ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής

Διασφάλιση Ιδιωτικότητας σε Προσωπικά Δίκτυα με Επίγνωση Κατάστασης

Διδακτορική Διατριβή

του

Δημητρίου Μ. Κυριαζάνου

Διπλωματούχου Ηλεκτρολόγου Μηχανικού και Μηχανικού Υπολογιστών
του Εθνικού Μετσόβιου Πολυτεχνείου

Αθήνα, Ιούλιος 2009

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Τομέας Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής

Διασφάλιση Ιδιωτικότητας σε Προσωπικά Δίκτυα με Επίγνωση Κατάστασης

Διδακτορική Διατριβή

του

Δημητρίου Μ. Κυριαζάνου

Διπλωματούχου Ηλεκτρολόγου Μηχανικού και Μηχανικού Υπολογιστών
του Εθνικού Μετσόβιου Πολυτεχνείου

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 17η Ιουλίου 2009.

Γ. Στασινόπουλος Καθηγητής Ε.Μ.Π.	Μ. Θεολόγου Καθηγητής Ε.Μ.Π.	Ε. Συκάς Καθηγητής Ε.Μ.Π.
Ε. Πρωτονοτάριος Καθηγητής Ε.Μ.Π.	Π. Τσανάκας Καθηγητής Ε.Μ.Π.	Β. Λούμος Καθηγητής Ε.Μ.Π.
	Δ. Ρείσης Αν. Καθηγητής Ε.Κ.Π.Α.	

Αθήνα, Ιούλιος 2009

.....

Δημήτριος Μ. Κυριαζάνος

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Αθήνα, Ιούλιος 2009

Με την ολοκλήρωση της διδακτορικής μου διατριβής, σηματοδοτείται το ευτυχές τέλος μιας δεκαετούς πορείας μου στο Ε.Μ.Π., αρχικά ως φοιτητής, μετέπειτα ως συνεργαζόμενος ερευνητής μηχανικός και από το 2005 και έπειτα, και ως υποψήφιος διδάκτωρ. Κοιτάζοντας πίσω τα χρόνια που πέρασαν χαίρομαι ιδιαίτερα για τις επιλογές που έκανα και για τη παραμονή μου στο κορυφαίο τεχνικό εκπαιδευτικό ίδρυμα της χώρας, καθώς είχα την ευκαιρία να καλλιεργήσω τη τέχνη του μηχανικού μέχρι το ανώτατο εκπαιδευτικό επίπεδο, δίπλα σε κορυφαίους καθηγητές του χώρου, να συνεργαστώ με τα πλέον δυνατά τεχνικά μυαλά και να αποκομίσω μοναδικές εμπειρίες και εφόδια που θα με ακολουθούν στο υπόλοιπο της ζωής μου.

Η επιλογή θέματος της διατριβής δεν προέκυψε απλώς τυχαία στη πορεία ούτε έγινε στα πλαίσια ανάθεσης θέματος. Για μένα η ιδιωτικότητα εκφράζει την αξιοπρέπεια που οφείλει να κρατήσει ο άνθρωπος μπροστά στην συνεχώς εξελισσόμενη, φαινομενικά παντοδύναμη αλλά και απρόσωπη συχνά τεχνολογία. Είναι το δικαίωμα να κρατηθεί η ανθρωπιά μας και να μην ξεπέσουμε στις ζοφερές προοπτικές ενός συστήματος που προσφέροντας μας όμορφα Κουτιά της Πανδώρας, θα μας στερεί την ελευθερία και θα μας ακρωτηριάζει το ανθρώπινο πνεύμα και θέληση. Επέλεξα ως περιβάλλον έρευνας τα Προσωπικά Δίκτυα καθώς εξορισμού αποτελούν την πρόταση για στροφή σε ανθρωποκεντρική σχεδίαση και σε τεχνολογίες που υποκλίνονται στον άνθρωπο, και όχι αντιστρόφως. Παραδίδω τη διατριβή μου έχοντας την ικανοποίηση ότι η έρευνα μου υπηρέτησε ως όφειλε τον άνθρωπο, όπως με έμαθαν ότι οφείλει να υπηρετεί από τη πρώτη μέρα στο Ε.Μ.Π. οι καθηγητές μου.

Θα ήθελα σε αυτό το σημείο να ευχαριστήσω εκ βάθους καρδιάς:

τον Καθηγητή Ε.Μ.Π. Ε. Πρωτονοτάριο για τις ευκαιρίες που μου έδωσε με τη συμμετοχή μου σε πλέον καινοτόμα πανευρωπαϊκά ερευνητικά προγράμματα, καθώς και για τη σοφή καθοδήγηση και διδασκαλία του αυτά τα χρόνια. Νιώθω ιδιαίτερη τιμή αλλά και εξαιρετικά τυχερός που είχα την ευκαιρία να μάθω τόσα πράγματα από μια κορυφαία προσωπικότητα του χώρου.

τον καθηγητή Ε.Μ.Π. Γ. Στασινόπουλο για την ισχυρή υποστήριξη του έργου της διδακτορικής μου διατριβής ως επιβλέπων καθηγητής μου. Πέραν της θερμής του καθοδήγησης, είμαι ευγνώμων στο καθηγητή γιατί από τη πρώτη μέρα γνωριμίας μας με ενέπνευσε για τις αρχές της ελευθερίας του πνεύματος και του ανθρωπισμού που πρέπει να διακρίνει έναν μηχανικό. Σε πολλά θέματα τολμώ να πω ότι ακολουθώ το παράδειγμα του.

τον Δρ. Ε.Μ.Π. Χ. Πατρικάκη, για την πολύτιμη συμβολή του στην έρευνα μου, τις ατελείωτες ώρες brainstorming αλλά και τη φιλική του υποστήριξη.

τους συναδέλφους με τους οποίους συνεργάστηκα στα πλαίσια των ευρωπαϊκών προγραμμάτων και ιδιαιτέρως το consortium του ευρωπαϊκού προγράμματος MAGNET. Ειδικότερα, θα ήθελα να ευχαριστήσω του καθηγητές του πανεπιστημίου του Aalborg Δανίας, Ramjee Prasad και Neeli Prasad, για τη γνώση που μοιράστηκαν μαζί μου αλλά και την ειλικρινή υποστήριξη τους.

τους συναδέλφους μου στο Ε.Μ.Π. και ειδικότερα τα «παιδιά του Telecom», για τις ωραίες στιγμές που ζήσαμε στα πλαίσια είτε της εργασίας, είτε της διασκέδασης.

την αδερφή μου Αλίκη γιατί είναι πάντα εκεί για μένα όταν τη χρειάζομαι.

Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου, Μιχάλη και Ελισάβετ γιατί με αγαπάνε και με στηρίζουν άνευ όρων σε όλη τη ζωή μου. Ό,τι είμαι το χρωστάω σε αυτούς και για αυτό τους αφιερώνω τη διατριβή μου.

Δημήτρης Μ. Κυριαζάνος

Περίληψη διατριβής

Η διατριβή πραγματεύεται την διασφάλιση της ιδιωτικότητας σε Προσωπικά Δίκτυα με επίγνωση κατάστασης. Αρχικά αναλύονται το περιβάλλον εφαρμογής, οι γενικές αλλά και ειδικές απαιτήσεις ασφαλείας και ιδιωτικότητας, με βάση τα σενάρια χρήσης Προσωπικών Δικτύων και συνασπισμών Προσωπικών Δικτύων. Η προσέγγιση αυτή αρμόζει στα πλαίσια του ανθρωποκεντρικού χαρακτήρα και σχεδίασης που διέπουν αυτά τα δίκτυα. Στη συνέχεια εξετάζεται τί πρέπει να προστατευτεί, από τί απειλείται και ποιες είναι οι υπάρχουσες λύσεις αλλά και προτάσεις της έρευνας σχετικά. Για το σκοπό αυτό πραγματοποιήθηκε εκτενής βιβλιογραφική μελέτη εστιασμένη στις ασύρματες προσωπικές επικοινωνίες για τεχνικές, τεχνολογίες και λύσεις σχετικά με: την προστασία της ηλεκτρονικής ταυτότητας και την υποστήριξη της ανωνυμίας (λύσεις Freedom, Anonymizer, Freenet κ.α.), την προστασία και την χρήση της προσωπικής πληροφορίας και πληροφορίας επίγνωσης κατάστασης στην ασφάλεια εφαρμογών και υπηρεσιών αλλά και στον έλεγχο πρόσβασης ειδικότερα (PBAC, RBAC, DRBAC, GRBAC μοντέλα κ.α.) καθώς και την ανάλυση απειλών και την επακόλουθη μέτρηση και αξιολόγηση παραμέτρων ασφαλείας του συστήματος (Swiderski-Snyder, Network Modelling, PTA Threat analysis κ.α.).

Με αυτές τις βάσεις, προτείνεται αρχικά ο μηχανισμός εγκαθίδρυσης σχέσεων εμπιστοσύνης με ανώνυμη και ασφαλή ανταλλαγή πληροφοριών που βασίζεται στη καινοτόμο πρόταση διαχωρισμού των πληροφοριών ταυτοποίησης από τις υπόλοιπες προσωπικές πληροφορίες. Στη συνέχεια, παρουσιάζεται η ολοκληρωμένη πρόταση διαχείρισης ασφάλειας και προστασίας της πληροφορίας με επίγνωση κατάστασης, μαζί με το καινοτόμο μοντέλο πληροφορίας ασφαλείας που χρησιμοποιεί και το οποίο ενσωματώνει δυναμικούς κανόνες τόσο για τη πληροφορία προφίλ αλλά και τη συγκείμενη πληροφορία και κατάστασης δικτύου. Τέλος, προτείνεται η μεθοδολογία ανάλυσης απειλών για αξιολόγηση και σχεδίαση ενίσχυσης ασφάλειας στα Προσωπικά Δίκτυα, με έμφαση στον ανθρωποκεντρικό χαρακτήρα του συστήματος. Η μεθοδολογία υιοθετεί μια ολιστική προσέγγιση αξιολόγησης καθώς προτείνεται μια νέα προσέγγιση αποδόμησης και ανάλυσης του συστήματος. Στη συνέχεια προτείνεται και ένα πρότυπο μετρικό σύστημα βαθμολόγησης και ιεράρχησης των απειλών.

