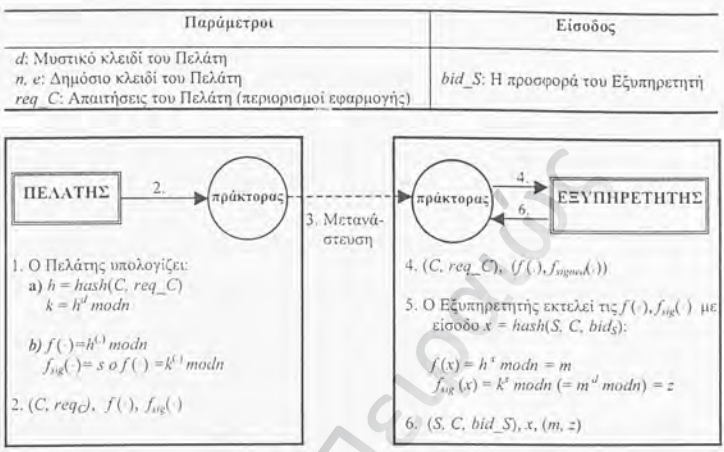
και

$$z = f_{sig}(x) = k^x \bmod n = (h^d)^x \bmod n = (h^x)^d \bmod n = m^d \bmod n = s(m). \quad (3.4.5)$$

Στο πρωτόκολλο αυτό ο πράκτορας λαμβάνει τις πιστοποιημένες απαιτήσεις του πελάτη (h, k), όπου $f(\cdot) = h^{(\cdot)} \bmod n$, $f_{sig}(\cdot) = k^{(\cdot)} \bmod n$. Ο εξυπηρετητής τις τροποποιεί συμπεριλαμβάνοντας την προσφορά bid_S μέσω της εισόδου x με τέτοιον τρόπο έτσι ώστε να αποκτήσει μία μη-αποσπώμενη υπογραφή (m, z) για τη συναλλαγή όπου $m = f(x)$ και $z = f_{sig}(x)$. Αυτό εξυπηρετεί σαν "πιστοποιητικό" το οποίο αυθεντικοποιείται από τον πελάτη ($z = m^d \bmod n$). Οι πιστοποιοιημένοι περιορισμοί του πελάτη, req_C, και η προσφορά του εξυπηρετητή bid_S, περιορίζουν το πεδίο του πιστοποιητικού (m, z) στις "βέλτιστες" συναλλαγές, δηλαδή σε εκείνες τις συναλλαγές όπου οι απαιτήσεις του πελάτη συμφωνούν με την προσφορά του εξυπηρετητή. Το πρωτόκολλο παρουσιάζεται στο Σχήμα 3.2. Στην περίπτωση που ο εξυπηρετητής αγνοήσει τους περιορισμούς req_C του πελάτη και εκτελέσει τις συναρτήσεις f, f_{sig} του Πράκτορα για να παράγει μια μη-αποσπώμενη υπογραφή του πελάτη για μια προσφορά μη συμβατή με τις απαιτήσεις req_C του πελάτη, η υπογραφή θα είναι άκυρη. Αν ο εξυπηρετητής δεν είναι πρόθυμος να δώσει κάποια προσφορά για μια αγορά, τότε προωθεί τον πράκτορα σε έναν άλλο εξυπηρετητή.

3.5 Το γενικευμένο σχήμα μη-αποσπώμενης υπογραφής RSA

Έστω ότι ένας χρήστης U θέλει να μεταβιβάσει τη συνάρτηση υπογραφής του σε ένα πράκτορα A με κάποιους περιορισμούς C_U εφαρμογής της συνάρτησης υπογραφής



Σχήμα 3.2: Ασφαλείς συναλλαγές με κινητούς πράκτορες

με τέτοιο τρόπο ώστε να είναι υπολογιστικά ανέφικτη: *α)* η απόσπαση των περιορισμών από κάθε παραγόμενη υπογραφή και *β)* η απόσπαση του μυστικού κλειδιού υπογραφής από τη συνάρτηση υπογραφής.

Ο χρήστης U επιλέγει ένα RSA modulus $n = p \cdot q$, όπου p, q είναι κατάλληλοι πρώτοι, και έναν εκθέτη e, τέτοιο ώστε $1 < e < \phi(n) = (p-1)(q-1)$, και $gcd(e, \phi(n)) = 1$. Έστω ότι d είναι τέτοιο ώστε $d \cdot e = 1 \bmod \phi(n)$, και $1 < d < \phi(n)$, και τέλος έστω ότι $hash$ είναι μια κατάλληλη συνάρτηση κατακερματισμού (για παράδειγμα SHA1, MD5). Το δημόσιο κλειδί του χρήστη U είναι (e, n) και το μυστικό κλειδί υπογραφής είναι (d, n).

Χρήστης U: Προετοιμασία του ζεύγους συναρτήσεων μη-αποσπώμενων υπογραφών

- Ο U επιλέγει τους περιορισμούς εφαρμογής C_U οι οποίοι θα συνδεθούν με την συνάρτηση υπογραφής του πράκτορα.
- Ο U υπολογίζει το αποτέλεσμα της συνάρτησης κατακερματισμού με είσοδο C_U: $h = hash(C_U)$.
- Ο U υπολογίζει την RSA υπογραφή του h: $k = h^d \bmod n$.
- Ο U δημιουργεί τον πράκτορα. Μέρος του εκτελέσιμου κώδικα είναι το ζεύγος συναρτήσεων μη-αποσπώμενων υπογραφών: $f(\cdot) = h^{(\cdot)} \bmod n$, και $f_{sig}(\cdot) = k^{(\cdot)} \bmod n$.

Πράκτορας A: Εκτέλεση του ζεύγους συναρτήσεων μη-αποσπώμενων υπογραφών

Έστω ότι M είναι ένα μήνυμα επιλεγόμενο από τον εξυπηρετητή εκτέλεσης, το οποίο υπόκειται στους περιορισμούς εφαρμογής C_U του χρήστη.

- Ο πράκτορας A υπολογίζει το αποτέλεσμα της συνάρτησης κατακερματισμού με είσοδο M: $m = hash(M)$.
- Ο πράκτορας A εκτελεί το ζεύγος συναρτήσεων $(f,\ f_{sig})$ με είσοδο m:

$$X = f(m) = h^m \bmod n, \quad \text{και} \quad Y = f_{sig}(m) = k^m \bmod n = (h^m)^d \bmod n.$$

Το ζεύγος $(X, Y) = (h^m \bmod n, (h^m)^d \bmod n)$ είναι μια RSA υπογραφή του χρήστη U στο h^m όπου συνδέει τους περιορισμούς C_U ($h = hash(C_U)$) στο μήνυμα M ($m = hash(M)$).

Επαλήθευση μίας μη-αποσπώμενης υπογραφής (X, Y) στο μήνυμα M με περιορισμούς C_U

- Έλεγχος ότι το μήνυμα M υπόκειται στους περιορισμούς C_U.
- Υπολογισμός των $h = hash(C_U)$ και $m = hash(M)$.
- Έλεγχος ότι $X = h^m \bmod n$ και $X = Y^e \bmod n$.

Η μη-αποσπώμενη υπογραφή δεν είναι έγκυρη αν οποιοσδήποτε από τους ελέγχους αποτύχει. Συνεπώς, μια υπογραφή υπολογισμένη από τον πράκτορα είναι έγκυρη, μόνο εάν το υπογεγραμμένο μήνυμα υπόκειται στους περιορισμούς C_U που επιβλήθηκαν απο τον ιδιοκτήτη του κλειδιού υπογραφής.

3.6 Ασφάλεια των μη-αποσπώμενων υπογραφών RSA

Η ασφάλεια των υπογραφών RSA μπορεί να αποδειχθεί στο μοντέλο *Random Oracles* [8] υπό την *Υπόθεση RSA*. Το μοντέλο Random Oracles είναι ένα τυπικό μοντέλο απόδειξης ασφάλειας στο οποίο οι συναρτήσεις κατακερματισμού αντιμετωπίζονται ως συναρτήσεις τυχαιότητας. Αυτό σημαίνει, ότι τα προς υπογραφή μηνύματα εισάγονται πριν την υπογραφή τους σε συναρτήσεις τυχαιότητας αντί σε συναρτήσεις κατακερματισμού.

Το πρόβλημα RSA. Δίνεται ένα τυχαίο RSA modulo n, ένας RSA εκθέτης e, και ένας τυχαίος αριθμός $h \in Z_n = \{y \mid 0 \leq y \leq n\}$. Να βρεθεί ένας αριθμός $k \in Z_n$, τέτοιος ώστε $k^e = h \in Z_n$. Η *Υπόθεση RSA* είναι ότι αυτό το πρόβλημα είναι υπολογιστικά δυσεπίλυτο. Στην συνέχεια εξετάζεται μια παραλλαγή αυτού του προβλήματος.

Το πρόβλημα μη-αποσπώμενου RSA. Δίνεται ένα τυχαίο RSA modulo n, ένας τυχαίος RSA εκθέτης e, ένας τυχαίος αριθμός $h \in Z_n$, και ένας τυχαίος αριθμός $u \in Z_n$. Να βρεθεί ένας αριθμός $K \in Z_n$, τέτοιος ώστε $K^e = h^u \in Z_n$. Η *Υπόθεση Μη-αποσπώμενου RSA* είναι ότι αυτό το πρόβλημα είναι δύσκολο.

Αποδεικνύεται ότι οι μη-αποσπώμενες υπογραφές RSA είναι ασφαλείς στο μοντέλο Random Oracles υπό αυτή την υπόθεση. Αρχικά σημειώνεται ότι το πρόβλημα μη-αποσπώμενου RSA δεν είναι δυσκολότερο από το πρόβλημα RSA. Πράγματι, αν k είναι μια λύση για ένα στιγμιότυπο του προβλήματος RSA, τότε $K = k^u \in Z_n$ είναι η λύση για την αντίστοιχη περίπτωση του μη-αποσπώμενου προβλήματος RSA. Ας παρατηρηθεί ότι με τις μη-αποσπώμενες υπογραφές RSA *δεν μπορεί* να χρησιμοποιηθεί $e = 3$ (ή γενικότερα μικρός εκθέτης ως δημόσιο κλειδί – για γρήγορη επαλήθευση) όπως γίνεται με ασφάλεια στις υπογραφές RSA. Αυτό συμβαίνει επειδή όταν $e = 3$ υπάρχει ένας τετριμμένος αλγόριθμος που θα επιλύσει το πρόβλημα της μη-αποσπώμενης υπογραφής RSA με πιθανότητα $\simeq 1/3$. Πράγματι, με αυτήν την πιθανότητα λαμβάνεται $u = 3u'$, αφού u είναι ένας τυχαίος αριθμός $\in Z_n$. Τότε το $K = h^{u'} \in Z_n$ είναι μια λύση του μη-αποσπώμενου προβλήματος RSA. Δεν είναι ξεκάθαρο εάν το πρόβλημα του μη-αποσπώμενου RSA είναι πράγματι λιγότερο ισχυρό από το πρόβλημα RSA όταν ο εκθέτης e είναι τυχαίος.

Θεώρημα 3.6.1. *Η μη-αποσπώμενη υπογραφή RSA είναι ασφαλής στο μουτέλο Random Oracles υπό την υπόθεση μη-αποσπώμενου RSA.*

Απόδειξη. Η απόδειξη είναι βασικά όμοια με αυτή για τις καθιερωμένες υπογραφές RSA. Στο μοντέλο Random Oracles [8], ένας δυνητικός πλαστογράφος μπορεί να δίνει ως είσοδο μηνύματα m_i, $i = 1, 2, \ldots, \ell$, της επιλογής του και να λαμβάνει τις αντίστοιχες υπογραφές, πριν την πλαστογράφηση μίας συγκεκριμένης μη-αποσπώμενης

υπογραφής σε ένα μήνυμα-στόχο. Στο μοντέλο Random Oracles θα χρησιμοποιηθεί μία συνάρτηση τυχαιότητας αντί μίας συνάρτησης κατακερματισμού (hash). Συνεπώς τα προς υπογραφή μηνύματα m_i θα τυχαιοποιηθούν λαμβάνοντας ως έξοδο h_i, και ο πλαστογράφος θα λάβει τις RSA υπογραφές k_i, με $k_i^e = h_i$ σε Z_n. Τότε οι συναρτήσεις των μη-αποσπώμενων υπογραφών θα είναι τα ζεύγη $(h_i^{(\cdot)}, k_i^{(\cdot)})$, $i = 1, 2, \ldots, \ell$.

Αυτή η διαδικασία δίδει την *άποψη (ιστορικό)* του πλαστογράφου, πριν την πλαστογραφία. Ας παρατηρηθεί ότι αυτό το ιστορικό μπορεί εύκολα να προσομοιωθεί, επειδή τα h_i είναι τυχαία και ομοιόμορφα κατανεμημένα. Για την προσομοίωση του ιστορικού του πλαστογράφου πριν την πλαστογραφία, επιλέγονται τυχαίοι αριθμοί k_i' σε Z_n και υπολογίζονται τα $h_i' = k_i'^e \in Z_n$. Οι προσομοιωμένες συναρτήσεις των μη-αποσπώμενων υπογραφών $(h_i'^{(\cdot)}, k_i'^{(\cdot)})$ δεν μπορούν να διακριθούν από τις πραγματικές συναρτήσεις $(h_i^{(\cdot)}, k_i^{(\cdot)})$.

Τώρα, ο πλαστογράφος πρέπει να υπολογίσει μια υπογραφή RSA σε ένα νέο μήνυμα, με ένα μη-αποσπώμενο μήνυμα ως εκθέτη. Και τα δυο μηνύματα θα πρέπει να τυχαιοποιηθούν. Έστω ότι τα τυχαία μηνύματα είναι h, u αντίστοιχα. Ο πλαστογράφος πρέπει να υπολογίσει έναν αριθμό $K \in Z_n$ τέτοιο ώστε $K^e = h^u \in Z_n$. Αυτό σημαίνει, ότι ο πλαστογράφος πρέπει να επιλύσει ένα στιγμιότυπο (n, e, h, u) του προβλήματος μη-αποσπώμενου RSA. Συνεπώς, το πρόβλημα της επιτυχημένης πλαστογραφίας έχει αναχθεί σε αυτό της επίλυσης του προβλήματος μη-αποσπώμενου RSA. □

3.7 Κύρια χαρακτηριστικά του σχήματος

Τα κύρια χαρακτηριστικά της μη αποσπώμενης υπογραφής RSA είναι τα ακόλουθα:

- Αποδοτικότητα: Η υλοποίηση του σχήματος μη-αποσπώμενης υπογραφής RSA απαιτεί για κάθε μη αποσπώμενη υπογραφή, μία εκθετική πράξη κατά την

αρχικοποίηση και δύο εκθετικές πράξεις κατά την δημιουργία και επαλήθευση της υπογραφής.

- Συμμετρικότητα καταλογισμού ευθύνης: Το πρωτόκολλο αυτό δεν είναι συμμετρικό όσον αφορά τον καταλογισμό ευθύνης του πράκτορα και του εξυπηρετητή, γιατί παρέχει καταλογισμό ευθύνης μόνο για τον πράκτορα (και κατ' επέκταση τον ιδιοκτήτη του). Σε πολλές εφαρμογές ο καταλογισμός ευθύνης του εξυπηρετητή μπορεί να είναι εκτός ενδιαφέροντος ή να αντιμετωπίζεται με ανεξάρτητες υπογραφές. Σε διαφορετική περίπτωση απαιτείται η ανάπτυξη των κατάλληλων πρωτοκόλλων πολυ-υπογραφών.

- Εμπιστευτικότητα: Στο πρωτόκολλο που περιγράφηκε δεν υπάρχει εμπιστευτικότητα. Τα ανταλλασόμενα δεδομένα μπορούν να υποκλαπούν από οποιονδήποτε παθητικό ωτακουστή. Για να επιτευχθεί εμπιστευτικότητα, ο χρήστης πρέπει να κρυπτογραφήσει τον κώδικα και τα δεδομένα του πράκτορα πριν την αποστολή του, με το δημόσιο κλειδί κρυπτογράφησης του εξυπηρετητή-παραλήπτη. Ο εξυπηρετητής πρέπει να κρυπτογραφήσει το αποτέλεσμα της εκτέλεσης του πράκτορα με το δημόσιο κλειδί κρυπτογράφησης του χρήστη - ιδιοκτήτη του πράκτορα.

- Πολλαπλές εκτελέσεις και σειρά εκτέλεσης: Σε πολλές εφαρμογές μπορεί η πολλαπλή εκτέλεση των συναρτήσεων υπογραφής του πράκτορα να δημιουργεί προβλήματα στο χρήστη. Για παράδειγμα, στην περίπτωση των ηλεκτρονικών αγορών ένας πράκτορας θα μπορούσε με αυτόν τον τρόπο να δεσμεύσει ένα χρήστη σε πολλαπλές αγορές του ίδιου αγαθού από διαφορετικά ηλεκτρονικά καταστήματα. Επίσης, σε περίπτωση πολλαπλών εκτελέσεων του πράκτορα σε

διαφορετικούς εξυπηρετητές, η σειρά εκτέλεσης μπορεί να απαιτεί επαλήθευση. Συνεπώς, το σχήμα της μη-αποσπώμενης υπογραφής RSA δεν μπορεί να χρησιμοποιηθεί για περιπτώσεις όπου απαιτούνται πολλαπλές εκτελέσεις του πράκτορα και επαλήθευση της σειράς εκτέλεσης.

Κεφάλαιο 4

Δυναμικές πολυ-υπογραφές για ασφαλείς αυτόνομους πράκτορες

Στο προηγούμενο κεφάλαιο αναλύθηκε το πρωτόκολλο μη-αποσπώμενης υπογραφής RSA, το οποίο επιτρέπει σε κινητούς πράκτορες να υπογράφουν με ασφάλεια μηνύματα, κατά τη διάρκεια της εκτέλεσής τους σε εχθρικά περιβάλλοντα. Όμως το σχήμα αυτό δεν είναι κατάλληλο για *αυτόνομους* πράκτορες, δηλαδή για πράκτορες που εκτελούνται διαδοχικά σε πολλαπλούς υπολογιστές.

Οι λύσεις που προτείνονται στη διεθνή βιβλιογραφία για ασφαλείς αυτόνομους πράκτορες είναι περισσότερο θεωρητικού ενδιαφέροντος εφόσον είναι μη πρακτικές για πραγματικές εφαρμογές. Σε αυτό το κεφάλαιο παρουσιάζεται ένα κρυπτογραφικό πρωτόκολλο για ασφαλείς αυτόνομους πράκτορες το οποίο βασίζεται σε δυναμικές πολυ-υπογραφές με ευελιξία μηνύματος. Το προτεινόμενο σχήμα είναι πρακτικό και ανθεκτικό σε επιθέσεις συνδυασμού κακόβουλων υπολογιστών.

4.1 Εισαγωγή

Οι ασθενείς τεχνολογίες κινητού κώδικα (π.χ. [57, 89]) παρέχουν τη δυνατότητα σε μια εφαρμογή να στείλει κώδικα σε μια απομακρυσμένη τοποθεσία ώστε να εκτελεστεί εκεί, ή να συνδέσει δυναμικά κώδικα που έχει ανακτηθεί από μια απομακρυσμένη τοποθεσία. Ο μεταφερόμενος κώδικας μπορεί να συνοδεύεται από ορισμένα δεδομένα αρχικοποίησης αλλά όχι και την κατάσταση εκτέλεσης. Οι ισχυρές τεχνολογίες κινητού κώδικα (π.χ. [58, 95]) παρέχουν τη δυνατότητα για την εκτέλεση κινητών πρακτόρων. Αυτές οι τεχνολογίες επιτρέπουν σε μια μονάδα εκτέλεσης (έναν κινητό πράκτορα) που εκτελείται σε ένα συγκεκριμένο εξυπηρετητή να σταματήσει την εκτέλεσή του, να μεταφερθεί σε έναν απομακρυσμένο εξυπηρετητή και να συνεχίσει την εκτέλεση στον απομακρυσμένο εξυπηρετητή μετά τη μετανάστευσή του. Οι κινητοί πράκτορες διαφέρουν από τον κινητό κώδικα στο ότι μπορούν επίσης να μεταφέρουν και να συντηρούν την *κατάσταση εκτέλεσης*, ώστε να πραγματοποιήσουν έναν υπολογισμό μέσα σε ένα κατανεμημένο περιβάλλον [112].

Οι *αυτόνομοι* κινητοί πράκτορες έχουν την επιπρόσθετη ιδιότητα ότι η εκτέλεσή τους δεν ολοκληρώνεται στον πρώτο απομακρυσμένο εξυπηρετητή. Αντίθετα, ο πράκτορας μεταναστεύει σε αρκετούς εξυπηρετητές για πολλαπλές εκτελέσεις, χωρίς καμία *αλληλεπίδραση* με τον αποστολέα του. Ένας ιδεατός αυτόνομος πράκτορας πρέπει να είναι ικανός να δημιουργεί δυναμικά το *δρομολόγιο* που θα ακολουθήσει, ανάλογα με την αλληλεπίδρασή του με τους επισκεπτόμενους εξυπηρετητές, καθώς και από τις δυναμικά δημιουργούμενες ανάγκες του. Η ταυτότητα των εξυπηρετητών που θα επισκεφτεί ή ακόμα και η διάταξη των εξυπηρετητών δεν θα πρέπει να είναι προκαθορισμένη αλλά θα πρέπει να παράγεται από τον πράκτορα κατά τη διάρκεια της μετανάστευσής του, με βάση τις οδηγίες του χρήστη. Με αυτόν τον τρόπο, ο πράκτορας μπορεί ενδεχομένως να εκμεταλλευτεί αρκετές διαθέσιμες υπηρεσίες σε ένα δίκτυο. Η

μεταφερσιμότητα και η αυτονομία κάνουν μη αναγκαίες τις μόνιμες συνδέσεις. Αυτό καθιστά τους αυτόνομους κινητούς πράκτορες κατάλληλους για συνδέσεις χαμηλού εύρους ζώνης και ασύγχρονη επικοινωνία [112].

Όμως, η εκτέλεση του πράκτορα σε πολλαπλούς υπολογιστές αυξάνει τα προβλήματα ασφάλειας των πρακτόρων. Αυτό ισχύει περισσότερο σε εφαρμογές όπου οι υπολογιστές εκτέλεσης μπορεί να έχουν αντικρουόμενα συμφέροντα. Για παράδειγμα σε εφαρμογές ηλεκτρονικού εμπορίου, όπου ο κινητός πράκτορας συλλέγει προσφορές από εξυπηρετητές ηλεκτρονικών καταστημάτων για κάποια αγορά. Σε αυτή την περίπτωση θα πρέπει, πέραν του κινητού πράκτορα, και οι εξυπηρετητές να δεσμεύονται στις προσφορές τους. Επίσης, θα πρέπει να υπάρχει η δυνατότητα επιβεβαίωσης της διάταξης των εξυπηρετητών, ώστε να υπάρχει η δυνατότητα επίλυσης διαφωνιών.

Το πρωτόκολλο της μη-αποσπώμενης υπογραφής RSA που παρουσιάστηκε στο προηγούμενο κεφάλαιο δεν παρέχει καταλογισμό ευθύνης για τον υπολογιστή εκτέλεσης, αλλά μόνο για τον πράκτορα. Επίσης, δεν μπορεί να χρησιμοποιηθεί για την εκτέλεση του πράκτορα σε πολλαπλούς υπολογιστές, επειδή δεν υπάρχει η δυνατότητα επαλήθευσης της διάταξης (σειράς) των υπολογιστών εκτέλεσης. Συνεπώς δεν είναι κατάλληλο για την προστασία αυτόνομων πρακτόρων [21, 72].

Οι Cachin *et al* [21] πρότειναν μια λύση για αυτόνομους πράκτορες η οποία βασίζεται σε *κωδικοποιημένα κυκλώματα* (encrypted circuits) [113] και στη μέθοδο *επιλήσμονος μεταφοράς* (oblivious transfer) [17]. Αν και αυτή η προσέγγιση είναι ενδιαφέρουσα από θεωρητική άποψη, είναι μη αποδοτική και για αυτό το λόγο μη πρακτική.

Στο κεφάλαιο αυτό περιγράφεται ένα πρωτόκολλο πολυ-υπογραφών, κατάλληλο για την εκτέλεση αυτόνομων κινητών πρακτόρων, το οποίο παρέχει καταλογισμό ευθύνης τόσο για τον πράκτορα όσο και για τους υπολογιστές εκτέλεσης. Το πρωτόκολλο

αυτό αποτελεί βελτίωση του σχήματος πολυ-υπογραφών των Mitomi και Miyaji [91].

Στην ενότητα 4.2 παρουσιάζεται το σχήμα πολυ-υπογραφών των Mitomi-Miyaji, αναλύεται η χρήση του σχήματος για αυτόνομους πράκτορες και παρουσιάζεται μία αδυναμία του σχήματος σε τέτοιες εφαρμογές. Στην ενότητα 4.2.2 παρουσιάζεται η τροποποίηση του σχήματος η οποία αντιμετωπίζει αυτή την αδυναμία. Τέλος η ενότητα 4.2.3 ολοκληρώνει το κεφάλαιο.

Σημείωση 4.1.1. Σε ένα σενάριο αυτόνομων πρακτόρων η λίστα των εξυπηρετητών που θα επισκεφτεί ένας πράκτορας δεν είναι προκαθορισμένη, αλλά παράγεται δυναμικά. Για παράδειγμα, κάθε εξυπηρετητής μπορεί να επιλέξει ανεξάρτητα τον επόμενο εξυπηρετητή. Η επιλογή αυτή μπορεί να περιοριστεί από τις απαιτήσεις του πελάτη, ή από τα αποτελέσματα των προηγούμενων εκτελέσεων του πράκτορα, εάν αυτά δεν είναι κρυπτογραφημένα. Στο πρωτόκολλο που παρουσιάζεται σε αυτό το κεφάλαιο θεωρείται για απλότητα, ότι κάθε εξυπηρετητής επιλέγει τον επόμενο εξυπηρετητή σύμφωνα με κάποιους κανόνες όχι αυστηρά καθορισμένους, οι οποίοι λαμβάνουν υπόψιν τις απαιτήσεις του πελάτη. Για παράδειγμα, οι απαιτήσεις του πελάτη μπορεί να υλοποιούνται μέσω *κανόνων πολιτικής* (policy rules) τους οποίους ακολουθεί ο πράκτορας κατά την εκτέλεσή του. Όμως το πρωτόκολλο μπορεί εύκολα να προσαρμοστεί σε άλλες διαδικασίες επιλογής.

4.2 Ασφαλίζοντας αυτόνομους πράκτορες με δυναμικά παραγόμενες πολυ-υπογραφές

Οι Mitomi και Miyaji [91] πρότειναν ένα σχήμα πολυ-υπογραφών με τρεις καινοτόμες ιδιότητες: α) *ευελιξία μηνύματος*, β) *ευελιξία σειράς* και γ) *επαληθευσιμότητα σειράς*[1]. Η ασφάλεια αυτού του σχήματος βασίζεται στο Πρόβλημα του Διακριτού Λογαρίθμου - ΠΔΛ (Discrete Logarithm Problem - DLP).[2] Σύμφωνα με αυτό το σχήμα, ένας χρήστης υπογράφει ένα μήνυμα και κατόπιν το προωθεί σε κάποιον άλλο χρήστη. Κάθε χρήστης μπορεί να τροποποιήσει το μήνυμα και να υπογράψει το τροποποιημένο μέρος. Η σειρά των χρηστών που υπογράφουν, ακόμη και οι ίδιοι οι χρήστες, δεν χρειάζονται να προσδιοριστούν εκ των προτέρων αλλά μπορούν να δημιουργηθούν δυναμικά. Η διαδικασία επαλήθευσης, αποδεικνύει ποιος χρήστης υπέγραψε ποια τροποποίηση καθώς και τη σειρά με την οποία συμμετείχαν οι χρήστες στο πρωτόκολλο πολυ-υπογραφής. Το σχήμα έχει ένα μόνο κύκλο εκτέλεσης (one-round), κάτι που το καθιστά κατάλληλο για αυτόνομους κινητούς πράκτορες, αφού δεν απαιτείται αλληλεπίδραση μεταξύ των συμμετεχόντων.

Παρακάτω, περιγράφεται το σχήμα πολυ-υπογραφών των Mitomi και Miyaji και τονίζεται μία αδυναμία του, αναφορικά με τη χρήση του για κινητούς αυτόνομους πράκτορες. Στη συνέχεια προτείνεται μία τροποποίηση η οποία αντιμετωπίζει αυτή την αδυναμία, και τελικά το τροποποιημένο πρωτόκολλο χρησιμοποιείται για ασφαλείς συναλλαγές αυτόνομων πρακτόρων.

[1] Το πρωτόκολλο της μη-αποσιώπητης υπογραφής RSA που παρουσιάστηκε στο τρίτο κεφάλαιο έχει επίσης αυτές τις ιδιότητες, αλλά στο πρωτόκολλο εκείνο εμπλέκονται μόνο δύο οντότητες.

[2] Ένα σχήμα πολυ-υπογραφών με αυτές τις ιδιότητες, βασισμένο στο κρυπτοσύστημα RSA προτάθηκε επίσης από τις Mitomi και Miyaji [91]. Όμως η ασφάλειά του είναι μόνο ευρεστική.

4.2.1 Το σχήμα πολυ-υπογραφών των Mitomi-Miyaji με ευελιξία μηνύματος

Έστω ότι οι p, q είναι επαρκώς μεγάλοι πρώτοι αριθμοί με $p = 2q + 1$, και $g \in Z_p^*$ ένας γεννήτορας τάξεως q. Κάθε χρήστης U_i, $1 \leq i \leq n$ παράγει ένα ζεύγος μυστικού/δημόσιου κλειδιού $x_i \in Z_q^*$ και $y_i = g^{x_i} \bmod p$, αντίστοιχα, και δημοσιεύει το δημόσιο κλειδί μαζί με τις πληροφορίες ταυτότητάς του ID_i μέσω μιας Αρχής Πιστοποίησης. Τέλος, έστω ότι h συμβολίζει μία κατάλληλη συνάρτηση κατακερματισμού (hash) και ότι "||" συμβολίζει την ένωση συμβολοσειρών.

Δημιουργία υπογραφής

1. Ο πρώτος χρήστης U_1 επιλέγει ένα μήνυμα m_1, και το υπογράφει ως εξής:

   Επιλογή τυχαίου αριθμού $k_1 \in Z_q^*$.

   Υπολογισμός των τιμών:

   $R_1 = g^{k_1} \bmod p$,

   $r_1 = (h(m_1||ID_1))^{-1} \cdot R_1 \bmod q$, και

   $s_1 = (x_1 r_1 + 1) \cdot k_1^{-1} \bmod q$.

   Στη συνέχεια ο χρήστης U_1 αποστέλλει τα (m_1, ID_1, s_1, r_1) στο χρήστη U_2.

2. Ο χρήστης U_j, $1 < j \leq n$, λαμβάνει τα $(m_1, \ldots, m_{j-1}||ID_1, \ldots, ID_{j-1}||s_1, \ldots, s_{j-1}||r_{j-1})$ από τον προηγούμενο χρήστη U_{j-1} και επιλέγει μια "τροποποίηση" m_j του μηνύματος m_1. Έπειτα ο χρήστης U_j υπογράφει το μήνυμα m_j ως εξής:

   Επιλογή τυχαίου αριθμού $k_j \in Z_q^*$.

   Υπολογισμός των τιμών:

   $R_j = g^{k_j} \bmod p$,

   $r_j = (h(m_j||ID_j)r_{j-1})^{-1} \cdot R_j \bmod q$, και

$s_j = (x_j r_j + 1) \cdot k_j^{-1} \bmod q$.

Στη συνέχεια ο χρήστης U_j αποστέλλει τα $(m_1, \ldots, m_j || ID_1, \ldots, ID_j || s_1, \ldots, s_j || r_j)$ στον επόμενο χρήστη U_{j+1}.

3. Ο τελευταίος χρήστης U_n χρησιμοποιεί τη μερική πολυ-υπογραφή που έλαβε από τον U_{n-1} για να υπολογίσει την πολυ-υπογραφή των μηνυμάτων $(m_1, \ldots, m_n)$ από τους χρήστες $U_1, \ldots, U_n$ ως:
$(ID_1, s_1, m_1), \ldots, (ID_{n-1}, s_{n-1}, m_{n-1}), (ID_n, s_n, r_n, m_n)$.

Επαλήθευση υπογραφής

Έστω ότι $(ID_1, s_1, m_1), \ldots, (ID_{n-1}, s_{n-1}, m_{n-1}), (ID_n, s_n, r_n, m_n)$ είναι μια πολυ-υπογραφή.

1. Για κάθε $j = n, n-1, \ldots, 2$, χρησιμοποιείται το δημόσιο κλειδί y_j του χρήστη U_j και υπολογίζεται:
$R'_j = g^{s_j^{-1}} \cdot y_j^{r_j s_j^{-1}} \bmod p$,
$T_j = R'_j \cdot r_j^{-1} \bmod q$, και
$r_{j-1} = T_j \cdot (h(m_j || ID_j))^{-1} \bmod q$.
Η διαδικασία επαναλαμβάνεται για $j = j - 1$.

2. Υπολογίζεται:
$R'_1 = g^{s_1^{-1}} \cdot y_1^{r_1 s_1^{-1}} \bmod p$,
$T_1 = R'_1 \cdot r_1^{-1} \bmod q$
και επαληθεύεται ότι $T_1 = h(m_1 || ID_1)$.

Σημειώνεται ότι ο αλγόριθμος επαλήθευσης μπορεί επίσης να χρησιμοποιηθεί για την επαλήθευση της ορθότητας των μερικών πολυ-υπογραφών.

4.2.2 Χρησιμοποιώντας πολυ-υπογραφές με ευελιξία μηνύματος για αυτόνομους πράκτορες

Για να γίνει κατανοητή η χρήση του σχήματος πολυ-υπογραφών για αυτόνομους κινητούς πράκτορες, παρουσιάζεται το ακόλουθο σενάριο. Ένας κινητός πράκτορας αποστέλλεται από έναν πελάτη για να αγοράσει κάποια αγαθά. Ο πελάτης είναι ο πρώτος χρήστης U_1 μιας δυναμικά παραγόμενης πολυ-υπογραφής με ευελιξία μηνύματος και m_1 είναι ένα μήνυμα που περιλαμβάνει τις προδιαγραφές του πελάτη για την αγορά, όπως η περιγραφή του προϊόντος, η μέγιστη τιμή, κτλ. Κάθε πωλητής U_i, $i = 2, 3, \ldots, n$ διαβάζει το μήνυμα m_1 και αν αποφασίσει να κάνει μια προσφορά για την αγορά, εκτελεί το πρωτόκολλο πολυ-υπογραφής με είσοδο ένα μήνυμα m_i, όπου m_i είναι η προσφορά του U_i. Για εμπιστευτικότητα, ο χρήστης U_i μπορεί να κρυπτογραφήσει την προσφορά του m_i, χρησιμοποιώντας το δημόσιο κλειδί κρυπτογράφησης του πελάτη U_1. Αφού ο πράκτορας έχει συλλέξει προσφορές από έναν επαρκή αριθμό πωλητών, επιστρέφει στον πελάτη με την πολυ-υπογραφή. Κατά τη διαδικασία της επαλήθευσης, ο πελάτης αποφασίζει ποια από τις προσφορές των χρηστών είναι η πλέον συμφέρουσα και τελικά τη δημοσιεύει μαζί με την πολυ-υπογραφή.