Τέλος, εξάγονται τα συμπεράσματα τις διατριβής καθώς και οι προοπτικές για μελλοντικές επεκτάσεις, με έμφαση στην ανάγκη για προτυποποίηση.

Πίνακας Περιεχομένων

Λίστα Εικόνων

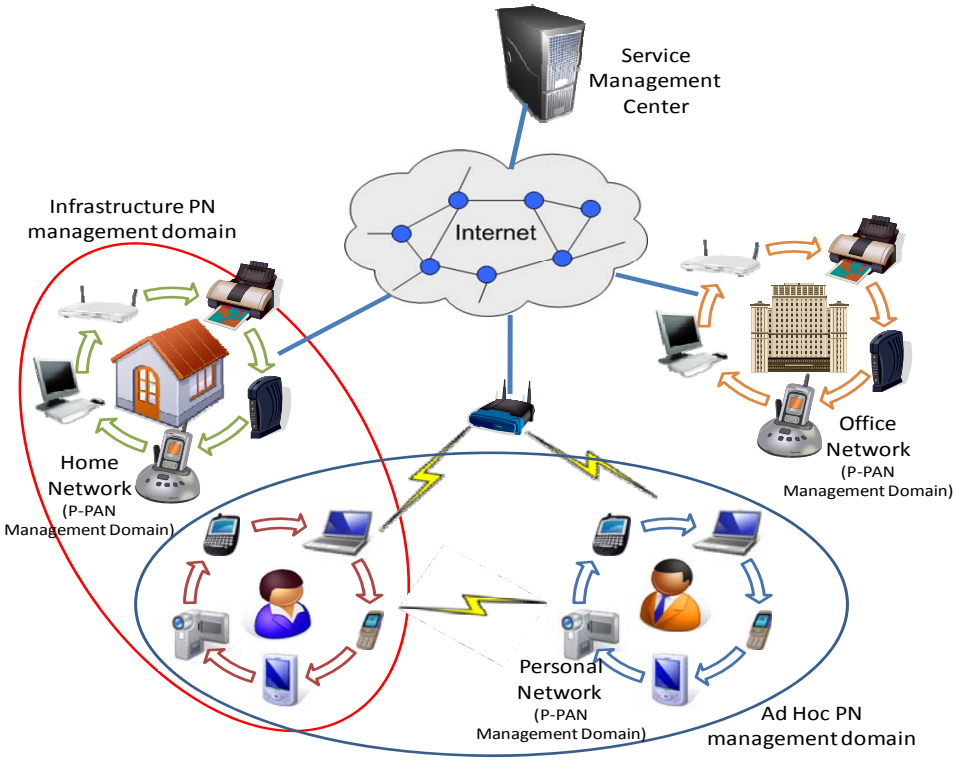
Λίστα Πινάκων

1. Εισαγωγή

Τα συστήματα πανταχού παρόντος και διεισδυτικού υπολογιστή εξελίχθησαν πολύ τα τελευταία χρόνια, καθώς οι τεχνολογίες ασύρματων και κινητών επικοινωνιών προχωρούν: άνθρωποι στη καθημερινή τους ζωή κινούνται φορώντας και φέροντας συσκευές που αλληλεπιδρούν ανεπαίσθητα με το περιβάλλον και τα περιβάλλοντα ασύρματα δίκτυα με χρήση διάφορων ραδιοτεχνολογιών. Από αυτή την εξέλιξη μια κατεύθυνση της έρευνας υιοθέτησε μια ανθρωποκεντρική προσέγγιση στις προκλήσεις και ευκαιρίες που προέκυψαν. Ως αποτέλεσμα, η έννοια του Προσωπικού Δικτύου (Personal Network – PN) άρχισε να υλοποιείται ως ο τρόπος ομογενοποίησης ενός συνόλου από διάφορα ετερογενή δίκτυα σε ένα υπερκείμενο δίκτυο γύρω από το χρήστη, πάνω στο οποίο νέες υπηρεσίες και εφαρμογές θα μπορούν να παρέχονται αδιάκοπα και οπουδήποτε μέσα στο δίκτυο. Παραδείγματα τέτοιων επιμέρους ετερογενών δικτύων είναι το «έξυπνο» σπίτι, το δίκτυο του γραφείου και το «έξυπνο» αυτοκίνητο.

Στα τελευταία δύο χρόνια, ιδιαίτερη πρόοδος έχει επιτευχθεί στον τομέα των PNs, και πλέον μια λειτουργική πρωτότυπη πλατφόρμα ήδη έχει αναπτυχθεί στα πλαίσια των ευρωπαϊκών ερευνητικών προγραμμάτων MAGNET και MAGNET Beyond. Παρατηρώντας την φυσική μορφή ενός PN στην Εικόνα 1, έχουμε καταρχήν την δυναμική συλλογή από προσωπικούς κόμβους και συσκευές γύρω από τον χρήστη, οι οποίες σχηματίζουν την «φούσκα» γύρω από το χρήστη γνωστή ως Ιδιωτικό Προσωπικό Δίκτυο (Private Personal Area Network - P-PAN). Επιπλέον, οι απομακρυσμένοι κόμβοι και συσκευές οργανωμένες σε διαφορετικές συστοιχίες (π.χ. συστοιχία σπιτιού, γραφείου) οι οποίες συνδέονται μεταξύ τους είτε μέσω δίκτυα υποδομής, όπως π.χ. μέσω του Διαδίκτυο στη πιο δημοφιλή περίπτωση ή και μέσω δικτύων κινητών τηλεπικοινωνιών, είτε συνδέονται απευθείας μεταξύ τους με αυτοργανούμενο τρόπο, όταν αυτό είναι δυνατό.

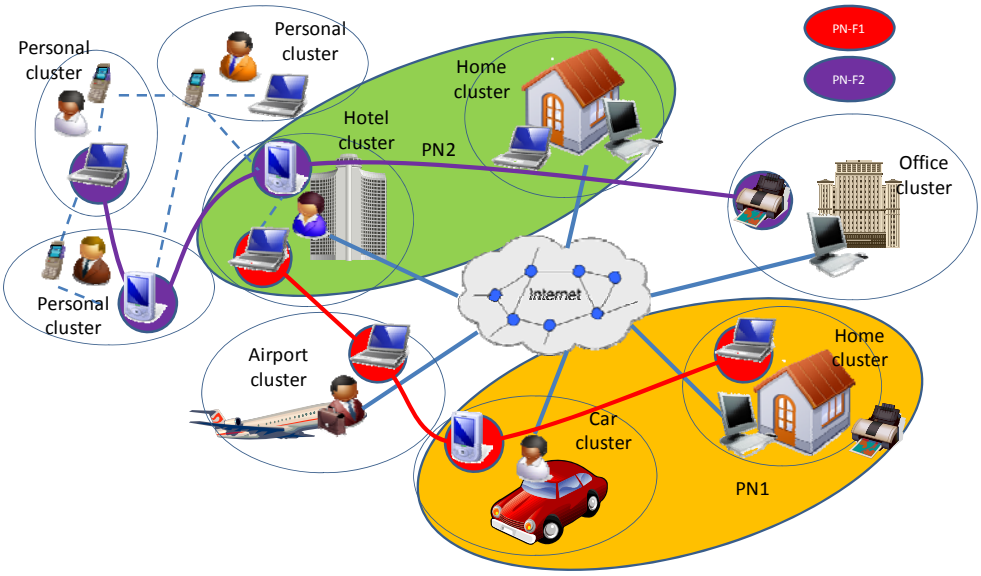
Ακολουθώντας τις απαιτήσεις χρήστη για απλή καθημερινή επικοινωνία, ή και μακροπρόθεσμη συνεργασία με άλλου χρήστες, πρόσφατα ξεκίνησε η έρευνα και η ανάπτυξη πάνω στις Συνομοσπονδίες Προσωπικών Δικτύων (PN Federation – PN-F). Το πρωτότυπο PN-F υλοποιήθηκε ως η διασύνδεση διανεμημένων PNs (Εικόνα 2), είτε επεκτείνοντας τους υπάρχοντες μηχανισμούς και στοιχεία είτε παρέχοντας καινούργιους, ώστε να αντιμετωπιστούν η αυξημένη πολυπλοκότητα του συστήματος και οι νέες προκλήσεις στην διευθυνσιοδότηση, συνδεσιμότητα, ασφάλεια, διαχείριση πολιτικών ασφαλείας του δικτύου κ.α.



Εικόνα 1. Η φυσική μορφή ενός Προσωπικού Δικτύου

Ειδικότερα, το θέμα της ασφάλειας στα PNs αποτελεί πρόκληση για την έρευνα για τους εξής βασικούς και ιδιαίτερους λόγους:

- Τα PNs εξ' ορισμού εμπεριέχουν ευαίσθητα και πολύτιμα προσωπικά δεδομένα, όπως π.χ. ηλεκτρονικές ταυτότητες, αριθμούς πιστωτικών καρτών, πληροφορίες υγείας και άλλες πληροφορίες. Όντας υψηλά προσωποποιημένα, κάθε επίθεση στο δίκτυο απειλεί άμεσα την ηλεκτρονική ταυτότητα του προσώπου με το οποίο συνδέεται το δίκτυο.
- Οι προσωπικές πληροφορίες υπάρχουν προκειμένου ο χρήστης να επωφεληθεί από υψηλά προσωποποιημένες υπηρεσίες και εφαρμογές. Η χρήση της πληροφορίας όμως την καθιστά στόχο για επιθέσεις κατά του απορρήτου και της ιδιωτικότητας.
- Καθότι αποτελούνται από διανεμημένα αλληλοσυνδεόμενα δίκτυα, πολύπλοκες κετρικοποιημένες υποδομές και αρχιτεκτονικές δεν μπορούν να θεωρηθούν διαθέσιμες ανά πάσα στιγμή και ομότιμες αρχιτεκτονικές και μηχανισμοί θα πρέπει να είναι διαθέσιμοι είτε ως κύριοι μηχανισμοί είτε εναλλακτικά.
- Τα PNs αναμένονται να είναι όσο το δυνατόν φιλικά προς το χρήστη, με υψηλές δυνατότητες προσωποποίησης αλλά και συγχρόνως αυτόνομα. Με αυτή την έννοια δεν θα πρέπει να θέτουν πολύπλοκα καθήκοντα διαχείρισης ασφαλείας στους απλούς καθημερινούς χρήστες τους.



Εικόνα 2. Η φυσική μορφή ενός Συνασπισμού Προσωπικών Δικτύων

1.1. Πεδίο Ενδιαφέροντος

Είναι προφανές από την εισαγωγή ό,τι η ασφάλεια είναι ένα ιδιαίτερο θέμα για τα Προσωπικά Δίκτυα. Επιπλέον, η προστασία της διαχειριζόμενης προσωπικής πληροφορίας αποτελεί το σημείο στο οποίο στηρίζονται όλες οι προσωποποιημένες εφαρμογές και υπηρεσίες. Σε αυτά τα πλαίσια το πεδίο ενδιαφέροντος της διατριβής αποτελεί η ασφάλεια ευρύτερα και διασφάλιση της ιδιωτικότητας στα Προσωπικά Δίκτυα ειδικότερα.

Όπως και για την ασφάλεια του κάθε συστήματος έτσι και για την ιδιωτικότητα απαιτούνται μηχανισμοί ασφαλείας από άκρο σε άκρο και σε όλα τα επίπεδα των Προσωπικών Δικτύων. Σε αυτό το πλαίσιο, ενδιαφέρον της διατριβής ήταν η εξέταση και ανάλυση ασφαλείας των Προσωπικών Δικτύων στο σύνολο και η συμπλήρωση των κενών ασφαλείας άφηναν οι υπάρχουσες υποδομές ασφαλείας όπως π.χ. οι τεχνολογίες Εικονικών Ιδιωτικών Δικτύων (Virtual Private Network – VPN), καθώς και των σχετικών μεθόδων μέτρησης απόδοσης συστημάτων ασφαλείας αλλά και ανάλυσης απειλών.

Επιπλέον, οι πλούσιες σε πληροφορίες προσωπικών δεδομένων και δεδομένων επίγνωσης καταστάσεις εφαρμογές, μπορεί να δημιουργούν πονοκέφαλο στους ειδικούς ασφαλείας, αλλά προσφέρουν μεγάλες δυνατότητες και εξυπηρέτηση στους χρήστες. Η σωστή διαχείριση αυτών τον πληροφοριών και η σωστή διάθεση τους αποτελεί ένα επιπλέον ενδιαφέρων στόχο, στόχος που απαιτεί μηχανισμούς πανταχού ελέγχου πρόσβασης και επιβολής σωστών πολιτικών ασφαλείας.

Τέλος, μια ευαίσθητη και ευάλωτη φάση για την ασφάλεια αποτελεί η επέκταση της εμπιστοσύνης σε νέους χρήστες, και η αρχική ανταλλαγή πληροφοριών με αυτούς. Η εγκαθίδρυση σχέσεων εμπιστοσύνης αλλά και γενικότερα η τήρηση της ανωνυμίας αλλά και η απεμπλοκή της ταυτότητας από πληροφορίες απαραίτητες στις σχετικές εφαρμογές είναι λοιπόν ένα επιπλέον πεδίο ενδιαφέροντος.

1.2. Κίνητρα και Σκοποί

Εφαλτήριο για την εκπόνηση της διατριβής αποτέλεσε η ενασχόληση με το IST FP6-IP MAGNET & MAGNET Beyond Project (2004-2008). Το ερευνητικό αυτό πρόγραμμα είχε ως στόχο την ανάπτυξη ολοκληρωμένης πρωτότυπης πλατφόρμας προσωπικού δικτύου και συνασπισμού προσωπικού δικτύου.

Κατά την διάρκεια του προαναφερθέντος προγράμματος, είχα την ευκαιρία να ασχοληθώ ως μέλος του τομέα της ασφάλειας του έργου με την σχεδίαση ασφάλειας σε όλα τα επίπεδα και από άκρη σε άκρη του δικτύου. Διετέλεσα δε και στη δεύτερη φάση του έργου επικεφαλής της ομάδας έργου «Ιδιωτικότητα και εμπιστοσύνη».

Είχα λοιπόν την ευκαιρία να διαπιστώσω τα εξής, που αποτέλεσαν κίνητρα για την διατριβή:

- Τα Προσωπικά Δίκτυα κρατάνε πολύτιμα «περιουσιακά στοιχεία»: η ηλεκτρονική ταυτότητα, προσωπικά δεδομένα και εμπιστευτικές πληροφορίες με μεγάλη υλική ή ψυχική αξία
- Οι προσωποκεντρικές εφαρμογές με επίγνωση κατάστασης προσφέρουν νέες δυνατότητες αλλά εγκυμονούν και νέες απειλές
- Η επίδραση του ανθρώπινου παράγοντα και οι προσωπικές προτιμήσεις δεν λαμβάνονται υπόψη σε ικανοποιητικό βαθμό στην ασφάλεια, όπως δείχνουν οι σχετικές αναλύσεις απειλών
- Υπάρχουσες λύσεις βασίζονται σε τεχνολογίες εικονικών ιδιωτικών δικτύων (Virtual Private Network – VPN) ή/και σε υποδομές δημοσίου κλειδιού (Public Key Infrastructure – PKI)
    - Οι VPN τεχνολογίες δεν αντιμετωπίζουν απειλές σε επίπεδο εφαρμογής και χρήστη, και τον ανθρώπινο παράγοντα γενικότερα
    - Το PKI έχει έλλειψη σε εργαλεία εγκαθίδρυσης εμπιστοσύνης με μηδενική αρχική γνώση καθώς και σε εργαλεία διασφάλισης ιδιωτικότητας για προσωπικές εφαρμογές με επίγνωση κατάστασης

Το αποτέλεσμα αυτών των κινητήριων συλλογισμών ήταν οι ιδέες, οι τεχνικές και οι ολοκληρωμένες λύσεις διασφάλισης της ιδιωτικότητας που προτείνονται στην παρούσα διατριβή. Πιο συγκεκριμένα η διατριβή στόχευσε καταρχήν στην διασφάλιση της ιδιωτικότητας κατά την αρχικοποίηση σχέσεων εμπιστοσύνης με νέους χρήστες με χρήση ανωνυμίας, ασφαλούς μεταφοράς και διαχωρισμού προσωπικής πληροφορίας από την ταυτότητα. Στη συνέχεια, στοχεύθηκε η προστασία της ιδιωτικότητας κατά την χρήση υπηρεσιών και εφαρμογών στη φυσιολογική λειτουργία του δικτύου βάσει ενός πανταχού παρόντος ολοκληρωμένου συστήματος διασφάλισης προσωπικής και συγκείμενης πληροφορίας. Παράλληλα, κάθε νέα και πρωτότυπη ιδέα προήλθε από τη σωστή αξιολόγηση και μέτρηση της απόδοσης ασφαλείας του Προσωπικού Δικτύου. Καθότι δε η σωστή μέτρηση της ασφάλειας αποτελεί πρόκληση για την έρευνα, αποτέλεσε και αυτή στόχο της διατριβής, έχοντας ως αποτέλεσμα τη πρόταση της σχετικής μεθοδολογίας αξιολόγησης ασφαλείας.

1.3. Καινοτομικά Στοιχεία

Ο καινοτομικός χαρακτήρας της διατριβής βασίζεται σε τρείς κύριους άξονες:

- **Δημιουργία σχέσεων εμπιστοσύνης με χρήση ανωνυμίας και απόρρητη μεταφορά πληροφορίας:**

  Η πρόταση βασίζεται στο καινοτόμο διαχωρισμό της ταυτότητας του χρήστη από τις προσωπικές του προτιμήσεις και τις λοιπές πληροφορίες όπως πληροφορίες κατάστασης. Αυτό επιτυγχάνεται με επιλεκτική κρυπτογράφηση μερών του προφίλ χρήστη και κατάλληλη διανομή κλειδιών, έτσι ώστε ανά πάσα στιγμή καμία οντότητα μέσα στο δίκτυο να μην είναι σε θέση να συνδέσει κάποιο αποκρυπτογραφημένο προφίλ με την αντίστοιχη ταυτότητα ή αντιστρόφως. Με αυτό το τρόπο μεταφέρεται απόρρητα η πληροφορία ως προς έναν τρίτο εξυπηρετητή, η οποία καταλήγει ως ανώνυμη στον τελικό αποδέκτη. Ως αποτέλεσμα μεταφέρεται γνώση χωρίς προσβολή της ιδιωτικότητας, πράγμα χρήσιμο σε καταστάσεις μηδενικής αρχικής γνώσης όπως π.χ. στη δημιουργία σχέσεων εμπιστοσύνης.

- **Ολοκληρωμένη διαχείρισης ασφάλειας και προστασία της πληροφορίας με επίγνωση κατάστασης:**

  Η πρόταση για μια ολοκληρωμένη πλατφόρμα η οποία εμπεριέχει ένα σύνολο ιδεών και τεχνικών ώστε να διασφαλίζεται στο περιβάλλον του προσωπικού δικτύου η προσωπική και συγκείμενη πληροφορία κατά τη χρήση εφαρμογών και υπηρεσιών. Εμπεριέχει ένα σύστημα ομότιμων σημείων εφαρμογής πολιτικών ασφαλείας, οι οποίες όντας διασυνδεδεμένες σε όλο το προσωπικό δίκτυο, παρέχεται πλήρη κάλυψη σε όλο το δίκτυο. Βασίζεται σε ανοιχτές τεχνολογίες και πρότυπα καθώς και τεχνολογίες XML, επιτρέποντας δυναμική εφαρμογή νέων πολιτικών και επεκτασιμότητα ενώ παρέχει μια ενιαία διεπαφή για όλες τις εφαρμογές και υπηρεσίες που χρησιμοποιούν προσωπικά δεδομένα και συγκείμενες πληροφορίες, διευκολύνοντας την ενσωμάτωση των εφαρμογών αυτών στο σύστημα. Έχει επίγνωση κατάστασης, οι οποίες, χωριζόμενες σε τρία επίπεδα ασφαλείας (Χαμηλό, Μέσο, Υψηλό) οδηγούν και σε δυναμική εφαρμογή διαφορετικού συνόλου πολιτικών ασφαλείας, προωθώντας την αυτοργάνωση και αυτοδιαχείριση της ασφάλειας και απαλλάσσοντας τον χρήστη από το δύσκολο διαχειριστικά έργο. Υποστηρίζει δε το προαναφερθέν μηχανισμό ανωνυμίας, φροντίζοντας ώστε η πληροφορία που δημοσιεύεται να μην οδηγεί σε άμεση ή έμμεση αποκάλυψη της ταυτότητας.