4.2.3 Μία επίθεση αποκλεισμού

Το σχήμα πολυ-υπογραφής των Mitomi και Miyaji υπόκειται σε επιθέσεις *αποκλεισμού* από κακόβουλους υπογράφοντες. Σε μια επίθεση αποκλεισμού, ένας ή περισσότεροι κακόβουλοι υπογράφοντες προσπαθούν να αποκλείσουν ορισμένους από τους προηγούμενους υπογράφοντες που έχουν ήδη συμμετάσχει στο πρωτόκολλο σε κάποια μερική πολυ-υπογραφή. Υπάρχουν αρκετά κίνητρα για τέτοιες επιθέσεις. Ένα τουλάχιστον κίνητρο για το σενάριο που εξετάζεται, είναι να αποκλείσουν ανταγωνιστικές

προσφορές.

Στη συνέχεια περιγράφεται πώς εκτελείται μία επίθεση αποκλεισμού. Έστω ότι ο U_a είναι ένας κακόβουλος χρήστης που έχει λάβει την μερική πολυ-υπογραφή των $U_1, \ldots, U_{a-1}$ στα μηνύματα $m_1, \ldots, m_{a-1}$. Ο U_a αρχικά εφαρμόζει τον αλγόριθμο επαλήθευσης (ο οποίος περιγράφηκε στην παράγραφο 4.2.1) στην μερική πολυ-υπογραφή που έλαβε από τον U_{a-1}, ώστε να ανακτήσει τα r_{a-j-1} για κάποιο $j > 1$. Έπειτα ο U_a εκτελεί το πρωτόκολλο υπογραφής χρησιμοποιώντας το ανακτημένο r_{a-j-1} με τον ίδιο τρόπο όπως θα έκανε ο πραγματικός χρήστης U_{a-j}, για να υπολογίσει μια μερική πολυ-υπογραφή των $U_1, \ldots, U_{a-j-1}, U_a$:

$$(ID_1, s_1, m_1), \ldots, (ID_{a-j-1}, s_{a-j-1}, m_{a-j-1}), (ID_a, s_a, r_a, m_a).$$

Τέλος, ο U_a αποστέλλει το αποτέλεσμα στον U_{a+1}. Αυτό αποκλείει τους j υπογράφοντες $U_{a-j}, \ldots, U_{a-1}$. Συνεπώς, υφίσταται η ανάγκη να υιοθετηθεί ένας μηχανισμός ο οποίος να μπορεί να χρησιμοποιηθεί για να αποδείξει την εγκυρότητα της αρχικής σειράς υπογραφόντων.

4.2.4 Μία βασική λύση για απόδειξη της σειράς των υπογραφόντων

Ένας τρόπος για την αντιμετώπιση αυτής της αδυναμίας, είναι η ακόλουθη τροποποίηση του αλγόριθμου δημιουργίας της πολυ-υπογραφής. Κάθε υπογράφοντας U_i επιλέγει τον επόμενο χρήστη (στην περίπτωση όπου το πρωτόκολλο χρησιμοποιείται για αυτόνομους πράκτορες τον επόμενο εξυπηρετητή εκτέλεσης) U_{i+1} και περιλαμβάνει στο μήνυμά του m_i τον προσδιοριστή του επόμενου χρήστη. Συνεπώς το m_i αντικαθίσταται από το $m_i || ID_{i+1}$. Με αυτήν την τροποποίηση, κάθε υπογράφοντας *δεσμεύεται* να αποστείλει τον πράκτορα σε ένα συγκεκριμένο προορισμό, κατά την

εκτέλεση του αλγόριθμου δημιουργίας της υπογραφής.

Ένας κακόβουλος χρήστης U_a που προσπαθεί να αποκλείσει j προηγούμενους χρήστες, θα πρέπει τώρα να πλαστογραφήσει την μερική πολυ-υπογραφή του χρήστη U_{a-j-1} με τέτοιο τρόπο ώστε αυτός ο συγκεκριμένος χρήστης να προσδιορίζει τον U_a ως τον επόμενο συμμετέχοντα. Όμως, όπως αποδεικνύεται στην εργασία [91] η ασφάλεια του σχήματος πολυ-υπογραφών των Mitomi-Miyaji στηρίζεται στη δυσκολία επίλυσης του Προβλήματος του Διακριτού Λογαρίθμου. Συνεπώς, ο κακόβουλος χρήστης θα αποτύχει, δεδομένης της υπολογιστικής ασφάλειας του Προβλήματος του Διακριτού Λογαρίθμου. Αυτή η τροποποίηση προσθέτει στο σχήμα πολυ-υπογραφής *αποδεδειγμένη* επαλήθευση σειράς, αφού τώρα κάθε χρήστης μπορεί να χρησιμοποιήσει την μερική πολυ-υπογραφή που έχει λάβει από τον προηγούμενο χρήστη ως απόδειξη συμμετοχής του στην αρχική πολυ-υπογραφή. Με αυτήν την τροποποίηση οι κακόβουλοι χρήστες που πραγματοποιούν επιθέσεις αποκλεισμού μπορούν να εντοπιστούν.

Παρόλα αυτά, η απόδειξη της σειράς με την οποία έχουν υπογράψει οι χρήστες, σε αυτή τη λύση, βασίζεται στη *μορφοποίηση του μηνύματος* και όχι στη δομή του σχήματος. Στην ενότητα 4.2.5 τροποποιείται το σχήμα των Mitomi-Miyaji [91] σε ένα δυναμικά παραγόμενο σχήμα πολυ-υπογραφής με ευελιξία μηνύματος και με *δομική* επαλήθευση σειράς υπογραφόντων, δηλαδή η συμμετοχή κάθε υπογράφοντα στην αρχική πολυ-υπογραφή ελέγχεται κατά τη διάρκεια της ίδιας της επαλήθευσης της υπογραφής.

4.2.5 Δομική επαλήθευση σειράς υπογράφοντος

Σε αυτήν την τροποποιημένη εκδοχή του σχήματος πολυ-υπογραφής των Mitomi-Miyaji, κάθε υπογράφων U_j επιλέγει τον επόμενο χρήστη U_{j+1} και χρησιμοποιεί το

δημόσιο κλειδί του U_{j+1} στην διαδικασία δημιουργίας της (μερικής) πολυ-υπογραφής. Εφόσον η ταυτότητα του επόμενου χρήστη είναι απαραίτητο μέρος της παραγωγής της υπογραφής, κάθε χρήστης που συμμετέχει στην πολυ-υπογραφή δεσμεύεται να στείλει τον πράκτορα σε έναν συγκεκριμένο προορισμό.

Δημιουργία υπογραφής

1. Ο πρώτος χρήστης U_1 επιλέγει ένα μήνυμα m_1 και τον επόμενο χρήστη U_2, το δημόσιο κλειδί του οποίου είναι y_2, και μετά υπογράφει το μήνυμα ως εξής:

   Επιλογή τυχαίου αριθμού $k_1 \in Z_q^*$.

   Υπολογισμός των τιμών:

   R_1, r_1, όπως στο Βήμα 1 της Ενότητας 4.2.1, και

   $s_1 = (x_1 r_1 + y_2) \cdot k_1^{-1} \bmod q$.

   Στη συνέχεια ο U_1 αποστέλλει τα (m_1, ID_1, s_1, r_1) στον επόμενο χρήστη U_2.

2. Ο χρήστης U_j, $1 < j \leq n$, λαμβάνει $(m_1, \ldots, m_{j-1} || \ ID_1, \ldots, ID_{j-1} || \ s_1, \ldots, s_{j-1} || \ r_{j-1})$ από τον U_{j-1} και επιλέγει μια τροποποίηση m_j του μηνύματος m_1 μαζί με τον επόμενο προορισμό U_{j+1}, του οποίου το δημόσιο κλειδί είναι y_{j+1}.

   Στη συνέχεια ο U_j υπογράφει το m_j ως εξής:

   Επιλογή τυχαίου αριθμού $k_j \in Z_q^*$.

   Υπολογισμός των τιμών:

   R_j, r_j, όπως στο Βήμα 2 της Ενότητας 4.2.1 και

   $s_j = (x_j r_j + y_{j+1}) \cdot k_j^{-1} \bmod q$.

   Κατόπιν ο U_j αποστέλλει τα $(m_1, \ldots, m_j || \ ID_1, \ldots, ID_j || \ s_1, \ldots, s_j || \ r_j)$ στον επόμενο χρήστη U_{j+1}.

3. Ο τελευταίος χρήστης U_n χρησιμοποιεί την μερική πολυ-υπογραφή που έλαβε από τον U_{n-1} για να υπολογίσει την τελική πολυ-υπογραφή και προσδιορίζει για

επόμενο προορισμό τον αρχικό χρήστη U_1 στον υπολογισμό του s_n ως: $s_n = (x_n r_n + y_1) \cdot k_n^{-1} \bmod q$.

Επαλήθευση υπογραφής

Έστω ότι $(ID_1, s_1, m_1), \ldots, (ID_{n-1}, s_{n-1}, m_{n-1}), (ID_n, s_n, r_n, m_n)$ είναι μία πολυ-υπογραφή παραγόμενη με τον παραπάνω αλγόριθμο δημιουργίας πολυ-υπογραφών.

1. Για $j = n, n-1, \ldots, 2$. χρησιμοποιείται το δημόσιο κλειδί y_j του U_j, όπως επίσης και το δημόσιο κλειδί y_{j+1} του επιλεγόμενου προορισμού U_{j+1} του U_j και υπολογίζεται:
   $R'_j = g^{s_j^{-1} \cdot y_{j+1}} \cdot y_j^{r_j s_j^{-1}} \bmod p$, $T_j = R'_j \cdot r_j^{-1} \bmod q$ και
   $r_{j-1} = T_j \cdot (h(m_j || ID_j))^{-1} \bmod q$. Το βήμα αυτό επαναλαμβάνεται για $j = j-1$. Για τον πρώτο γύρω όπου $j = n$, τίθεται $y_{j+1} := y_1$.

2. Υπολογίζεται $R'_1 = g^{s_1^{-1} \cdot y_2} \cdot y_1^{r_1 s_1^{-1}} \bmod p$, $T_1 = R'_1 \cdot r_1^{-1} \bmod q$ και επαληθεύεται ότι $T_1 = h(m_1 || ID_1)$.

Παρατήρηση 1. Ένας συνδυασμός κακόβουλων χρηστών θα μπορούσε να επανεκτελέσει το πρωτόκολλο πολυ-υπογραφών για να παρακάμψει έναν ή περισσότερους συμμετέχοντες. Αυτό όμως θα είναι για ένα μήνυμα με διαφορετική σειρά. Οι αποκλειόμενοι χρήστες μπορούν τότε να παράγουν τις μερικές πολυ-υπογραφές τους με την αρχική σειρά, ως απόδειξη του αποκλεισμού τους. Προφανώς τέτοιες καταχρήσεις δεν μπορούν να παρεμποδιστούν, και το καλύτερο που μπορεί να επιτευχθεί είναι εκ των υστέρων ανίχνευση.

Παρατήρηση 2. Η επιλογή του επόμενου προορισμού μπορεί να προσδιοριστεί με αρκετούς τρόπους. Για παράδειγμα, μπορεί να προσδιορίζεται από τη διαδικασία προσφορών. Θα πρέπει να παρατηρηθεί όμως, ότι ένας κακόβουλος εξυπηρετητής μπορεί πάντα να μεταβάλλει τη διαδρομή του πράκτορα εάν αυτή δεν είναι κρυπτογραφικά προκαθορισμένη. Παρόλα αυτά, μπορεί να επιτραπεί στον πράκτορα να διαδραματίσει έναν ρόλο στο δρομολόγιο, αν οι απαιτήσεις m_1 του πελάτη εμπεριέχουν κάποιους κανόνες προορισμού.

4.3 Συμπεράσματα

Οι αυτόνομοι κινητοί πράκτορες εκμεταλλεύονται τα πλεονεκτήματα των κατανεμημένων εφαρμογών στα ανοικτά δίκτυα. Όμως, απαιτείται η προστασία αυτόνομων πρακτόρων από δυνητικούς κακόβουλους εξυπηρετητές, μιας και οι υπάρχουσες λύσεις είναι μη πρακτικές για ασφαλείς εκτελέσεις του πράκτορα σε πολλαπλούς εξυπηρετητές. Σε αυτό το κεφάλαιο παρουσιάστηκε μία λύση για ασφαλείς αυτόνομους πράκτορες, η οποία βασίζεται σε δυναμικά παραγόμενες πολυ-υπογραφές. Στο προτεινόμενο σχήμα, δεν είναι δυνατό ένας ή περισσότεροι κακόβουλοι χρήστες να αποκλείσουν τα αποτελέσματα εκτέλεσης οποιουδήποτε προηγούμενου χρήστη, χωρίς να ανιχνευτεί μία τέτοια επίθεση.

Κεφάλαιο 5

Ισχυρή χρονική ασφάλεια

Η χρονική ασφάλεια έχει προταθεί ως μέθοδος ελαχιστοποίησης των συνεπειών από τη μη-εξουσιοδοτημένη αποκάλυψη ενός μυστικού κλειδιού. Σε αυτό το κεφάλαιο αναλύεται αυτή η μέθοδος και εξετάζεται μια αδυναμία της, η οποία οφείλεται στο γεγονός ότι η αποκάλυψη του μυστικού κλειδιού μπορεί να μην εντοπιστεί έγκαιρα. Όλα τα κρυπτοσυστήματα χρονικής ασφάλειας που έχουν προταθεί μέχρι τώρα είναι ευπαθή κατά την περίοδο ανάμεσα στην αποκάλυψη κλειδιού και στον εντοπισμό της αποκάλυψης. Στη συνέχεια, παρουσιάζεται η έννοια της ισχυρής χρονικής ασφάλειας η οποία στοχεύει να προστατέψει τα κρυπτογραφικά παραγόμενα στοιχεία όχι μόνο για τις περιόδους πριν την αποκάλυψη του κλειδιού αλλά και μετά από αυτήν. Τέλος, παρουσιάζονται δυο εφαρμογές με αυτή την πρωτότυπη ιδιότητα: μία βασική λύση εφαρμόσιμη σε οποιοδήποτε κρυπτοσύστημα δημόσιου κλειδιού και ένα σχήμα διαμοίρασης κλειδιού (key escrow system) βασισμένο στο κρυπτοσύστημα ElGamal.

5.1 Εισαγωγή

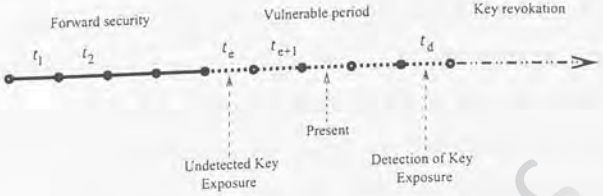
Ένα σημαντικό θέμα ασφάλειας σε όλα τα κρυπτοσυστήματα είναι η προστασία των μυστικών κλειδιών από μη-εξουσιοδοτημένη αποκάλυψη. Αν ο αντίπαλος αποκτήσει τα μυστικά κλειδιά ενός χρήστη για κάποιο σχήμα κρυπτογράφησης, τότε ο αντίπαλος μπορεί να αποκρυπτογραφήσει όλα τα κρυπτογραφήματα που προορίζονται για αυτόν το χρήστη και συνεπώς χάνεται η εμπιστευτικότητα του σχήματος. Στην περίπτωση που η αποκάλυψη αφορά ένα σχήμα υπογραφής, τότε ο αντίπαλος μπορεί να υποκριθεί ένα νόμιμο χρήστη. Το πρόβλημα της αποκάλυψης κλειδιού είναι κρίσιμο σε ανοιχτά περιβάλλοντα όπως το διαδίκτυο, όπου κάθε κόμβος υπολογιστών είναι δυνητικό θύμα των χάκερ. Συνεπώς, είναι αναγκαία η υιοθέτηση μηχανισμών που ελαχιστοποιούν τις συνέπειες της αποκάλυψης κλειδιού. Μέχρι τώρα, αυτοί οι μηχανισμοί γενικά στηρίζονται σε κατανεμημένους υπολογισμούς, περιοδική ανανέωση κλειδιού και μηχανισμούς ανάκλησης κλειδιού.

Ο Gunther [52] ήταν ο πρώτος που πρότεινε έναν κρυπτογραφικό μηχανισμό με ανανέωση κλειδιού που προστατεύει την εμπιστευτικότητα όλων των κρυπτογραφημένων μηνυμάτων πριν την αποκάλυψη του κλειδιού. Με αυτόν το μηχανισμό όλο το κρυπτογραφημένο υλικό προστατεύεται από την αποκάλυψη κλειδιού, από τη στιγμή που πραγματοποιείται η ανανέωση των κλειδιών. Αυτή η ιδιότητα ονομάστηκε *χρονική μυστικότητα* (forward secrecy). Με την χρονική μυστικότητα, η αποκάλυψη μυστικών κλειδιών μακράς διάρκειας δεν θέτει σε κίνδυνο την μυστικότητα προηγούμενου κρυπτογραφημένου υλικού [39, 52]. Μια λύση για χρονική μυστικότητα σε συστήματα πολλαπλής μετάδοσης πραγματικού χρόνου με δυναμικές ομάδες, προτάθηκε από τους McGrew και Sherman [85]. Οι Burmester, Desmedt, και Seberry [20] πρότειναν ένα σύστημα διαμοίρασης με χρονική μυστικότητα. Επίσης, έχουν προταθεί

λύσεις για το αντίστοιχο πρόβλημα προστασίας από αποκάλυψη κλειδιών που χρησιμοποιούνται για ψηφιακές υπογραφές. Οι Herzberg *et al* [54] πρότειναν threshold σχήματα υπογραφών (βλέπε επίσης [36]) στα οποία οι χρήστες ανανεώνουν τα μερίδια των κλειδιών τους (key shares) σε τακτά χρονικά διαστήματα. Αυτά τα σχήματα προσφέρουν χρονική ασφάλεια,[1] όμως η διανομή των μεριδίων των κλειδιών και ο κατανεμημένος υπολογισμός που απαιτείται για τον υπολογισμό των υπογραφών τα καθιστά μη αποδοτικά [7]. Οι Bellare και Miner [7] πρότειναν ένα σχήμα χρονικής ασφάλειας για ψηφιακές υπογραφές, η ασφάλεια του οποίου μπορεί να αποδειχθεί στο μοντέλο Random Oracles [8]. Πρόσφατα ο Krawczyk [75] πρότεινε μια λύση που μπορεί να χρησιμοποιηθεί με οποιοδήποτε σχήμα υπογραφών.

Υπάρχει μία εγγενής αδυναμία στα συστήματα χρονικής ασφάλειας, που προκύπτει από το γεγονός ότι δεν προσδιορίζεται τι συμβαίνει *μετά* από μια εισβολή, όταν η μυστική πληροφορία έχει αποκαλυφθεί στον αντίπαλο, και *μέχρι* τον εντοπισμό της, όταν δηλαδή γίνεται ανάκληση του δημόσιου κλειδιού. Κατά τη διάρκεια αυτής της περιόδου διακυβεύεται η ασφάλεια του συστήματος. Για παράδειγμα, ας υποτεθεί ότι ο αντίπαλος (π.χ. ένας χάκερ) έχει αποκτήσει τα μυστικά κλειδιά της Alice κατά τη διάρκεια της συνεδρίας t_e αλλά η εισβολή δεν έχει εντοπιστεί (βλέπε Σχήμα 5.1). Ο αντίπαλος θα είναι ικανός να ανανεώσει τα κλεμμένα κλειδιά με τον ίδιο τρόπο όπως η Alice και να παράγει τα μυστικά κλειδιά για τις επόμενες συνεδρίες $t_{e+1}, \ldots, t_d$, έως ότου εντοπιστεί η εισβολή. Αυτό σημαίνει ότι δεν παρέχεται καμία προστασία για τα κρυπτογραφικά επεξεργασμένα στοιχεία μετά την αποκάλυψη του κλειδιού και μέχρι τον εντοπισμό της επίθεσης. Όλα τα σχήματα χρονικής ασφάλειας που περιγράφονται στη διεθνή βιβλιογραφία [7, 52, 75, 20] είναι ευάλωτα κατά τη διάρκεια αυτής της περιόδου. Προσφέρουν προστασία μόνο για συνεδρίες πριν την αποκάλυψη του

[1] Υιοθετείται ο όρος χρονική ασφάλεια τόσο για σχήματα κρυπτογράφησης - αντί του όρου χρονική μυστικότητα - όσο και για σχήματα υπογραφής.



Σχήμα 5.1: Χρονική ασφάλεια

κλειδιού.

Δομή του κεφαλαίου. Σε αυτό το κεφάλαιο αναλύεται η χρονική ασφάλεια και εξετάζεται μια νέα απειλή ασφάλειας στην οποία ο αντίπαλος σφετερίζεται *όλα* τα μυστικά κλειδιά ενός χρήστη χωρίς να εντοπιστεί άμεσα. Στην ενότητα 5.2 εξετάζεται η έννοια της ισχυρής χρονικής ασφάλειας, σύμφωνα με την οποία κρυπτογραφικά επεξεργασμένα στοιχεία προστατεύονται όχι μόνο για τις περιόδους πριν την αποκάλυψη κλειδιού αλλά και για τις περιόδους μετά την αποκάλυψη κλειδιού. Στην ενότητα 5.3 παρουσιάζεται ένα σχήμα για ισχυρή χρονική ασφάλεια το οποίο μπορεί να εφαρμοστεί σε οποιοδήποτε κρυπτοσύστημα δημόσιου κλειδιού και στην ενότητα 5.4 προτείνεται ένα σχήμα διαμοίρασης/ανάκτησης κλειδιού με ισχυρή χρονική ασφάλεια, το οποίο βασίζεται στο κρυπτοσύστημα ElGamal. Το κεφάλαιο ολοκληρώνεται στην Ενότητα 5.5.

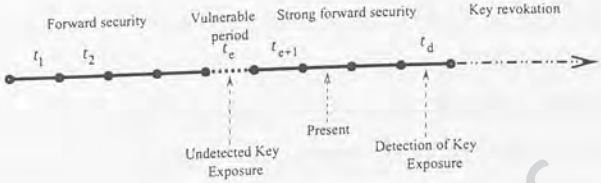
5.2 Από την χρονική ασφάλεια στην ισχυρή χρονική ασφάλεια

Έστω ότι η Alice χρησιμοποιεί ένα κρυπτοσύστημα χρονικής ασφάλειας και ότι ο αντίπαλος έχει σφετεριστεί *όλα* τα μυστικά κλειδιά της (κλειδιά συνεδρίας και κλειδιά

μακράς διάρκειας) κατά την συνεδρία t_e – βλέπε Σχήμα 5.1. Ο αντίπαλος δεν θα είναι ικανός να αποκτήσει τα κλειδιά για τις προηγούμενες συνεδρίες $t_j < t_e$, αλλά θα μπορεί να ανανεώσει τα κλειδιά της συνεδρίας t_e κατά τον ίδιο τρόπο όπως η Alice και να αποκτήσει τα κλειδιά για τις συνεδρίες $t_{e+1}, \ldots$, μέχρι την συνεδρία t_d, όταν θα εντοπιστεί η εισβολή. Στο σχήμα κρυπτογράφησης που περιγράφεται στην εργασία [20], η ανανέωση είναι *ντετερμινιστική*. Συνεπώς, ο αντίπαλος θα μπορέσει να δημιουργήσει ακριβώς το ίδιο κλειδί με αυτό της Alice, και θα είναι ικανός να αποκρυπτογραφεί όλα τα κρυπτογραφήματα που προορίζονται για την Alice. Το ίδιο ισχύει για τα σχήματα υπογραφών [7, 75]. Σε αυτήν την περίπτωση ο αντίπαλος μπορεί να πλαστογραφήσει τις υπογραφές της Alice. Με το σχήμα κρυπτογράφησης του Gunther [52], το οποίο χρησιμοποιεί *τυχαία* ανανέωση, ο αντίπαλος θα παράγει ένα διαφορετικό κλειδί. Όμως ο αντίπαλος μπορεί να αποδείξει αυθεντικοποιήσει το κλειδί αυτό με τον ίδιο τρόπο όπως και η Alice, μιας και ο αντίπαλος έχει επίσης υποκλέψει και τα μακράς διάρκειας κλειδιά αυθεντικοποίησης της Alice.

Ανεξάρτητα από το αν ο μηχανισμός ανανέωσης είναι ντετερμινιστικός ή τυχαίος, όλα τα κρυπτογραφικά επεξεργασμένα στοιχεία βρίσκονται σε κίνδυνο κατά την διάρκεια της περιόδου μεταξύ της αποκάλυψης κλειδιού και του εντοπισμού της αποκάλυψης. Προστασία από εισβολές στις οποίες αποκαλύπτονται όλα τα μυστικά κλειδιά της Alice (κλειδιά συνεδρίας και κλειδιά μακράς διαρκείας) μπορεί να επιτευχθεί χρησιμοποιώντας μη-κρυπτογραφικά μέσα. Όμως, με την τυχαία ανανέωση κλειδιού η επίτευξη αυτής της προστασίας είναι ευκολότερη, επειδή το κλειδί που θα παραχθεί από την Alice θα είναι διαφορετικό από αυτό που παράγεται από τον εισβολέα (με μεγάλη πιθανότητα).

Ορισμός 5.2.1. Ένα σύστημα είναι *ισχυρής* χρονικής ασφάλειας εάν η αποκάλυψη των μυστικών κλειδιών δεν θέτει σε κίνδυνο την ασφάλεια του συστήματος για



Σχήμα 5.2: Ισχυρή χρονική ασφάλεια

συνεδρίες πριν την αποκάλυψη ($t_j < t_e$) και μετά την αποκάλυψη ($t_j > t_e$) -βλέπε Σχήμα 5.2.

5.2.1 Μία πρακτική λύση με μεγάλο κόστος

Η ισχυρή χρονική ασφάλεια μπορεί εύκολα να επιτευχθεί με οποιοδήποτε κρυπτοσύστημα δημόσιου κλειδιού χρησιμοποιώντας threshold κρυπτοσυστήματα [36, 48, 49]. Για τον σκοπό αυτό το μυστικό κλειδί διαμοιράζεται μεταξύ αρκετών χρηστών, οι οποίοι από κοινού εκτελούν την κρυπτογραφική συνάρτηση. Τα μερίδια ανανεώνονται σε τακτά χρονικά διαστήματα [47, 46, 54, 53]. Η ισχυρή χρονική ασφάλεια εξαρτάται από το threshold του συστήματος.

Όμως, με αυτά τα σχήματα κάθε κρυπτογραφική πράξη (κρυπτογράφηση ή ψηφιακή υπογραφή) απαιτεί έναν κατανεμημένο υπολογισμό και συνεπώς μπορεί να είναι αρκετά δαπανηρή (όπως τονίστηκε και από τους Bellare - Miner [7]). Επιπλέον, η διανομή των μεριδίων των κλειδιών μπορεί να είναι δαπανηρή.

5.2.2 Η προτεινόμενη λύση

Η προτεινόμενη λύση σκοπό έχει να επιτύχει ισχυρή χρονική ασφάλεια με πρακτικό και αποδοτικό τρόπο. Ο χρήστης πρέπει να είναι ικανός να πιστοποιεί τα κλειδιά

των νέων συνεδριών με ελάχιστο κόστος, *χωρίς* αυθεντικοποίηση εκτός εύρους (out-of-band authentication). Επιπλέον, η προτεινόμενη λύση δεν θα περιλαμβάνει δαπανηρούς κατανεμημένους υπολογισμούς για κάθε κρυπτογραφική πράξη (κρυπτογράφηση ή υπογραφή). Για το σκοπό αυτό συνδυάζεται τυχαία ανανέωση κλειδιού με πιστοποίηση κλειδιού.

Εάν κάποιος υποκλέψει τα μυστικά κλειδιά ενός νόμιμου χρήστη και κατόπιν προσπαθήσει να πιστοποιήσει ένα ανανεωμένο κλεμμένο κλειδί, τότε δυο έγκυρα δημόσια κλειδιά που αντιστοιχούν στον ίδιο χρήστη θα υποβληθούν για πιστοποίηση: το νόμιμο κλειδί και το κλειδί του αντιπάλου. Η εισβολή θα εντοπιστεί εάν όλα τα δημόσια κλειδιά ενός χρήστη πιστοποιούνται από την ίδια Αρχή Πιστοποίησης. Συνεπώς, η ασφάλεια των κρυπτογραφικών κλειδιών θα είναι σε κίνδυνο μόνο κατά τη διάρκεια της συνεδρίας της εισβολής.

5.3 Μία βασική λύση για κάθε κρυπτοσύστημα δημόσιου κλειδιού

Με βάση το πλαίσιο που παρουσιάστηκε στην ενότητα 5.2.2, η ισχυρή χρονική ασφάλεια μπορεί να επιτευχθεί με οποιοδήποτε κρυπτοσύστημα δημόσιου κλειδιού. Αρχικά, εξετάζεται η περίπτωση σχημάτων ψηφιακών υπογραφών.

Έστω, ότι το ζεύγος δημόσιου/μυστικού κλειδιού της Alice για τη συνεδρία t, είναι $(PK_{A,t}, SK_{A,t})$ και ότι $Cert(ID_A, PK_{A,t})$ είναι ένα πιστοποιητικό για το δημόσιο κλειδί το οποίο έχει εκδοθεί από μία Αρχή Πιστοποίησης CA, όπου ID_A είναι ένας μοναδικός προσδιοριστής της Alice. Για την επόμενη συνεδρία, η Alice επιλέγει ένα τυχαίο ζεύγος δημόσιου/μυστικού κλειδιού $(PK_{A,t+1}, SK_{A,t+1})$, και το υπογράφει ψηφιακά μαζί με τον προσδιοριστή ID_A, χρησιμοποιώντας το προηγούμενο μυστικό

κλειδί της: $sig_{SK_{A,t}}(ID_A, PK_{A,t+1})$. Στη συνέχεια η Alice στέλνει αυτή την υπογραφή, μαζί με το πιστοποιητικό της $Cert(ID_A, PK_{A,t})$ στην Αρχή Πιστοποίησης, η οποία επαληθεύει την υπογραφή της Alice χρησιμοποιώντας το τρέχον κλειδί $PK_{A,t}$. Αν η υπογραφή είναι έγκυρη, η Αρχή Πιστοποίησης στέλνει στην Alice ένα νέο πιστοποιητικό $Cert(ID_A, PK_{A,t+1})$.

Εάν ένας εισβολέας υποκλέψει όλα τα μυστικά κλειδιά της Alice στη διάρκεια της συνεδρίας t (και πιο ειδικά το $SK_{A,t}$) και εάν ο εισβολέας υποβάλλει ένα ανανεωμένο δημόσιο κλειδί στην Αρχή Πιστοποίησης, τότε δύο δημόσια κλειδιά θα υποβληθούν, και τα δυο εκ μέρους της Alice: το $PK_{A,t+1}$ και ένα ψευδώνυμο $\overline{PK}_{A,t+1}$. Εάν συμβεί αυτό η Αρχή Πιστοποίησης θα ανακαλέσει όλα τα δημόσια κλειδιά της Alice για την τρέχουσα περίοδο.

Μια παρόμοια προσέγγιση μπορεί να χρησιμοποιηθεί για σχήματα κρυπτογράφησης δημόσιου κλειδιού. Σε αυτή την περίπτωση όμως η Alice χρειάζεται δύο ζεύγη κλειδιών, το ένα για την κρυπτογράφηση και το άλλο για την αυθεντικοποίηση των κλειδιών κρυπτογράφησης.

Αυτό το βασικό σχήμα επιτυγχάνει ισχυρή χρονική ασφάλεια και είναι πολύ αποτελεσματικό. Συγκεκριμένα, η πιστοποίηση των δημόσιων κλειδιών σε κάθε συνεδρία δεν απαιτεί μεθόδους για εκτός εύρους αυθεντικοποίηση. Επιπροσθέτως, το μέγεθος των κλειδιών και των υπογραφών δεν αυξάνεται κατά την ανανέωση των κλειδιών. Εντούτοις, αυξάνεται γραμμικά ο αριθμός των πιστοποιητικών.

Σχόλιο 1. Αν και η προστασία της ισχυρής χρονικής ασφάλειας είναι εμφανής στην περίπτωση της κρυπτογράφησης, θα μπορούσε κανείς να υποστηρίξει ότι στα πλαίσια των ψηφιακών υπογραφών δεν προσφέρει καμία επιπλέον προστασία από τη χρονική ασφάλεια. Εξετάζεται η περίπτωση όπου ο Bob έχει υποκλέψει το κλειδί υπογραφής της Alice. Τότε, αν και ο Bob δεν θα είναι ικανός να ανανεώσει το κλεμμένο κλειδί

χωρίς να γίνει αντιληπτός, θα μπορούσε έμμεσα να προσπεράσει την ασφάλεια του συστήματος για μελλοντικές συνεδρίες. Για παράδειγμα, θα μπορούσε να υπογράφει μεταχρονολογημένες επιταγές εκ μέρους της Alice. Όμως, υπάρχουν περιπτώσεις όπου η ισχυρή χρονική ασφάλεια έχει νόημα στα πλαίσια των υπογραφών. Για παράδειγμα, όταν η διάρκεια ζωής του κλειδιού υπογραφής περιορίζει επίσης τον σκοπό του μηνύματος που πρόκειται να υπογραφεί. Αυτό θα έκανε τις μεταχρονολογημένες επιταγές (για επόμενες συνεδρίες) άκυρες.

Σχόλιο 2. Στο σχήμα που παρουσιάστηκε θεωρείται ότι ένας εισβολέας δεν μπορεί να παρεμποδίσει το νόμιμο χρήστη από το να έχει πρόσβαση στην Αρχή Πιστοποίησης. Σε αντίθετη περίπτωση, η ισχυρή χρονική ασφάλεια δεν μπορεί να επιτευχθεί, αφού ο εισβολέας θα είναι ικανός να προσποιηθεί το νόμιμο χρήστη για όσο χρόνο ο χρήστης δεν έχει πρόσβαση στην Αρχή Πιστοποίησης. Κανένα κρυπτοσύστημα δεν μπορεί να αντιμετωπίσει μια τέτοια επίθεση.