- **Αξιολόγηση ασφαλείας με έμφαση στον ανθρώπινο παράγοντα και ολική μοντελοποίηση της ασφάλειας του συστήματος με συνδυασμένη χρήση Δένδρων Επίθεσης και ανοιχτού πρότυπου αξιολόγησης απειλών (CVSS):**

  Η συγκεκριμένη πρόταση συνδυάζει μια δομημένη ολιστική άποψη του πλαισίου ασφαλείας, που να εμπεριέχει όλα τα τρωτά σημεία του συστήματος, τις σχέσεις μεταξύ τους και την αλληλεπίδραση με τους μηχανισμούς ασφαλείας, αν υπάρχουν με μια πρότυπη μέθοδος μέτρησης που να εκφράζει τη σοβαρότητα και το ρίσκο κάθε τρωτού σημείου, και επομένως την σημασία και τις πιθανότητες επιτυχίας της σχετικής απειλής. Προτείνεται μια νέα προσέγγιση αποδόμησης και ανάλυσης του συστήματος βασισμένη σε UML διαγράμματα περιπτώσεων χρήσης και ακολουθιών και ανάλυση σε περιγραφικούς πίνακες. Συνδέοντας το μοντέλο απειλών με την ανάλυση κινδύνων, προτείνεται συνδυασμός χρήσης των Δένδρων Επίθεσης του Bruce Schneier και του ανοιχτού προτύπου για βαθμολόγηση κοινών τρωτών σημείων (Common Vulnerability

Scoring System - CVSS) μέσω μιας μεθοδολογίας έτσι ώστε να καλύπτεται ο ανθρώπινος παράγοντας και να υποστηρίζονται επιθέσεις σε περισσότερα βήματα.

1.4. Δομή της Διατριβής

Η διατριβή απαρτίζεται από 7 κεφάλαια τα οποία δομούνται ως εξής:

Στο κεφάλαιο 1 παρουσιάζεται η εισαγωγή στο αντικείμενο της διατριβής, το πεδίο ενδιαφέροντος, τα κίνητρα και οι σκοποί καθώς και μια συνοπτική περιγραφή του καινοτομικού χαρακτήρα όπως αυτός χωρίζεται σε τρεις βασικούς άξονες.

Στο κεφάλαιο 2 παρουσιάζεται σύντομη επίδειξη του πρωτότυπου προσωπικού δικτύου το οποίο αναπτύχθηκε στα πλαίσια του προγράμματος MAGNET αποτέλεσε τη βάση για τις προτάσεις που παρουσιάζονται σε αυτή τη διατριβή.

Στο κεφάλαιο 3 αναλύονται οι γενικές αλλά και ειδικές απαιτήσεις ασφαλείας και ιδιωτικότητας, με βάση τα σενάρια χρήσης Προσωπικών Δικτύων και συνασπισμών Προσωπικών Δικτύων. Η προσέγγιση αυτή αρμόζει στα πλαίσια του ανθρωποκεντρικού χαρακτήρα και σχεδίασης που διέπουν αυτά τα δίκτυα. Στη συνέχεια εξετάζεται τί πρέπει να προστατευτεί, από τί απειλείται και ποιες είναι οι υπάρχουσες λύσεις αλλά και προτάσεις της έρευνας σχετικά.

Στο κεφάλαιο 4 παρουσιάζεται ο μηχανισμός εγκαθίδρυσης σχέσεων εμπιστοσύνης με ανώνυμη και ασφαλή ανταλλαγή πληροφοριών που βασίζεται στη καινοτόμο πρόταση διαχωρισμού των πληροφοριών ταυτοποίησης από τις υπόλοιπες προσωπικές πληροφορίες.

Στο κεφάλαιο 5 παρουσιάζεται η ολοκληρωμένη πρόταση διαχείρισης ασφάλειας και προστασίας της πληροφορίας με επίγνωση κατάστασης, μαζί με το καινοτόμο μοντέλο πληροφορίας ασφαλείας που χρησιμοποιεί και το οποίο ενσωματώνει δυναμικούς κανόνες τόσο για τη πληροφορία προφίλ αλλά και τη συγκείμενη πληροφορία και κατάστασης δικτύου.

Στο κεφάλαιο 6 παρουσιάζεται η μεθοδολογία ανάλυσης απειλών για αξιολόγηση και σχεδίαση ενίσχυσης ασφάλειας στα Προσωπικά Δίκτυα, με έμφαση στον ανθρωποκεντρικό χαρακτήρα του συστήματος. Η μεθοδολογία υιοθετεί μια ολιστική προσέγγιση αξιολόγησης καθώς προτείνεται μια νέα προσέγγιση αποδόμησης και ανάλυσης του συστήματος. Στη συνέχεια προτείνεται και ένα πρότυπο μετρικό σύστημα βαθμολόγησης και ιεράρχησης των απειλών.

Τέλος, η διατριβή καταλήγει στα συμπεράσματα και τις προοπτικές για μελλοντικές επεκτάσεις στο κεφάλαιο 7.

2. Το Πρωτότυπο Προσωπικού Δικτύου MAGNET

2.1. Εισαγωγή

Σε αυτό το κεφάλαιο παρουσιάζεται το πρωτότυπο προσωπικού δικτύου [6] το οποίο αποτέλεσε τη βάση για τις προτάσεις που παρουσιάζονται σε αυτή τη διατριβή. Πρόκειται για το προϊόν του προγράμματος MAGNET (Φάση Ι) πάνω στο οποίο αναπτύχθηκαν όλες οι επεκτάσεις σχετικά με τη συνομοσπονδία Προσωπικών Δικτύων. Υπήρξα ο κύριος συντελεστής στη σχεδίαση και ανάπτυξη των μηχανισμών ελέγχου πρόσβασης του πρωτοτύπου και οι προκλήσεις που προέκυψαν με την είσοδο της έννοιας της συνομοσπονδίας Προσωπικών Δικτύων κατά τη δεύτερη φάση του προγράμματος αποτέλεσε και το εφαλτήριο του διδακτορικού μου το 2005-2006. Αρχικά παρουσιάζονται συνοπτικά τα ερευνητικά προγράμματα και μετά ακολουθεί μια σύντομη επίδειξη της πλατφόρμας, με στόχο την καλύτερη κατανόηση του πως λειτουργεί τελικά ένα προσωπικό δίκτυο και ειδικότερα πως επιλύονται θέματα σχηματισμού και εγγραφής συσκευών, δικτύωσης, υπηρεσιών και ασφάλειας.

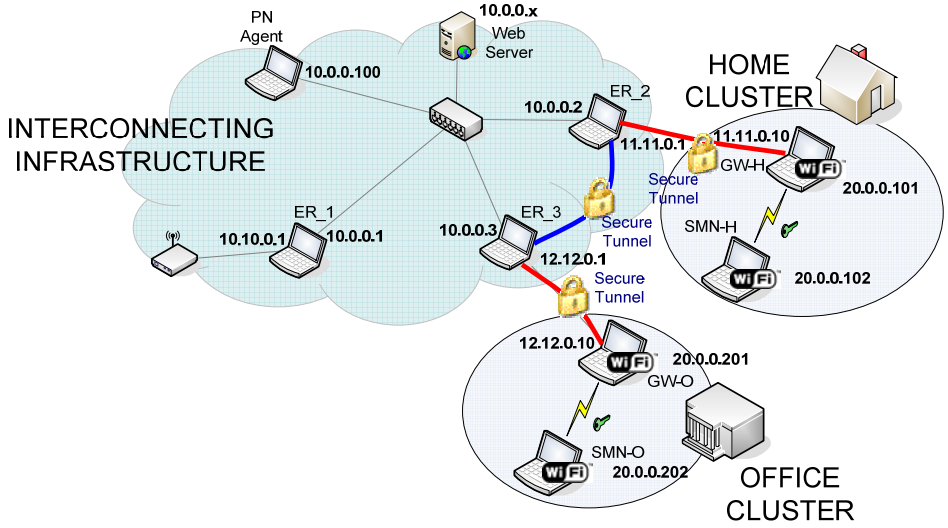
2.2. Τα ερευνητικά προγράμματα MAGNET & MAGNET Beyond

Τα MAGNET & MAGNET Beyond (Φάση Ι & Φάση ΙΙ) [1] ήταν Ολοκληρωμένα Προγράμματα (*Integrated Project -IP*) που υποστηρίχτηκαν από το 6^{ο} Πρόγραμμα Πλαίσιο για την έρευνα της Ευρωπαϊκής Ένωσης [2]. Τα κύρια πεδία ενδιαφέροντος του προγράμματος ήταν η ανθρωποκεντρικότητα (user-centricity), η προσωποποίηση (personalisation) και φυσικά η προσωπική δικτύωση (personal networking). Διήρκησε η φάση Ι από το 2004 έως 2006 και έως το 2008 η φάση ΙΙ ενώ εμπεριείχε πάνω από 30 συνέταιρους από 15 χώρες.

Ο συνολικός στόχος ήταν η σχεδίαση, ανάπτυξη, επίδειξη και επαλήθευση της ιδέα ενός ευλύγιστου Προσωπικού Δικτύου, που υποστηρίζει αποθεματικά αποδοτικές, εύρωστες (*robust*) προσωπικές υπηρεσίες παντού και ανά πάσα στιγμή για κινητούς χρήστες μέσα σε ένα ασφαλές ετερογενές δικτυακό περιβάλλον. Τα προγράμματα επίσης έδιναν μεγάλη σημασία στην παροχή των υπηρεσιών χωρίς όμως να γίνεται το σύστημα «φορτικό» (*obtrusive*) καθώς επίσης και σε θέματα διασφάλισης της ιδιωτικότητας των χρηστών και των δεδομένων τους.

2.3. Επίδειξη πρωτότυπου

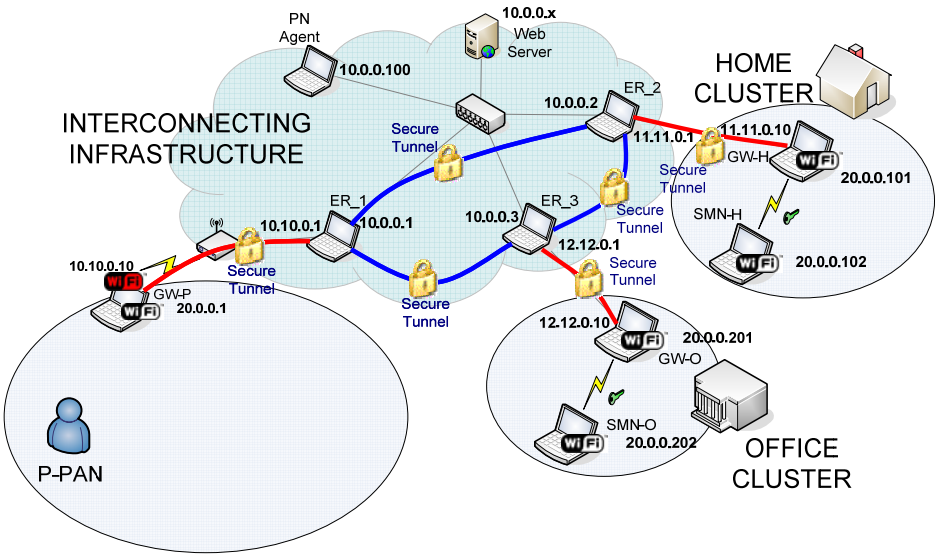
Η επίδειξη παρουσιάζει την περίπτωση ενός δημοσιογράφου που πρέπει να παραστεί στην επόμενη σύσκεψη αρχηγών στις Βρυξέλλες. Την ίδια ημέρα της σύσκεψης, ο δημοσιογράφος πετάει από τη πατρίδα του στις Βρυξέλλες. Ταξιδεύει με το laptop του, το κινητό του, την κάμερα του και του νέου PDA που αγόρασε πρόσφατα. Καθώς μπαίνει στο αεροπλάνο πρέπει να απενεργοποιήσει όλες τις ηλεκτρονικές του συσκευές. Ωστόσο οι υπόλοιπες προσωπικές του συσκευές παραμένουν ανοιχτές: στο γραφείο (WORK) έχει ακόμα δύο συσκευές (2 υπολογιστές: –GW_O, SMN_O–) και στο σπίτι (HOME) έχει το δίκτυο του σπιτιού του με απομακρυσμένο έλεγχο και εγκαταστάσεις ασχολίας ελεύθερου χρόνου (ακόμα 2 υπολογιστές –GW_H, SMN_H–). Η κατάσταση φαίνεται στην Εικόνα 3.



Εικόνα 3 – Το PN δημοσιογράφου αποτελούμενο από τη συστάδα σπιτιού και γραφείου

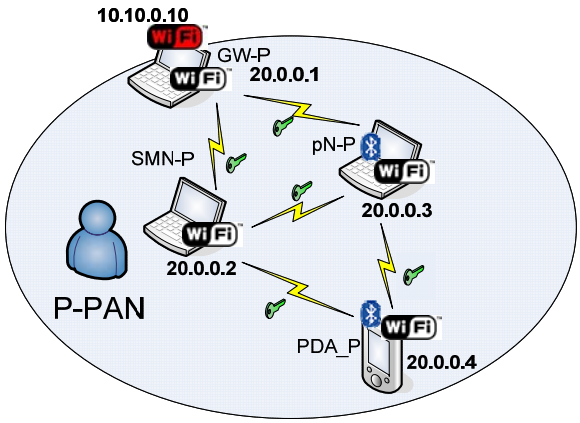
Όπως φαίνεται, και οι δύο συστάδες είναι διασυνδεδεμένες μέσω ασφαλών καναλιών επικοινωνίας (tunnelling). Με την άφιξη του αεροπλάνου, ο δημοσιογράφος αρχίζει να ενεργοποιεί τις προσωπικές συσκευές που μεταφέρει. Όπως φαίνεται και στην Εικόνα 4, ενεργοποιεί καταρχήν το κινητό του (GW_P), και καθώς η συσκευή μπορεί να συνδεθεί στο Διαδίκτυο, αυτόματα εγγράφεται στην διαχειριστική οντότητα, γνωστής και ως πράκτορας του PN (*PN Agent*) προκειμένου να μπορέσει να εγκαταστήσει ασφαλή σύνδεση με τις απομακρυσμένες συστάδες στο σπίτι και στο γραφείο. Οι ασφαλείς δίαυλοι (tunnels) εγκαταστάθηκαν και το προσωπικό δίκτυο μεγάλωσε με μία ακόμη συστάδα, αυτή του Ιδιωτικού Δικτύου Προσωπικής Περιοχής (*Private Personal Area Network – P-PAN*).

Κάθε κόμβος μέσα σε μια συστάδα μπορεί να γίνει Κόμβος Πύλη (*Gateway Node*) για τα άλλα μέλη της συστάδας, επιτρέποντας απομακρυσμένη επικοινωνία ανάμεσα στις συστάδες και εντός των ορίων του PN. Σαν αποτέλεσμα επιτυχούς ολοκλήρωσης ανακάλυψης Ακραίο Δρομολογητή (*Edge Router - ER*) εντός ενός προσωπικού κόμβου, ανακτάται μια διεύθυνση IP. Αυτό το γεγονός θα πυροδοτήσει τον μηχανισμό διαπραγμάτευσης κλειδιού IPSec [3] προκειμένου να στηθεί ένας ασφαλές δίαυλος μεταξύ της δημόσιας διεπαφής του προσωπικού κόμβου και του δρομολογητή ER. Η άμεση συνέπεια της εγκαθίδρυσης IPSec tunnel είναι ότι ο προσωπικός κόμβος γίνεται κόμβος Πύλη. Μόλις συμβεί αυτό, ο (νέος) Κόμβος Πύλη ενημερώνει τους υπόλοιπους κόμβους στη συστάδα για τη νέα του δυνατότητα.



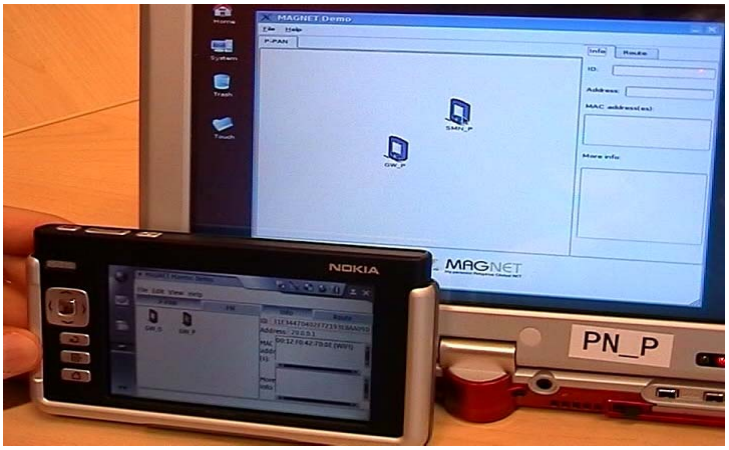
Εικόνα 4 – Εγγραφή P-PAN στο PN του δημοσιογράφου

Όλες οι συσκευές του δημοσιογράφου ανακαλύπτουν η μία την άλλη και σχηματίζουν το P-PAN ανταλλάσοντας κλειδιά συνόδου που θα τους επιτρέψουν να μιλάνε με ασφαλή τρόπο. Τέλος, οι υπόλοιποι κόμβοι ανακαλύπτουν το κινητό τηλέφωνο (GW_P) σαν τη Πύλη τους προς το Διαδίκτυο, οπότε και εγγράφονται στον πράκτορα του PN ώστε και οι υπόλοιπες συστάδες να αποκτήσουν γνώση της ακριβούς σύνθεσης του P-PAN. Όπως φαίνεται και στην Εικόνα 5 μια Γραφική Διεπαφή Χρήστη (*Graphical User Interface – GUI*) υλοποιήθηκε ώστε να επιτρέπεται στο χρήστη η διαχείριση της σύνθεσης του P-PAN. Σε αυτά τα GUI οι προσωπικοί κόμβοι εμφανίζονται με μπλε και οι ξένοι με κόκκινο χρώμα (ή σκούρο/ανοιχτό για ασπρόμαυρη εκτύπωση). Χάρη στο GUI, ο χρήστης αντιλαμβάνεται ότι δεν έχει περάσει από διαδικασία αποτύπωσης [4] του PDA με την κάμερα (δηλαδή δεν έχουν εγκαταστήσει τα μακροπρόθεσμα μυστικά που θα αρχικοποιήσουν την σχέση εμπιστοσύνης μεταξύ των προσωπικών κόμβων). Η Εικόνα 6 δείχνει το χειρισμό του GUI από το δημοσιογράφο προκειμένου να εκκινήσει τη διαδικασία αποτύπωσης.