5.4 Ένα σχήμα διαμοίρασης κλειδιού με ισχυρή χρονική ασφάλεια

Η λύση που προτείνεται στην ενότητα 5.3 δεν είναι ικανοποιητική για σχήματα διαμοίρασης κλειδιού, επειδή τα ανανεωμένα κλειδιά πρέπει να διανέμονται μεταξύ των πρακτόρων διαμοίρασης (μια εξαιρετική έρευνα για τα συστήματα διαμοίρασης κλειδιού δίνεται από τους Denning και Branstad στην εργασία [35]). Στη συνέχεια, περιγράφεται ένα σχήμα διαμοίρασης κλειδιού με ισχυρή χρονική ασφάλεια το οποίο μειώνει το κόστος της διανομής και ανανέωσης του κλειδιού. Αυτό επιτυγχάνεται με τη ρύθμιση της διαδικασίας συγχρονισμού της ανανέωση του κλειδιού από τους ίδιους

τους πράκτορες διαμοίρασης.

Περιγράφεται ένα βασικό (2,2) σχήμα διαμοίρασης κλειδιού με πράκτορες διαμοίρασης EA_1, EA_2, όπου η Αρχή Επιβολής Νόμου (Law Enforcement Agency - LEA) λειτουργεί επίσης ως Αρχή Πιστοποίησης. Θεωρείται ότι οι πράκτορες διαμοίρασης και η Αρχή Επιβολής Νόμου ακολουθούν πιστά το πρωτόκολλο.

Κάθε χρήστης, έστω η Alice, στη διάρκεια της αρχικοποίησης, επιλέγει ένα μακράς διάρκειας μυστικό κλειδί και το διαμοιράζει μεταξύ των πρακτόρων διαμοίρασης με επαληθεύσιμο τρόπο. Μετά, στην αρχή κάθε συνεδρίας t οι πράκτορες διαμοίρασης επιλέγουν έναν προσδιοριστή χρονικού ελέγχου h_t. Αυτό μεταδίδεται από την Αρχή LEA και θα χρησιμοποιηθεί από *όλους* τους χρήστες του συστήματος ανανέωσης κλειδιού. Πιο ειδικά, η Alice θα ανανεώσει το μυστικό της κλειδί SK_{t-1} σε SK_t χρησιμοποιώντας το μακράς διάρκειας μυστικό κλειδί της, κάποιο τυχαίο αριθμό και τον προσδιοριστή χρονικού ελέγχου h_t. Μετά από κάθε ανανέωση, η Alice και οι πράκτορες διαμοίρασης διαγράφουν όλες τις πληροφορίες που θα μπορούσαν να χρησιμεύσουν σε έναν αντίπαλο, για την ανάκτηση προηγούμενων κλειδιών. Επιπροσθέτως, η Alice ανανεώνει το δημόσιο κλειδί της PK_t, και αποδεικνύει στην Αρχή LEA με μηδενική γνώση ότι αυτό έχει κατασκευαστεί με κατάλληλο τρόπο. Ύστερα, η Αρχή LEA πιστοποιεί το ανανεωμένο δημόσιο κλειδί PK_t.

Ένας αντίπαλος που επιτυγχάνει να σφετεριστεί τα μυστικά κλειδιά της Alice μπορεί να προσπαθήσει να ανανεώσει το κλεμμένο κλειδί συνεδρίας και να το πιστοποιήσει μέσω της Αρχής LEA. Όμως, η Alice θα υποβάλλει και αυτή το ανανεωμένο κλειδί της για πιστοποίηση. Τα δυο κλειδιά είναι διαφορετικά (με πολύ μεγάλη πιθανότητα). Η Αρχή LEA θα παρατηρήσει ότι δύο διαφορετικά κλειδιά που αντιστοιχούν στον ίδιο χρήστη για την ίδια περίοδο έχουν υποβληθεί για πιστοποίηση, θα εντοπίσει την εισβολή και θα ανακαλέσει όλα τα δημόσια κλειδιά της Alice.

Υπόβαθρο. Χρησιμοποιείται ένα σχήμα κρυπτογράφησης ElGamal [41]. Επιλέγεται μία υπο-ομάδα H του συνόλου Z_q^* με γεννήτορα h πρώτης τάξεως r, τέτοια ώστε $q = 2r + 1$, για επαρκώς μεγάλο πρώτο αριθμό q. Επίσης, επιλέγεται μία υπο-ομάδα G του συνόλου Z_p^* με γεννήτορα g πρώτης τάξεως q, τέτοια ώστε $p = 2q+1$ για επαρκώς μεγάλο πρώτο αριθμό p. Για απλότητα, όπου δεν υπάρχει ασάφεια, δεν χρησιμοποιείται παρακάτω ο modulo τελεστής. Ο συντελεστής Diffie-Hellman [38] DH ορίζεται ως $DH(g^a, g^b) = g^{ab}$. Δεδομένων των αριθμών g^a και g^b, το πρόβλημα της εύρεσης του συντελεστή $DH(g^a, g^b)$, είναι γνωστό ως *πρόβλημα Diffie-Hellman*. Το πρόβλημα της αναγνώρισης εάν ένας αριθμός $z \in Z_p$ είναι συντελεστής Diffie-Hellman, εάν δηλαδή $z = DH(g^a, g^b)$, ονομάζεται πρόβλημα *Απόφασης* Diffie-Hellman [38] (Decision Diffie-Hellman problem).

Αρχικοποίηση. Η Alice επιλέγει ένα μακράς διάρκειας ιδιωτικό κλειδί[2] $x_A \in_R Z_q^*$ και υπολογίζει $y_A = g^{x_A}$. Η Alice αποστέλλει το μακράς διάρκειας δημόσιο κλειδί της $PK_A =< p, q, g, y_A >$ στην Αρχή LEA, το αυθεντικοποιεί με μη-κρυπτογραφικά (εκτός εύρους) μέσα, και λαμβάνει ένα πιστοποιητικό $Cert(ID_A, PK_A)$. Τότε,

1. Η Alice επιλέγει μερίδια του κλειδιού $x_1 \in_R Z_q^*$ και $x_2 = x_A(x_1)^{-1}$. Η Alice δίδει τα μερίδια x_1, x_2 στους πράκτορες διαμοίρασης EA_1, EA_2, αντίστοιχα, χρησιμοποιώντας κάποια μέθοδο που διαφυλάσσει την εμπιστευτικότητα της αποστολής.

2. Οι πράκτορες διαμοίρασης ελέγχουν ότι $y_A = DH(g^{x_1}, g^{x_2})$. Εάν όχι, η Alice αναφέρεται στην Αρχή LEA.

[2] το σύμβολο $a \in_R A$ υποδεικνύει ότι το στοιχείο a έχει επιλεγεί τυχαία με ομοιόμορφη κατανομή από το σύνολο A.

Ανανέωση Κλειδιού (για τις συνεδρίες $t = 1, 2, \ldots$). Οι πράκτορες EA_1, EA_2 επιλέγουν αριθμούς $r_{1,t}$, $r_{2,t} \in_R Z_r^*$ αντίστοιχα και από κοινού κατασκευάζουν $h^{r_t} = h^{r_{1,t}r_{2,t}}$ με ασφαλή τρόπο, χρησιμοποιώντας το πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman [38]. Οι πράκτορες στέλνουν το h^{r_t} στην Αρχή LEA, η οποία το δημοσιεύει. Αυτός ο αριθμός προσδιορίζει τη συνεδρία t, και χρησιμοποιείται από *όλους* τους χρήστες του συστήματος. Αυτό αντιπροσωπεύει την τυχαιότητα που χρησιμοποιούν οι πράκτορες διαμοίρασης στη διαδικασία ανανέωσης κλειδιού και είναι ίδιος για όλους τους χρήστες σε κάθε χρονική περίοδο t. Οι πράκτορες τότε διαγράφουν τους εκθέτες $r_{1,t-1}$ και $r_{2,t-1}$ της προηγούμενης συνεδρίας (όταν $t > 1$). Τότε:

1. Η Alice επιλέγει έναν αριθμό $r_{A,t} \in_R Z_r^*$, υπολογίζει $h^{r_{A,t}}$ και το αποστέλλει στην Αρχή LEA. Η Alice υπολογίζει επίσης το κλειδί Diffie-Hellman $h_t = h^{r_t r_{A,t}}$.

2. Η Alice ανανεώνει το μυστικό κλειδί της για τη συνεδρία t σε $SK_{A,t} = h_t x_A$. Τότε υπολογίζει $y_{A,t} = g^{h_t x_A}$, και στέλνει στην Αρχή LEA το δημόσιο κλειδί της συνεδρίας $PK_{A,t} = < p, q, r, g, h, y_{A,t} >$. Η Alice αποδεικνύει με μηδενική γνώση (βλέπε Παράρτημα) ότι $y_{A,t} = g^{DH(h^{r_t}, h^{r_{A,t}}) DL(g^{x_A})}$, όπου $DL(g^{x_A})$ είναι ο διακριτός λογάριθμος του g^{x_A}. Αν η απόδειξη είναι σωστή, η Αρχή LEA πιστοποιεί το ανανεωμένο δημόσιο κλειδί και εφοδιάζει την Alice με ένα πιστοποιητικό $Cert(ID_A, PK_{A,t})$. Τότε η Alice διαγράφει τον εκθέτη $r_{A,t}$ και το μυστικό κλειδί της προηγούμενης συνεδρίας.

Ανάκτηση του Διαμοιρασμένου Κλειδιού. Έστω ότι έχει εκδοθεί μία δικαστική εντολή να αποκρυπτογραφηθούν όλα τα κρυπτογραφημένα μηνύματα που προορίζονται για την Alice κατά τη διάρκεια της συνεδρίας t. Τότε η Αρχή LEA θα παρακολουθήσει την επικοινωνία της Alice. Έστω ότι $(g^k, m(y_{A,t})^k)$ είναι μια κρυπτογράφηση

ενός μηνύματος m που αποστέλλεται στην Alice κατά τη διάρκεια αυτής της συνεδρίας. Η Αρχή LEA θα αποστείλει τα g^k και $h^{r_{A,t}}$ στους πράκτορες διαμοίρασης. Οι πράκτορες πρώτα υπολογίζουν το κλειδί Diffie-Hellman $h_t = h^{r_t r_{A,t}}$, και μετά τον παράγοντα $(y_{A,t})^k = (((g^k)^{h_1})^{x_1})^{x_2}$. Στη συνέχεια, στέλνουν στην Αρχή το $(y_{A,t})^k$ για αποκρυπτογράφηση.

Θεώρημα 5.4.1. *Εάν υπάρχει πολυωνυμικός αλγόριθμος ο οποίος παραβιάζει την ισχυρή χρονική ασφάλεια του προτεινόμενου σχήματος διαμοίρασης, τότε ο αλγόριθμος αυτός μπορεί να χρησιμοποιηθεί για την επίλυση του προβλήματος Απόφασης Diffie-Hellman.*

Απόδειξη. Ας υποτεθεί ότι υπάρχει ένας αλγόριθμος πολυωνυμικού χρόνου $\mathcal{A}$ που παραβιάζει την ασφάλεια του προτεινόμενου σχήματος διαμοίρασης κλειδιού. Δηλαδή, με είσοδο:

- το ιδιωτικό κλειδί μακράς διαρκείας $x_A \in_R Z_q^*$ του χρήστη A
- το ιδιωτικό κλειδί $SK_{A,t} = h_t x_A$ για κάποια συνεδρία t, όπου $h_t = h^{r_t r_{A,t}}$
- τις παραμέτρους h^{r_j} και $h^{r_{A,j}}$
- το δημόσιο κλειδί μακράς διαρκείας $PK_A =< p, q, g, g^{x_A} >$ καθώς και το δημόσιο κλειδί $PK_{A,j} =< p, q, r, g, h, g^{h_j x_A} >$,

ο αλγόριθμος $\mathcal{A}$ μπορεί να αποκρυπτογραφήσει κρυπτογραφήματα τα οποία έχουν δημιουργηθεί με το ιδιωτικό κλειδί $SK_{A,j} = h_j x_A$ οποιασδήποτε συνεδρίας $j \neq t$.

Έστω ότι $z, h^a, h^b \in_R Z_q^*$ είναι μια είσοδος για το πρόβλημα Απόφασης Diffie-Hellman. Τότε, ο πολυωνυμικός αλγόριθμος $\mathcal{A}$ μπορεί να χρησιμοποιηθεί για την επίλυση του προβλήματος Απόφασης Diffie-Hellman.

Αρχικά δημιουργείται ένα ιστορικό για ζεύγη κρυπτογραφημάτων - μηνυμάτων $(\hat{c}, \hat{m})$ για τον αλγόριθμο $\mathcal{A}$, ως εξής: επιλέγονται τυχαία $\hat{m} \in_R Z_p^*$, $\hat{k}, \hat{x}_A \in_R Z_q^*$ και $\hat{r}_t, \hat{r}_{A,t} \in_R Z_r^*$ και λαμβάνονται τα κρυπτογραφήματα $\hat{c} = (g^{\hat{k}}, \hat{m} g^{k\hat{x}_A} h^{\hat{r}_t \hat{r}_{A,t}})$.

Στη συνέχεια δίνονται ως είσοδος στον αλγόριθμο $\mathcal{A}$ τα ακόλουθα: το ιδιωτικό κλειδί μακράς διαρκείας x_A, το ιδιωτικό κλειδί $SK_{A,t} = h_t x_A$ της συνεδρίας t, το δημόσιο κλειδί μακράς διαρκείας και το δημόσιο κλειδί της συνεδρίας j, τα h^a, h^b αντί των $h^{r_{A,t}}$, h^{r_j} και το "κρυπτογράφημα": (g^k, mg^{kzx_A}). Έστω ότι το αποτέλεσμα του $\mathcal{A}$ είναι m'. Αν $m' = m$ τότε η απόφαση είναι ότι $z = h^{ab}$, αλλιώς $z \neq h^{ab}$. Συνεπώς, με αυτό τον αλγόριθμο επιλύεται το πρόβλημα Απόφασης Diffie-Hellman. □

Σχόλιο 3. Η αλληλεπιδραστική απόδειξη της μηδενικής γνώσης στο Βήμα 2 της ανανέωσης κλειδιού μπορεί να αντικατασταθεί από μια υπογραφή, χρησιμοποιώντας την *ευρεστική* προσέγγιση των Fiat και Shamir [45]. Όμως θα έπρεπε να παρατηρηθεί ότι αν χρησιμοποιηθούν τέτοιες υπογραφές τότε η ασφάλεια του σχήματος μπορεί να αποδειχθεί μόνο στο μοντέλο Random Oracles [8].

Σχόλιο 4. Στην ενότητα 5.2 εξετάστηκε μία λύση για την κατανομή των μυστικών κλειδιών μέσω μυστικής διαμοίρασης και τακτικής ανανέωσης. Στο πρωτόκολλο που παρουσιάστηκε παραπάνω, ο μηχανισμός είναι παρόμοιος με τους μηχανισμούς τακτικής ανανέωσης (proactive key updating). Όμως, στο σχήμα διαμοίρασης που παρουσιάστηκε, δεν απαιτείται κατανεμημένος υπολογισμός για κάθε κρυπτογραφική πράξη.

Σχόλιο 5. Οι πράκτορες διαμοίρασης παρέχουν ασφαλή αποθήκευση για τα μακράς διαρκείας μυστικά κλειδιά όλων των χρηστών του συστήματος. Οι πράκτορες επιπλέον παράγουν έναν τυχαίο αριθμό h^{r_i}. Στο πρωτόκολλο που παρουσιάστηκε, αυτός ο

αριθμός χρησιμοποιείται για μια συγκεκριμένη χρονική περίοδο και είναι ο ίδιος για *όλους* τους χρήστες του συστήματος. Στην ακόλουθη περίοδο ένας νέος τυχαίος αριθμός επιλέγεται και ο παλιός απορρίπτεται. Σημειώνεται ότι η πρόσθεση ή η αφαίρεση ενός χρήστη από το σύστημα δεν επηρεάζει τη λειτουργικότητα των πρακτόρων.

Σχόλιο 6. Το σχήμα διαμοίρασης που περιγράφηκε παραπάνω μπορεί εύκολα να τροποποιηθεί σε σχήμα Ανάκτησης Κλειδιού (Key Recovery) αντικαθιστώντας την Αρχή Εφαρμογής Νόμου LEA και τους πράκτορες διαμοίρασης με μια Αντιπροσωπεία Ανάκτησης Δεδομένων και με πράκτορες ανάκτησης κλειδιού αντίστοιχα. Σημειώνεται ότι εάν τα κλειδιά που θα ανακτηθούν κρυπτογραφούν αρχειοθετημένα δεδομένα, τότε δεν έχει νόημα η υιοθέτηση ενός σχήματος Ανάκτησης Κλειδιού με χρονική ασφάλεια, όπως παρατηρήθηκε στην εργασία [1]. Συνεπώς, το προτεινόμενο σχήμα μπορεί να χρησιμοποιηθεί μόνο για την ανάκτηση κρυπτογραφημένης κίνησης (encrypted traffic).

Γενικεύσεις

1. Είναι εύκολο να γενικευτεί αυτό το σχήμα σε ένα (t, l) σχήμα διαμοίρασης κλειδιού. Για ευρωστία (robustness) μπορεί να χρησιμοποιηθούν οι προσεγγίσεις των εργασιών [48, 49]. Επιπλέον, το προτεινόμενο σχήμα μπορεί εύκολα να τροποποιηθεί για να αποτρέψει *επιθέσεις υποσυνείδητων καναλιών* (subliminal channel attacks), όπως περιγράφεται στην εργασία [67].

2. Είναι γνωστό ότι το σχήμα κρυπτογράφησης ElGamal δεν είναι σημασιολογικά ασφαλές (semantically secure) [51]. Για σημασιολογική ασφάλεια, μπορεί να χρησιμοποιηθεί η επέκταση των Cramer - Shoup [32] στο σχήμα ElGamal.

5.5 Συμπέρασμα

Με τη χρονική ασφάλεια, μπορούν να προστατευτούν δεδομένα τα οποία έχουν επεξεργαστεί κρυπτογραφικά πριν από την αποκάλυψη του μυστικού κλειδιού. Όμως, σε πολλές εφαρμογές είναι δύσκολο να εντοπιστούν εισβολές. Αντίθετα, ο αντίπαλος μπορεί να μη χρησιμοποιήσει τα υποκλεμμένα κλειδιά μέχρις ότου αυτό να είναι πρόσφορο ή κερδοφόρο. Είναι συνεπώς σημαντικό να εξεταστούν μηχανισμοί, οι οποίοι προστατεύουν κρυπτογραφικά επεξεργασμένα δεδομένα μετά από μία εισβολή. Η ισχυρή χρονική ασφάλεια προσφέρει τέτοια προστασία.

Η ισχυρή χρονική ασφάλεια μπορεί να προσφέρει αυξημένη ασφάλεια σε εφαρμογές κινητών πρακτόρων με αποδοτικό τρόπο. Για παράδειγμα, κρυπτογραφικά κλειδιά που χρησιμοποιούνται σε εφαρμογές κινητών πρακτόρων, μπορούν να ανανεώνονται με αυτό το μηχανισμό ώστε να μειώνουν τις συνέπειες από πιθανή αποκάλυψη των κλειδιών. Στο έβδομο κεφάλαιο παρουσιάζεται ένας κρυπτογραφικός μηχανισμός για μεταβίβαση ρόλων μεταξύ κινητών πρακτόρων, ο οποίος χρησιμοποιεί ένα μηχανισμό ανανέωσης κλειδιών με ισχυρή χρονική ασφάλεια.

Παράρτημα Α - Ορθότητα κατασκευής διαμοιραζόμενου κλειδιού

Έστω

$$\mathcal{L} = \{(p, q, r, g, g^a, h^b, h^c, z) \mid p, q, r \text{ πρώτοι}, p = 2q + 1, q = 2r + 1, g \text{ ένας γεννήτορας του } Z_p^*, h \text{ ένας γεννήτορας του } Z_q^*, a \in Z_q^*, b, c \in Z_r^*, \text{και } z \in Z_p^* \text{ με } z = g^{a(h^{bc})} \bmod p\}.$$

Μία αλληλεπιδραστική απόδειξη μηδενικής γνώσης για την συμμετοχή στην ομάδα $\mathcal{L}$

Το πρωτόκολλο που ακολουθεί μπορεί να χρησιμοποιηθεί κατά την ανανέωση κλειδιού του σχήματος διαμοίρασης της ενότητας 5.4, για να αποδείξει η Alice στην Αρχή LEA με μηδενική γνώση, ότι το δημόσιο κλειδί συνεδρίας που επέλεξε έχει την αποδεκτή μορφή (δηλαδή είναι ένα στοιχείο x το οποίο ανήκει στην ομάδα $\mathcal{L}$).

Είσοδος: $x = (p, q, r, g, g^a, h^b, h^c, z)$

Επανέλαβε k φορές ($k = \Theta(\log p)$):

1. Η Alice επιλέγει $k \in_R Z_q^*$, $t \in_R Z_r^*$, υπολογίζει $u = ka \bmod q$, $v = c + t \bmod r$, και στη συνέχεια αποστέλλει στην Αρχή LEA:

$$X = g^{a(h^{bv})},\ Y = g^u,\ Z = h^v.$$

2. Η Αρχή LEA αποστέλλει στην Alice ένα ψηφίο ερώτησης $e \in \{0, 1\}$.

3. Η Alice στέλνει στην Αρχή LEA:

$$\begin{cases} (u, v) & , \text{ εάν } e = 0 \\ (k, t) & , \text{ εάν } e = 1. \end{cases}$$

Επαλήθευση: Η Αρχή LEA ελέγχει ότι:

$$\begin{aligned} &\text{όταν } e=0 \quad , \quad X = g^{u(h^b)^v},\ Y = g^u,\ Z = h^v \\ &\text{όταν } e=1 \quad , \quad X = z^{k(h^b)^t},\ Y = (g^a)^k,\ Z = h^c h^t. \end{aligned}$$

Η Αρχή LEA αποδέχεται ότι $x \in \mathcal{L}$ εάν η επαλήθευση ικανοποιείται για όλες τις k επαναλήψεις.

Απόδειξη ορθότητας

Πληρότητα (Completeness): Εάν $x \in \mathcal{L}$ τότε η Αρχή LEA πάντοτε θα αποδέχεται τη συμμετοχή.

Ακρίβεια (Soundness): Εάν η Αρχή LEA αποδέχεται με μη αμελητέα πιθανότητα ($\geq 1/poly(\log p)$), τότε η Alice πρέπει να απαντά σωστά και για τις δύο ερωτήσεις $e=0$, $e=1$ για κάποια τριάδα X, Y, Z. Συνεπώς,

$$\begin{aligned} Z &= h^v = h^c h^t && \Rightarrow \quad v = c + t \mod r \\ Y &= g^u = (g^a)^k && \Rightarrow \quad u = ak \mod q \\ X &= g^{akh^{(b(c+t))}} = z^{kh^{(bt)}} && \Rightarrow \quad z = g^{a(h^{bc})}. \end{aligned}$$

Συνεπάγεται ότι $x \in \mathcal{L}$.

Προσομοίωση:

όταν $e=0$, επιλέγονται τυχαία u, v και κατασκευάζονται X, Y, Z όπως στο Βήμα 1.

όταν $e=1$, επιλέγονται τυχαία k, t και κατασκευάζονται $X = z^{k(h^b)^t}$, $Y = (g^a)^k$, και $Z = h^c h^t$.

Κεφάλαιο 6

Το μοντέλο κύριου πράκτορα – εξαρτημένων πρακτόρων

Στην προηγούμενη ενότητα της διατριβής, παρουσιάστηκαν κρυπτογραφικά πρωτόκολλα τα οποία μπορούν να χρησιμοποιηθούν με ασφάλεια από κινητούς πράκτορες ή/και εξυπηρετητές πρακτόρων για τον υπολογισμό ψηφιακών υπογραφών ή για τη χρονική προστασία μυστικών κλειδιών. Το παρόν κεφάλαιο αποτελεί το πρώτο κεφάλαιο της τρίτης και τελευταίας ενότητας της διατριβής, που σκοπό έχει να παρουσιάσει αρχιτεκτονικές και μηχανισμούς, οι οποίοι επιλύουν συγκεκριμένα προβλήματα ασφάλειας σε εφαρμογές κινητών πρακτόρων.

Στο κεφάλαιο αυτό, περιγράφεται ένα πολυ-πρακτορικό σύστημα για την ασφαλή διεκπεραίωση ηλεκτρονικών αγορών. Το σύστημα αυτό στηρίζεται σε μία αρχιτεκτονική που συνδυάζει ένα στατικό με n κινητούς πράκτορες για τη συναλλαγή ενός χρήστη με n ηλεκτρονικά καταστήματα.

6.1 Εισαγωγή

Η χαοτική δομή του διαδικτύου δεν διευκολύνει πιθανούς αγοραστές να επισκεφτούν πολλά ηλεκτρονικά καταστήματα και διαφορετικές εφαρμογές Ηλεκτρονικού Εμπορίου, ώστε να μπορέσουν εύκολα να συγκρίνουν διαφορετικές προσφορές πριν πραγματοποιήσουν μία αγορά. Για παράδειγμα, η σύγκριση της τιμής ενός προϊόντος από διαφορετικά ηλεκτρονικά καταστήματα, απαιτεί πολύ χρόνο από το χρήστη. Μία προσέγγιση στο πρόβλημα αυτό είναι η χρήση ειδικευμένων ενδιάμεσων εμπορικών υπηρεσιών, για παράδειγμα ηλεκτρονικών μεσιτών (electronic brokers). Οι υπηρεσίες αυτές χρησιμοποιούν κατανεμημένες τεχνολογίες (για παράδειγμα την τεχνολογία CORBA) και παρέχουν σε χρήστες συστήματα αναζήτησης προϊόντων ή υπηρεσιών, διαπραγμάτευση των όρων της συμφωνίας και εξασφάλιση παράδοσης των αγαθών. Παραδείγματα τέτοιων υπηρεσιών μπορούν να βρεθούν στις εργασίες [10, 62, 30].

Μία διαφορετική προσέγγιση στο πρόβλημα είναι η χρήση της τεχνολογίας των κινητών πρακτόρων. Ένας κινητός πράκτορας μπορεί να αλληλεπιδράσει με κάποιο χρήστη - υποψήφιο αγοραστή, ώστε να συλλέξει τις απαραίτητες πληροφορίες και να λειτουργήσει ως αντιπρόσωπός του για κάποια αγορά. Στη συνέχεια, μπορεί αυτόνομα να μεταναστεύσει σε διάφορα ηλεκτρονικά καταστήματα ώστε να συλλέξει πληροφορίες για το ζητούμενο προϊόν όπως τιμή ή ημερομηνία παράδοσης, να διαπραγματευτεί για λογαριασμό του χρήστη και τελικά να επιστρέψει στον αρχικό χρήστη και να του παρουσιάσει τα αποτελέσματα της αναζήτησης. Επίσης, οι κινητοί πράκτορες μπορούν να εργάζονται με κατανεμημένο τρόπο - για παράδειγμα διαφορετικοί πράκτορες συνεργάζονται ενώ εκτελούνται σε διαφορετικούς υπολογιστές. Αν και όπως αναφέρθηκε στην ενότητα 1.2 οι κινητοί πράκτορες μειώνουν το κόστος απομακρυσμένης επικοινωνίας, εισαγάγουν σοβαρά προβλήματα ασφάλειας [28, 29, 55, 87, 104, 109, 114, 116]. Οι Merwe και Solms [87] πρότειναν ένα σύστημα για ασφαλείς συναλλαγές, το οποίο

βασίζεται στην τεχνολογία των πρακτόρων. Στο σύστημα αυτό όμως οι πράκτορες υλοποιούνται ως κατανεμημένα αντικείμενα που εκτελούνται σε συγκεκριμένα περιβάλλοντα και συνεπώς πολλά από τα πλεονεκτήματα των κινητών πρακτόρων όπως η μεταφερσιμότητα και η αυτονομία κίνησης δεν αξιοποιούνται. Οι Yi et al [114] παρουσίασαν ένα σύστημα συναλλαγών κινητών πρακτόρων, η ασφάλεια του οποίου στηρίζεται στην ύπαρξη ενός Κέντρου Υπηρεσιών Πρακτόρων (βλέπε ενότητα 2.1.2). Αν και το κόστος επικοινωνίας για τη λειτουργία αυτού του κέντρου δεν είναι υπερβολικό, η ασφάλεια του συστήματος στηρίζεται αποκλειστικά στην ορθή λειτουργία του κέντρου αυτού. Οι Zapf et al [116] καθόρισαν απαιτήσεις ασφάλειας για τη χρήση κινητών πρακτόρων σε ηλεκτρονικές αγορές και υλοποίησαν ορισμένες από αυτές τις απαιτήσεις, κυρίως για την ασφάλεια του περιβάλλοντος εκτέλεσης, στο σύστημά τους AMETAS.

Στο κεφάλαιο αυτό παρουσιάζεται ένα νέο σύστημα το οποίο βασίζεται σε κινητούς πράκτορες για τη συλλογή και εκτίμηση ανταγωνιστικών προσφορών αγοράς. Το σύστημα αυτό είναι μία αρχιτεκτονική λύση για την προστασία του περιβάλλοντος εκτέλεσης από κακόβουλους πράκτορες, ενώ παράλληλα χρησιμοποιεί και μηχανισμούς παθητικής παρεμπόδισης επιθέσεων εχθρικών υπολογιστών εναντίον κινητών πρακτόρων. Είναι ένα πολυ-πρακτορικό σύστημα (multi-agent system) το οποίο χρησιμοποιεί $n+1$ συνεργαζόμενους πράκτορες για τη διαπραγμάτευση με n ηλεκτρονικά καταστήματα. Ένας από τους πράκτορες ονομάζεται *κύριος πράκτορας* (master agent) και είναι στατικός, δηλαδή εκτελείται μόνο στον υπολογιστή του χρήστη - αγοραστή, ενώ οι υπόλοιποι ονομάζονται *εξαρτημένοι πράκτορες* (slave agents) και είναι κινητοί.

Ο κύριος πράκτορας είναι υπεύθυνος για να παρέχει στους εξαρτημένους πράκτορες άδειες πρόσβασης για τους εξυπηρετητές των ηλεκτρονικών καταστημάτων (electronic shopping servers). Κάθε εξαρτημένος πράκτορας μεταναστεύει σε έναν

εξυπηρετητή με τη βοήθεια της άδειας πρόσβασης και διαπραγματεύεται για συγκεκριμένα προϊόντα. Σε περίπτωση συμφωνίας επιστρέφει στην αρχική πηγή του με μία προσφορά αγοράς, υπογεγραμμένη από το ηλεκτρονικό κατάστημα. Ο κύριος πράκτορας συγκρίνει τις υπογεγραμμένες προσφορές αγοράς και παρουσιάζει τα αποτελέσματα στον υποψήφιο αγοραστή, ο οποίος μπορεί να αγοράσει τα ζητούμενα προϊόντα ή υπηρεσίες από το κατάστημα με τη βέλτιστη προσφορά.

Το κεφάλαιο αυτό είναι διαρθρωμένο ως εξής: Στην ενότητα 6.2 παρουσιάζεται το προτεινόμενο μοντέλο. Στην ενότητα 6.3 αναλύεται η ασφάλεια του μοντέλου αυτού τόσο για τον αγοραστή (πράκτορα) όσο και για τα ηλεκτρονικά καταστήματα (περιβάλλον εκτέλεσης). Τέλος, στην ενότητα 6.4 συζητούνται τα πλεονεκτήματα και μειονεκτήματα αυτής της προσέγγισης σε σχέση με άλλα προτεινόμενα συστήματα.

6.2 Το προτεινόμενο μοντέλο

Θεωρούμε έναν αγοραστή B (Buyer) ο οποίος επιθυμεί να αγοράσει κάποια προϊόντα από ηλεκτρονικά καταστήματα στο Διαδίκτυο. Ο αγοραστής μπορεί να επισκεφτεί n ηλεκτρονικά καταστήματα $S_1, S_2, \ldots, S_n$ (Servers) και να συγκρίνει n ανταγωνιστικές προσφορές. Αντί να επισκεφτεί χειρονακτικά όλες τις ιστοσελίδες μέσω του Διαδικτύου, αναθέτει την διαδικασία αυτή σε μία ομάδα συνεργαζόμενων πρακτόρων $A_0, A_1, \ldots, A_n$. Ο πράκτορας A_0 είναι στατικός και ονομάζεται *κύριος* πράκτορας (master agent), ενώ οι υπόλοιποι είναι κινητοί πράκτορες και ονομάζονται *εξαρτημένοι* (slave agents). Το προτεινόμενο μοντέλο χωρίζεται σε πέντε φάσεις.

- Στην πρώτη φάση, ο αγοραστής αρχικοποιεί τον κύριο πράκτορα και αλληλεπιδρά μαζί του, ώστε να δημιουργήσει τις απαιτήσεις για κάποια αγορά.

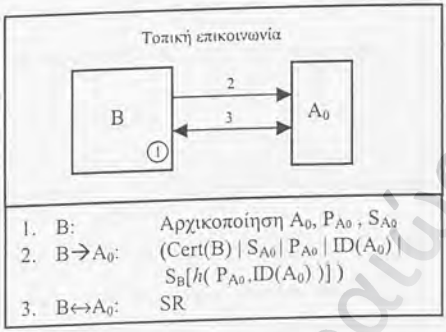
- Στη δεύτερη φάση ο κύριος πράκτορας επικοινωνεί με τα ηλεκτρονικά καταστήματα S_i, $i \in [1, n]$, για να ζητήσει *άδειες πρόσβασης* (permission tokens) για τους εξαρτημένους πράκτορες A_i, $i \in [1, n]$.

- Στην τρίτη φάση, ο κύριος πράκτορας δημιουργεί τους εξαρτημένους πράκτορες και εφοδιάζει τον καθένα με μία άδεια πρόσβασης, ώστε να αυθεντικοποιηθεί σε ένα ηλεκτρονικό κατάστημα. Οι εξαρτημένοι πράκτορες μεταναστεύουν στους εξυπηρετητές των ηλεκτρονικών καταστημάτων και διαπραγματεύονται εκ μέρους του αγοραστή.

- Στην τέταρτη φάση, οι εξαρτημένοι πράκτορες επιστρέφουν στην πηγή τους με προσφορές αγοράς, υπογεγραμμένες από τα ηλεκτρονικά καταστήματα. Ο κύριος πράκτορας είναι υπεύθυνος για την εκτίμηση των προσφορών.