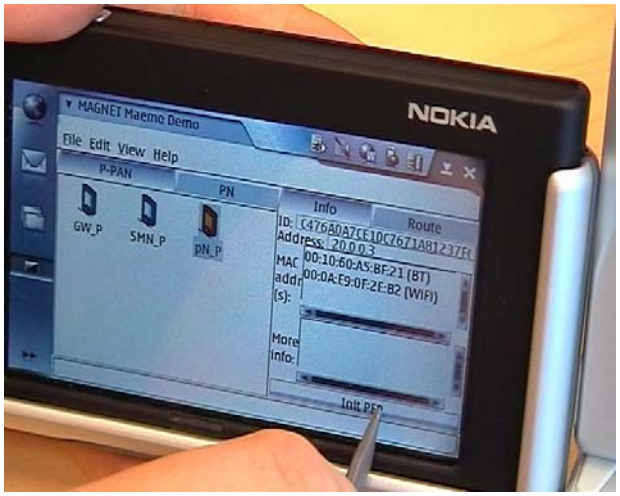
(a)

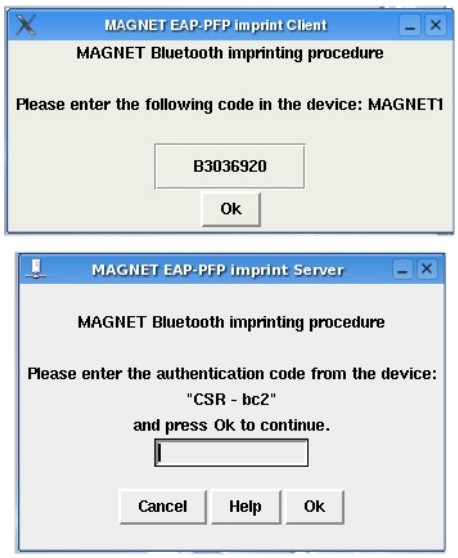
(b)



(c)

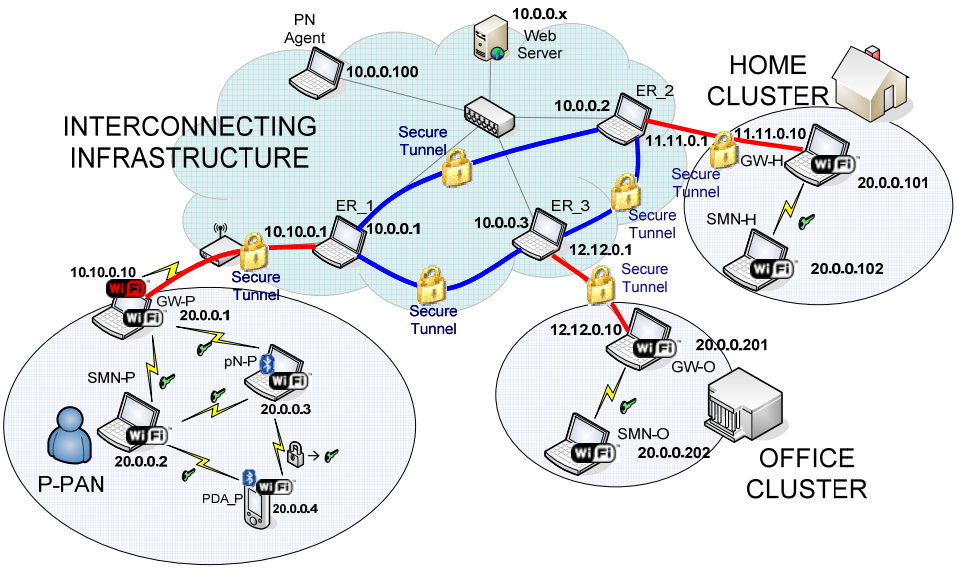
Εικόνα 5 – Εγγραφή P-PAN, δείγματα εικόνων οθόνης





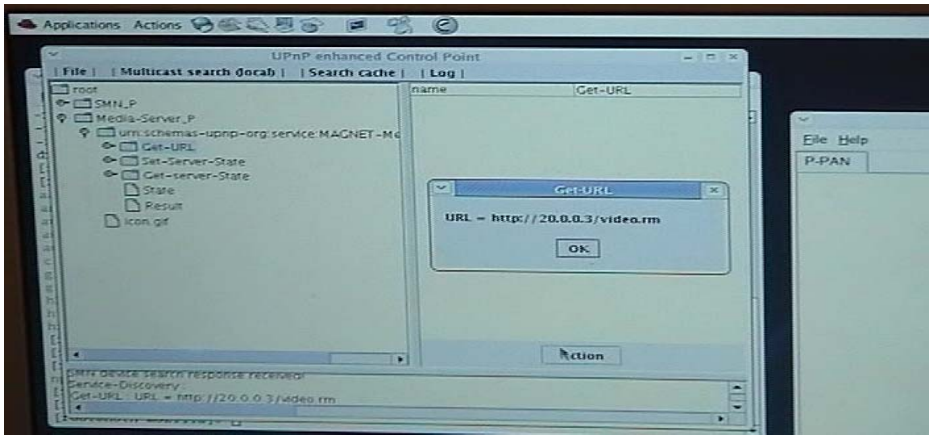
Εικόνα 6 – Διαδικασία αποτύπωσης (imprinting)

Το αποτέλεσμα της διαδικασίας είναι η ανταλλαγή μακροπρόθεσμων κρυπτογραφικών μυστικών που θα χρησιμοποιηθούν για να εξάγουν κλειδιά συνόδου και να τροφοδοτήσουν μηχανισμούς ταυτοποίησης προκειμένου να προστατευτεί η επικοινωνία μεταξύ ζεύγους κόμβων. Αυτόνομα και αόρατα από το χρήστη, όλες οι συσκευές του πλέον έχουν σχηματίσει το Προσωπικό Δίκτυο όπως φαίνεται στην Εικόνα 7, ένα προστατευμένο και ασφαλές δίκτυο εστιασμένο σε αυτόν, που συνδέει όλες τις ενεργές συσκευές του, όχι μόνο τις τοπικές, αλλά και τις προσωπικές συσκευές που βρίσκονται σε απομακρυσμένα μέρη όπως συσκευές στο δίκτυο του γραφείου, του σπιτιού και του αυτοκινήτου.



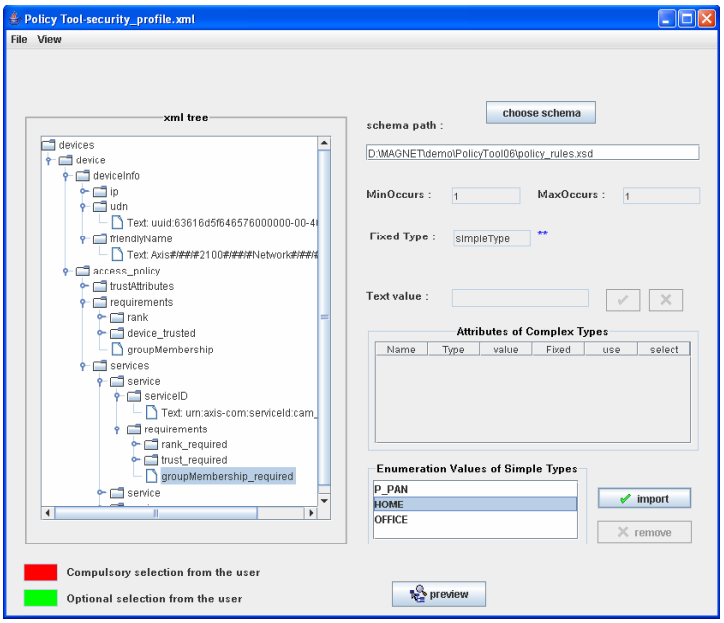
Εικόνα 7 – Σύνθεση PN

Εφόσον σχηματιστεί το PN, ο δημοσιογράφος μπορεί να αποκτήσει πρόσβαση σε οποιαδήποτε υπηρεσία παρέχεται από προσωπική του συσκευή μέσα στο δίκτυο, με ασφαλές και με διασφάλιση της ιδιωτικότητας του [7]. Ο δημοσιογράφος μπορεί να ανακαλύψει όλες τις διαθέσιμες υπηρεσίες όπως δείχνει η Εικόνα 8.



Εικόνα 8 – Ανακάλυψη υπηρεσίας

Ο δημοσιογράφος είναι τώρα ικανός να αποκτήσει πρόσβαση από το laptop του στο ρεύμα δεδομένων video και ήχου που παράγει η κάμερα του. Με χρήση της εφαρμογής τροποποίησης video, αρχίζει την εγγραφή, προσθέτοντας σχόλιο και επιπλέον κομμάτια video. Αντιλαμβάνεται ότι κάποια έγγραφα που άφησε στον υπολογιστή του γραφείου θα ήταν πολύ χρήσιμα για να ολοκληρώσει την αναφορά του για τη σύσκεψη. Χρησιμοποιώντας το ίδιο GUI της Εικόνα 8, ανακαλύπτει την υπηρεσία πρόσβασης σε περιεχόμενο που βρίσκεται στο γραφείο του. Καταφέρνει να αποκτήσει πρόσβαση σε όλο το υλικό που έψαχνε πατώντας μόνο μερικά κουμπιά. Όταν τελειώσει την αναφορά του, την ανεβάζει μέσω δικτύου σε ένα φάκελο τον οποίο μπορούν να το ελέγξουν μόνο συγκεκριμένοι συνάδελφοι του. Η σχετική υπηρεσία συνεργάζεται με τον μηχανισμό ελέγχου πρόσβασης, ο οποίος τροφοδοτείται από τις πολιτικές και κανόνες ασφαλείας [5]. Αυτές τις είχε ορίσει παλιότερα με χρήστη ειδικού GUI διαχείρισης πολιτικών ασφαλείας (Εικόνα 9) για το PN του. Στη συνέχεια, ξεκινάει μια βίντεο-διάσκεψη με τους συναδέλφους του στο γραφείο για να συζητήσει την αναφορά. Όλη η κίνηση μεταφέρεται ασφαλώς πάνω από το δίκτυο χωρίς κανείς να μπορεί να την αναχαιτίσει.



Εικόνα 9 – Διαχείριση πολιτικών ασφαλείας

Με το που τελειώσει τη δουλεία του και περιμένοντας στη πύλη επιβίβασης, εκμεταλλεύεται τις δυνατότητες του PN του και συνδέεται απομακρυσμένα στο δίκτυο τοθ σπιτιού του, όπου ελέγχει το συναγερμό και τα φώτα. Τέλος, και καθώς του περισσεύει λίγος χρόνος παρακολουθεί μια ταινία που είχε κατεβάσει το προηγούμενο βράδυ στον υπολογιστή του σπιτιού του.