- Τέλος, ο αγοραστής χρησιμοποιεί ένα σύστημα πληρωμής για να αγοράσει τα ζητούμενα αγαθά από το ηλεκτρονικό κατάστημα που πρότεινε τη βέλτιστη προσφορά, σύμφωνα με τους όρους του συγκεκριμένου υπογεγραμμένου συμβολαίου.

Στη συνέχεια του κεφαλαίου, χρησιμοποιούνται οι ακόλουθοι συμβολισμοί: με S_X, P_X συμβολίζεται το ζεύγος μυστικού / δημόσιου κλειδιού κάποιας οντότητας X, (όπου $X \in B, A_0, S_i$) τα οποία παράγονται με τη βοήθεια ενός κρυπτογραφικού συστήματος δημόσιου κλειδιού (π.χ. RSA [103]). Θεωρείται ότι τα ζεύγη κλειδιών πιστοποιούνται μέσω μίας Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure - PKI). Με $Cert(X)$ συμβολίζεται το ψηφιακό πιστοποιητικό της οντότητας X. Με $K_X[M]$ συμβολίζεται η κρυπτογράφηση ενός μηνύματος M χρησιμοποιώντας το κλειδί K_X και τέλος με h συμβολίζεται μια συνάρτηση κατακερματισμού (hash) - για παράδειγμα MD5, SHA1 [86].



Σχήμα 6.1: Αλληλεπίδραση αγοραστή και κύριου πράκτορα

6.2.1 Αρχικοποίηση του κύριου πράκτορα

Ο αγοραστής B αρχικοποιεί τον κύριο πράκτορα A_0 και ξεκινά τη διαδικασία της εύρεσης ανταγωνιστικών συμβολαίων αγοράς. Ο αγοραστής δημιουργεί ένα ζεύγος μυστικού / δημόσιου κλειδιού για τον κύριο πράκτορα και το πιστοποιεί μέσω της Υποδομής Δημόσιου Κλειδιού (βλέπε σχήμα 6.1).

Χρησιμοποιώντας μία ψευδοτυχαία γεννήτρια, δημιουργεί έναν μοναδικό αριθμό αναγνώρισης $ID(A_0)$ για τον κύριο πράκτορα και αυθεντικοποιεί τον κύριο πράκτορα ως τον νόμιμο αντιπρόσωπό του, εφοδιάζοντάς τον με το ψηφιακό πιστοποιητικό $Cert(B)$ και υπογράφοντας τον αριθμό αναγνώρισης και το δημόσιο κλειδί του κύριου πράκτορα. Αυτά τα βήματα μπορούν να επαναληφθούν εάν ο αγοραστής υποπτευθεί παραβίαση της ακεραιότητας του κύριου πράκτορα. Κατόπιν ο αγοραστής και ο κύριος πράκτορας αλληλεπιδρούν ώστε να δημιουργήσουν τις συγκεκριμένες απαιτήσεις αγοράς (SR - Shopping Requirements) του αγοραστή. Ο κύριος πράκτορας δεν λαμβάνει απλώς απαντήσεις σε προκαθορισμένες ερωτήσεις αλλά μπορεί να εκμεταλλευτεί την προηγούμενη συμπεριφορά του αγοραστή ώστε να τον καθοδηγήσει ή/και να υποβάλλει προτάσεις. Στο τέλος αυτής της διαδικασίας, ο κύριος πράκτορας

γνωρίζει τις απαιτήσεις αγοράς SR του αγοραστή και είναι ικανός να συνεχίσει την αναζήτηση χωρίς να απασχολήσει ξανά τον αγοραστή, έως την φάση ολοκλήρωσης της αγοράς.

6.2.2 Έκδοση αδειών πρόσβασης για τους κινητούς πράκτορες

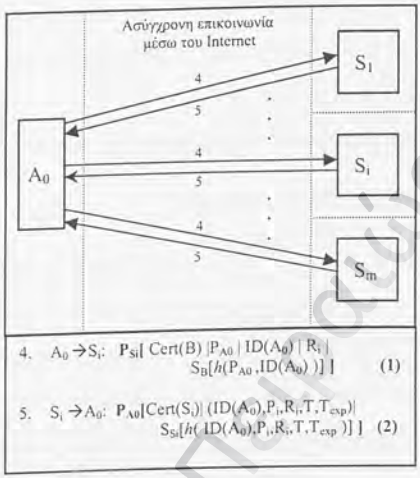
Ο κύριος πράκτορας επικοινωνεί με τα ηλεκτρονικά καταστήματα $S_i i \in [1, m]$, για να ζητήσει άδειες πρόσβασης για τους εξαρτημένους πράκτορες. Ο αγοραστής αρχικά δημιουργεί μία λίστα με τις ηλεκτρονικές διευθύνσεις των ηλεκτρονικών καταστημάτων που προτιμά. Ο κύριος πράκτορας συμβουλεύεται αυτή τη λίστα για να επικοινωνήσει με τα συγκεκριμένα ηλεκτρονικά καταστήματα και την συντηρεί έχοντας δικαιώματα πρόσβασης για να προσθέσει περισσότερες διευθύνσεις στην λίστα ή να διαγράψει άλλες, βασιζόμενος στις προτιμήσεις του αγοραστή. Δηλαδή, ο κύριος πράκτορας μαθαίνει από την προηγούμενη αγοραστική συμπεριφορά του αγοραστή τα καταστήματα που προτιμά.

Ο κύριος πράκτορας επικοινωνεί με τον εξυπηρετητή κάθε καταστήματος S_i και ζητά μία άδεια πρόσβασης για μελλοντική αλληλεπίδραση ενός εξαρτημένου πράκτορα A_i με το κατάστημα, στέλνοντας το μήνυμα (1), όπως περιγράφεται στο σχήμα 6.2. Το R_i είναι ένας μοναδικός αριθμός αίτησης, παραγόμενος από τον κύριο πράκτορα.

Το κατάστημα S_i λαμβάνει το μήνυμα (1), το αποκρυπτογραφεί και ελέγχει την εγκυρότητα του πιστοποιητικού $Cert(B)$ και της υπογραφής του αγοραστή:

$$P_B[S_B[h(P_{A_0}, ID(A_0))]] \stackrel{?}{=} h(PA0, ID(A0)).$$

Αν η επαλήθευση είναι επιτυχής τότε το κατάστημα S_i δέχεται τον κύριο πράκτορα ως αντιπρόσωπο του αγοραστή και στέλνει σε αυτόν μία (ή περισσότερες) άδεια πρόσβασης $(ID(A_0), P_i, R_i, T, T_{\epsilon\tau\rho})$, όπως φαίνεται στο μήνυμα (2). Το P_i είναι ένας



Σχήμα 6.2: Αλληλεπίδραση κύριου πράκτορα και ηλεκτρονικών καταστημάτων

μοναδικός αριθμός έγκρισης, ενώ τα $T, Texp$ είναι ο χρόνος έκδοσης και λήξης της άδειας πρόσβασης, αντίστοιχα. Ο κύριος πράκτορας λαμβάνει το μήνυμα (2), το αποκρυπτογραφεί και ελέγχει το πιστοποιητικό $Cert(S_i)$, καθώς και την εγκυρότητα της υπογραφής του ηλεκτρονικού καταστήματος στην άδεια πρόσβασης:

$$P_{S_i}[S_{S_i}[h(ID\langle A_0\rangle, P_i, R_i, T, Texp)]] \stackrel{?}{=} (ID(A_0), P_i, R_i, T, Texp).$$

Εάν όλα τα ανταλασσόμενα μηνύματα είναι έγκυρα, ο κύριος πράκτορας δέχεται την αυθεντικότητα της άδειας πρόσβασης, επαναλαμβάνει την διαδικασία και συλλέγει m άδειες πρόσβασης. Όταν οι εξαρτημένοι πράκτορες έχουν χρησιμοποιήσει κάποια από αυτά και ο αριθμός των υπολειπόμενων αδειών πρόσβασης φτάσει ένα προκαθορισμένο αριθμό l, ο κύριος πράκτορας αυτόματα επαναλαμβάνει αυτή τη φάση. Αν και ο αγοραστής πρέπει να είναι on-line για να επιτρέψει στον κύριο πράκτορα να εκτελέσει αυτά τα βήματα, η επικοινωνία μπορεί να είναι ασύγχρονη. Για να ελαχιστοποιηθεί

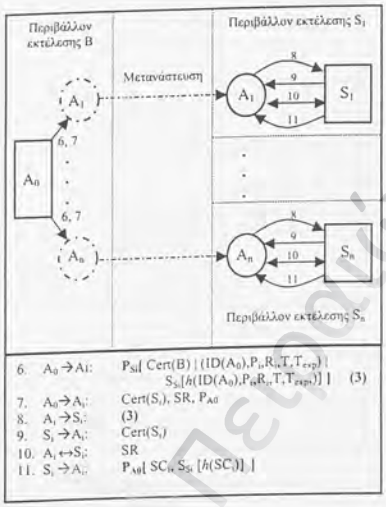
το προστιθέμενο βάρος, ο κύριος πράκτορας μπορεί να εκτελείται ως μία διαδικασία παρασκηνίου και να συλλέγει άδειες πρόσβασης από ηλεκτρονικά καταστήματα.

6.2.3 Διαπραγμάτευση εξαρτημένου πράκτορα A_i και ηλεκτρονικού καταστήματος S_i

Ο κύριος πράκτορας αρχίζει τη διαπραγμάτευση με τα ηλεκτρονικά καταστήματα παράγοντας n εξαρτημένους πράκτορες $A_i i \in [1, n]$ και εφοδιάζοντας καθέναν από αυτούς με μία άδεια πρόσβασης για τον εξυπηρετητή S_i, όπως φαίνεται στο σχήμα 6.3. Ο αριθμός n των ηλεκτρονικών καταστημάτων από τα οποία ο κύριος πράκτορας θα ζητήσει άδειες πρόσβασης ποικίλει ανάλογα με τις ιδιαίτερες ανάγκες του αγοραστή: δηλαδή, μπορεί να γίνει διαπραγμάτευση με ένα μικρό σχετικά αριθμό ηλεκτρονικών καταστημάτων για μια γρήγορη απόφαση, ή με μεγαλύτερο αριθμό καταστημάτων για μία βέλτιστη απόφαση.

Επίσης, ο κύριος πράκτορας εφοδιάζει κάθε εξαρτημένο πράκτορα A_i με τις αγοραστικές απαιτήσεις SR του αγοραστή. Ο πράκτορας A_i είναι έτοιμος να μεταναστεύσει στον εξυπηρετητή S_i και να διαπραγματευτεί με αυτόν βασιζόμενος στις αγοραστικές απαιτήσεις SR του αγοραστή. Για λόγους ασφαλείας, ο εξυπηρετητής S_i απαιτεί αυθεντικοποίηση από τον εξαρτημένο πράκτορα A_i πριν του επιτρέψει την πρόσβασή του. Ο εξαρτημένος πράκτορας A_i δίδει στο κατάστημα S_i τέτοια απόδειξη στέλνοντας μήνυμα (3). Το ηλεκτρονικό κατάστημα S_i λαμβάνει το μήνυμα (3) και ελέγχει την εγκυρότητα των $Cert(B)$ και $S_{S_i}[h(ID(A_0), P_i, R_i, T, T_{exp})]$. Επίσης ελέγχει το χρόνο λήξης T_{exp} της άδειας πρόσβασης.

Εάν επιτύχει η διαδικασία επαλήθευσης, το ηλεκτρονικό κατάστημα S_i παρέχει στον εξαρτημένο πράκτορα A_i περιβάλλον εκτέλεσης. Ο εξαρτημένος πράκτορας αναζητά το/τα συγκεκριμένο/α αγαθό/ά χρησιμοποιώντας τις απαιτήσεις αγοράς SR.

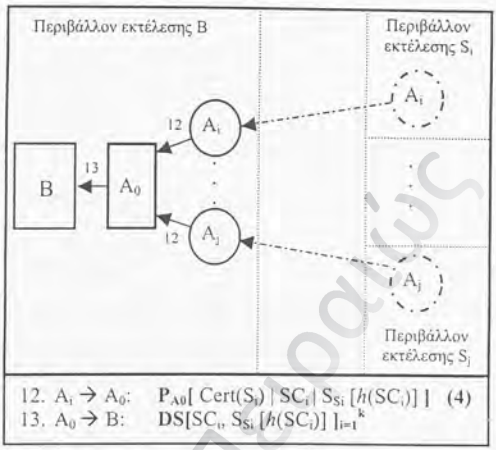


Σχήμα 6.3: Αλληλεπίδραση εξαρτημένων πρακτόρων και ηλεκτρονικών καταστημάτων

Σε περίπτωση επιτυχούς διαπραγμάτευσης το αποτέλεσμα της επικοινωνίας είναι μία προσφορά SC_i, υπογεγραμμένη από το ηλεκτρονικό κατάστημα S_i. Ο εξαρτημένος πράκτορας λαμβάνει την προσφορά κρυπτογραφημένη με το δημόσιο κλειδί του κύριου πράκτορα και η διαπραγμάτευση τερματίζεται.

6.2.4 Εκτίμηση των προσφορών

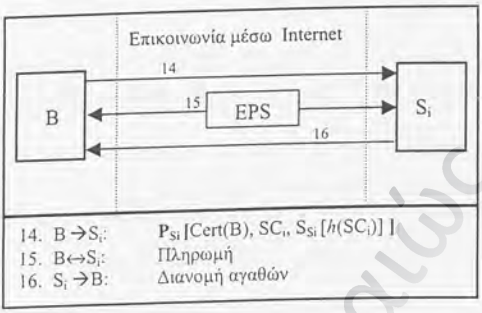
Οι εξαρτημένοι πράκτορες A_i, $1 \leq i \leq n$, επιστρέφουν στην πηγή τους και προμηθεύουν τον κύριο πράκτορα με το μήνυμα (4) (βλέπε σχήμα 6.4). Τονίζεται ότι λαμβάνεται υπόψιν η πιθανότητα ότι δεν επιστρέφουν όλοι οι n αρχικοί εξαρτημένοι πράκτορες στην πηγή τους. Κακόβουλοι εξυπηρετητές, αποτυχία του δικτύου ή άλλες αιτίες θα μπορούσαν να προκαλέσουν την απώλεια ορισμένων εξαρτημένων πρακτόρων. Παρόλα αυτά, η εκτίμηση των υπόλοιπων $k \leq n$ αποτελεσμάτων μπορεί να συνεχίσει.



Σχήμα 6.4: Συλλογή και εκτίμηση υπογεγραμμένων προσφορών αγοράς

Ο κύριος πράκτορας αποκρυπτογραφεί το μήνυμα (4) από κάθε εξαρτημένο πράκτορα και επαληθεύει τις υπογεγραμμένες προσφορές. Στην περίπτωση που ορισμένες προσφορές δεν είναι υπογεγραμμένες, ο κύριος πράκτορας τις απορρίπτει και συνεχίζει την εκτίμηση των υπόλοιπων.

Ο κύριος πράκτορας χρησιμοποιεί ένα μηχανισμό *DS* για την εκτίμηση των προσφορών ο οποίος βασίζεται στις προσωπικές απαιτήσεις του αγοραστή. Για παράδειγμα, εάν για μία συγκεκριμένη αγορά ο αγοραστής απαιτεί γρήγορη παράδοση, τα αποτελέσματα κατατάσσονται με βάση τον χρόνο παράδοσης, ως το πλέον σημαντικό κριτήριο.



Σχήμα 6.5: Εκτέλεση της βέλτιστης προσφοράς αγοράς

6.2.5 Ολοκλήρωση αγοράς

Ο αγοραστής χρησιμοποιεί τη βέλτιστη προσφορά αγοράς, σύμφωνα με τα αποτελέσματα της προηγούμενης φάσης και αγοραζει το/τα προϊόν/προϊόντα από το συγκεκριμένο ηλεκτρονικό κατάστημα S_i. Το ηλεκτρονικό κατάστημα εξετάζει την υπογραφή του στο συμβόλαιο και εάν είναι έγκυρη δεν μπορεί να αρνηθεί τους όρους του συμβολαίου. Ο αγοραστής χρησιμοποιεί ένα ηλεκτρονικό σύστημα πληρωμής (EPS) το οποίο είναι αποδεκτό από το ηλεκτρονικό κατάστημα και πληρώνει για τα προϊόντα. Τελικά, το κατάστημα παραδίδει τα αγαθά (βλέπε σχήμα 6.5).

Προφανώς, εάν τα αγαθά είναι φυσικά και όχι ψηφιακά (π.χ. λογισμικό), η παράδοση των αγαθών εκτελείται off-line.

6.3 Ανάλυση ασφάλειας

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, η ασφάλεια των μοντέλων κινητών πρακτόρων μπορεί να διαχωριστεί σε δύο μεγάλες περιοχές: την προστασία των κινητών πρακτόρων έναντι εχθρικών εξυπηρετητών και την προστασία των εξυπηρετητών

έναντι κακόβουλων πρακτόρων.

6.3.1 Προστασία των εξυπηρετητών των ηλεκτρονικών καταστημάτων

Στο προτεινόμενο μοντέλο, οι χρήστες των ηλεκτρονικών καταστημάτων ζητούν επαρκή απόδειξη αυθεντικοποίησης, προτού δεχθούν περαιτέρω αλληλεπίδραση με έναν πράκτορα. Ο κύριος πράκτορας A_0 αυθεντικοποιείται ως ο νόμιμος αντιπρόσωπος του αγοραστή στην πρώτη φάση, όπου ο αγοραστής εφοδιάζει τον κύριο πράκτορα με το πιστοποιητικό του, καθώς και με μία υπογραφή στο δημόσιο κλειδί και στον αριθμό αναγνώρισης του κύριου πράκτορα: $S_B[h(P_{A_0}, ID(A_0))]$. Αργότερα, ο κύριος πράκτορας A_0 αποστέλλει αυτήν την απόδειξη αυθεντικοποίησης στο ηλεκτρονικό κατάστημα S_i. Το κατάστημα μπορεί να αρνηθεί την επικοινωνία με τον κύριο πράκτορα, ο οποίος δεν είναι αυθεντικοποιημένος από έναν νόμιμο και εντοπίσιμο αγοραστή. Κάθε εξαρτημένος πράκτορας A_i αυθεντικοποιείται στο αντίστοιχο κατάστημα S_i, παρέχοντας στο κατάστημα την άδεια πρόσβασης που είχε εκδώσει το κατάστημα για τον κύριο πράκτορα.

Ο εξυπηρετητής μπορεί να ακολουθήσει μια αποτελεσματική πολιτική ελέγχου πρόσβασης, λαμβάνοντας αρκετά αντίμετρα ώστε να αποτρέψει επιθέσεις ασφάλειας ενός κακόβουλου κινητού πράκτορα [63]. Στο προτεινόμενο μοντέλο, ένας εξυπηρετητής αποτρέπει τέτοιες επιθέσεις αρνούμενος την πρόσβαση σε οποιονδήποτε κινητό πράκτορα χωρίς επαρκείς αποδείξεις αυθεντικοποίησης, δηλαδή μία έγκυρη άδεια πρόσβασης και ένα έγκυρο πιστοποιητικό του ιδιοκτήτη του πράκτορα. Το ηλεκτρονικό κατάστημα απαιτεί αυτήν την απόδειξη αυθεντικοποίησης ώστε να μπορεί να συνδέσει κάθε πράκτορα με τον ιδιοκτήτη του, αν παραστεί ανάγκη. Επιπρόσθετα, ο

χρήστης του καταστήματος ελέγχει τον κώδικα κάθε πράκτορα για να αποτρέψει επιθέσεις ιών και άλλου κακόβουλου κώδικα, προτού προμηθεύσει τον κινητό πράκτορα με περιβάλλον εκτέλεσης. Εάν ένας πράκτορας είναι ύποπτος για εχθρική συμπεριφορά, ο χρήστης μπορεί να αναστείλει τα δικαιώματά του, ακόμη και να διαγράψει τον πράκτορα. Η εμπιστευτικότητα των ανταλλασσόμενων μηνυμάτων μέσω του Διαδικτύου εξασφαλίζεται με κρυπτογράφηση δημόσιου κλειδιού.

6.3.2 Προστασία των πρακτόρων

Ο κύριος πράκτορας είναι στατικός και συνεπώς ένας κακόβουλος εξυπηρετητής δεν μπορεί να απειλήσει άμεσα την ασφάλειά του. Η κύρια υπηρεσία ασφάλειας του κύριου πράκτορα είναι η αυθεντικοποίηση των εξυπηρετητών των ηλεκτρονικών καταστημάτων. Ο εξυπηρετητής κάθε ηλεκτρονικού καταστήματος αυθεντικοποιείται στέλνοντας στον κύριο πράκτορα το πιστοποιητικό του, μαζί με την υπογραφή της άδειας πρόσβασης $S_{S_i}[h(ID(A_0), P_i, R_i, T, T_{exp})]$.

Περισσότερες απειλές ασφάλειας σχετίζονται με την προστασία των εξαρτημένων πρακτόρων, εφόσον είναι κινητοί. Κάθε εξαρτημένος πράκτορας A_i μεταναστεύει από τον υπολογιστή του αγοραστή στον εξυπηρετητή του καταστήματος S_i. Ένας εχθρικός εξυπηρετητής μπορεί να αρνηθεί να προμηθεύσει τον A_i με περιβάλλον εκτέλεσης ή να προσπαθήσει να παραβιάσει την ακεραιότητά του. Στο προτεινόμενο μοντέλο, οι εξυπηρετητές των ηλεκτρονικών καταστημάτων δεν έχουν κανένα κίνητρο να παραβιάσουν την ακεραιότητα των εξαρτημένων πρακτόρων, μιας και οι εξαρτημένοι πράκτορες δεν μεταφέρουν ευαίσθητες πληροφορίες που θα ήταν χρήσιμες για το ηλεκτρονικό κατάστημα. Ειδικότερα, κάθε εξαρτημένος πράκτορας μεταναστεύει και διαπραγματεύεται με ένα κατάστημα χωρίς να μεταφέρει προηγούμενα αποτελέσματα διαπραγματεύσεων (π.χ. συμβόλαια αγοράς υπογεγραμμένα από άλλα ηλεκτρονικά καταστήματα).

Επιπρόσθετα, οι εξαρτημένοι πράκτορες δεν μεταφέρουν μυστικά κλειδιά, καθώς η φάση αγοράς ανατίθεται στον αγοραστή.

Ένας κακόβουλος εξυπηρετητής μπορεί να προκαλέσει άρνηση εξυπηρέτησης σε έναν αυθεντικοποιημένο εξαρτημένο πράκτορα με έγκυρη άδεια πρόσβασης ή ακόμη και να τερματίσει τον πράκτορα. Είναι πολύ απίθανο ο εξυπηρετητής ενός ηλεκτρονικού καταστήματος να ενεργήσει με αυτόν τον τρόπο, αφού ο κύριος πράκτορας γνωρίζει την ταυτότητα του χρήστη που επισκέπτεται κάθε εξαρτημένος πράκτορας. Εάν ο κύριος πράκτορας εντοπίσει εχθρική συμπεριφορά εναντίον ενός συγκεκριμένου εξαρτημένου πράκτορα, μπορεί να προσθέσει το αντίστοιχο ηλεκτρονικό κατάστημα σε μια "μαύρη λίστα" και να διακόψει κάθε μελλοντική συναλλαγή με αυτό.

Για να εξασφαλιστεί η μυστικότητα του υπογεγραμμένου συμβολαίου αγοράς που φέρει ο εξαρτημένος πράκτορας, το συμβόλαιο αγοράς που προκύπτει από κάθε διαπραγμάτευση, κρυπτογραφείται μέχρι να επιστρέψει ο πράκτορας στην πηγή του.

Ένα ηλεκτρονικό κατάστημα δεν μπορεί να αρνηθεί να πωλήσει το/τα ζητούμενο/α προϊόν/προϊόντα με τους όρους του συμβολαίου αγοράς που εξέδωσε, επειδή προηγουμένως το υπέγραψε. Τα ανυπόγραφα συμβόλαια αγοράς δεν γίνονται αποδεκτά προς εκτίμηση από τον κύριο πράκτορα.

Το προτεινόμενο μοντέλο είναι ανθεκτικό σε άρνηση εξυπηρέτησης μερικών ενδεχόμενων εχθρικών εξυπηρετητών, χωρίς την επανεκκίνηση όλης της διαδικασίας. Ειδικότερα, αν k από n εξαρτημένους πράκτορες δεν επιστρέψουν στον αγοραστή, το σύστημα μπορεί να συνεχίσει την εκτίμηση των υπόλοιπων $n - k$ προσφορών. Είναι φανερό ότι η αξιοπιστία του αποτελέσματος είναι αντιστρόφως ανάλογη του k.

6.4 Συζήτηση

Ορισμένα συστήματα συναλλαγών βασισμένα σε κινητούς πράκτορες προτείνουν την απασχόληση ενός κινητού πράκτορα, ο οποίος επισκέπτεται και διαπραγματεύεται με n ηλεκτρονικά καταστήματα διαδοχικά, π.χ. [114]. Σε αυτά τα συστήματα ο πράκτορας μεταφέρει όλα τα προηγούμενα αποτελέσματα των διαπραγματεύσεων όταν επισκέπτεται $k+1$ καταστήματα, συνεπώς είναι αναγκαία η προστασία αυτών των αποτελεσμάτων. Για να είναι εφικτή η ανίχνευση ενός δυνητικού εχθρικού εξυπηρετητή ο αγοραστής χρειάζεται τη συνεργασία μίας έμπιστης οντότητας, η οποία παράγει τον πράκτορα για λογαριασμό του αγοραστή, παρακολουθεί την διαδικασία και επιστρέφει τα αποτελέσματα.

Το προτεινόμενο μοντέλο απαιτεί την συνεργασία ενός κύριου και n εξαρτημένων πρακτόρων για να διαπραγματευτεί με n καταστήματα. Επιπρόσθετα, η φάση έκδοσης αδειών πρόσβασης φαινομενικά υποβαθμίζει ένα βασικό πλεονέκτημα των κινητών πρακτόρων, δηλαδή την ασύγχρονη και off-line επικοινωνία. Η χρήση n αντί ενός κινητού πράκτορα δεν μειώνει αισθητά την αποτελεσματικότητα του μοντέλου σε μη ανεκτό επίπεδο. Κάθε ένας από τους n εξαρτημένους πράκτορες έχει το έργο της διαπραγμάτευσης με ένα μόνο ηλεκτρονικό κατάστημα και της επιστροφής του αποτελέσματος στον κύριο πράκτορα. Η διαδικασία μπορεί να εκτελεστεί με παράλληλο τρόπο, ένα σημαντικό κέρδος έναντι του σειριακού τρόπου αποστολής ενός πράκτορα στους εξυπηρετητές $S_1, S_2 \ldots S_n$ διαδοχικά. Επιπλέον, η ανάγκη έκδοσης αδειών πρόσβασης μέσω on-line επικοινωνίας μεταξύ του κύριου πράκτορα και των ηλεκτρονικών καταστημάτων μπορεί να πραγματοποιηθεί ασύγχρονα. Ο κύριος πράκτορας μπορεί να διατηρήσει μια βάση δεδομένων με άδειες πρόσβασης, ταξινομημένες με βάση ομογενή καταστήματα. Έτσι το επιπρόσθετο βάρος στην εκτέλεση που επιβάλλεται από αυτήν την φάση, μπορεί να ελαχιστοποιηθεί σημαντικά, ενώ η ανάγκη για μία

έμπιστη οντότητα, που παρακολουθεί την διαδικασία μετανάστευσης του πράκτορα, εξαλείφεται.

Κάθε εξαρτημένος πράκτορας δεν φέρει ευαίσθητες πληροφορίες ασφάλειας όταν μεταναστεύει στον εξυπηρετητή S_i. Αυτό το γεγονός ελαχιστοποιεί τις ανάγκες ασφάλειας του κινητού πράκτορα σε ανίχνευση επιθέσεων παρά σε παρεμπόδιση επιθέσεων, η οποία θα απαιτούσε πολύπλοκες κρυπτογραφικές τεχνικές ή λύσεις βασιζόμενες σε ασφαλές υλικό [101, 110]. Ένα ηλεκτρονικό κατάστημα που ενεργεί με εχθρικό τρόπο σε έναν αυθεντικοποιημένο εξαρτημένο πράκτορα μπορεί εύκολα να εντοπιστεί από τον κύριο πράκτορα και να μη χρησιμοποιηθεί σε μελλοντικές αγορές.

Το προτεινόμενο σχήμα παρέχει ανεκτικότητα σε λάθη έναντι σχημάτων τα οποία χρησιμοποιούν έναν μόνο κινητό πράκτορα [87, 114]. Εάν αυτός ο κινητός πράκτορας δεν επιστρέψει στον χρήστη εξαιτίας ενός εχθρικού εξυπηρετητή ή αποτυχίας του δικτύου, ολόκληρη η διαδικασία πρέπει να επαναληφθεί από την αρχή. Το προτεινόμενο μοντέλο είναι ανθεκτικό σε αποτυχία k εξαρτημένων πρακτόρων και μπορεί να συνεχίσει με τους εναπομείναντες $n - k$ κινητούς πράκτορες. Αυτή η προσέγγιση είναι προς όφελος των έντιμων εξυπηρετητών, καθώς οι προσφορές τους δεν χάνονται λόγω επιθέσεων ενός κακόβουλου εξυπηρετητή.

Το προτεινόμενο μοντέλο δεν προσφέρει ανώνυμη επικοινωνία. Η τροποποίηση του σχήματος για την παροχή ανώνυμης επικοινωνίας πρακτόρων, είναι ανοικτό πρόβλημα. Η ανωνυμία της πληρωμής δεν σχετίζεται με την ανωνυμία των πρακτόρων, επειδή ο αγοραστής μπορεί να χρησιμοποιήσει ένα σύστημα ανώνυμης πληρωμής για να εκτελέσει την συναλλαγή.

Κεφάλαιο 7

Ασφαλής μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων

Οι μηχανισμοί μεταβίβασης ρόλου που έχουν προταθεί στη διεθνή βιβλιογραφία για συστήματα κινητών πρακτόρων υποστηρίζουν μόνο μεταβίβαση ρόλου από στατικές οντότητες σε κινητούς πράκτορες και δεν μπορούν να χρησιμοποιηθούν για μεταβίβαση ρόλου *μεταξύ* κινητών πρακτόρων. Αυτό οφείλεται στο γεγονός ότι στηρίζονται σε συμβατικές ψηφιακές υπογραφές, οι οποίες δεν μπορούν να υποστηρίξουν τη δυναμική κατάσταση εκτέλεσης των κινητών πρακτόρων: μια υπογεγραμμένη μεταβίβαση σε μία κατάσταση εκτέλεσης δεν θα είναι έγκυρη για την επόμενη κατάσταση του πράκτορα. Σε αυτό το κεφάλαιο προτείνεται ένας κρυπτογραφικός μηχανισμός για ασφαλή μεταβίβαση ρόλων μεταξύ κινητών πρακτόρων ο οποίος παρέχει προστασία από κακόβουλο περιβάλλον εκτέλεσης των πρακτόρων.

7.1 Εισαγωγή

Οι πολιτικές ελέγχου πρόσβασης σε συστήματα κινητών πρακτόρων, καθορίζουν τους κανόνες αυθεντικοποίησης και εξουσιοδότησης με βάση τους οποίους οι κινητοί πράκτορες έχουν πρόσβαση σε συγκεκριμένους πόρους ενός συστήματος. Οι κανόνες αυθεντικοποίησης χρησιμοποιούνται για την απόδειξη της αυθεντικότητας των κινητών πρακτόρων, ενώ οι κανόνες εξουσιοδότησης χρησιμοποιούνται για να αποφασιστεί το επίπεδο πρόσβασης που θα δοθεί σε έναν αυθεντικοποιημένο πράκτορα. Για παράδειγμα, οι κανόνες εξουσιοδότησης θα μπορούσαν να προσδιορίζουν τα αρχεία στα οποία μπορεί να έχει πρόσβαση ο πράκτορας, το ποσό διαθέσιμης μνήμης, ή το εάν επιτρέπεται στον πράκτορα να εκκινήσει μια σύνδεση δικτύου με έναν απομακρυσμένο διακομιστή. Υπάρχουν αρκετά μοντέλα ασφάλειας για συστήματα κινητών πρακτόρων των οποίων ο έλεγχος πρόσβασης βασίζεται σε *ρόλους* [22, 64, 66, 92].

Οι ρόλοι είναι σημασιολογικές δομές οι οποίες αντανακλούν τις διαφορετικές υπευθυνότητες των υποκειμένων μίας εφαρμογής. Ο διαχειριστής αντιστοιχεί *άδειες πρόσβασης* (ή *προνόμια πρόσβασης*) των πόρων του συστήματος σε *ρόλους*. Οι *οντότητες* του συστήματος (χρήστες ή τμήματα λογισμικού που ελέγχονται από τους χρήστες) αντιστοιχίζονται σε ρόλους. Οι ρόλοι καθορίζουν ποιες οντότητες έχουν άδεια πρόσβασης σε ποια αντικείμενα του συστήματος. Με τον Έλεγχο Πρόσβασης Βασισμένο σε Ρόλους (Role Based Access Control - RBAC) [105, 100] ο ρόλος ενός εντολέα ελέγχεται σε κάθε κλήση πρόσβασης. Εάν η οντότητα που εκκινεί μία κλήση δεν ανήκει σε κάποιο ρόλο ο οποίος περιλαμβάνει άδεια πρόσβασης σε ένα αντικείμενο, η κλήση αποτυγχάνει. Οι οντότητες έχουν πρόσβαση στους πόρους του συστήματος σύμφωνα με τους *περιορισμούς* που καθορίζονται στα πλαίσια των ρόλων στους οποίους ανήκουν [2].

Η μεταβίβαση ρόλου είναι μια σημασιολογική δομή ιδιαίτερης σημασίας στα μοντέλα RBAC, η οποία επιτρέπει σε μία οντότητα να μεταβιβάσει έναν ρόλο σε μια άλλη οντότητα, για μια συγκεκριμένη χρονική περίοδο. Για παράδειγμα, ο διαχειριστής μίας βάσης δεδομένων μπορεί να μεταβιβάσει τον ρόλο του/της σε έναν άλλο εντολέα, επιτρέποντας έτσι στον τελευταίο να εκτελέσει λειτουργίες ανανέωσης στη βάση δεδομένων. Η μεταβίβαση έχει αρκετά πλεονεκτήματα όπως δυναμική κατανομή, παραλληλοποίηση, συνεχή εκτέλεση, και αποτελεσματική χρήση των υπηρεσιών και των πόρων. Όμως, η μεταβίβαση ρόλων πρέπει να υπόκειται σε αποτελεσματικούς ελέγχους, ώστε να αποφεύγεται ανεπιθύμητη διαρροή δικαιωμάτων πρόσβασης.

Υπάρχει μια φυσική ομοιότητα μεταξύ των κινητών πρακτόρων και της μεταβίβασης ρόλων: στους κινητούς πράκτορες αναθέτονται συνήθως στόχοι εκτέλεσης εκ μέρους άλλων οντοτήτων, ενώ με τη μεταβίβαση ρόλων παραχωρούνται δικαιώματα πρόσβασης σε κάποια οντότητα για να εκτελέσει κάποια δραστηριότητα εκ μέρους της μεταβιβάζουσας οντότητας. Για αυτό το λόγο η μεταβίβαση ρόλων έχει χρησιμοποιηθεί σε πολιτικές πρόσβασης για συστήματα πρακτόρων [9, 42, 66, 22, 64, 92]. Εντούτοις, τα σχήματα που προτάθηκαν έως τώρα εξετάζουν μόνο τη μεταβίβαση ρόλου από στατικές οντότητες (χρήστες ή τμήματα λογισμικού που εκτελούνται τοπικά και ελέγχονται από χρήστες) σε κινητούς πράκτορες. Μέχρι στιγμής, δεν έχουν προταθεί μηχανισμοί που υποστηρίζουν μεταβίβαση ρόλων μεταξύ κινητών πρακτόρων, κυρίως εξαιτίας των αδυναμιών ασφάλειας των κινητών πρακτόρων κατά τη εκτέλεσή τους σε εχθρικά (μη αξιόπιστα) περιβάλλοντα.

Το υπόλοιπο κεφάλαιο είναι διαρθρωμένο ως ακολούθως. Στην ενότητα 7.2 παρουσιάζεται μία σύντομη ανασκόπηση σχετικά με τη μεταβίβαση ρόλου σε συστήματα βασιζόμενα σε πράκτορες, ενώ εξετάζονται πιθανές εφαρμογές στις οποίες η μεταβίβαση ρόλων μεταξύ κινητών πρακτόρων επεκτείνει την αποτελεσματικότητα και την

ευελιξία του συστήματος. Στην ενότητα 7.3 εξετάζονται τα θέματα ασφάλειας της μεταβίβασης ρόλου μεταξύ κινητών πρακτόρων. Κατόπιν παρουσιάζεται ένας κρυπτογραφικός μηχανισμός για ασφαλή μεταβίβαση ρόλων μεταξύ κινητών πρακτόρων. Στην ενότητα 7.4 περιγράφονται τα δομικά συστατικά αυτού του μηχανισμού ενώ στην ενότητα 7.5 συνδυάζονται αυτά τα δομικά συστατικά για το σχεδιασμό ενός πρωτοκόλλου μεταβίβασης ρόλων μεταξύ πρακτόρων. Στην ενότητα 7.6 αναλύεται η ασφάλεια αυτού του πρωτοκόλλου. Τέλος, στην ενότητα 7.7 παρουσιάζονται τα συμπεράσματα του κεφαλαίου.

7.2 Μεταβίβαση σε συστήματα πρακτόρων

7.2.1 Σχετική βιβλιογραφία

Υπάρχουν αρκετές αρχιτεκτονικές ασφάλειας για συστήματα βασιζόμενα σε πράκτορες που χρησιμοποιούν μηχανισμούς μεταβίβασης από στατικές οντότητες σε κινητούς πράκτορες [9, 42, 66, 22, 64, 92]. Οι ρόλοι (ή προνόμια πρόσβασης σε μερικά μοντέλα) μεταβιβάζονται συνδυάζοντας ψηφιακές υπογραφές με μηχανισμούς όπως γλώσσες εξουσιοδότησης [9, 22, 64, 92], λίστες πρόσβασης [65], μηχανισμούς αποτίμησης κατάστασης [9, 42] και πιστοποιητικά χαρακτηριστικών [64]. Η μεταβιβάζουσα οντότητα μπορεί να είναι ο δημιουργός, ο αποστολέας ή κάποιος εκτιμητής του πράκτορα (μία έμπιστη οντότητα).

Αν και έχουν προταθεί στη διεθνή βιβλιογραφία αρκετές λύσεις για μεταβίβαση ρόλου από στατικές οντότητες σε κινητούς πράκτορες, το αντίθετο συμβαίνει στην περίπτωση της μεταβίβασης ρόλου μεταξύ κινητών πρακτόρων. Η ασφαλής μεταβίβαση ρόλων μεταξύ πρακτόρων έχει αναγνωριστεί ως ένα δυσεπίλυτο πρόβλημα [56], αφού

οι προτεινόμενες έως τώρα λύσεις βασίζονται σε υποθέσεις εμπιστοσύνης για το περιβάλλον εκτέλεσης. Ο μηχανισμός που προτείνεται σε αυτό το κεφάλαιο δεν στηρίζεται σε υποθέσεις εμπιστοσύνης για το περιβάλλον εκτέλεσης.

7.2.2 Μεταβίβαση ρόλων μεταξύ κινητών πρακτόρων: χρήσιμα παραδείγματα

Υπάρχουν αρκετές εφαρμογές όπου η μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων θα επεκτείνει την ευελιξία της πολιτικής πρόσβασης. Ο μεταβιβαζόμενος πράκτορας μπορεί να είναι είτε ένας υπάρχων πράκτορας που αποκτά νέους ρόλους, ή ένας κλώνος πράκτορας που κληρονομεί την τελευταία κατάσταση του μεταβιβάζοντα πράκτορα μαζί με τους ρόλους του, καθώς και πιθανούς περιορισμούς. Παραδείγματα εφαρμογών μεταβίβασης ρόλου μεταξύ κινητών πρακτόρων είναι η δυναμική αυθεντικοποίηση πρακτόρων και η διαχείριση ευφυών δικτύων.

Δυναμική αυθεντικοποίηση πρακτόρων

Όπως έχει ήδη αναφερθεί, οι κινητοί πράκτορες εκτελούνται διαδοχικά σε αρκετούς διακομιστές ώστε να πραγματοποιήσουν έναν κατανεμημένο υπολογισμό. Μετά από μερική εκτέλεση σε κάθε διακομιστή ο πράκτορας φτάνει σε μια νέα κατάσταση, από την οποία συνεχίζει την εκτέλεση μέχρι να φτάσει στον επόμενο διακομιστή. Αφού οι περιπλανώμενοι πράκτορες αλλάζουν την κατάστασή τους δυναμικά, η μεταβίβαση ενός ρόλου στον αρχικό πράκτορα δεν θα είναι έγκυρη για τις επόμενες καταστάσεις. Σε τέτοιες περιπτώσεις, η συνήθης πρακτική είναι να χρησιμοποιείται μία έμπιστη οντότητα η οποία παράγει νέα διαπιστευτήρια εξουσιοδότησης για τις νέες καταστάσεις του πράκτορα (για παράδειγμα εκδίδει ένα νέο πιστοποιητικό χαρακτηριστικών

για κάθε κατάσταση του πράκτορα όπως προτείνεται από τον Jansen [64]). Η μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων επιτρέπει στους περιπλανώμενους πράκτορες να εξουσιοδοτήσουν αυτόνομα τις νέες καταστάσεις τους για εκτέλεση σε πολλαπλούς διακομιστές. Η μετάβαση ενός πράκτορα σε μία νέα κατάσταση μπορεί επίσης να θεωρηθεί ως η δημιουργία του μεταβιβαζόμενου πράκτορα. Συνεπώς ένας πράκτορας μπορεί να μεταβιβάσει τους ρόλους του (πιθανώς με επιπρόσθετους περιορισμούς) στη νέα του κατάσταση μετά από μερική εκτέλεση σε έναν διακομιστή και πριν από τη μετανάστευσή του στον επόμενο διακομιστή. Κατά αυτόν τον τρόπο ένας περιπλανώμενος πράκτορας μπορεί να είναι αυτο-εξουσιοδοτούμενος για πολλαπλές μεταναστεύσεις και εκτελέσεις, χωρίς ενεργή εμπλοκή των έμπιστων οντοτήτων.

Διαχείριση ευφυών δικτύων

Αρκετές αρχιτεκτονικές ευφυών δικτύων κάνουν χρήση τεχνολογιών κινητών πρακτόρων για τη διαχείριση ευφυών δικτύων [18, 26]. Η ανανέωση της λειτουργικότητας των κόμβων του δικτύου πραγματοποιείται μέσω κινητών πρακτόρων. Όταν η λειτουργικότητα (service logic) ενός κόμβου του δικτύου πρόκειται να ανανεωθεί, ένας ειδικού-σκοπού *κόμβος διοίκησης* παράγει έναν πράκτορα με την ενημερωμένη λειτουργικότητα του κόμβου στόχου ως μέρος του εκτελέσιμου κώδικα του πράκτορα. Ο κινητός πράκτορας μεταναστεύει στον στόχο και ενημερώνει την λειτουργικότητά του. Για να εξουσιοδοτήσει την εκτέλεση του πράκτορα στον κόμβο στόχο, ο κόμβος διοίκησης μεταβιβάζει στον πράκτορα ένα πιστοποιητικό χαρακτηριστικών με τους κατάλληλους ρόλους [40]. Σε περίπτωση όπου η λειτουργικότητα αρκετών κόμβων του ευφυούς δικτύου πρέπει να ενημερωθεί, τότε ένας εξουσιοδοτημένος πράκτορας παράγεται για κάθε έναν κόμβο στόχο. Συνεπώς, το κόστος επικοινωνίας είναι ανάλογο προς τον αριθμό των αιτημάτων. Με τη μεταβίβαση ρόλων από πράκτορα σε πράκτορα,

οι πράκτορες θα μπορούσαν να μεταβιβάσουν τους απαιτούμενους ρόλους σε άλλους πράκτορες (πιθανώς κλώνους). Οι πράκτορες μεταβίβασης θα εκτελούσαν λειτουργική ενημέρωση σε πολλαπλούς κόμβους, χωρίς να απαιτείται να επικοινωνήσουν με τον απομακρυσμένο κόμβο διοίκησης για εξουσιοδότηση. Αυτό θα ελάττωνε σημαντικά το κόστος επικοινωνίας που σχετίζεται με τη διοίκηση δικτύου.

7.3 Απειλές ασφάλειας

Αν και η μεταβίβαση ρόλου προσφέρει πολλά πρακτικά πλεονεκτήματα στις εφαρμογές πρακτόρων, υπάρχουν αρκετές απειλές ασφάλειας κατά τη διαδικασία της μεταβίβασης ρόλων που πρέπει να αντιμετωπιστούν. Αν η μεταβίβαση ρόλου δεν προστατεύεται επαρκώς, μπορεί να προκληθεί μη-ελεγχόμενη ροή προνομίων πρόσβασης. Οι απειλές αφορούν κυρίως την αυθεντικοποίηση, την ανάκληση της μεταβίβασης και την κατάχρηση πρακτόρων.

Αυθεντικοποίηση

Ένας πράκτορας θα πρέπει να είναι ικανός να αυθεντικοποιεί τη μεταβίβαση ενός ρόλου σε έναν άλλο πράκτορα. Η συνήθης πρακτική είναι η χρήση ψηφιακών υπογραφών: η οντότητα που μεταβιβάζει ένα ρόλο, υπογράφει τον ρόλο αυτό μαζί με τον προσδιοριστή της οντότητας η οποία είναι ο στόχος της μεταβίβασης. Ο προσδιοριστής είναι το αποτέλεσμα μίας κατάλληλης συνάρτησης κατακερματισμού (hash) με είσοδο τον κώδικα, τα δεδομένα και την τρέχουσα κατάσταση εκτέλεσης του πράκτορα στον οποίο μεταβιβάζεται ο ρόλος.

Όμως, οι γνωστές ψηφιακές υπογραφές δεν μπορούν να χρησιμοποιηθούν για μεταβίβαση ρόλου μεταξύ πρακτόρων, επειδή δεν περιλαμβάνουν την περίπτωση όπου

ο πράκτορας που δέχεται τη μεταβίβαση έχει διαφορετική κατάσταση εκτέλεσης από τον αρχικό στόχο της μεταβίβασης. Μια απλή λύση θα ήταν να προσαρτηθεί στον πράκτορα μία λίστα από υπογεγραμμένες μεταβιβάσεις ρόλου σε προκαθορισμένες καταστάσεις εκτέλεσης. Όμως, αυτή η λύση δεν μπορεί να υποστηρίξει δυναμική μεταβίβαση σε μη προκαθορισμένους στόχους. Μια άλλη λύση θα ήταν να παραχωρηθεί στους πράκτορες η συνάρτηση υπογραφής του ιδιοκτήτη τους. Όμως αυτή η λύση δεν είναι κατάλληλη για εκτέλεση πρακτόρων σε διακομιστές οι οποίοι δεν είναι έμπιστοι [29, 71, 72, 104, 109], εκτός εάν η συνάρτηση υπογραφής προστατεύεται κρυπτογραφικά.

Ανάκληση της μεταβίβασης ρόλου

Η ανάκληση είναι ένα σημαντικό χαρακτηριστικό της μεταβίβασης ρόλου. Οι διαφορετικές κατηγορίες ανάκλησης μεταβίβασης ρόλου που έχουν προσδιοριστεί είναι οι ακόλουθες [6]:

- *Διαδοχική ανάκληση.* Με την διαδοχική ανάκληση ένας ρόλος που έχει μεταβιβαστεί σε μία οντότητα ανακαλείται, εάν ανακληθεί ο ρόλος από την οντότητα που πραγματοποίησε την αρχική μεταβίβαση.

- *Εξάρτηση μεταβιβάζοντα.* Σε περίπτωση όπου η μεταβίβαση ρόλου πραγματοποιείται με εξάρτηση μεταβιβάζοντα, μόνο η συγκεκριμένη οντότητα που πραγματοποίησε τη μεταβίβαση επιτρέπεται να ανακαλέσει το ρόλο. Σε αντίθετη περίπτωση, η ανάκληση ενός ρόλου μπορεί να πραγματοποιηθεί από οποιοδήποτε οντότητα η οποία είναι αρχικό μέλος του ρόλου αυτού.

- *Χρονική εξάρτηση.* Η ανάκληση είναι χρονικά εξαρτώμενη αν ο μεταβιβαζόμενος ρόλος συνοδεύται από κάποια ημερομηνία λήξης. Σε αντίθετη περίπτωση είναι

χρονικά ανεξάρτητη.

Η διαδοχική ανάκληση είναι η πλέον κατάλληλη για μεταβίβαση ρόλου μεταξύ πρακτόρων. Αν ένας ρόλος μεταβιβάζεται σε έναν πράκτορα ο οποίος με τη σειρά του μεταβιβάζει αυτό το ρόλο σε έναν άλλο πράκτορα, τότε η ανάκληση του ρόλου από τον αρχικό χρήστη θα έπρεπε να καταλήγει στην ανάκληση όλων των μεταβιβαζόμενων ρόλων. Σε αντίθετη περίπτωση, ο χρήστης θα μπορούσε να συνεχίσει να χρησιμοποιεί τα δικαιώματα πρόσβασης του ρόλου έμμεσα μέσω των μεταβιβαζόμενων στους πράκτορες ρόλων. Επιπλέον, η ανάκληση θα έπρεπε να είναι εξαρτώμενη από τον μεταβιβάζοντα. Ειδάλλως, δεν θα μπορούσε να εντοπιστεί ένας κακόβουλος χρήστης – μέλος ενός ρόλου, ο οποίος ανακαλεί αυτόν τον ρόλο από ένα πράκτορα ο οποίος ανήκει σε κάποιο άλλο χρήστη. Τέλος, η χρονικά εξαρτώμενη ανάκληση είναι επιθυμητή, αφού η ζωή ενός πράκτορα είναι από μόνη της χρονικά περιορισμένη. Όμως, κατάλληλα χρονικά όρια θα πρέπει να επιλέγονται, ώστε να αποφευχθεί η πιθανότητα της λήξης ενός ρόλου προτού ο πράκτορας εκτελέσει το έργο του.

Κατάχρηση πράκτορα

Κάθε διακομιστής στον οποίο μεταναστεύει ένας πράκτορας εκτελεί εν μέρει τον πράκτορα και κατόπιν προωθεί τον πράκτορα σε έναν άλλο διακομιστή. Ένας κακόβουλους διακομιστής μπορεί να προσπαθήσει να χρησιμοποιήσει τον πράκτορα για κάποια διαφορετική εργασία από αυτήν που του έχει ανατεθεί στον από τον δημιουργό του και/ή από τους προηγούμενους διακομιστές εκτέλεσης. Ένας κακόβουλος διακομιστής μπορεί να αφαιρέσει τους περιορισμούς μεταβίβασης του πράκτορα και να χρησιμοποιήσει τον πράκτορα για την εκτέλεση ενός διαφορετικού έργου. Εναλλακτικά, ένας κακόβουλος εσωτερικός διακομιστής μπορεί να καταστρέψει τον πράκτορα. Ένας κακόβουλος εξωτερικός διακομιστής μπορεί να κλωνοποιήσει τον πράκτορα,

υποκλέπτοντας την επικοινωνία των εσωτερικών διακομιστών κατά τη διάρκεια της μετανάστευσης, ώστε να χρησιμοποιήσει τους κλωνοποιημένους πράκτορες για δικούς του σκοπούς.

7.4 Ασφαλής μεταβίβαση ρόλου μεταξύ πρακτόρων: τα δομικά συστατικά

Ο κρυπτογραφικός μηχανισμός για ασφαλή μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων ο οποίος προτείνεται σε αυτό το κεφάλαιο, χρησιμοποιεί ως δομικά συστατικά τα πιστοποιητικά χαρακτηριστικών [81], την ισχυρή χρονική ασφάλεια [19] και τις μη-αποσπώμενες υπογραφές [71], τα οποία περιγράφονται συνοπτικά παρακάτω:

- Πιστοποιητικά χαρακτηριστικών. Ενώ τα πιστοποιητικά ταυτότητας (π.χ. X.509 v.3) συνδέουν οντότητες με δημόσια κλειδιά, τα πιστοποιητικά χαρακτηριστικών συνδέουν οντότητες με ορισμένα χαρακτηριστικά. Ένα πιστοποιητικό χαρακτηριστικών περιέχει επίσης έναν προσδιοριστή και μία ημερομηνία λήξης και πιστοποιείται (μέσω ψηφιακής υπογραφής) από μια αρχή πιστοποίησης CA. Τα πιστοποιητικά χαρακτηριστικών έχουν χρησιμοποιηθεί στην υλοποίηση ελέγχου πρόσβασης βασισμένου σε ρόλους σε κατανεμημένα συστήματα [81]. Ο Jansen [64] πρότεινε ένα σχήμα ελέγχου πρόσβασης για συστήματα πρακτόρων, στο οποίο οι ρόλοι υλοποιούνται με πιστοποιητικά χαρακτηριστικών. Γενικά, τα πιστοποιητικά χαρακτηριστικών μπορούν να χρησιμοποιηθούν για να αποδωθούν ρόλοι σε οντότητες και να προσδιοριστούν περιορισμοί των ρόλων για την αποφυγή καταχρήσεων. Για παράδειγμα, μέσω πιστοποιητικών χαρακτηριστικών μπορούν να αποδωθούν διάφοροι ρόλοι σε μία ή περισσότερες οντότητες, για να επιτευχθεί διαχωρισμός καθηκόντων (separation of duties). Ένα πιστοποιητικό

χαρακτηριστικών AC που συνδέει μια οντότητα U με έναν ρόλο R περιγράφεται ως $AC = (ID_U, R, P_1, \ldots, P_i, C_1, \ldots, C_j, T_{AC})$, $SIGN_{CA}(AC)$, όπου ID_U είναι ένας προσδιοριστής για την οντότητα U, $P_1, \ldots, P_i$ είναι τα προνόμια πρόσβασης του ρόλου R, $C_1, \ldots, C_j$ είναι περιορισμοί επιβαλλόμενοι στον ρόλο, T_{AC} είναι η ημερομηνία λήξης και $SIGN_{CA}(AC)$ είναι η ψηφιακή υπογραφή της αρχής πιστοποίησης που αυθεντικοποιεί το πιστοποιητικό χαρακτηριστικών.

- Ισχυρή χρονική ασφάλεια. Η ισχυρή χρονική ασφάλεια έχει προταθεί ως μία μέθοδος για την ελαχιστοποίηση των συνεπειών της αποκάλυψης κλειδιού για κρυπτοσυστήματα δημόσιου κλειδιού [19]. Αυτό επιτυγχάνεται με την συστηματική ανανέωση των ζευγών δημόσιου/μυστικού κλειδιού χρησιμοποιώντας έναν μηχανισμό τυχαίας ανανέωσης. Η ανανέωση επιβεβαιώνει ότι πιθανή αποκάλυψη του μυστικού κλειδιού δεν θα θέσει σε κίνδυνο την ασφάλεια του συστήματος για συνεδρίες *πριν* και *μετά* την αποκάλυψη. Το σχήμα της ισχυρής χρονικής ασφάλειας περιγράφηκε αναλυτικά στο πέμπτο κεφάλαιο.

- Μη-αποσπώμενη υπογραφή RSA. Οι μη-αποσπώμενες υπογραφές είναι ψηφιακές υπογραφές οι οποίες επιτρέπουν σε κινητούς πράκτορες να υπογράφουν με ασφάλεια, ενώ εκτελούνται σε δυνητικά εχθρικά περιβάλλοντα. Αυτό επιτυγχάνεται συνδέοντας την συνάρτηση υπογραφής με περιορισμούς εφαρμογής, με τέτοιο τρόπο ώστε η υπογραφή να μην μπορεί να αποσπαστεί και να χρησιμοποιηθεί για εφαρμογές άλλες από αυτές που προσδιορίζονται από τους περιορισμούς. Στο μηχανισμό μεταβίβασης ρόλου χρησιμοποιείται το σχήμα της RSA μη-αποσπώμενης υπογραφής, το οποίο περιγράφηκε αναλυτικά στο τρίτο κεφάλαιο.

7.5 Ένας κρυπτογραφικός μηχανισμός για ασφαλή μεταβίβαση ρόλου μεταξύ πρακτόρων

7.5.1 Αρχικοποίηση

Σε αυτή την ενότητα παρουσιάζεται ο κρυπτογραφικός μηχανισμός για ασφαλή μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων, ο οποίος συνδυάζει τα δομικά συστατικά που αναφέρθηκαν στην προηγούμενη παράγραφο. Αρχικά κάθε οντότητα (χρήστης) U επιλέγει ένα RSA ζεύγος δημόσιου/μυστικού κλειδιού $(PK_{U,0}, SK_{U,0})$ και το αυθεντικοποιεί εκτός-εύρους μέσω μίας αρχής πιστοποίησης CA. Η αρχή πιστοποίησης CA εκδίδει το πιστοποιητικό ταυτότητας (δημόσιου κλειδιού) $Cert_{CA}(ID_U, PK_{U,0}, T_{Cert,0})$, όπου ID_U είναι ένας προσδιοριστής του χρήστη U και $T_{Cert,0}$ είναι η ημερομηνία λήξης. Το ζεύγος δημόσιου/μυστικού κλειδιού του χρήστη U ανανεώνεται τακτικά για ισχυρή χρονική ασφάλεια ως ακολούθως. Έστω ότι $(PK_{U,t-1}, SK_{U,t-1})$ είναι το RSA ζεύγος δημόσιου/μυστικού κλειδιού του χρήστη U για τη συνεδρία $t-1$. Επιπλέον, έστω ότι $Cert_{CA}(ID_U, PK_{U,t-1}, T_{Cert,t-1})$ είναι το πιστοποιητικό του. Για την επόμενη συνεδρία t, ο χρήστης U επιλέγει ένα τυχαίο ζεύγος δημόσιου/μυστικού κλειδιού $(PK_{U,t}, SK_{U,t})$ ως ακολούθως. Αρχικά, επιλέγει τυχαίους πρώτους αριθμούς p_t, q_t όπου το μήκος καθενός από τους τυχαίου αριθμούς είναι περίπου το μισό από το μήκος του επιθυμητού modulus. Επιλέγει $n_t = p_t \cdot q_t$ και e_t, d_t τέτοια ώστε $1 < e_t, d_t < \phi(n_t)$, όπου e_t είναι επιλεγμένα τυχαία με $gcd(e_t, \phi(n_t)) = 1$ και $d_t \cdot e_t = 1 \bmod \phi(n_t)$. Το δημόσιο κλειδί του χρήστη U για τη συνεδρία t είναι $PK_{U,t} = (e_t, n_t)$ και το μυστικό κλειδί είναι $SK_{U,t} = (d_t, n_t)$. Το ανανεωμένο δημόσιο κλειδί $PK_{U,t}$ για τη συνεδρία t πιστοποιείται από την αρχή πιστοποίησης CA, στην οποία υποβάλλονται τα ακόλουθα:

- το ανανεωμένο δημόσιο κλειδί συνεδρίας $PK_{U,t}$ και η ημερομηνία λήξης του $T_{Cert,t}$
- το πιστοποιητικό δημόσιου κλειδιού $Cert_{CA}(ID_U, PK_{U,t-1}, T_{Cert,t-1})$ της συνεδρίας $t-1$ και
- η υπογραφή $SIGN_{SK_{U,t-1}}(ID_U, PK_{U,t}, T_{Cert,t})$.

Η αρχή πιστοποίησης CA ελέγχει την ορθότητα αυτών των στοιχείων και επιβεβαιώνει ότι δεν έχει υποβληθεί άλλη απαίτηση πιστοποιητικού για τον ίδιο χρήστη U υπογεγραμμένη με το κλειδί $SK_{U,t-1}$ κατά τη συγκεκριμένη περίοδο πιστοποίησης. Στη συνέχεια, η αρχή εκδίδει ένα πιστοποιητικό $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$ για το νέο δημόσιο κλειδί. Σημειώνεται ότι η ημερομηνία λήξης για το κλειδί συνεδρίας δεν χρειάζεται να καθοριστεί. Επιπλέον, με την ίδια διαδικασία, η αρχή CA πιστοποιεί ένα δημόσιο κλειδί κρυπτογράφησης για κάθε διακομιστή.

7.5.2 Ανάθεση ρόλου με πιστοποιητικό χαρακτηριστικών

Έστω ότι ο χρήστης U έχει το ρόλο R με προνόμια πρόσβασης $P_1, \ldots, P_i$, περιορισμούς $C_1, \ldots, C_j$ και ημερομηνία λήξης T_{AC}. Η ανάθεση του ρόλου R στην οντότητα U πιστοποιείται από την αρχή πιστοποίησης CA, με ένα πιστοποιητικό χαρακτηριστικών:

$$AC = (ID_U, R, P_1, \ldots, P_i, C_1, \ldots, C_j, T_{AC}),\ SIGN_{CA}(AC).$$

Τα προνόμια και οι περιορισμοί που συμπεριλαμβάνονται στο πιστοποιητικό χαρακτηριστικών μπορεί να είναι εκτελέσιμοι κανόνες εξουσιοδότησης που αντανακλούν την λειτουργικότητα του ρόλου. Μια τέτοια προσέγγιση έχει προταθεί σε πολιτικές εξουσιοδότησης για κινητό κώδικα [44] και κινητούς πράκτορες [64] για την κατανομή της πολιτικής μεταξύ των κινητών αντικειμένων/πρακτόρων και των διακομιστών.

Εναλλακτικά το πιστοποιητικό χαρακτηριστικών μπορεί να περιλαμβάνει μόνο ένα κλειδί το οποίο σχετίζεται με το ρόλο R (σύμφωνα με άλλες προτάσεις, όπως των Lampson *et al* [76]) ενώ οι συσχετιζόμενοι κανόνες εξουσιοδότησης αποθηκεύονται στο τμήμα της πολιτικής του κάθε διακομιστή. Αν και στο μηχανισμό που παρουσιάζεται σε αυτή την ενότητα εξετάζεται η πρώτη προσέγγιση, αυτό το πρωτόκολλο μπορεί να χρησιμοποιηθεί και με την δεύτερη εναλλακτική.

Ας παρατηρηθεί ότι το πιστοποιητικό χαρακτηριστικών AC δεν εμπεριέχει το δημόσιο κλειδί της οντότητας U και συνεπώς δεν μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση. Για το σκοπό αυτό, το πιστοποιητικό χαρακτηριστικών συνδέεται κρυπτογραφικά με το πιστοποιητικό ταυτότητας $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$ του χρήστη U για την τρέχουσα συνεδρία, μέσω του προσδιοριστή ID_U. Η οντότητα U πρώτα αυθεντικοποιείται αποδεικνύοντας την γνώση του μυστικού κλειδιού που σχετίζεται με το πιστοποιημένο δημόσιο κλειδί. Στη συνέχεια ο χρήστης U παρουσιάζει το πιστοποιητικό χαρακτηριστικών που περιέχει τον ίδιο προσδιοριστή για να αποδείξει την συμμετοχή στον ρόλο R και να αποκτήσει συγκεκριμένη εξουσιοδότηση. Με αυτόν τον συνδυασμό αποφεύγονται επιθέσεις "κλεμμένων διαπιστευτηρίων", αφού ένας κακόβουλος χρήστης δεν μπορεί να χρησιμοποιήσει ένα πιστοποιητικό χαρακτηριστικών που έχει εκδοθεί για άλλη οντότητα ώστε να αποκτήσει μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, επιτρέπει την ανεξάρτητη διαχείριση των δημόσιων κλειδιών και των ρόλων μιας οντότητας.

7.5.3 Μεταβίβαση ρόλου από στατικές οντότητες σε κινητούς πράκτορες με υπογραφές

Έστω ότι A_1 είναι ένας πράκτορας ο οποίος δημιουργήθηκε από τον χρήστη U. Ο ρόλος R μεταβιβάζεται στον πράκτορα A_1 προσκολλώντας στον κώδικά του το πιστοποιητικό ταυτότητας $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$, το πιστοποιητικό χαρακτηριστικών $AC, SIGN_{CA}(AC)$ και την υπογραφή $SIGN_{PK_{U,t}}(ID_U, ID_{A_1}, AC)$ που αυθεντικοποιεί την μεταβίβαση. Στον παραπάνω τύπο, το ID_{A_1} είναι ο προσδιοριστής του πράκτορα και υπολογίζεται ως το αποτέλεσμα μίας συνάρτησης κατακερματισμού με είσοδο τον κώδικα, τα δεδομένα και την τρέχουσα κατάσταση εκτέλεσης του πράκτορα. Ας υποτεθεί τώρα ότι ο πράκτορας A_1 συναντά ένας άλλο πράκτορα A_2 σε έναν διακομιστή εκτέλεσης απροσδιόριστης εμπιστοσύνης. Ο πράκτορας A_2 μπορεί να παράγεται από τον χρήστη U, ή από κάποια άλλη οντότητα. Για να μεταβιβάσει το ρόλο R στον πράκτορα A_2, ο πράκτορας A_1 θα πρέπει να είναι ικανός να υπογράψει τη μεταβίβαση αυτού του ρόλου εκ μέρους του χρήστη U. Ας παρατηρηθεί ότι η υπογραφή $SIGN_{PK_{U,t}}(ID_U, ID_{A_1}, AC)$ δεν μπορεί να χρησιμοποιηθεί για αυτό το σκοπό επειδή συνδέεται με τον προσδιοριστή ID_{A_1} και όχι με τον προσδιοριστή ID_{A_2}. Η μόνη πιθανή λύση είναι να παραχωρήσει ο χρήστης U στον πράκτορα A_1 τη δυνατότητα να εξουσιοδοτεί την μεταβίβαση του ρόλου R, δηλαδή κάποιο κρυπτογραφικό κλειδί ή συνάρτηση υπογραφής. Για να προστατευθεί το κλειδί υπογραφής του χρήστη U από αποκάλυψη ή αυθαίρετη χρήση από κακόβουλους διακομιστές, χρησιμοποιείται μια διαδικασία μεταβίβασης η οποία βασίζεται σε μη-αποσπώμενες υπογραφές.

7.5.4 Μεταβίβαση ρόλου από στατικές οντότητες σε κινητούς πράκτορες με μη-αποσπώμενες υπογραφές

Για απλότητα, κατά την διάρκεια οποιασδήποτε συνεδρίας t, έστω ότι $n = n_t$, $e = e_t$ και $d = d_t$.

Πρωτοκολλο

1. Η οντότητα U επιλέγει τους περιορισμούς $C'_1, \ldots, C'_\ell$ για την μεταβίβαση του ρόλου R στον πράκτορα A_1.

2. Η οντότητα U επιλέγει την ημερομηνία λήξης $t_1 \leq min\{T_{AC}, T_{Cert,t}\}$ για τη μεταβίβαση του ρόλου R στον πράκτορα A_1 (όπου T_{AC} είναι η ημερομηνία λήξης του πιστοποιητικού χαρακτηριστικών και $T_{Cert,t}$ ο χρόνος λήξης του δημόσιου κλειδιού $PK_{U,t} = (e, n)$ για την τρέχουσα συνεδρία t).

3. Η οντότητα U υπολογίζει τον προσδιοριστή του πράκτορα A_1 ως το αποτέλεσμα μίας συνάρτησης κατακερματισμού, στον κώδικα, τα δεδομένα και την τρέχουσα κατάσταση του πράκτορα: $ID_{A_1} = hash(code_{A_1}, data_{A_1}, current\_state_{A_1})$.

4. Η οντότητα U υπολογίζει $h_1 = hash(ID_U, ID_{A_1}, AC, C'_1, \ldots, C'_\ell, t_1)$ και την RSA υπογραφή του h_1: $k_1 = {h_1}^d \bmod n$.

5. Η οντότητα U προσκολλά στον πράκτορα A_1 τα παρακάτω δεδομένα, τα οποία χρησιμοποιούνται για να πιστοποιήσουν την μεταβίβαση:

   - το πιστοποιητικό χαρακτηριστικών AC, $SIGN_{CA}(AC)$,
   - το πιστοποιητικό $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$,
   - τους περιορισμούς $C'_1, \ldots, C'_\ell$.

- την ημερομηνία λήξης t_1, και
- την RSA υπογραφή (h_1, k_1).

6. Ο χρήστης U προσκολλά στον πράκτορα A_1, ως μέρος του εκτελέσιμου κώδικά του, το ζεύγος συναρτήσεων μη-αποσπώμενων υπογραφών:

$$f_1(\cdot) = {h_1}^{(\cdot)} \bmod n, \quad \text{και} \quad f_{1,sign}(\cdot) = {k_1}^{(\cdot)} \bmod n.$$

7. Τελικά, ο χρήστης U κρυπτογραφεί τον πράκτορα με το δημόσιο κλειδί κρυπτογράφησης του διακομιστή προορισμού.