2.4. Συμπεράσματα

Σε αυτό το κεφάλαιο έγινε επίδειξη του πρωτότυπου Προσωπικού Δικτύου κατά την οποία παρουσιάστηκαν:

- Σχηματισμός P-PAN και PN αθόρυβα από το χρήστη και με ασφάλεια
- Διαδικασία αποτύπωσης για εγκατάσταση σχέσεων εμπιστοσύνης μεταξύ προσωπικών κόμβων του ίδιου PN
- Διασύνδεση όλων των κόμβων και συστάδων στο PN πάνω από ασφαλείς διαύλους επικοινωνίας IPSec και μέσω κόμβων που αναλαμβάνουν σε κάθε συστάδα το ρόλο του gateway
- Ανακάλυψη υπηρεσιών οπουδήποτε μέσα στο PN με ασφαλές τρόπο και σύμφωνα με έλεγχο πρόσβασης και τις αντίστοιχες πολιτικές ασφαλείας

Με βάση αυτό το πρωτότυπο σχεδιάστηκαν οι επεκτάσεις για συνομοσπονδία μεταξύ PN, ενσωμάτωση επίγνωσης κατάστασης και συγκείμενης πληροφορίας στις υπηρεσίες εφαρμογές και ασφάλεια, προστασία και διασφάλιση της ιδιωτικότητας του σαφώς πιο πλούσιο μοντέλου πληροφορίας του PN-F.

2.5. *Ειδική ορολογία κεφαλαίου*

Ελληνικός όρος / φράση	Αγγλικός όρος / φράση
Ακραίος Δρομολογητής	Edge Router
Ανθρωποκεντρικός	User-centric
Ανθρωποκεντρικότητα	User-centricity
Γραφική Διεπαφή Χρήστη	Graphical User Interface
Διαστρωματική	Cross-layer
Διεπαφή	Interface
Εύρωστος	Robust
Ιδιωτικό δίκτυο προσωπικής περιοχής	Private Personal Area Network – P-PAN
Κόμβος	Node
Προσωπική δικτύωση	Personal networking
Προσωπικό Δικτύο	Personal Network - PN
Προσωποποίηση	Personalisation
Πύλη	Gateway
Ταυτοποίηση	Authentication
Φορτικός, ενοχλητικός	Obtrusive

2.6. *Βιβλιογραφικές Αναφορές*

[1] MAGNET Beyond project website: http://magnet.aau.dk/

[2] Επεξήγηση 6ου Προγράμματος Πλαισίου από τον ιστότοπο της Ευρωπαϊκής Ένωσης: http://www.cordis.lu/fp6/whatisfp6.htm

[3] Guide to IPSec VPNs, NIST, US Departmenet of Commerce, available online at: http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

[4] Dimitris M. Kyriazanos, John Williams Floroiu et al, "MAGNET Personal Network Security Model: Trust Establishment, Policy Management and AAA Infrastructure", WWRF15 Meeting, Paris, France, December 2005

[5] Dimitris M. Kyriazanos, George I. Stassinopoulos(ICCS-NTUA), Neeli R. Prasad, (AAU), "Ubiquitous Access Control and Policy Management in Personal Networks", submitted and accepted for oral presentation on IEEE Mobiquitous 2006, San Jose, California, USA, July 17, 2006

[6] Dimitris M. Kyriazanos, Michael Argyropoulos, Luis Sanchez, Jorge Lanza, Mikko Alutoin, Jeroen Hoebeke and Charalampos Z. Patrikakis, "Overview of a Personal Network Prototype", IEC Annual review of telecommunications vol. 59, 2007

[7] Dimitris M. Kyriazanos, Wassef Louati, Marc Girod Genet, Djamal Zeghlache, Michael Argyropoulos, Charalampos Z. Patrikakis, "An Architecture for Secure Wide-Area Service Discovery in Personal Peer-to-Peer Networks", paper presented as poster on IST Mobile Summit 2006,Mykonos, Greece, June 2006

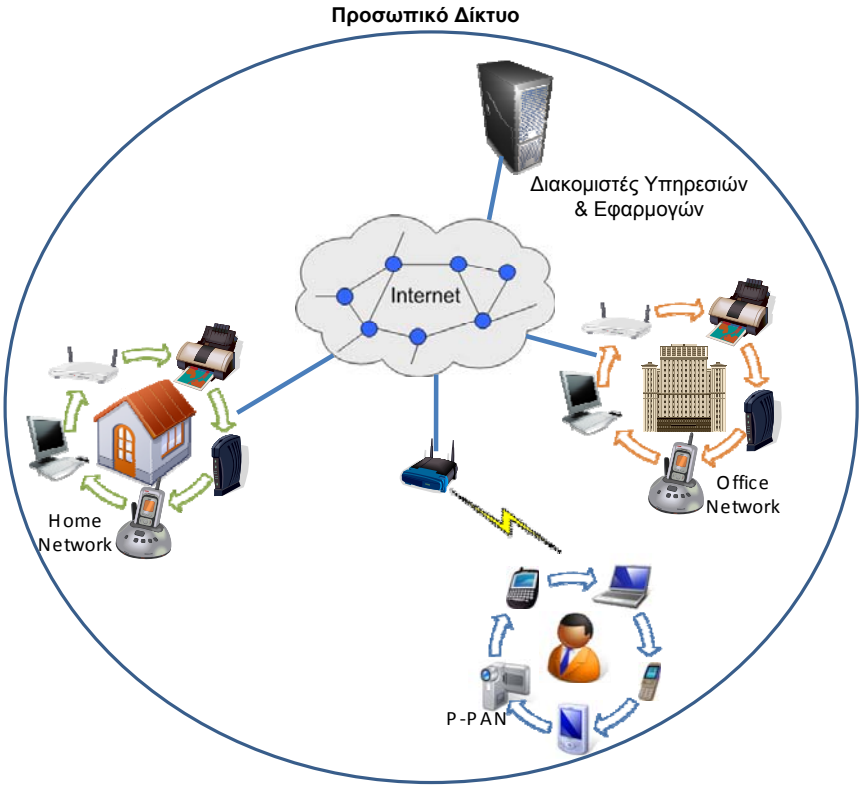
3. Η Ασφάλεια και Ιδιωτικότητα σε Προσωπικά Δίκτυα και συνασπισμούς Προσωπικών Δικτύων

3.1. Εισαγωγή

Ο τρόπος με τον οποίο οι άνθρωποι αποκτούν πρόσβαση σε πληροφορίες έχει αλλάξει δραματικά τα τελευταία χρόνια χάριν στις κατακτήσεις των τεχνολογιών πληροφορικής και τηλεπικοινωνιών. Ειδικότερα, η γοργή ανάπτυξη τεχνολογιών ασύρματων και κινητών επικοινωνιών σε συνδυασμό με την ευρεία διάδοση κινητών συσκευών, επέτρεψε την πρόσβαση σε αποθέματα πληροφορίες οπουδήποτε και ανά πάσα στιγμή. Τα αποτελέσματα αυτής της ανάπτυξης φαίνονται σε διάφορες πλευρές της ζωής μας, με χαρακτηριστικό παράδειγμα αυτό του προσωπικού χώρου εργασίας. Ήδη για πολλούς ανθρώπους το παραδοσιακό γραφείο επεκτείνεται και σε άλλους χώρους, με το λεγόμενο εικονικό γραφείο όπου η πρόσβαση σε δεδομένα δουλειάς και άλλα προσωπικά δεδομένα επεκτείνεται οπουδήποτε με χρήση τεχνολογιών Διαδικτύου και την εξάπλωση της ευρυζωνικότητας. Ως αποτέλεσμα αυτών των εξελίξεων η έρευνα συνέλαβε την ιδέα του Προσωπικού Δικτύου (*Personal Network - PN*)[1][2] σαν το ομογενοποιημένο σύνολο ετερογενών δικτύων και συσκευών, που σχηματίζει ένα δίκτυο επικάλυψης (*overlay network*) γύρω από το χρήστη. Πάνω από αυτό το δίκτυο παρέχονται καινοτόμες υπηρεσίες και εφαρμογές οπουδήποτε και ανά πάσα στιγμή. (Εικόνα 10). Ως παραδείγματα των επί μέρους ετερογενών δικτύων είναι η «φούσκα» (*bubble*) συσκευών που φέρει ο χρήστης μαζί του πάντα (στο PN είναι γνωστό ως ιδιωτικό δίκτυο προσωπικής περιοχής, *Private Personal Area Network – P-PAN*), το έξυπνο σπίτι, δίκτυο γραφείου και το «έξυπνο» αυτοκίνητο [3][4].

Ωστόσο, μαζί με την διάθεση πληροφορίας και αποθεμάτων, είναι λογική συνέπεια να αυξάνονται και οι σχετικοί κίνδυνοι για την ασφάλεια και την ιδιωτικότητα. Συγκεκριμένα, προκειμένου να προστατευτεί ο κινητός χρήστης από κακόβουλες προσπάθειες εισβολής στο προσωπικό του χώρο δεδομένων, καθώς και από άλλες δικτυακές επιθέσεις, πρέπει να οργανωθεί η κατάλληλη άμυνα, που θα θέσει περιορισμού και μηχανισμούς ασφαλείας. Τέτοιοι μηχανισμοί μπορεί να είναι παραδοσιακά συστήματα ασφαλείας δικτύου, με χρήση καλά προστατεμένων κεντρικών διακομιστών για την αποθήκευση της πληροφορίας ή ομότιμες αρχιτεκτονικές επιτρέποντας την διαχείριση των δεδομένων χωρίς την μεσολάβηση τρίτων, έστω και έμπιστων μερών. Κατά πόσο όμως το όραμα του ασφαλούς Προσωπικού Δικτύου όπως εξελίσσεται από την έρευνα καλύπτεται από υπάρχουσες λύσεις; Οι νέες απαιτήσεις ασφαλείας που προκύπτουν από τις καινοτομίες που φέρνουν τα PN ώθησαν την έρευνα στα θέματα ασφαλείας και ιδιωτικότητας να δώσουν νέες λύσεις στο χώρο αυτό. Η ίδια ώθηση άλλωστε αποτέλεσε και το κίνητρο για την παρούσα διατριβή.