ΕΠΑΛΗΘΕΥΣΗ

Για να επαληθευθεί ότι ο πράκτορας A_1 είναι ένα μεταβιβαζόμενο μέλος του ρόλου R από το αρχικό μέλος U του ρόλου, ο διακομιστής εκτελεί τις ακόλουθες εργασίες:

1. Αποκρυπτογραφεί τον πράκτορα A.
2. Επαληθεύει το πιστοποιητικό δημόσιου κλειδιού $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$ και το πιστοποιητικό χαρακτηριστικών AC και ελέγχει τη λίστα ανάκλησης πιστοποιητικών της αρχής CA.
3. Υπολογίζει τον προσδιοριστή $ID_{A_1} = hash(code_{A_1}, data_{A_1}, current\_state_{A_1})$.
4. Ελέγχει την RSA υπογραφή (h_1, k_1) του πράκτορα A_1, επαληθεύοντας ότι ${k_1}^e = h_1 \bmod n$, όπου $h_1 = hash(ID_U, ID_{A_1}, AC, C'_1, \ldots, C'_\ell, t_1)$ και το δημόσιο κλειδί $(e, n) = PK_{U,t}$ λαμβάνεται από το πιστοποιητικό δημόσιου κλειδιού.

Αν όλοι οι έλεγχοι είναι επιτυχείς, ο διακομιστής παραχωρεί πρόσβαση στον πράκτορα A_1 με τα προνόμια $P_1, \ldots, P_i$ του ρόλου R υπό τους περιορισμούς $C_1, \ldots, C_j$, του πιστοποιητικού χαρακτηριστικών και $C'_1, \ldots, C'_\ell$ της μεταβιβαζόμενης οντότητας U.

7.5.5 Μεταβίβαση ρόλου μεταξύ πρακτόρων με μη-αποσπώμενα πιστοποιητικά χαρακτηριστικών

Το ζεύγος συναρτήσεων μη-αποσπώμενων υπογραφών $(f_1,\ f_{1,sign})$ επιτρέπει στον πράκτορα A_1 να εξουσιοδοτήσει τη μεταβίβαση του ρόλου R σε έναν πράκτορα A_2 υπολογίζοντας ένα *μη-αποσπώμενο πιστοποιητικό χαρακτηριστικών* ως ακολούθως.

Πρωτοκολλο

1. Ο πράκτορας A_1 επιλέγει επιπλέον περιορισμούς $C''_1, \ldots, C''_\ell$ για την μεταβίβαση του ρόλου R στον πράκτορα A_2.

2. Ο πράκτορας A_1 επιλέγει ένα χρόνο λήξης $t_2 \leq min\{T_{AC}, T_{Cert,t}\}$ για τη μεταβίβαση του ρόλου R στον πράκτορα A_2.

3. Ο πράκτορας A_1 υπολογίζει τον προσδιοριστή του πράκτορα A_2 ως το αποτέλεσμα μίας συνάρτησης κατακερματισμού στον κώδικα, τα δεδομένα και την κατάσταση εκτέλεσης του πράκτορα: $ID_{A_2} = hash(code_{A_2}, data_{A_2}, current\_state_{A_2})$.

4. Ο πράκτορας A_1 υπολογίζει το $m_1 = hash(ID_{A_1}, ID_{A_2}, C''_1, \ldots, C''_\ell, t_2)$. (Για ευκολία δεν συμπεριλαμβάνονται τα μερικά αποτελέσματα εκτέλεσης, τα οποία φυσιολογικά θα ήταν μέρος της μεταβίβασης, δηλαδή μέρος του m_1.)

5. Ο πράκτορας A_1 εκτελεί τις συναρτήσεις $(f_1, f_{1,sign})$ με είσοδο m_1:

$$h_2 = f_1(m_1) = {h_1}^{m_1} \bmod n, \quad k_2 = f_{1,sign}(m_1) = {k_1}^{m_1} = ({h_1}^{m_1})^d \bmod n.$$

6. Το μη-αποσπώμενο πιστοποιητικό χαρακτηριστικών το οποίο είναι προσκολλημένο στον πράκτορα A_2 για να πιστοποιεί τη μεταβίβαση αποτελείται από:

- το πιστοποιητικό χαρακτηριστικών AC, $SIGN_{CA}(AC)$,
- το πιστοποιητικό $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$,
- τους περιορισμούς $C'_1, \ldots, C'_\ell$, και $C''_1, \ldots, C''_\ell$,
- την ημερομηνία λήξης t_2,
- τον προσδιοριστή ID_{A_1} του μεταβιβάζοντα πράκτορα και
- τη μη-αποσπώμενη υπογραφή $(h_2, k_2) = (h_1{}^{m_1}, (h_1{}^{m_1})^d)$.

7. Ο πράκτορας A_1 προσκολλά στον πράκτορα A_2, ως μέρος του εκτελέσιμου κώδικά του, το ζεύγος συναρτήσεων μη-αποσπώμενων υπογραφών:

$$f_2(\cdot) = h_2{}^{(\cdot)} \bmod n, \quad \text{και} \quad f_{2,sign}(\cdot) = k_2{}^{(\cdot)} \bmod n.$$

8. Τέλος, ο διακομιστής κρυπτογραφεί τον πράκτορα με το δημόσιο κλειδί κρυπτογράφησης του επόμενου διακομιστή προορισμού.

ΕΠΑΛΗΘΕΥΣΗ

Για να επαληθεύσει τη μεταβίβαση ρόλου R από τον πράκτορα A_1 στον πράκτορα A_2, ο διακομιστής ο οποίος παραλαμβάνει τον πράκτορα A_2, εκτελεί τις παρακάτω εργασίες:

1. Αποκρυπτογραφεί τον πράκτορα A_2.
2. Επαληθεύει το πιστοποιητικό ταυτότητας $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$ και το πιστοποιητικό χαρακτηριστικών AC και ελέγχει τη λίστα ανάκλησης πιστοποιητικών της αρχής CA.
3. Υπολογίζει τον προσδιοριστή: $ID_{A_2} = hash(code_{A_2}, data_{A_2}, current\_state_{A_2})$.

4. Ελέγχει την RSA υπογραφή (h_1, k_1) του πράκτορα A_2. Δηλαδή επαληθεύει ότι $k_1{}^e = h_1 \bmod n$, όπου $h_1 = hash(ID_U, ID_{A_1}, AC, C'_1, \ldots, C'_\ell, t_1)$, ID_{A_1} λαμβάνεται από την δεδομένα πιστοποίησης του A_2 και $(e, n) = PK_{U,1}$.

5. Ελέγχει την μη-αποσπώμενη RSA υπογραφή (h_2, k_2), που αποτελεί μέρος του κώδικα του πράκτορα A_2, υπολογίζοντας $m_1 = hash(ID_{A_1}, ID_{A_2}, C''_1, \ldots, C''_\ell, t_2)$ και μετά ελέγχοντας ότι: $h_2 = h_1^{m_1} \bmod n$ και $k_2{}^e = h_2 \bmod n$.

Αν όλοι οι έλεγχοι είναι επιτυχείς, ο διακομιστής παραχωρεί πρόσβαση στον πράκτορα A_2 με τα προνόμια $P_1, \ldots, P_r$ του ρόλου R υπό τους περιορισμούς $C_1, \ldots, C_j$ του πιστοποιητικού χαρακτηριστικών, $C'_1, \ldots, C'_\ell$ του αρχικού μέλους U του ρόλου R και $C''_1, \ldots, C''_\ell$ του μεταβιβάζοντος πράκτορα A_1. Το ζεύγος συναρτήσεων μη-αποσπώμενων υπογραφών $(f_2,\ f_{2,sign})$ επιτρέπει στον πράκτορα A_2 την περαιτέρω μεταβίβαση ρόλου με ένα μη-αποσπώμενο πιστοποιητικό χαρακτηριστικών, δεδομένου ότι αυτό επιτρέπεται από τους αρχικούς περιορισμούς $C_1, \ldots, C_\ell$ του ρόλου, που συμπεριλαμβάνονται στο πιστοποιητικό χαρακτηριστικών.

Παρατήρηση 7.5.1. *Μεταβίβαση πολλών βημάτων.* Στην περίπτωση μεταβίβασης πολλών βημάτων, οι συναρτήσεις μεταβίβασης στο βήμα i θα είναι: $f_i(\cdot) = h_1^{m_1 \ldots m_i(\cdot)}$, $f_{i,sig}(\cdot) = k_1^{m_1 \ldots m_i(\cdot)}$ δηλαδή περιέχουν τους προηγούμενους περιορισμούς μεταβίβασης που συμπεριλαμβάνονται στο $m_1, \ldots m_i$.

Παρατήρηση 7.5.2. *Είδος μεταβίβασης.* Η ολική ή η μερική μεταβίβαση ενός ρόλου μπορεί να ελεγχθεί από τους περιορισμούς της μεταβίβασης. Αμφίπλευρη συμφωνία, όπου και ο μεταβιβαστής και ο μεταβιβαζόμενος πράκτορας πρέπει να συμφωνήσουν για την μεταβίβαση μπορεί να επιτευχθεί χρησιμοποιώντας μη-αποσπώμενες υπογραφές και για τους δυο πράκτορες.

Παρατήρηση 7.5.3. *Πολλαπλοί ρόλοι.* Για στατικές οντότητες που είναι μέλη πολλαπλών ρόλων, είναι προτιμότερο να εκδοθεί ένα ανεξάρτητο πιστοποιητικό χαρακτηριστικών για κάθε ανάθεση ρόλου. Ο διαχωρισμός των πιστοποιητικών χαρακτηριστικών όχι μόνο απλοποιεί την μεταβίβαση ρόλου, αλλά επίσης βοηθά στην διαχείριση των ρόλων μίας οντότητας.

7.6 Ανάλυση ασφάλειας

Το πρωτόκολλο μεταβίβασης ρόλου μεταξύ πρακτόρων ικανοποιεί τις βασικές απαιτήσεις ασφάλειας που σχετίζονται με την εξουσιοδότηση και την ανάκληση.

Εξουσιοδοτημένη μεταβίβαση ρόλου

Το πιστοποιητικό δημόσιου κλειδιού $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$ συνδέει κρυπτογραφικά τον προσδιοριστή του χρήστη ID_U με το δημόσιο κλειδί της τρέχουσας συνεδρίας $PK_{U,t}$. Το πιστοποιητικό χαρακτηριστικών AC, $SIGN_{CA}(AC)$, συνδέει τον προσδιοριστή ID_U (που περιέχεται στο πιστοποιητικό ταυτότητας του χρήστη U) με τα προνόμια και τους περιορισμούς του ρόλου. Συνεπώς το πιστοποιητικό χαρακτηριστικών συνδέεται με ένα δημόσιο κλειδί και μόνο ο νόμιμος κάτοχος είναι εξουσιοδοτημένος να χρησιμοποιεί ή να μεταβιβάζει το πιστοποιητικό χαρακτηριστικών. Η RSA υπογραφή (h_1, k_1) συνδέει τον προσδιοριστή του χρήστη U με τον προσδιοριστή του πράκτορα A_1, το πιστοποιητικό χαρακτηριστικών AC, τους περιορισμούς $C'_1, \ldots, C'_\ell$ και την ημερομηνία λήξης t_1, αφού $h_1 = hash(ID_U, ID_{A_1}, AC, C'_1, \ldots, C'_\ell, t_1)$ και k_1 είναι η RSA υπογραφή του h_1 με το κλειδί συνεδρίας του U. Τέλος, η μη-αποσπώμενη RSA υπογραφή (h_2, k_2) συνδέει τους προσδιοριστές των U και A_1 με τον προσδιοριστή του πράκτορα A_2, το πιστοποιητικό χαρακτηριστικών AC, τους περιορισμούς

$C'_1, \ldots, C'_\ell, C''_1, \ldots, C''_\ell$ και την ημερομηνία λήξης t_2. Αυτό συμβαίνει επειδή $h_2 = h_1^{m_1}$, όπου $m_1 = hash(ID_{A_1}, ID_{A_2}, C''_1, \ldots, C''_\ell, t_2)$ και k_2 είναι η μη-αποσπώμενη RSA υπογραφή του h_2 με το κλειδί της τρέχουσας συνεδρίας του χρήστη U. Συνεπώς κατά τη διάρκεια οποιασδήποτε περιόδου t, όλες οι μεταβιβάσεις είναι εξουσιοδοτημένες με το κλειδί υπογραφής $d = SK_{U,t}$ της οντότητας U, το οποίο αυθεντικοποιείται μέσω του πιστοποιητικού $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$. Ας παρατηρηθεί ότι ο προσδιοριστής $ID_A = hash(code_A, data_A, current\_state_A)$ ενός πράκτορα A είναι δυναμικός, και αλλάζει καθώς αλλάζουν ο κώδικας, τα δεδομένα και η κατάσταση του A. Ένας πλαστός πράκτορας $\widetilde{A}$ που ισχυρίζεται ότι έχει τον προσδιοριστή ενός νόμιμου πράκτορα A θα αποτύχει. Ο διακομιστής θα δημιουργήσει το hash του κώδικα, των δεδομένων και της κατάστασης του πλαστού πράκτορα και θα ελέγξει αυτό με τα διαπιστευτήρια που παρουσιάζει ο πλαστός πράκτορας. Αυτό δεν θα είναι ταυτόσημο με τον προσδιοριστή ID_A που περιέχεται στην (κλεμμένη) υπογεγραμμένη πιστοποίηση δεδομένων του νόμιμου πράκτορα A.

Μη-αποσπώμενη μεταβίβαση ρόλου

Αν και ο διακομιστής που εκτελεί τον πράκτορα έχει πλήρη πρόσβαση στον κώδικα του πράκτορα κατά την διάρκεια της εκτέλεσής του, είναι ο μεταβιβαστής πράκτορας που ελέγχει την μεταβίβαση. Αυτό οφείλεται στο γεγονός ότι το τμήμα του κώδικα του πράκτορα που εκτελεί την μεταβίβαση (ο υπολογισμός ενός μη-αποσπώμενου πιστοποιητικού χαρακτηριστικών) προστατεύεται κρυπτογραφικά. Το ζεύγος συναρτήσεων μη-αποσπώμενων υπογραφών $(f_1(\cdot),\ f_{1,sign}(\cdot))$ συνδέει το κλειδί υπογραφής του U με ένα συγκεκριμένο πιστοποιητικό χαρακτηριστικών AC του μεταβιβαζόμενου ρόλου R

με περιορισμούς $C_1, \ldots, C_j$ και τους περιορισμούς μεταβίβασης $C'_1, \ldots, C'_\ell$ (προσδιορισμένες από τον U), μέσω της τιμής hash h_1. Ένας κακόβουλος διακομιστής που προσπαθεί να σφετεριστεί την δυνατότητα υπογραφής του πράκτορα A_1 εξουσιοδοτώντας μια μεταβίβαση άλλη από αυτήν που καθορίζεται από τους περιορισμούς μεταβίβασης, πρέπει να πλαστογραφήσει μια μη-αποσπώμενη υπογραφή RSA. Όμως, όπως έχει αποδειχθεί στο τρίτο κεφάλαιο, η πλαστογράφηση της μη αποσπώμενης υπογραφής RSA είναι υπολογιστικά δυσεπίλυτο πρόβλημα. Το ίδιο συμβαίνει για τα ακόλουθα ζεύγη συναρτήσεων μη-αποσπώμενων υπογραφών $(f_2, f_{2,sign}), \ldots, (f_i, f_{i,sign})$.

Επιπλέον, οι περιορισμοί μεταβίβασης των προηγούμενων διακομιστών είναι συνδεδεμένες με μη-αποσπώμενο τρόπο με τη συνάρτηση μεταβίβασης. Ο διακομιστής $i+1$ λαμβάνοντας τον πράκτορα από τον διακομιστή i με το ζεύγος των συναρτήσεων μη-αποσπώμενης υπογραφής $f_i(\cdot) = h_1^{m_1 \ldots m_i(\cdot)}, f_{i,sig}(\cdot) = k_1^{m_1 \ldots m_i(\cdot)}$ δεν μπορεί να αποσπάσει τους περιορισμούς μεταβίβασης που υποβλήθηκαν από το μήνυμα m_i στον εκθέτη $m_1 \ldots m_i$, χωρίς την βοήθεια του διακομιστή i ή ενός από τους προηγούμενους διακομιστές.

Ανάκληση μεταβίβασης ρόλου

Αυτή υποστηρίζεται από τον συνδυασμό του μηχανισμού ανανέωσης κλειδιού της ισχυρής χρονικής ασφάλειας με τα πιστοποιητικά χαρακτηριστικών.

- *Διαδοχική ανάκληση*: Αν ο ρόλος R της μεταβιβάζουσας οντότητας U πρέπει να ανακληθεί, τότε η αρχή CA ανακαλεί το πιστοποιητικό χαρακτηριστικών AC της οντότητας U. Ως συνέπεια η αλυσίδα των μεταβιβάσεων του ρόλου R από τον χρήστη U στον πράκτορα A_1 και από τον πράκτορα A_1 στον πράκτορα A_2 θα είναι άκυρη. Συνεπώς η ανάκληση είναι διαδοχική.

- *Ανάκληση με εξάρτηση μεταβιβάζοντα*: Εκτός από την αρχή CA, μόνο η μεταβιβάζουσα οντότητα μπορεί να ανακαλέσει έναν μεταβιβασμένο ρόλο. Ας παρατηρηθεί ότι ο U μπορεί να ανακαλέσει την μεταβίβαση, *δίχως* να ανακαλέσει τους δικούς ρόλους. Αυτό επιτυγχάνεται με την ανανέωση του δημόσιου κλειδιού συνεδρίας $PK_{U,t}$ σε ένα νέο κλειδί $PK_{U,t+1}$. Κατά συνέπεια ο χρήστης U μπορεί να διατηρήσει την ιδιότητα μέλους στον ρόλο R (αφού το πιστοποιητικό χαρακτηριστικών δεν έχει ανακληθεί), ενώ οι πράκτορες A_1 και A_2 θα χάσουν τον μεταβιβαζόμενο ρόλο (αφού το πιστοποιητικό $Cert_{CA}(ID_U, PK_{U,t}, T_{Cert,t})$ έχει ανακληθεί και μία μεταβίβαση με το μυστικό κλειδί $SK_{U,t}$ δεν θα είναι έγκυρη).

- *Χρονικά ελεγχόμενη ανάκληση*: Ο χρόνος ελέγχεται μέσω του χρόνου λήξης t_2 της μεταβίβασης από τον A_1 στον A_2. Ας παρατηρηθεί ότι η μεταβίβαση είναι έγκυρη μόνο αν $t_2 \leq min\{T_{AC}, T_{Cert,t}\}$. όπου T_{AC} είναι ο χρόνος λήξης του πιστοποιητικού χαρακτηριστικών και $T_{Cert,t}$ είναι ο χρόνος λήξης του τρέχοντος κλειδιού συνεδρίας.

Εμπιστευτικότητα μεταβίβασης ρόλου

Πριν την μετανάστευση, ο πράκτορας είναι κρυπτογραφημένος με το δημόσιο κλειδί του διακομιστή προορισμού. Συνεπώς, κάθε φορά μόνο ο διακομιστής προορισμός μπορεί να αποκρυπτογραφήσει τον πράκτορα και να εκτελέσει τις συναρτήσεις μεταβίβασης $(h^{(\cdot)}, k^{(\cdot)}), (h_1^{(\cdot)} = h^{m_1(\cdot)}, k_1^{(\cdot)} = k^{m_1(\cdot)}), \ldots, (h_i^{(\cdot)} = h^{m_1 \ldots m_i(\cdot)}, k_i^{(\cdot)} = k^{m_1 \ldots m_i(\cdot)})$ και η μεταβίβαση προστατεύεται από επιθέσεις εξωτερικών ωτακουστών. Για μεγαλύτερη αποτελεσματικότητα, μπορεί να χρησιμοποιηθεί υβριδική κρυπτογράφηση. Σε αυτή την περίπτωση, ο πράκτορας κρυπτογραφείται πριν τη μετανάστευσή του με ένα συμμετρικό κλειδί. Για την αναταλλαγή του συμμετρικού κλειδιου χρησιμοποιείται το δημόσιο κλειδί του διακομιστή προορισμού. Επιπρόσθετα, σύμφωνα με τις ανάγκες

της εφαρμογής ενδέχεται να απαιτείται κρυπτογράφηση μόνο για ορισμένα τμήματα του πράκτορα. Σε αυτήν την περίπτωση, μόνο οι συναρτήσεις μεταβίβασης πρέπει να κρυπτογραφηθούν.

Παρατήρηση 7.6.1. *Περιορισμοί των μη-αποσπώμενων υπογραφών: Καταλογισμός ευθύνης των διακομιστών.* Ο προτεινόμενος μηχανισμός δεν προσφέρει καταλογισμό ευθύνης για τους διακομιστές εκτέλεσης των πρακτόρων, κάτι που μπορεί να επιτευχθεί χρησιμοποιώντας δυναμικές πολυ-υπογραφές [72], αντί για μη-αποσπώμενες υπογραφές.

7.7 Συμπεράσματα

Αν και οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για να αυθεντικοποιήσουν την μεταβίβαση ρόλου στατικών οντοτήτων δεν μπορούν να χρησιμοποιηθούν για μεταβίβαση ρόλου από κινητούς πράκτορες, η κατάσταση των οποίων αλλάζει δυναμικά. Επειδή η μεταβίβαση ρόλου μεταξύ πρακτόρων μπορεί να πραγματοποιηθεί σε εχθρικά (μη έμπιστα) περιβάλλοντα εκτέλεσης, μπορεί να οδηγήσει σε ανεξέλεγκτη ροή προνομίων πρόσβασης. Συνεπώς απαιτείται η λήψη κατάλληλων μέτρων ασφάλειας τα οποία να προστατεύουν την αυθεντικότητα και γνησιότητα της μεταβίβασης ρόλου μεταξύ κινητών πρακτόρων. Σε αυτό το κεφάλαιο παρουσιάστηκε ένας μηχανισμός για ασφαλή μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων, συνδυάζοντας μη-αποσπώμενες RSA υπογραφές με πιστοποιητικά χαρακτηριστικών και ισχυρή χρονική ασφάλεια. Η καινοτομία του προτεινόμενου μηχανισμού οφείλεται στο γεγονός ότι η ασφάλειά του δεν βασίζεται σε υποθέσεις εμπιστοσύνης για τους διακομιστές εκτέλεσης των πρακτόρων και συνεπώς δεν περιορίζει την κινητικότητα ή την αυτονομία των πρακτόρων. Η μεταβίβαση ρόλου μεταξύ κινητών πρακτόρων αυξάνει τα δυναμικά

χαρακτηριστικά του βασισμένου σε ρόλους ελέγχου πρόσβασης σε συστήματα πρακτόρων, αφού επιτρέπει την ανάθεση των κινητών πρακτόρων σε ρόλους σύμφωνα με δυναμικά παραγόμενες ανάγκες εφαρμογών. Ο μηχανισμός μεταβίβασης ρόλου μπορεί να χρησιμοποιηθεί για αρκετές εφαρμογές, όπως αυτόνομη εξουσιοδότηση περιπλανώμενων πρακτόρων με μειωμένο κόστος. Ο προτεινόμενος μηχανισμός χρησιμοποιεί μία πρακτική τεχνική ανανέωσης κλειδιού η οποία δεν απαιτεί εκτός εύρους αυθεντικοποίηση. Επιπλέον, είναι αποτελεσματικός αφού απαιτεί ένα μικρό αριθμό εκθετικών πράξεων για κάθε μεταβίβαση.

Κεφάλαιο 8

Κινητοί πράκτορες στην ασφάλεια ευφυών δικτύων

Τα Ευφυή Δίκτυα – ΕΔ (Intelligent Networks) διαχωρίζουν τη διαδικασία ελέγχου και κλήσης από τη δρομολόγηση, οδηγώντας σε γρήγορες και ανεξάρτητες δικτύου υπηρεσίες, με μειωμένο κόστος ανάπτυξης. Η ενοποίηση νέων τεχνολογιών όπως η τεχνολογία CORBA και η τεχνολογία κινητών πρακτόρων βελτιώνει την απόδοση των ΕΔ. Όμως, η χρήση κατανεμημένων τεχνολογιών αυξάνει τα προβλήματα ασφάλειας. Σε αυτό το κεφάλαιο παρουσιάζεται μια ασφαλής αρχιτεκτονική ΕΔ χρησιμοποιώντας μηχανισμούς ασφαλείας όπως είναι υπηρεσίες ασφάλειας CORBA, υπηρεσίες ασφάλειας της πλατφόρμας πρακτόρων Grasshopper και υπηρεσίες Τρίτης Έμπιστης Οντότητας.

8.1 Εισαγωγή

Οι νέες κατευθύνσεις στο χώρο των τηλεπικοινωνιών απαιτούν ταχεία ανάπτυξη των υπηρεσιών, αυτοματοποιημένη συνδρομή και ευκολία ενσωμάτωσης νέων υπηρεσιών. Υπό αυτήν την έννοια τα Ευφυή Δίκτυα έχουν έναν σημαντικό ρόλο. Στο παραδοσιακό τηλεπικοινωνιακό δικτυακό περιβάλλον (Public Switched Telecommunication Environment -PSTN), τα στοιχεία του δικτύου ήταν στατικά, για συγκεκριμένες υπηρεσίες και με οριοθετημένες ικανότητες. Ως αποτέλεσμα, η εισαγωγή νέων υπηρεσιών ήταν μία χρονοβόρα δραστηριότητα, με αρκετά υψηλό κόστος.

Στο περιβάλλον των ΕΔ, η διαδικασία ελέγχου και κλήσης έχει διαχωριστεί από τη δρομολόγηση και έχει τοποθετηθεί μέσα στο δίκτυο, οδηγώντας σε ταχύτητα εξυπηρέτησης, ανεξαρτησία από την δικτυακή αρχιτεκτονική ή τον κατασκευαστή και σε αξιόλογη μείωση του κόστους ανάπτυξης [18, 26]. Η αρχιτεκτονική των ΕΔ γίνεται περισσότερο ισχυρή και δυναμική με την χρήση νέων τεχνολογιών, όπως η πλατφόρμα κατανεμημένης επικοινωνίας CORBA (Common Object Request Broker) [97] και οι τεχνολογίες κινητών πρακτόρων. Με τη χρήση της CORBA γίνεται καλύτερη εκμετάλλευση της κατανεμημένης φύσης των ΕΔ. Η χρήση των κινητών πρακτόρων επιτρέπει μια εύρωστη και δυναμικά οργανωμένη εφαρμογή με μειωμένο κόστος επικοινωνίας. Μια τέτοια ενσωμάτωση έχει προταθεί στη διεθνή βιβλιογραφία [18, 26], όπου η αρχιτεκτονική των ΕΔ βασίζεται σε τεχνολογία CORBA και στην πλατφόρμα πρακτόρων Grasshopper [58].

Αυτές οι αρχιτεκτονικές είναι αρκετά ευέλικτες ώστε να υποστηρίζουν εφαρμογές οι οποίες ικανοποιούν εκτεταμένες ανάγκες του πελάτη. Παραδείγματα αυτών των εφαρμογών συμπεριλαμβάνουν υπηρεσίες Interactive Multimedia Retrieval - IMR και πιο ειδικά Video-on-Demand - VoD και News-on-Demand - NoD. Η αλληλεπίδραση μεταξύ του χρήστη και του δικτύου οδηγεί σε υψηλής ποιότητας υπηρεσίες.

Η υλοποίηση δικτυακών αρχιτεκτονικών με κατανεμημένες τεχνολογίες πάνω από ανοικτά και μη-ασφαλή κανάλια επικοινωνίας όπως το διαδίκτυο, δημιουργεί σοβαρές απειλές ασφάλειας, οι οποίες μπορεί να περιλαμβάνουν επιθέσεις άρνησης εξυπηρέτησης, παράκαμψη ελέγχου πρόσβασης, ή αλλοίωση της επικοινωνίας μεταξύ διαφόρων στοιχείων του δικτύου.

Αρκετές τεχνικές έχουν προταθεί για την αντιμετώπιση αυτών των απειλών ασφάλειας στο πλαίσιο των ευφυών δικτύων. Οι Aura *et al* [4] προτείνουν ένα σύστημα ελέγχου πρόσβασης βασισμένο σε μεταβίβαση, για τον έλεγχο της εξουσιοδότησης των μεταξύ των προμηθευτών υπηρεσιών και των χρηστών του ΕΔ. Αυτό το σύστημα στηρίζεται στην αρχιτεκτονική ΕΔ Calypso [70]. Οι Breugst *et al* [18] προτείνουν την χρήση μιας έμπιστης οντότητας για τον έλεγχο της ακεραιότητας των κινητών πρακτόρων σε Ενεργά Ευφυή Δίκτυα (Active Intelligent Networks).

Αν και έχουν προταθεί αρκετές αρχιτεκτονικές ασφάλειας για εφαρμογές που βασίζονται στην τεχνολογία CORBA (για παράδειγμα, βλέπε [77, 102]) και τα θέματα ασφάλειας σε συστήματα κινητών πρακτόρων γίνονται ενεργό πεδίο έρευνας (βλέπε δεύτερο κεφάλαιο της παρούσας διατριβής), δεν υπάρχει ευρύτητα εργασιών στα θέματα ασφάλειας αυτών των τεχνολογιών στο πεδίο των Ευφυών Δικτύων.

Σε αυτό το κεφάλαιο, προτείνεται μια ασφαλής αρχιτεκτονική ΕΔ, εφαρμοσμένη πάνω στην αρχιτεκτονική ΕΔ των Chatzipapadopoulos *et al* [26]. Εφόσον η συγκεκριμένη αρχιτεκτονική ΕΔ βασίζεται στην τεχνολογία CORBA και στην πλατφόρμα πρακτόρων Grasshopper, το προτεινόμενο μοντέλο ασφαλείας στηρίζεται στην Υπηρεσία Ασφάλειας CORBA (CORBA Security Service) [98] και στην Υπηρεσία Ασφάλειας Grasshopper (Grasshopper Security Service) [59]. Επιπρόσθετα, χρησιμοποιούνται και άλλοι μηχανισμοί ασφάλειας, όπως Υπηρεσία Τρίτης Έμπιστης Οντότητας.

Το υπόλοιπο αυτού του κεφαλαίου είναι διαρθρωμένο ως εξής. Στην ενότητα 8.2,

περιγράφεται εν συντομία η αρχιτεκτονική ΕΔ που χρησιμοποιεί το προτεινόμενο μοντέλο ασφάλειας. Στην ενότητα 8.3, παρουσιάζεται η προτεινόμενη αρχιτεκτονική ασφάλειας. Τέλος, στην ενότητα 8.5 συζητώνται οι πιθανές επεκτάσεις της προτεινόμενης αρχιτεκτονικής.

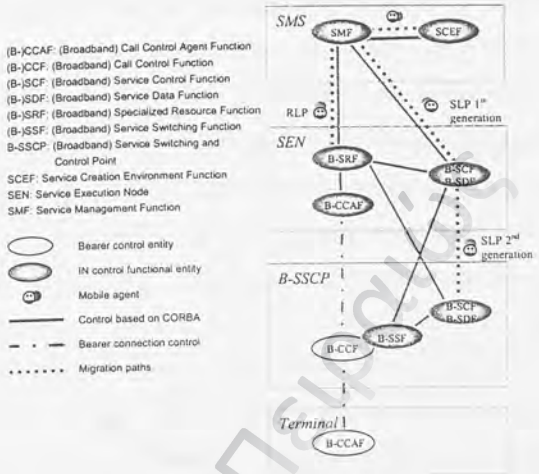
8.2 Αρχιτεκτονική ευφυούς δικτύου

Η χρήση των τεχνολογιών CORBA και κινητών πρακτόρων σε ένα δίκτυο μεγάλου εύρους οδήγησε στην έννοια του Κατανεμημένου Ευφυούς Δικτύου – ΚΕΔ [18, 26]. Αυτές οι αρχιτεκτονικές χαρακτηρίζονται από υπηρεσίες μεγάλου εύρους και από κατανεμημένες υποδομές στο τμήμα ελέγχου του ΕΔ και μπορούν να εφαρμοστούν σε ποικίλες εφαρμογές όπως σε υπηρεσίες IMR.

Τα ΚΕΔ έχουν το πλεονέκτημα της ελαστικότητας που προσφέρουν οι τεχνολογίες CORBA και κινητών πρακτόρων (πιο συγκεκριμένα η πλατφόρμα πρακτόρων Grasshopper) για να μειώσουν το φόρτο κίνησης του δικτύου. Αυτό επιτυγχάνεται με την υλοποίηση βασικών λειτουργιών ελέγχου, μέσω κινητών πρακτόρων. Το σχήμα 8.1 παρουσιάζει την κατανομή των λειτουργικών οντοτήτων στους φυσικούς κόμβους της αρχιτεκτονικής του ΚΕΔ.

Η αρχιτεκτονική ΚΕΔ των Chatzipapadopoulos *et al* [26] χρησιμοποιεί – πέραν του τερματικού κόμβου (Terminal node) ο οποίος φιλοξενεί τους τελικούς χρήστες – τρεις φυσικούς κόμβους οι οποίοι φιλοξενούν τις λειτουργικές οντότητες. Αναλυτικότερα, τον *κόμβο μεταγωγής* (Broadband Service Switching and Control Point – B-SSCP), τον *κόμβο εκτέλεσης* (Service Execution Node – SEN) και τον *κόμβο διαχείρισης* (Service Management Service – SMS).

Ο κόμβος SMS φιλοξενεί τις οντότητες που είναι υπεύθυνες για την δημιουργία



Σχήμα 8.1: Κατανεμημένο Ευφυές Δίκτυο βασιζόμενο σε τεχνολογία CORBA και κινητούς πράκτορες

(SCEF[1]) και για την διαχείριση (SMF) των υπηρεσιών που προσφέρονται από το δίκτυο. Η χρήση της τεχνολογίας CORBA και των κινητών πρακτόρων παρέχει τη δυνατότητα σχεδιασμού υπηρεσιών, που απαιτούν από το σχεδιαστή να γνωρίζει μόνο εκείνες τις λεπτομέρειες του δικτύου που αφορούν τη λογική της συγκεκριμένης υπηρεσίας.

Ο κόμβος SEN αφορά κυρίως την εκτέλεση υπηρεσίας. Φιλοξενεί, μεταξύ άλλων, τις οντότητες ελέγχου υπηρεσιών και δεδομένων (B-SCF/B-SDF). Αυτές οι οντότητες εκτελούν τους κινητούς πράκτορες Service Logic Programs (SLP) και Resource Logic Programs (RLP) μετά τη μετανάστευσή τους από τον κόμβο SMS.

Ο κόμβος B-SSCP σχετίζεται κυρίως με τη μεταγωγή του δικτύου. Όμως, φιλοξενεί επίσης μια έκδοση των οντοτήτων B-SCF και B-SDF. Οι οντότητες αυτές μπορούν να

[1]Η επεξήγηση των διαφόρων οντοτήτων της αρχιτεκτονικής, παρουσιάζεται στο σχήμα 8.1.

εκτελέσουν κινητούς πράκτορες SLP, οι οποίοι μεταναστεύουν από την οντότητα B-SCF/B-SDF που φιλοξενείται στον κόμβο SEN. Και οι δύο οντότητες B-SCF/B-SDF (η μια φιλοξενείται στον κόμβο SEN και η άλλη που φιλοξενείται στον κόμβο B-SSCP) έχουν παρόμοια υποδομή. Εντούτοις, εκείνη που βρίσκεται στον κόμβο B-SSCP λαμβάνει και εξυπηρετεί αιτήματα μόνο υπό ορισμένες προϋποθέσεις. Αυτό συνήθως συμβαίνει όταν είναι αυξημένη η κίνηση του δικτύου ή όταν αποστέλλονται στο δίκτυο πολλαπλές αιτήσεις για την ίδια υπηρεσία. Ο ρόλος της οντότητας B-CCF σχετίζεται με τον έλεγχο των κλήσεων/ συνδέσεων. Τέλος, στον τερματικό κόμβο, η οντότητα B-CCAF είναι η οντότητα διεπαφής ανάμεσα στον χρήστη στο δίκτυο.

Όταν ο χρήστης δέχεται μια κλήση IMR, αυτή προωθείται σε κάποιον κόμβο που φιλοξενεί την λογική υπηρεσίας (τον κόμβο SEN ή τον κόμβο B-SSCP). Μετά τη συλλογή και την επεξεργασία της κατάλληλης πληροφορίας χρήστη (για παράδειγμα εξουσιοδότηση, επιλογή υπηρεσίας) η λογική υπηρεσίας αποφασίζει εάν η υπηρεσία μεταγωγής θα επιτρέψει μία σύνδεση μεταξύ του κατάλληλου εξυπηρετητή και του χρήστη.

Εφαρμόζοντας τον έλεγχο της υπηρεσίας μέσω κινητών πρακτόρων, μειώνεται η απομακρυσμένη επικοινωνία και αυξάνεται η απόδοση του δικτύου. Οι κινητοί πράκτορες (RLP και SLP) κλωνοποιούνται τοπικά στους κόμβους SEN και B-SSCP, και συνεπώς η υπηρεσία κλήσης εκτελείται μέσω τοπικής επικοινωνίας (για μια λεπτομερή περιγραφή της αρχιτεκτονικής δικτύου, βλέπε [26]).

8.3 Απειλές και μηχανισμοί ασφάλειας

8.3.1 Απειλές ασφάλειας

Η αρχιτεκτονική του Κατανεμημένου Ευφυούς Δικτύου (ΚΕΔ) βασίζεται πάρα πολύ σε κατανεμημένες τεχνολογίες. Επιπλέον η επικοινωνία μεταξύ στοιχείων του δικτύου εκτελείται μέσω ανοιχτών καναλιών επικοινωνίας, όπως είναι το διαδίκτυο. Αυτό μπορεί να οδηγήσει σε αρκετές απειλές ασφάλειας. Αυτές οι απειλές περιλαμβάνουν:

- *Επιθέσεις πλαστοπροσωπίας*. Μη εξουσιοδοτημένοι χρήστες μπορεί να προσπαθήσουν να αποκτήσουν πρόσβαση στις υπηρεσίες ενός ΚΕΔ.

- *Επιθέσεις μεταμφίεσης*. Ένας καταγεγραμμένος χρήστης μπορεί να προσπαθήσει να παρακάμψει την πολιτική ασφάλειας και να αποκτήσει παράνομα πρόσβαση σε υπηρεσίες στις οποίες δεν του επιτρέπεται η πρόσβαση.

- *Επιθέσεις άρνησης εξυπηρέτησης*. Ένας αντίπαλος μπορεί να προσπαθήσει να εμποδίσει νόμιμους χρήστες στην πρόσβασή τους στις υπηρεσίες του ΚΕΔ, για παράδειγμα αποστέλλοντας ταυτόχρονα έναν μεγάλο αριθμό αιτήσεων στο σύστημα.

- *Υποκλοπή ή τροποποίηση της επικοινωνίας*. Ένας αντίπαλος μπορεί να προσπαθήσει να υποκλέψει και/ή να τροποποιήσει την επικοινωνία ανάμεσα σε έναν νόμιμο χρήστη και στα στοιχεία υπηρεσίας του ΚΕΔ.

- *Αδυναμία καταλογισμού ευθύνης*. Αν το ΚΕΔ δεν είναι ικανό να ελέγξει την επικοινωνία μεταξύ χρηστών και των υπηρεσιών του, τότε δεν θα είναι δυνατός ο καταλογισμός ευθύνης για τους χρήστες, για παράδειγμα η χρέωση των χρηστών για τις προσφερόμενες υπηρεσίες.

8.3.2 Μηχανισμοί ασφάλειας

Για την ασφαλή επικοινωνία μεταξύ των οντοτήτων του συστήματος, χρησιμοποιείται συμμετρική και μη-συμμετρική κρυπτογράφηση. Κάθε τερματικός χρήστης, όπως επίσης κάθε κόμβος του ΚΕΔ, κατέχει ένα ζεύγος δημόσιου/μυστικού κλειδιού για κρυπτογράφηση (π.χ. RSA κλειδιά). Για μεγαλύτερη αποτελεσματικότητα, οι οντότητες του συστήματος χρησιμοποιούν τα δικά τους μη-συμμετρικά κλειδιά για την ανταλλαγή συμμετρικών κρυπτογραφικών κλειδιών (π.χ. DES κλειδιά), εφόσον η συμμετρική κρυπτογράφηση είναι σημαντικά ταχύτερη. Για την προστασία της αυθεντικότητας των δημόσιων κλειδιών των χρηστών, χρησιμοποιείται μία Αρχή Πιστοποίησης (certification Authority – CA) , η οποία εκδίδει X.509 πιστοποιητικά δημόσιου κλειδιού [60].

Για την μυστικότητα και την ακεραιότητα της επικοινωνίας μεταξύ των μη-CORBA οντοτήτων, χρησιμοποιείται το πρωτόκολλο TLS [37]. Επιπλέον συνδυάζοντας το πρωτόκολλο TLS με X.509 πιστοποιητικά, μπορεί να επιτευχθεί διπλή αυθεντικοποίηση μεταξύ απομακρυσμένων κόμβων. Τέλος, για την ασφάλεια της μετανάστευσης των πρακτόρων, γίνεται χρήση του ασφαλούς διαύλου μετανάστευσης της πλατφόρμας Grasshopper [59].

Μηχανισμοί ασφάλειας της CORBA

Οι περισσότεροι από τους μηχανισμούς ασφάλειας που χρησιμοποιούνται βασίζονται στην τεχνολογία CORBA, εφόσον οι περισσότερες από τις οντότητες του συστήματος είναι CORBA αντικείμενα. Η χρήση αυτών των μηχανισμών απαιτεί την ενσωμάτωση πακέτων CORBA Secure Interoperability (CSI), τα οποία είναι δομημένα σε αρκετά επίπεδα. Λεπτομερής περιγραφή των πακέτων ασφαλείας και των μηχανισμών βρίσκεται στις προδιαγραφές υπηρεσιών ασφάλειας της CORBA [98].

Η προτεινόμενη αρχιτεκτονική απαιτεί το πακέτο Main Security Functionality Package Level 2, το οποίο επιτρέπει στις εφαρμογές να ελέγχουν την ασφάλεια που παρέχεται κατά την κλήση αντικειμένων. Επιπλέον, απαιτείται το πακέτο SECIOP Interoperability έτσι ώστε να είναι δυνατή η ασφαλής επικοινωνία των ORB αντικειμένων μέσω TCP/IP συνδέσεων. Απαιτείται επίσης η χρήση των πακέτων ORB Services Replaceability και Security Replaceability. Αυτά τα πακέτα επιτρέπουν την αντικατάσταση των καθιερωμένων υπηρεσιών ασφάλειας της CORBA, όπου αυτό είναι αναγκαίο.

Χρησιμοποιείται επίσης το πακέτο Common Secure Interoperability Feature (CSI Level 2), το οποίο επιτρέπει το σχεδιασμό ευέλικτης πολιτικής πρόσβασης. Μέσω αυτού του πακέτου οι οντότητες της εφαρμογής μπορούν να κατέχουν προνόμια πρόσβασης που καθιστούν δυνατή την πρόσβασή τους σε υπηρεσίες. Τα προνόμια πρόσβασης διακρίνονται σε *ταυτότητες* και *χαρακτηριστικά πρόσβασης*. Κάθε οντότητα μπορεί να έχει μία ή περισσότερες ταυτότητες, οι οποίες μπορεί να χρησιμοποιηθούν για να προσδιορίσουν την πηγή ενός μηνύματος, να κάνουν έναν χρήστη υπόλογο των πράξεών του ή να χρεώσουν τον χρήστη του συστήματος. Τα χαρακτηριστικά πρόσβασης διακρίνουν τους χρήστες σε *ομάδες*, ή *ρόλους*, με διαφορετικά δικαιώματα πρόσβασης στις υπηρεσίες. Επιπλέον, το πακέτο CSI Level 2 επιτρέπει την *ελεγχόμενη μεταβίβαση* ταυτοτήτων και χαρακτηριστικών πρόσβασης μεταξύ των αντικειμένων CORBA με εξάρτηση μεταβιβάζοντα.

Εκτός από τα πακέτα ασφαλείας, χρησιμοποιούνται επίσης μηχανισμοί ασφαλείας της CORBA. Για να αυθεντικοποιηθεί και να προστατευτεί η ακεραιότητα των διαπιστευτηρίων ενός χρήστη, χρησιμοποιούνται τα *πιστοποιητικά χαρακτηριστικών προνομίων* Privilege Attribute Certificates (PACs). Ένα PAC περιλαμβάνει τα διαπιστευτήρια ενός χρήστη, και αποτελεί μία υλοποίηση των πιστοποιητικών χαρακτηριστικών

που αναφέρθηκαν στο έβδομο κεφάλαιο. Χρησιμοποιώντας την μέθοδο μεταβίβασης Protection Value / Control Value (PV/CV), το PAC προστατεύεται από την χρησιμοποίησή του από μη-εξουσιοδοτημένους χρήστες. Επιπλέον, η μέθοδος PV/CV ελέγχει τους επιτρεπόμενους στόχους μεταβίβασης των PAC. Το PAC περιλαμβάνει επίσης μια ημερομηνία λήξης και είναι υπογεγραμμένο από την αρχή πιστοποίησης CA. Σημειώνεται ότι τα PAC είναι ένας πρόσφορος μηχανισμός για την εφαρμογή δυναμικών και ευέλικτων πολιτικών πρόσβασης βασισμένων σε ρόλους (Role Based Access Control - RBAC). Διαφορετικά PAC μπορούν να εκδοθούν για διαφορετικούς ρόλους της εφαρμογής (όπως για παράδειγμα για τον διαχειριστή των υπηρεσιών του ΕΔ, τον διαχειριστή των κόμβων και τον τερματικό χρήστη), τα οποία να περιλαμβάνουν τα προνόμια πρόσβασης και τους περιορισμούς που αφορούν κάθε ρόλο.

Τέλος, για την ασφαλή επικοινωνία των αντικειμένων CORBA, χρησιμοποιείται το πρωτόκολλο CSI-ECMA [77], το οποίο υποστηρίζει τα PAC για ελεγχόμενη μεταβίβαση. Το πρωτόκολλο CSI-ECMA επιτρέπει την χρήση συμμετρικής και μη συμμετρικής κρυπτογράφησης για την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας μεταξύ των CORBA οντοτήτων.

8.4 Μία ασφαλής αρχιτεκτονική ευφυών δικτύων

Από λειτουργική άποψη, οι υπηρεσίες ασφάλειας των ΚΕΔ μπορούν να διαχωριστούν σε *Υπηρεσίες Υποστήριξης Χρήστη* (User Supporting Services), *Υπηρεσίες Ελέγχου Πρόσβασης* (Access Control Services) και *Υπηρεσίες Έμπιστης Οντότητας* (Trusted Services).

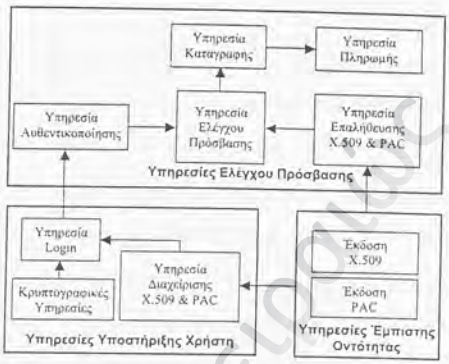
Οι Υπηρεσίες Υποστήριξης Χρήστη χρησιμοποιούνται τοπικά από τους τερματικούς χρήστες του δικτύου, για τη διαχείριση των πιστοποιητικών (δημόσιου κλειδιού και

PAC), όπως επίσης την διαδικασία login και για τους κρυπτογραφικούς αλγόριθμους και τα χρησιμοποιούμενα πρωτόκολλα.

Οι Υπηρεσίες Ελέγχου Πρόσβασης αφορούν τις υπηρεσίες ασφάλειας που εφαρμόζονται στα διαφορετικά επίπεδα της αρχιτεκτονικής του ΚΕΔ και ελέγχουν την αυθεντικοποίηση χρήστη και την διαχείριση των λογαριασμών των χρηστών που προσδιορίζουν τα δικαιώματα πρόσβασής τους. Επιπλέον, περιλαμβάνουν την υπηρεσία που είναι υπεύθυνη για την επαλήθευση των πιστοποιητικών (δημόσιου κλειδιού και PAC) των χρηστών και την υπηρεσία καταγραφής (audit service). Τέλος, μπορεί να περιλαμβάνουν μια υπηρεσία πληρωμής.

Τέλος, οι Υπηρεσίες Έμπιστης Οντότητας περιλαμβάνουν την διαχείριση (έκδοση και ανάκληση) των πιστοποιητικών (X.509 και PAC) για τους τερματικούς χρήστες, τους διαχειριστές και τους κόμβους του ΚΕΔ. Αυτές τις υπηρεσίες τις διαχειρίζεται μια Αρχή Πιστοποίησης, όπως αναφέρθηκε στην προηγούμενη ενότητα. Στο σχήμα 8.2 περιγράφεται η λειτουργική αρχιτεκτονική ασφάλειας του ΚΕΔ. Η αρχιτεκτονική του ασφαλούς ΚΕΔ παρουσιάζεται στο σχήμα 8.3. Κάθε τερματικός χρήστης που είναι καταγεγραμμένος σε μια υπηρεσία IMR, πρέπει να έχει αυθεντικοποιηθεί με εκτός-εύρους μέσα αυθεντικοποίησης από την Αρχή Πιστοποίησης και η αρχή να έχει εκδώσει ένα πιστοποιητικό X.509 για κάθε δημόσιο κλειδί του χρήστη. Επιπλέον, η Αρχή Πιστοποίησης έχει εκδώσει ένα PAC για κάθε καταγεγραμμένο χρήστη, το οποίο περιλαμβάνει τις ταυτότητες, προνόμια πρόσβασης και περιορισμούς μεταβίβασης του συγκεκριμένου χρήστη.

Ένας χρήστης που επιθυμεί να έχει πρόσβαση σε μια υπηρεσία IMR, προετοιμάζει ένα μήνυμα αίτησης, το οποίο αποστέλλεται στην οντότητα B-CCF του κόμβου B-SSCP (βλέπε σχήμα 8.3). Η υπηρεσία login και η υπηρεσία αυθεντικοποίησης του κόμβου B-CCAF χρησιμοποιούν τα ψηφιακά πιστοποιητικά του τερματικού χρήστη και του



Σχήμα 8.2: Λειτουργική αρχιτεκτονική ασφάλειας

κόμβου B-SSCP αντίστοιχα, ώστε να εγκαθιδρύσουν μια ασφαλή επικοινωνία μέσω του πρωτοκόλλου TLS (βήμα 1). Ο τερματικός χρήστης αυθεντικοποιείται στον κόμβο B-SSCP και αναταλλάσεται ένα συμμετρικό κλειδί. Αυτό το κλειδί θα χρησιμοποιηθεί για την μυστικότητα της υπόλοιπης συνεδρίας. Η υπηρεσία αυθεντικοποίησης της οντότητας B-CCF, η οποία ελέγχει την επικοινωνία με τους τερματικούς χρήστες, επιτρέπει μόνο μια αίτηση για κάθε τερματικό χρήστη, ώστε να αποφευχθούν επιθέσεις άρνησης εξυπηρέτησης.

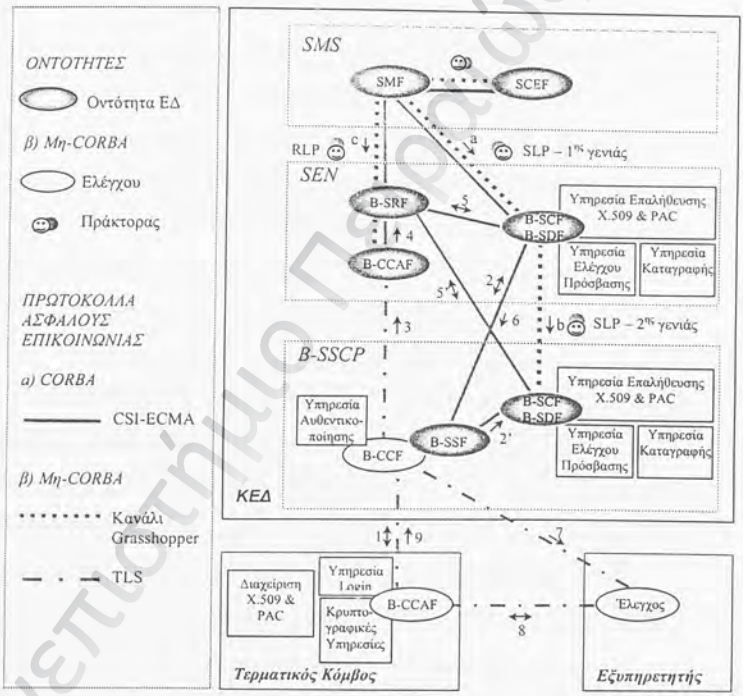
Κατόπιν, η υπηρεσία login της οντότητας B-CCAF χρησιμοποιεί την υπηρεσία διαχείρισης PAC για να μεταδώσει μέσω του καναλιού TLS το PAC του χρήστη μαζί με την αίτηση IMR της οντότητας B-CCF. Ας παρατηρηθεί ότι η οντότητα B-CCF δεν είναι CORBA οντότητα και δεν μπορεί να χρησιμοποιεί τα διαπιστευτήρια που περιλαμβάνονται στο PAC. Όμως, χρησιμοποιώντας κατάλληλους μετατροπείς, το PAC μπορεί να μεταβιβαστεί στην οντότητα B-SSF, που είναι CORBA οντότητα. Αυτό μπορεί να

επιτευχθεί εφαρμόζοντας την προσέγγιση που προτείνεται στο [43] η οποία χρησιμοποιεί GSS-API. Ενδιαφέρουσες εναλλακτικές θα ήταν είτε η μεταβίβαση των PAC με την χρήση αλυσίδων πιστοποιητικών και υπογραφών όπως προτείνεται στο [4] ή η υβριδική λύση του [3] που ενσωματώνει PAC στο πρωτόκολλο TLS.

Η μέθοδος PV/CV, η οποία ελέγχει την μεταβίβαση του PAC, επιτρέπει μόνο απλή μεταβίβαση. Επιπλέον, περιορίζει τον στόχο της εξουσιοδότησης ώστε να είναι μία από τις δυο οντότητες B-SCF/B-SDF, που βρίσκεται είτε στον κόμβο B-SSCP είτε στον κόμβο SEN. Αυτό οφείλεται στο γεγονός ότι σύμφωνα με την λογική λειτουργίας (service logic) του ΚΕΔ, μια αίτηση θα εξυπηρετηθεί από μία από αυτές τις δύο όμοιες οντότητες (είτε το βήμα 2 είτε το βήμα 2' θα εκτελεστεί για κάθε αίτηση). Και στις δύο περιπτώσεις, η μεταβίβαση του PAC επιτυγχάνεται μέσω του πρωτοκόλλου CSI-ECMA. Όμως, εάν η οντότητα B-SSF πρέπει να επικοινωνήσει με την οντότητα B-SCF/B-SDF του ανώτερου επιπέδου (του κόμβου SEN), τότε χρησιμοποιείται ο μηχανισμός κρυπτογράφησης του πρωτοκόλλου CSI-ECMA, ο οποίος βασίζεται σε βασικά κλειδιά και σε κλειδιά συνεδρίας. Σε αυτήν την περίπτωση, τα πιστοποιητικά X.509 των κόμβων B-SSCP και SEN χρησιμοποιούνται για την ανταλλαγή ενός βασικού κλειδιού, που με την σειρά του χρησιμοποιείται για την κατασκευή ενός (συμμετρικού) κλειδιού συνεδρίας. Το κλειδί συνεδρίας χρησιμοποιείται κατόπιν για συμμετρική κρυπτογράφηση.

Η οντότητα B-SCF/B-SDF που θα εξυπηρετήσει την αίτηση χρησιμοποιεί την υπηρεσία επαλήθευσης των PAC, για να επαληθεύσει την αυθεντικότητα και την εγκυρότητά του, προτού η αίτηση εξυπηρετηθεί.

Ο τερματικός χρήστης επικοινωνεί επίσης με την οντότητα B-SRF μέσω της οντότητας B-CCAF του κόμβου SEN (βήματα 3, 4). Αυτό το κανάλι χρησιμοποιείται για να προμηθεύσει τον χρήστη με οθόνες επιλογής και δείγματα βίντεο, έτσι ώστε ο χρήστης να προσδιορίσει ένα περισσότερο ακριβές αίτημα. Αυτή η επικοινωνία, δεν



Σχήμα 8.3: Αρχιτεκτονική ασφαλούς ΚΕΔ

απαιτεί κρυπτογράφηση, εφόσον τα δείγματα βίντεο είναι διαθέσιμα σε κάθε χρήστη, εγγεγραμμένο ή όχι, για εμπορικούς λόγους.

Η οντότητα B-SCF/B-SDF θα επικοινωνήσει τώρα με την οντότητα B-SRF του κόμβου SEN, για να λάβει επιπρόσθετη πληροφόρηση σχετικά με το αίτημα του χρήστη (βήμα 5). Κατόπιν, χρησιμοποιείται η υπηρεσία ελέγχου πρόσβασης, για να ελέγξει εάν τα διαπιστευτήρια του χρήστη είναι κατάλληλα για την συγκεκριμένη υπηρεσία IMR. Εάν πετύχει η επαλήθευση, τότε η οντότητα B-SCF/B-SDF θα στείλει στην οντότητα B-SSF (βήμα 6) την κατάλληλη πληροφόρηση για το αίτημα υπηρεσίας π.χ. την διεύθυνση IP του εξυπηρετητή. Και πάλι, εάν η επικοινωνία πραγματοποιείται μεταξύ της οντότητας B-SCF/B-SDF του κόμβου SEN και της οντότητας B-SSF του κόμβου B-SSCP, χρησιμοποιείται το πρωτόκολλο CSI-ECMA με κρυπτογράφηση δύο επιπέδων.

Σε αυτό το σημείο, η οντότητα B-SSF διαθέτει όλη την αναγκαία πληροφόρηση για να συμπληρώσει το αίτημα υπηρεσίας. Η πληροφόρηση του αιτήματος υπηρεσίας περνά μέσω της οντότητας B-CCF στον επιλεγόμενο εξυπηρετητή, μαζί με τα πιστοποιητικά του χρήστη (βήμα 7). Ο εξυπηρετητής χρησιμοποιεί αυτά τα πιστοποιητικά, για να εγκαθιδρύσει μια σύνδεση TLS με τον χρήστη, (βήμα 8) και να ολοκληρώσει το αίτημα. Η οντότητα B-CCF πληροφορείται τέλος για την επιτυχία της επικοινωνίας (βήμα 9) και με τη σειρά της πληροφορεί την υπηρεσία καταγραφής για την συγκεκριμένη συναλλαγή (χρήστης, εξυπηρετητής, χρόνος επικοινωνίας, κ.τ.λ.). Εάν πρόκειται να χρησιμοποιηθεί μια υπηρεσία πληρωμής, τότε η υπηρεσία καταγραφής μπορεί να παράσχει όλες τις αναγκαίες πληροφορίες για τις συναλλαγές κάθε χρήστη.

Οι οντότητες SMF και SCEF του κόμβου SMS ελέγχουν την λειτουργικότητα του ΕΔ. Στην περίπτωση που συμβαίνουν λειτουργικές αλλαγές (για παράδειγμα πρόσθεση νέων χρηστών ή επανακατανομή υπηρεσιών μεταξύ των οντοτήτων B-SCF/B-SDF) τότε

οι οντότητες B-SCF/B-SDF των κόμβων SEN και B-SSCP πρέπει να πληροφορηθούν για αυτές τις αλλαγές. Αυτό αντιμετωπίζεται με την μετανάστευση πρακτόρων. Πρώτα, η οντότητα SMF του κόμβου SMS, εγκαθιστά ένα ασφαλές κανάλι μετανάστευσης με την οντότητα B-SCF/B-SDF του κόμβου SEN (βήμα a), για την μετανάστευση των πρακτόρων πρώτης γενιάς. Χρησιμοποιώντας τα πιστοποιητικά των κόμβων SMS και SEN, εξασφαλίζεται διπλή αυθεντικοποίηση και εγκαθίσταται ένα κρυπτογραφικό κανάλι για εμπιστευτικότητα. Τέλος, οι οντότητες B-SCF/B-SDF των κόμβων SEN και B-SSCP προετοιμάζουν ένα ασφαλές κανάλι μετανάστευσης για τους πράκτορες δεύτερης γενιάς, για να ολοκληρώσουν την ανανέωση της λειτουργικότητας του ΚΕΔ (βήμα b). Η ίδια προσέγγιση ακολουθείται για την μετανάστευση των πρακτόρων RLP στην οντότητα B-SRF (βήμα c).

8.5 Πιθανές επεκτάσεις και συμπεράσματα

Το προτεινόμενο μοντέλο ασχολείται με ΚΕΔ σε εφαρμογές IMR. Όμως, η προτεινόμενη αρχιτεκτονική ασφάλειας ΚΕΔ μπορεί εύκολα να τροποποιηθεί ώστε να καλύψει ανάγκες διαφορετικών εφαρμογών. Για παράδειγμα, εάν η πολιτική ασφάλειας απαιτεί περισσότερο ευέλικτο έλεγχο πρόσβασης, είναι εύκολο να δημιουργηθεί μία βαθύτερη ιεραρχία ρόλων μέσω της χρήσης των πιστοποιητικών PAC που να στηρίζεται στις ανάγκες της εφαρμογής. Το ίδιο ισχύει και για την πολιτική μεταβίβασης ρόλων. Για παράδειγμα, είναι δυνατό να χρησιμοποιηθεί το πρωτόκολλο μεταβίβασης ρόλων που παρουσιάστηκε στο έβδομο κεφάλαιο για να επιτρέψει τη μεταβίβαση ρόλων μεταξύ πρακτόρων, πέραν των διαφορετικών επιτρεπόμενων σχημάτων μεταβίβασης του πρωτοκόλλου CSI-ECMA.

Στο προτεινόμενο μοντέλο δεν χρησιμοποιείται καμία υπηρεσία για καταλογισμό

ευθύνης. Εάν η χρήση τέτοιας υπηρεσίας απαιτείται, τότε η υπηρεσία καταλογισμού ευθύνης της CORBA μπορεί να χρησιμοποιηθεί. Αυτό βέβαια θα απαιτούσε την έκδοση ενός επιπλέον ζεύγους κλειδιών και πιστοποιητικού για κάθε χρήστη, καθώς η χρήση του ίδιου κλειδιού τόσο για ψηφιακές υπογραφές, όσο και για κρυπτογράφηση δεν θεωρείται ασφαλής.

Η αποδοτικότητα του μοντέλου μπορεί να παραμετροποιηθεί, ανάλογα με τις ανάγκες της εφαρμογής, μέσω της πολιτικής ασφάλειας και της πολιτικής διαχείρισης δικτύου. Η σχεδίαση της πολιτικής ασφάλειας, μπορεί να οδηγήσει σε καλύτερη απόδοση του δικτύου. Σε επικοινωνίες που παρουσιάζουν βαρύ φόρτο δικτύου, όπως είναι η μεταφορά βίντεο, κρυπτογράφηση χαμηλότερου επιπέδου κρίνεται ως περισσότερο αποδοτική. Επίσης, η εφαρμογή ελέγχων πρόσβασης και η καταγραφή της πρόσβασης των χρηστών μπορεί να εφαρμοστεί μόνο σε κόμβους του δικτύου που απαιτούν αυξημένη προστασία.

Η πολιτική διαχείρισης του δικτύου μπορεί επίσης να βελτιώσει την απόδοση της προτεινόμενης αρχιτεκτονικής. Για παράδειγμα, μπορεί να προσφέρει μία αποδοτικότερη κατανομή πόρων σε εκείνους τους κόμβους που παρουσιάζουν τις μεγαλύτερες υπολογιστικές ανάγκες λόγω της παρουσίας των υπηρεσιών ασφάλειας. Επίσης, οι υπηρεσίες που εκτελούνται σε κόμβους με μεγάλο φόρτο δικτύου, θα πρέπει να σχεδιαστούν ώστε να απαιτούν όσο το είναι όσο δυνατό λιγότερους υπολογιστικούς πόρους. Το προτεινόμενο μοντέλο ασφάλειας παρέχει αρκετή ευελιξία στο σχεδιαστή υπηρεσιών του δικτύου, ώστε ανάλογα με τις απαιτήσεις των προσφερόμενων υπηρεσιών να είναι δυνατή η διαμόρφωση του δικτύου στο επιθυμητό επίπεδο ασφάλειας.

Κεφάλαιο 9

Συμπεράσματα και ανοικτά ερευνητικά πεδία

Στο κεφάλαιο αυτό παρουσιάζονται τα γενικά συμπεράσματα που προκύπτουν από τα θέματα που εξετάστηκαν σην παρούσα διατριβή, ενώ επίσης παρουσιάζονται ορισμένα ανοικτά ερευνητικά προβλήματα καθώς και οι τελευταίες εξελίξεις στο εξεταζόμενο ερευνητικό πεδίο.

9.1 Συμπεράσματα

Όπως αναφέρθηκε στο πρώτο κεφάλαιο της διατριβής, η τεχνολογία των κινητών πρακτόρων προσφέρει σημαντικά πλεονεκτήματα σε ένα εκτεταμένο εύρος εφαρμογών οι οποίες απαιτούν κατανεμημένους υπολογισμούς και ασύγχρονη επικοινωνία. Ο κατανεμημένος χαρακτήρας των κινητών πρακτόρων μπορεί να οδηγήσει σε βελτιστοποιημένη χρήση υπολογιστικών πόρων. Η δυνατότητα ασύγχρονης επικοινωνίας ελαττώνει την ανάγκη για επικοινωνία σε πραγματικό χρόνο για τον τελικό χρήστη.

Η δυνατότητα αυτόνομης μεταφοράς και εκτέλεσης κώδικα σε διαφορετικά περιβάλλοντα, συμβάλλει στην ελάττωση του κόστους εύρους ζώνης δικτύου, καθώς και στην ανάπτυξη εφαρμογών με αυξημένη διαλειτουργικότητα [84, 93, 112].

Όμως ο κατανεμημένος και δυναμικός χαρακτήρας των κινητών πρακτόρων εντείνει πολλά από τα γνωστά προβλήματα ασφάλειας κατανεμημένου υπολογισμού και απομακρυσμένης πρόσβασης όπως είναι η πλαστοπροσωπία, η μεταμφίεση, η άρνηση εξυπηρέτησης, η ενεργητική και παθητική παρακολούθηση. Επιπλέον δημιουργεί νέα προβλήματα ασφάλειας, όπως είναι η αυθαίρετη τροποποίηση του κώδικα και των προηγούμενων αποτελεσμάτων εκτέλεσης ενός πράκτορα, ή ο αυθαίρετος καταλογισμός ευθύνης εναντίον (του ιδιοκτήτη) ενός πράκτορα με δυνατότητα υπογραφής.

Μία βασική διαφορά των συστημάτων κινητών πρακτόρων σε σχέση με άλλα κατανεμημένα συστήματα, είναι η ιδιαίτερη δυσκολία αντιμετώπισης των *εσωτερικών επιθέσεων ασφάλειας*. Σε ένα σύστημα κινητών πρακτόρων, οι κινητοί πράκτορες κατά τη διάρκεια του κύκλου ζωής τους μεταναστεύουν κατά κύριο λόγο σε εσωτερικούς υπολογιστές εκτέλεσης, δηλαδή σε εξυπηρετητές του συστήματος. Όμως, μπορεί να μεταναστεύσουν και σε εξωτερικούς υπολογιστές εκτέλεσης, για παράδειγμα για λόγους δρομολόγησης. Επιπλέον, εξωτερικοί εξυπηρετητές μπορεί να υποκλέψουν ένα πράκτορα κατά τη διάρκεια της μετανάστευσής του, να τον κλωνοποιήσουν και να τον χρησιμοποιήσουν για μη εξουσιοδοτημένες χρήσεις.

Για την προστασία των συστημάτων κινητών πρακτόρων από εξωτερικές επιθέσεις ασφάλειας, μπορούν να χρησιμοποιηθούν αρκετοί γνωστοί μηχανισμοί ασφάλειας, όπως αυθεντικοποίηση προορισμού πριν τη μετανάστευση, έλεγχος εξουσιοδότησης, κρυπτογράφηση (point-to-point και end-to-end encryption) και μηχανισμοί ελέγχου ακεραιότητας. Όμως, όπως προκύπτει και από τα προβλήματα που εξετάστηκαν στην

παρούσα διατριβή, οι μηχανισμοί αυτοί δεν επαρκούν για την αντιμετώπιση των εσωτερικών επιθέσεων ασφάλειας. Εάν και οι εσωτερικές επιθέσεις ασφάλειας είναι κατά κανόνα δυσκολότερες, στα συστήματα κινητών πρακτόρων το πρόβλημα γίνεται ακόμα πιο έντονο για διάφορους λόγους όπως:

Πλήρης έλεγχος του πράκτορα από το περιβάλλον εκτέλεσης. Εφόσον το περιβάλλον εκτέλεσης έχει πρόσβαση στον κώδικα, τα δεδομένα και την κατάσταση εκτέλεσης του πράκτορα, είναι δύσκολο για τον πράκτορα να χρησιμοποιήσει κάποια πληροφορία, για παράδειγμα κάποιο τμήμα κώδικα ή κάποια μυστική πληροφορία όπως ένα κρυπτογραφικό κλειδί, χωρίς να την αποκαλύψει.

Μη αποδοτικότητα μηχανισμών παρακολούθησης επιθέσεων. Αν και για τον εντοπισμό εσωτερικών επιθέσεων ασφάλειας έχουν χρησιμοποιηθεί σε πολλές εφαρμογές διάφορα συστήματα παρακολούθησης και ανίχνευσης επιθέσεων, η χρήση τέτοιων συστημάτων δεν είναι αποδοτική για συστήματα πρακτόρων. Ο λόγος είναι ότι υποβαθμίζουν ένα βασικό πλεονέκτημα της τεχνολογίας των κινητών πρακτόρων που είναι η μη αλληλεπιδραστική εκτέλεση υπολογισμών. Το κόστος δικτύου του μηχανισμού παρακολούθησης του πράκτορα μπορεί να είναι μεγαλύτερο από το κόστος δικτύου για ίδια την εκτέλεση του πράκτορα.

Ανεπάρκεια μηχανισμών ανίχνευσης επιθέσεων. Ένας άλλος βασικός λόγος για αυτή τη δυσκολία, είναι ότι σε πολλές εφαρμογές η εκ των υστέρων ανίχνευση δεν είναι αρκετή για την ικανοποιητική προστασία του αποστολέα του πράκτορα, όπως για παράδειγμα στην περίπτωση ηλεκτρονικών δοσοληψιών.

Δυσκολία διάκρισης μεταξύ επιθέσεων ασφάλειας και σφαλμάτων. Στην περίπτωση καταστροφής ενός πράκτορα δεν είναι εύκολο να διακριθούν επιθέσεις άρνησης εξυπηρέτησης κακόβουλων εξυπηρετητών, από σφάλματα δικτύου που οδήγησαν

στην απώλεια του πράκτορα.

Πολλές από τις λύσεις που προτάθηκαν στην διατριβή αυτή αντιμετωπίζουν αποτελεσματικά τόσο εσωτερικές όσο και εξωτερικές απειλές ασφάλειας. Αναλυτικότερα:

- Τα πρωτόκολλα των μη-αποσπώμενων υπογραφών και των δυναμικών πολυυπογραφών που παρουσιάστηκαν στο τρίτο και τέταρτο κεφάλαιο αντίστοιχα, μπορούν να αντιμετωπίσουν επιθέσεις αυθαίρετου καταλογισμού ευθύνης προερχόμενες από κακόβουλους εσωτερικούς ή εξωτερικούς υπολογιστές εκτέλεσης. Τα πρωτόκολλα αυτά αποτελούν στιγμιότυπα των μεθόδων Υπολογισμού με Κρυπτογραφημένες Συναρτήσεις (βλέπε παράγραφο 2.1.2 καθώς και αναφορές [50, 104]), εφόσον τόσο το μυστικό κλειδί υπογραφής όσο και ολόκληρη η συνάρτηση υπογραφής δεν αποκαλύπτονται στον υπολογιστή κατά τη διάρκεια της εκτέλεσης.

- Η αρχιτεκτονική ασφάλειας δοσοληψιών μέσω κινητών πρακτόρων που παρουσιάστηκε στο έκτο κεφάλαιο προσφέρει παθητική προστασία (ανίχνευση) τόσο από εσωτερικές όσο και από εξωτερικές επιθέσεις κακόβουλων υπολογιστών εκτέλεσης.

- Ο μηχανισμός μεταβίβασης ρόλων μεταξύ κινητών πρακτόρων που παρουσιάστηκε στο έβδομο κεφαλαίο, προσφέρει ενεργητική προστασία των κινητών πρακτόρων από εσωτερικές ή εξωτερικές επιθέσεις μη εξουσιοδοτημένης τροποποίησης και πρόσβασης.

Άλλες λύσεις που παρουσιάστηκαν στη διατριβή, στοχεύουν στην προστασία εξωτερικών μόνο επιθέσεων ασφάλειας. Πιο συγκεκριμένα:

- Ο μηχανισμός της ισχυρής χρονικής ασφάλειας που περιγράφηκε στο πέμπτο κεφάλαιο, μπορεί να προσφέρει παθητική προστασία από εξωτερικές επιθέσεις

υποκλοπής μυστικού κλειδιού. Αξίζει να σημειωθεί ότι ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί πέραν από την προστασία συστημάτων κινητών πρακτόρων, σε πολλές άλλες εφαρμογές Υποδομής Δημόσιου Κλειδιού.

- Τέλος, η αρχιτεκτονική ασφάλειας κατανεμημένων ευφυών δικτύων που παρουσιάστηκε στο όγδοο κεφάλαιο, στοχεύει επίσης στην προστασία από εξωτερικές επιθέσεις ασφάλειας, μέσω της χρήσης κινητών πρακτόρων για τη διαχείριση του δικτύου.

Παρόλο που τα κρυπτογραφικά πρωτόκολλα, οι μηχανισμοί και οι αρχιτεκτονικές ασφάλειας που προτείνονται τόσο στην παρούσα διατριβή όσο και στη διεθνή βιβλιογραφία επιλύουν αρκετά προβλήματα ασφάλειας των συστημάτων κινητών πρακτόρων, δεν είναι εύκολο να προταθούν γενικές λύσεις. Είναι προφανές ότι η επιλογή των κατάλληλων μέτρων ασφάλειας για την προστασία των συστημάτων κινητών πρακτόρων, εξαρτάται πάντοτε από τα ιδιαίτερα χαρακτηριστικά κάθε συγκεκριμένης εφαρμογής. Για κάθε σύστημα κινητών πρακτόρων το οποίο απαιτείται να προστατευτεί θα πρέπει αρχικά να εφαρμοστεί κάποια μεθοδολογία εκτίμησης κινδύνου ώστε να προσδιοριστούν οι απειλές ασφάλειας στις οποίες υπόκειται το εξεταζόμενο σύστημα, οι αδυναμίες του συστήματος και ο συνολικός κίνδυνος ασφάλειας. Μετά από τη μέτρηση αυτών των χαρακτηριστικών κάθε συστήματος κινητών πρακτόρων, είναι ευκολότερο να προσδιοριστούν οι καταλληλότερες λύσεις για την προστασία του, λαμβάνοντας υπόψη τους συγκεκριμένους πόρους που πρέπει να προστατευθούν, τις απαιτούμενες υπηρεσίες ασφάλειας και το συνολικό κόστος από την επιλογή κάθε λύσης.

9.2 Ανοικτά ερευνητικά πεδία

Στην ενότητα αυτή παρουσιάζονται ορισμένα ανοικτά προβλήματα καθώς και ορισμένα πιθανά πεδία έρευνας, τα οποία αφορούν άμεσα την ασφάλεια των συστημάτων κινητών πρακτόρων. Όπως αναφέρθηκε στην ενότητα 2.1.2, πολλές από τις προτεινόμενες λύσεις για την προστασία των κινητών πρακτόρων τόσο στην παρούσα διατριβή όσο και στη διεθνή βιβλιογραφία, βασίζονται στη μέθοδο Ασφαλούς Υπολογισμού Συναρτήσεων [50] και ειδικότερα σε μη-αλληλεπιδραστικό Υπολογισμό Κρυπτογραφημένων Συναρτήσεων. (ΥΚΣ) [104]. Οι Sander και Tschudin παρατήρησαν ότι ένας κινητός πράκτορας μπορεί να υλοποιήσει μη-αλληλεπιδραστικούς ΥΚΣ για *οποιαδήποτε* πολυωνυμική συνάρτηση, χρησιμοποιώντας αλγεβρικά ομοιομορφικά κρυπτοσυστήματα δημόσιου κλειδιού. Δυστυχώς όμως μέχρι στιγμής δεν υπάρχουν αποδεδειγμένα ασφαλή αλγεβρικά ομοιομορφικά κρυπτοσυστήματα. Αντιθέτως, υπάρχουν ενδείξεις για το αντίθετο. Για παράδειγμα, οι Boneh και Lipton [12] απέδειξαν ότι δεν μπορεί να κατασκευαστεί ασφαλές ντετερμινιστικό και αλγεβρικά ομοιομορφικό κρυπτοσύστημα. Από την άλλη πλευρά, δεν υπάρχουν μέχρι στιγμής αποδείξεις για την ύπαρξη ή μη, ασφαλών *μη-ντετερμινιστικών* αλγεβρικά ομοιομορφικών κρυπτοσυστημάτων. Από τα παραπάνω προκύπτει το ακόλουθο ανοικτό πρόβλημα:

Ανοικτό Πρόβλημα 1. *Εύρεση μη-ντετερμινιστικού αλγεβρικά ομοιομορφικού κρυπτοσυστήματος δημόσιου κλειδιού με αποδεδειγμένη υπολογιστική ασφάλεια.*

Όπως προκύπτει από τα προηγούμενα, σε περίπτωση επίλυσης του προβλήματος αυτού, θα ήταν δυνατό για ένα κινητό πράκτορα να υπολογίσει μία οποιαδήποτε πολυωνυμική συνάρτηση, χωρίς να την αποκαλύπτει στον υπολογιστή εκτέλεσης. Βέβαια, η επίδραση από την επίλυση αυτού του προβλήματος στην ασφάλεια των συστημάτων κινητών πρακτόρων θα ήταν περιορισμένη, εφόσον αφορά μόνο τις εφαρμογές

εκείνες όπου η προστασία υπολογισμού πολυωνυμικών συναρτήσεων έχει πρακτικό ενδιαφέρον.

Για την υλοποίηση Ασφαλών Υπολογισμών Συναρτήσεων για κινητούς πράκτορες, οι Cachin *et al* [21] πρότειναν μία άλλη λύση η οποία βασίζεται σε κρυπτογραφημένα κυκλώματα (encrypted circuits) [113] και στη μέθοδο της επιλήσμονος μεταφοράς (oblivious transfer) [17]. Σύμφωνα με αυτή τη λύση ένας κινητός πράκτορας μπορεί να υπολογίσει με ασφάλεια *οποιασδήποτε συνάρτηση πολυωνυμικού χρόνου*. Όμως, έχει μόνο θεωρητική αξία, επειδή για τον έλεγχο της ορθότητας των αποτελεσμάτων, οι παράμετροι εισόδου θα πρέπει να είναι εκθετικά μεγάλοι [21]. Συνεπώς, η παραπάνω λύση δεν είναι πρακτικά εφαρμόσιμη και το πρόβλημα Ασφαλούς Υπολογισμού Συναρτήσεων παραμένει ανοικτό. Μάλιστα, πρόσφατα οι Barak *et al* [5] έδειξαν ότι οι πιθανότητες επιτυχίας οποιασδήποτε μεθοδολογίας Ασφαλούς Υπολογισμού Συναρτήσεων είναι περιορισμένη. Όμως, επειδή δεν υπάρχει ακόμα απόδειξη για τη μη ύπαρξη λύσης, το πρόβλημα παραμένει ακόμα ανοικτό.

Ανοικτό Πρόβλημα 2. *Εύρεση μεθοδολογίας Ασφαλούς Υπολογισμού Συναρτήσεων ή απόδειξης για τη μη ύπαρξή της.*

Σε περίπτωση επίλυσης του προβλήματος αυτού, θα ήταν δυνατό για ένα κινητό πράκτορα να υπολογίσει μία ασφάλεια οποιαδήποτε συνάρτηση πολυωνυμικού χρόνου. Η επίδραση από την επίλυση αυτού του προβλήματος στην ασφάλεια των συστημάτων κινητών πρακτόρων θα ήταν μεγάλη, εφόσον θα οδηγούσε σε πρακτικές και αποδοτικές εφαρμογές κινητών πρακτόρων με πλήρη προστασία του κώδικα του πράκτορα.

Όπως αναλύθηκε στη διατριβή, η χρήση των κινητών πρακτόρων σε εφαρμογές

όπως είναι οι ηλεκτρονικές δοσοληψίες, οι ηλεκτρονικές δημοπρασίες και η διαχείριση ευφυών δικτύων, οδηγεί σε προβλήματα ασφάλειας τα οποία απαιτούν αντιμετώπιση. Ένα άλλο πεδίο στο οποίο οι κινητοί πράκτορες διαφαίνονται ως κατάλληλη τεχνολογία για εφαρμογή είναι τα *ασύρματα κινητά ad hoc δίκτυα* (wireless mobile ad hoc networks) [111]. Λόγω της έλλειψης στατικής υποδομής για δρομολόγηση, καθώς επίσης και της μη προκαθορισμένης κίνησης των κόμβων, τα κινητά ad hoc δίκτυα είναι ευάλωτα σε κατάτμηση του δικτύου [11, 69, 119]. Οι κινητοί πράκτορες, λόγω της ευελιξίας τους και της προσαρμογής τους σε αλλαγές δικτύου, θα μπορούσαν να αποτελέσουν μία πιθανή τεχνολογία για την υποστήριξη της δρομολόγησης και της συνεκτικότητας των ad hoc δικτύων. Βεβαίως, κάτι τέτοιο θα απαιτούσε την ανάπτυξη κατάλληλων κρυπτογραφικών πρωτοκόλλων και μηχανισμών ασφάλειας για την προστασία τόσο από εξωτερικές όσο και από εσωτερικές απειλές ασφάλειας.

Βιβλιογραφία

[1] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, and B. Schneier, *The risks of key recovery, key escrow, trusted third party & encryption*, Digital Issues (1998), no. 3, 1-18.

[2] G-J. Ahn and R. Sandhu, *Role-based authorization constraints specification*, ACM Transactions on Information and System Security **3** (2000), no. 4, 207-226.

[3] P. Ashley, M. Vandenwauer, and J. Claessens, *Using sesame to secure web based applications on an intranet*, Proceedings of the IFIP TC6/TC11 (Leuven, Belgium), 1999, pp. 303-317.

[4] T. Aura, P. Koponen, and J. Rasanen, *Delegation-based access control for intelligent network services*, Proceedings of ECOOP Workshop on Distributed Object Security (Brussels, Belgium), July 1998.

[5] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang, *On the (im)possibility of obfuscating programs*, Advances in Cryptology - Crypto'2001, Lecture Notes in Computer Scince Vol. 2139, Springer,

2001, pp. 1-18.

[6] E. Barka and R. Sandhu, *Framework for role-based delegation models*, Proceedings of the 6th Annual Computer Security Applications Conference, IEEE, 2000, pp. 167-177.

[7] M. Bellare and S. Miner, *A forward-secure digital signature scheme*, Advances in Cryptology — Crypto '99, Lecture Notes in Computer Science Vol. 1666, Springer, 1999, pp. 197-207.

[8] M. Bellare and P. Rogaway, *Random oracles are practical: A paradigm for designing efficient protocols*, Proceedings of the 1st Annual Conference on Computer and Communications Security, ACM, 1993, pp. 62-73.

[9] S. Berkovits, J. Guttman, and V. Swarup, *Authentication for mobile agents*, Lecture Notes in Computer Science Vol. 1419, Springer, 1998, pp. 114-136.

[10] M. Bichler, C. Beam, and A. Segev, *Offer: A broker-centered object framework for electronic requisitioning*, Procceedings of the IFIP/GI Working Conference, TREC'98, Lecture Notes in Computer Science Vol. 1402, Springer, 1998, pp. 154-165.

[11] J. Binkley and W. Trost, *Authenticated ad hoc routing at the link layer for mobile systems*, In Wireless Networks **7** (2001), no. 2, 139-145.

[12] D. Boneh and R. Lipton, *Searching for elements in black-box fields and applications*, Proceedings of Advances in Cryptology - Crypto'96, Lecture Notes in Computer Science Vol. 1109, Springer, 1996, pp. 283-297.

[13] N. Borselius, *Mobile agent security*, IEE Electronics and Communication Engineering Journal **14** (2002), no. 5, 211-218.

[14] N. Borselius, C. Mitchell, and A. Wilson, *On mobile agent based transactions in moderately hostile environments*, Proceedings of the 1st IFIP TC11/WG11.4 Conference on Network Security, Kluwer Academic Publishers, November 2001, pp. 173-186.

[15] ———, *Undetachable threshold signatures*, Proceedings of the 8th IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science Vol. 2260, Springer, December 2001, pp. 239-244.

[16] ———, *A pragmatic alternative to undetachable signatures*, ACM SIGOPS Operating Systems Review **36** (2002), no. 2, 6-11.

[17] G. Brassard, C. Crepeau, and J. M. Robert, *Information theoretic reductions among disclosure problems*, Proceedings of of 27th FOCS, 1986.

[18] M. Breugst and T. Magendaz, *Mobile agents - enabling technology for active intelligent network implementation*, IEEE Network Magazine **12** (1998), no. 3, 53-60.

[19] M. Burmester, V. Chrissikopoulos, P. Kotzanikolaou, and E. Magkos, *Strong forward security*, Procceedings of IFIP/SEC Conference (Paris, France), Kluwer Academic Publishers, June 2001, pp. 109-121.

[20] M. Burmester, Y. Desmedt, and J. Seberry, *Equitable key escrow with limited time span (or how to enforce time expiration cryptographically)*, Advances in

Cryptology —AsiaCrypt '98, Lecture Notes in Computer Science Vol. 1514, Springer, 1998, pp. 380-391.

[21] C. Cachin, J. Camenisch, J. Kilian, and J. Muller, *The one-round secure computation and secure autonomous mobile agents*, Proceedings of of 27th ICALP, Lecture Notes in Computer Science Vol. 1853, Springer, 2000, pp. 512-523.

[22] R. Campbell and T. Qian, *Dynamic agent-based security architecture for mobile computers*, Procceedings of 2nd International Conference on Parallel and Distributed Computing and Networks, IASTED, 1998.

[23] K. Cartrysse and J.C.A. van der Lubbe, *An agent digital signature in an untrusted environment*, Proceedings of SEMAS 2002 Workshop, pp. 12-17.

[24] K. Cartrysse, J.C.A. van der Lubbe, and A. Youssouf *Privacy Incorporated Software Agents (PISA) - Cryptographic mechanisms to be applied*, Research report, Delft University of Technology and GlobalSign, May 2002.

[25] K. Cartrysse, J.C.A. van der Lubbe, and A. Youssouf *Privacy Incorporated Software Agents (PISA) - Privacy protection software design*, Research report, Delft University of Technology and GlobalSign, September 2002.

[26] F. Chatzipapadopoulos, M. Perdikeas, and I. Venieris, *Mobile agent and corba technologies in the broadband intelligent network*, IEEE Communications Magazine (2000), 116-124.

[27] D. Chess, *Security issues in mobile code systems*, Mobile Agents and Security, Lecture Notes in Computer Science Vol. 1419, Springer, 1998, pp. 1-14.

[28] D. Chess, B. Grosof, C. Harrison, D. Levine, C. Parris, and G. Tsudik, *Itinerant agents for mobile computing*, Technical Report, RC 20010, IBM T.J. Watson Research Center, 1995.

[29] D. Chess, C. Harrison, and A. Kershenbaum, *Mobile agents: Are they a good idea?*, Proccedings of Mobile Object Systems, Lecture Notes in Computer Science Vol. 1222, Springer, 1996, pp. 25–48.

[30] Andersen Consulting, *Bargainfinder*, http://bf.cstar.ac.com/bf/.

[31] D. Coppersmith, J. Stern, and S. Vaudenay, *Attacks on the birational permutation signature schemes*, Proceedings of Crypto'93 - Lecture Notes in Computer Science Vol. 773, Springer, 1993, pp. 435-443.

[32] R. Cramer and V. Shoup, *A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*, Advances in Cryptology — Crypto '98, Lecture Notes in Computer Science Vol. 1492, Springer, 1998, pp. 13-25.

[33] S.A. Demurjian, Y. He, T.C. Ting, and M. Saba, *Software agents for role based security*, IFIP WG11.3 Conference on Database Security, Kluwer Academic Publishers, 1999, pp. 79-93.

[34] D. Denning, *A latice model of secure information flow*, Communications of ACM **19** (1976), no. 5, 236-243.

[35] D. Denning and D. Branstad, *A taxonomy of key escrow encryption systems*, Communications of the ACM **39** (1996), no. 3, 24-40.

[36] Y. Desmedt, *Threshold cryptography*, European Transactions on Tellecommunications **5** (1994), no. 4, 449-457.

[37] T. Dierks and C. Allen, *The TLS protocol version 1.0*, RFC 2246, 1999.

[38] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22** (1976), 644-654.

[39] W. Diffie, P. Van Oorschot, and M. Wiener, *Authentication and authenticated key exchanges*, Designs, Codes and Cryptography **2** (1992), 107-125.

[40] C. Douligeris, R. Mavropodi, and P. Kotzanikolaou, *Agent-based security in intelligent multimedia retrieval in intelligent networks*, Procceedings of INFORMS 2001 Annual Meeting Cluster, Telecommunications: Performance Issues in High Speed Networks, 2001.

[41] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **31** (1985), 469-472.

[42] W. Farmer, J. Guttman, and V. Swarup, *Security for mobile agents: Authentication and state appraisal*, In Proccedings of ESORICS'96, Lecture Notes in Computer Science Vol. 1146, Springer, 1996, pp. 118-130.

[43] S. Farrell, *Tls extensions for attribute certificate based authorization*, Internet Draft, 1999.

[44] A. Fayad, S. Jajodia, D. Faatz, and V. Doshi, *Going beyond MAC and DAC using mobile policies*, Procceedings of IFIP/SEC Conference (Paris, France), Kluwer Academic Publishers, June 2001, pp. 245-260.

[45] A. Fiat and A. Shamir, *How to prove yourself: Practical solutions to identification and signature problems*, Advances in Cryptology —Crypto '86, Lecture Notes in Computer Science Vol. 263, Springer, 1986, pp. 186-194.

[46] Y. Frankel, P. Gemmel, P.D. MacKenzie, and M. Yung, *Optimal-resilience proactive public-key cryptosystems*, 38th Annual Symp. on Foundations of Computer Science, IEEE, 1997, pp. 384-393.

[47] ———, *Proactive RSA*, Advances in Cryptology —Crypto '97, Lecture Notes in Computer Science Vol. 1109, Springer, 1997, pp. 440-454.

[48] Y. Frankel, P. Gemmel, and M. Yung, *Witness based cryptographic program checking and robust function sharing*, 28th annual ACM Symp. Theory of Computing, Proceedings, ACM, 1996, pp. 499-508.

[49] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, *Robust and efficient sharing of rsa functions*, Advances in Cryptology —Crypto '96, Lecture Notes in Computer Science Vol. 1109, Springer, 1996, pp. 157-172.

[50] O. Goldreigh, S. Micali, and A. Widgerson, *How to play any mental game or a completeness theorem for protocols with honest majority*, Proceedings of the 19th STOC, 1987, pp. 218-229.

[51] S. Goldwasser and S. Micali, *Probabilistic encryption*, Journal of Computer and System Sciences **28** (1984), 270-299.

[52] C. Gunther, *An identity-based key-exchange protocol*, Advances in Cryptology —Eurocrypt '89, Lecture Notes in Computer Science Vol. 434, Springer, 1989, pp. 29-37.

[53] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung, *Proactive public key and signature schemes*, 4th Annual Conference on Computer and Communications Security, Proceedings, ACM, 1997, pp. 100–110.

[54] A. Herzberg, S. Jarecki, S. Krawczyk, and M. Yung, *Proactive secret sharing*, Advances in Cryptology —Crypto '95, Lecture Notes in Computer Science Vol. 963, Springer, 1995, pp. 339–352.

[55] F. Hohl, *Time limited blackbox security: Protecting mobile agents from malicious hosts*, Lecture Notes in Computer Science Vol. 1419, 1998, pp. 92–113.

[56] Yuh-Jong Hu, *Some thoughts on agent trust and delegation*, Proceedings of 5th International Conference of Autonomous Agents (Montreal, Canada), ACM, June 2001.

[57] IBM, *The aglets workbench*, http://www.trl.ibm.co.jp/~ aglets.

[58] IKV++, *Grasshopper 2*, http://www.grasshopper.de/~ index.html.

[59] ———, *Grasshopper security service*, http://www.grasshopper.de/ download/doc/pguide2.2.pdf.

[60] ITU, *Recomendation X.509. the directory: Abstract service definition*, International Telecommunications Union, Telecommunication Standardization Sector (ITU-T), 1993.

[61] M. Jakobsson and A. Juels, *X-cash: Executable digital cash*, Lecture Notes in Computer Science Vol. 1465, Springer, 1998, pp. 16–27.

[62] Jango, *Netbot*, http://www.jango.com.

[63] W. Jansen, *Countermeasures for mobile agent security*, Elsevier Computer Communications **23** (2000), 1667-1676.

[64] ———, *A privilege management scheme for mobile agent systems*, Proceedings of 1st International Workshop on Security of Mobile Multi-agent Systems, Autonomous Agents Conference, 2001, pp. 46-53.

[65] G. Karjoth, *Secure mobile agent-based merchant brokering in distributed marketplaces*, Proceedings of the Joint Symposium on Agent Systems and Applications, Lecture Notes in Computer Science, Vol. 1882, Springer, 2000, pp. 44-56.

[66] G. Karjoth, D. Lange, and M. Oshima, *A security model for aglets*, IEEE Internet Computing **1** (1997), 68-77.

[67] J. Kilian and T. Leighton, *Fair cryptosystems, revisited*, Advances in Cryptology —EuroCrypt '95, Lecture Notes in Computer Science Vol. 963, Springer, 1995, pp. 208-220.

[68] H. Kim, J. Baek, B. Lee, and K. Kim, *Secret computation with secrets for mobile agent using one-time proxy signature*, Symposium on Cryptography and Information Security Vol 2/2, The Institute of Electronics, Information and Communication Engineers, January 2001, pp. 845-850.

[69] J. Kong, H. Luo, K. Xu, D. Gu, M. Gerla, and S. Lu, *Adaptive security for multilevel ad hoc networks*, Wireless Communications and Mobile Computing, Wiley Interscience Press **2** (2002), 533-547.

[70] P. Koponen, J. Rasanen, and O. Martikainen, *Calypso service architecture for broadband networks*, Proceedings of the 2nd IFIP Conference on Intelligent Networks and Intelligence in Networks, 1997, pp. 73–82.

[71] P. Kotzanikolaou, M. Burmester, and V. Chrissikopoulos, *Secure transactions with mobile agents in hostile environments*, Proceedings of 5th ACISP, Lecture Notes in Computer Science Vol. 1841, Springer, July 2000, pp. 289–297.

[72] ———, *Dynamic multi-signatures for secure autonomous agents*, Proceedings of DEXA'01 – Mobility of Database and Distrubuted Systems Workshop (Munich, Germany), IEEE, October 2001, pp. 582–586.

[73] P. Kotzanikolaou, M. Burmester, V. Chrissikopoulos, and C. Douligeris, *Role based access control policies in the mobile agent paradigm*, Informatik Forum, Special Issue on Mobile Agent Technology, accepted, August (2002).

[74] P. Kotzanikolaou, G. Katsirelos, and V. Chrissikopoulos, *Mobile agents for secure electronic transactions*, Recent Advances in Signal Processing and Communications, Proceedings of CSCC'99 (Athens, Greece), World Scientific and Engineering Society Press, June 1999, pp. 363–368.

[75] H. Krawczyk, *Simple forward-secure signatures for any signature scheme*, 7th ACM Conference on Computer and Communications Security, ACM, 2000, pp. 108–115.

[76] B. Lampson, M. Abadi, M. Burrows, and E. Wobber, *Authentication in distributed systems: Theory and practice*, ACM Trans. Comput. Syst. **10** (1992), no. 4, 265–310.

[77] U. Lang, *Corba security on the web. an overview*, Future Generation Computer Systems **16** (2000), no. 4, 417–421.

[78] B. Lee, H. Kim, and K. Kim, *Secure mobile agent using strong non-designated proxy signature*, Proceedings of ACISP 2001, Lecture Notes in Computer Science Vol. 2119, Springer, 2001, pp. 474–486.

[79] ———, *Strong proxy signatures and its applications*, Symposium on Cryptography and Information Security Vol 1/2, The Institute of Electronics, Information and Communication Engineers, January 2001, pp. 603–608.

[80] T. Li and K-Y. Lam, *A secure group solution for multi-agent EC system*, Proceedings of IPDPS2001 – International Parallel and Distributed Processing Symposium (San Francisco, California, USA), IEEE Computer Society, April 2001.

[81] J. Linn and M. Nystrom, *Attribute certification: An enabling technology for delegation and role-based controls in distributed environments*, Procceedings of ACM workshop on role-based access control (Fairfax, VA USA), ACM, October 1999.

[82] S. Loureiro and R. Molva, *Privacy for mobile code*, In proceedings of Distributed Object Security Workshop OOPSLA'99 (Denver), Springer, November 1999.

[83] Z. Maamar, H. Yahyaoui, and N. Sahlis, *Moving code vs. inviting code: What strategy should software agents follow?*, Informatik/Informatique,

Swiss Federation of Information Processing Societies. http://www.svifsi.ch/revue/pages/issues/n021/in021Mosaic.html **1** (2000).

[84] P. Maes, R. Guttman, and A. Moukas, *Agents that buy and sell*, Communications of the ACM **42** (1999), no. 3, 81–91.

[85] D. McGrew and A. Sherman, *Key establishment in large dynamic groups*, IEEE Transactions on Software Engineering, Submitted.

[86] A. Menezes, P. van Ooschort, and S. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.

[87] J. Merwe and S. H. Solms, *Electronic commerce with secure intelligent trade agents*, Proceedings of the ICICS'97, Lecture Notes in Computer Science, Vol. 1334, Springer, 1997, pp. 452–462.

[88] Microsoft, *Activex*, http://www.microsoft.com.

[89] Sun Microsystems, *Java programming language*, http://www.javasoft.com.

[90] C. Mitchell and N. Hur, *On the security of a structural proven signer ordering multisignature scheme*, Procceedings of the 6th IFIP TC6/TC11 Communications and Multimedia Security Conference, (Portoroz, Slovenia), Kluwer Academic Publishers, September 2002, pp. 1–8.

[91] S. Mitomi and A. Miyaji, *A multisignature scheme with message flexibility, order flexibility and order verifiability*, Procceedings of 5th ACISP, Lecture Notes in Computer Science Vol. 1841, Springer, July 2000, pp. 298–312.

[92] R. Montanari, C. Stefanelli, and N. Dulay, *Flexible security policies for mobile agent systems*, Elsevier Microprocessors and Microsystems **25** (2001), 93-99.

[93] M. Moses, *Agents in e-commerce*, Communications of the ACM **42** (1999), no. 3, 79-80.

[94] D. Naccache and J. Stern, *A new public-key cryptosystem*, Procceedings of Eurocrypt'97, Lecture Notes in Computer Science Vol. 1223, Springer, 1997, pp. 27-36.

[95] ObjectSpace, *Voyager*, http://www.objectspace.com/~products/voyager.

[96] T. Oguara, *Secure transaction between intelligent agents*, Research proposal, The Manchester Metropolitan University, Center for Agent Research and Development, Department of Computing and Mathematics, December 2000.

[97] OMG, *Corba 3*, http://www.omg.org/technology/corba/corba3releaseinfo.htm.

[98] ———, *Corba security service, version 1.7*, http://www.omg.org/technology/documents/formal/security_service.htm, 1999.

[99] K. Onbilger, R. Chow, and R. Newman, *Remote digital signing with mobile agents*, Proceedings of the 2nd International Workshop for Asia Public Key Infrastructure - IWAP2002, Taipei, October, 2002.

[100] S. Osborn, R. Sandhu, and Q. Munawer, *Configuring role-based access control to enforce mandatory and discretionary access control policies*, ACM Transactions on Information and System Security **3** (2000), no. 2, 85-106.

[101] E. Palmer, *An introduction to citadel - a secure crypto coprocessor for workstations*, Procceedings of IFIP/SEC'94, Kluwer Academic Publishers, 1994.

[102] I. Papadakis, V. Chrissikopoulos, and D. Polemi, *Secure web-based medical digital library architecture based on TTPs*, Proceedings of MIE2000, 2000, pp. 610-616.

[103] R. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, Communications of ACM **21** (1978), no. 2, 120-126.

[104] T. Sander and C. Tschudin, *Protecting mobile agents against malicious hosts*, Lecture Notes in Computer Science Vol. 1419, Springer, 1998, pp. 44-60.

[105] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, *Role-based access control models*, IEEE Computer **29** (1996), no. 2, 38-47.

[106] V. Shoup, *Practical threshold signatures*, In Proceedings of Eurocrypt 2000 Lecture Notes in Computer Science Vol. 1807, Springer, 2000, pp. 207-220.

[107] K. Shum and V.K. Wei, *A strong proxy signature scheme with proxy signer privacy protection*, Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, (WETICE"02), IEEE, 2002, pp. 55-57.

[108] V. Varadharajan, P. Allen, and S. Black, *An analysis of the proxy problem in distributed systems*, In Proceedings of 1991 IEEE Symposium on Research on Security and Privacy (USA), IEEE, 1991.

[109] G. Vigna, *Cryptographic traces for mobile agents*, Lecture Notes in Computer Science Vol. 1419, Springer, 1998, pp. 137-153.

[110] U.G. Wilhelm, *Cryptographically protected objects*, Technical Report, Ecole Polytechnique Federale de Lausanne, Switzerland, 1997.

[111] Wireless LAN Alliance, *The IEEE 802.11 wireless LAN standard*, http://www.wlana.com, 1999.

[112] D. Wong, N. Paciorek, and D. Moore, *Java-based mobile agents*, Communications of the ACM **42** (1999), no. 3, 92-102.

[113] A.C. Yao, *How to generate and exchange secrets*, Procceedings of the 27th FOCS, 1986, pp. 162-167.

[114] X. Yi, X. F. Wang, and K. Y. Lam, *A secure intelligent trade agent system*, Procceedings of the International IFIPGI Working Conference, TREC'98, Lecture Notes in Computer Science Vol. 1402, Springer, 1998, pp. 218-228.

[115] A. Young and M. Yung, *Encryption tools for mobile agents: Sliding encryption*, In proceedings of FSE'97, Lecture Notes in Computer Science Vol. 1267, Springer, 1997, pp. 230-241.

[116] M. Zapf, H. Muller, and K. Geiths, *Security requirements for mobile agents in electronic marketplaces*, Procceedings of the International IFIPGI Working Conference, TREC'98, Lecture Notes in Computer Science Vol. 1402, Springer, 1998, pp. 205-217.

[117] M. Zhang, A. Karmouch, and R. Impey, *Adding security features to fipa agent platforms*, The Security WG at the 23rd FIPA - Pleasanton (London, UK), October 2001.

[118] ———, *Towards a secure agent platform based on fipa*, Proceedings of the Mobile Agents for Telecommunication Applications Workshop - MATA 2001, Lecture Notes in Computer Science Vol. 2164 (Montreal, Canada), Springer, August 2001, pp. 277-289.

[119] L. Zhou and Z. Haas, *Securing ad hoc networks*, IEEE Network Magazine **13** (1999), no. 6, 24-30.