Σε αυτό το κεφάλαιο εξετάζονται οι γενικές αλλά και ειδικές απαιτήσεις ασφαλείας και ιδιωτικότητας, με βάση τα σενάρια χρήσης Προσωπικών Δικτύων και συνασπισμών Προσωπικών Δικτύων (*Personal Networks Federation – PN-F*). Η προσέγγιση αυτή είναι στα πλαίσια του ανθρωποκεντρικού (*user-centric*) χαρακτήρα και σχεδίασης που διέπουν αυτά τα δίκτυα. Στη συνέχεια εξετάζεται τί πρέπει να προστατευτεί, από τί απειλείται και ποιες είναι οι υπάρχουσες λύσεις αλλά και προτάσεις της έρευνας σχετικά. Τέλος, αναγνωρίζονται οι απαιτούμενες ελλείψεις οι οποίες ουσιαστικά εκκίνησαν την έρευνα της διδακτορικής μου διατριβής.



Εικόνα 10 – Φυσική Μορφή Προσωπικού Δικτύου

3.2. Προσωπικά Δίκτυα και συνασπισμοί: περιπτώσεις χρήσης και σενάρια

Το PN είναι ένα ασφαλές ανθρωποκεντρικό δίκτυο που περιέχει μια δυναμική συλλογή από κοντινούς ή απομακρυσμένους προσωπικούς κόμβους και συσκευές, παρέχοντας παράλληλα προσωποποιημένες υπηρεσίες και εφαρμογές με επίγνωση κατάστασης. Κόμβοι του ίδιου PN μοιράζονται κοινή σχέση ασφαλείας και συνδέονται μεταξύ τους μέσω διασυνδεδεμένων δομών. Η αρχιτεκτονική δικτύου PN κάνει όλες τις υπηρεσίες και ψηφιακά αποθέματα ενός ανθρώπου διαθέσιμα σε αυτόν, οπουδήποτε και ανά πάσα στιγμή [2].

Ξεκινώντας από αυτή την ανάλυση και προκειμένου να επεκταθεί η έννοια του ανθρωποκεντρικού PN ώστε να ανταποκρίνεται στις συχνές αλληλεπιδράσεις μεταξύ πολλών χρηστών και PN με κοινά ενδιαφέροντα και σε διάφορα πλαίσια, προσωπικά ή επαγγελματικά, εισάγεται η έννοια του συνασπισμού Προσωπικών Δικτύων PN-F ως η ασφαλής και με επίγνωση κατάστασης συνεργασία. Ένας τέτοιος συνασπισμός αποτελείται από τον Ιδιοκτήτη και ένα ή περισσότερα Μέλη. Αμέσως προκύπτουν θέματα όπως ο ασφαλής σχηματισμός, διατήρηση και διάλυση του συνασπισμού, ασφαλής ανακάλυψης μελών και ταυτοποίησης, συνδεσιμότητας δικτύου και υποστήριξης κινητικότητας [1][2]. Με σκοπό την αλληλεπίδραση μεταξύ των PNs και τη δημιουργία PN-Fs άξιων εμπιστοσύνης, σχετικοί κανόνες και πολιτικές ασφαλείας πρέπει να συμφωνηθούν εκ των προτέρων και να εφαρμοστούν. Την όλη διαδικασία σχηματισμού ενός PN-F βοηθάει και συντονίζει μια κεντρική οντότητα η οποία ανήκει ουσιαστικά στο PN του ιδιοκτήτη του συνασπισμού, και είναι γνωστή και ως διαχειριστής συνασπισμών (*federation manager*).

Προκειμένου να συνδεθούν οι απαιτήσεις ασφαλείας που να ανταποκρίνονται στη πραγματικότητα, η μελέτη συνεχίζει βάσει πραγματικών σεναρίων χρήσης τα οποία ακολουθούν, και στα οποία περιλαμβάνεται και η εγκαθίδρυση ενός συνασπισμού.

Σενάριο 1: Η Εκδήλωση

Προκειμένου να χρησιμοποιηθούν οι υπηρεσίες που παρέχονται σε μία εκδήλωση, π.χ. μια εμπορική ή βιομηχανική έκθεση ή μια δεξίωση γάμου θα πρέπει οι άνθρωποι που βρίσκονται σε μια σχετικά μικρή εμβέλεια της γεωγραφικής θέσης της εκδήλωσης να εισέλθουν στο PN-F που έχει δημιουργήσει εκ των προτέρων ο οργανωτής της εκδήλωσης. Με την άφιξη των καλεσμένων, η κινητή συσκευή τους λειτουργεί σαν κάρτα πρόσβασης και αυτόματα εντοπίζεται ο συνασπισμός και οι υπηρεσίες που παρέχονται. Γίνονται δεκτοί στην εκδήλωση με τη συγκεκριμένη ταυτότητα που έχουν δημιουργήσει. Επίσης συνδεδεμένα με τη ταυτότητα είναι και οι κανόνες και οι πολιτικές ασφαλείας που επιβάλλονται στις αλληλεπιδράσεις μέσα στο συνασπισμό, καθώς και ένα μέρος του προφίλ τους που έχει ακριβώς και μόνο τη πληροφορία που θέλουν να μοιραστούν με τα άλλα μέλη. Όταν οι συμμετέχοντες γνωρίσουν πρόσωπα είναι είτε πιθανές νέες επαγγελματικές επαφές ή ανθρώπους με κοινά χαρακτηριστικά, βάσει του προφίλ συμμετοχής στο συνασπισμό, οι χρήστες μπορεί να αποφασίσουν να ανταλλάξουν ψηφιακές επαγγελματικές κάρτες ή μεγαλύτερο μέρος της προσωπικής τους πληροφορίας. Επιπλέον υπηρεσίες, όπως χρήση εξοπλισμού της εκδήλωσης (π.χ. μια οθόνη) ή πρόσβαση σε αρχεία (π.χ. πρόγραμμα εκδήλωσης) είναι επίσης διαθέσιμα στα μέλη του PN-F [4].

Σενάριο 2: Κέντρο εκτύπωσης

Αυτό το σενάριο αφορά ένα κέντρο εκτύπωσης, όπου οι πελάτες μπορούν να κάνουν χρήση εξοπλισμού εκτύπωσης με συγκεκριμένη χρέωση, ανάλογα με το χρόνο ή τα αποθέματα που χρησιμοποιούνται. Στο σενάριο, ο πελάτης εισέρχεται στο κατάστημα και χρησιμοποιώντας το PDA (*Personal Digital Assistant*) ή το laptop του, ζητά πρόσβαση σε συσκευές εκτύπωσης για να εκτυπώσει ένα έγγραφο. Η πρόσβαση δίνεται στον πελάτη κατόπιν ανταλλαγής της απαραίτητης πληροφορίας και το σχηματισμό PN-F [5]. Ο πελάτης αποκτά πρόσβαση σε έναν εικονικό εκτυπωτή, ο οποίος αντιστοιχεί σε κάποια πραγματική συσκευή. Ο πελάτης μπορεί να εκτυπώσει απευθείας το έγγραφο, αφού το μετατρέψει σε μια πρότυπη μορφή όπως PDF. Η χρονική περίοδος που ο συγκεκριμένος συνασπισμός παραμένει ανοιχτός και ο πελάτης έχει πρόσβαση στον εκτυπωτή, περιορίζεται από τον ιδιοκτήτη του αποθέματος και δημιουργό του PN-F (στη περίπτωση μας ο υπάλληλος του καταστήματος). Όταν ο πελάτης τελειώσει με την εκτύπωση, η πρόσβαση στα σχετικά αποθέματα απενεργοποιείται [3].

Σενάριο 3: Πρόσβαση ως επισκέπτης σε εταιρικό περιβάλλον

Το σενάριο αυτό αφορά μια εταιρεία όπου το γραφείο διαχείρισης μπορεί να δώσει πρόσβαση ή να προσφέρει υπηρεσίες σε επισκέπτες της εταιρείας ανάλογα με τις ειδικές απαιτήσεις της επίσκεψης. Προκειμένου να συμμετάσχει στο PN-F της εταιρείας, το οποίο είναι ήδη δημιουργημένο, ο χρήστης πρέπει να έχει τα απαραίτητα πιστοποιητικά που θα του έχουν δοθεί κατά την είσοδο του στην εταιρεία από τον υπεύθυνο υποδοχής. Ανάλογα με το σκοπό της επίσκεψης το δοθέν πιστοποιητικό θα συνδέεται και με τα ελάχιστα απαραίτητα προνόμια, προκειμένου να γίνει χρήστη με ασφάλεια των σχετικών αποθεμάτων και υπηρεσιών.

3.3. *Περιουσιακά στοιχεία προσωπικού δικτύου*

Προκειμένου να αντιμετωπιστούν τα ζητήματα ασφαλείας που προκύπτουν βάσει της ανάλυσης και των σεναρίων, πρέπει καταρχήν να καθοριστεί τι είναι αυτό που πρέπει να προστατευτεί. Με άλλα λόγια, πρέπει να οριστεί ποια περιουσιακά στοιχεία του προσωπικού δικτύου είναι σε κίνδυνο, και να αναγνωριστούν οι σχετικές απαιτήσεις ασφαλείας. Στον παρουσιάζεται η λίστα από τα γενικά περιουσιακά στοιχεία ενός PN.

Πίνακας 1 - Γενικά Περιουσιακά Στοιχεία ενός PN

Όνομα	**Περιγραφή**
ID χρήστη, ID PN, Εικονικές Ταυτότητες (Virtual Identities – VID)	Δεδομένα ταυτοποίησης
Προσωπικά δεδομένα, προφίλ χρήστη	Πληροφορίες σχετικά με το χρήστη
Υπηρεσίες	Ιδιοκτησία υπηρεσιών ή δικαιώματα πρόσβασης σε υπηρεσίες
Αποθέματα Δικτύου	Η διαθεσιμότητα του εύρους της σύνδεσης και των σχετικών πρωτοκόλλων επικοινωνίας στους νόμιμους δικαιούχους
Δεδομένα PN	Εμπιστευτικότητα δεδομένων προσωπικού δικτύου (π.χ. πληροφορίες δικτύου, διευθύνσεις IP, MAC κτλ)
Ρόλοι, εξουσιοδοτήσεις	Κανόνες που δίνουν συγκεκριμένα δικαιώματα και προνόμια στο χρήστη κατά τον έλεγχο πρόσβασης
Φήμη	Κεκτημένο επίπεδο εμπιστοσύνης από το χρήστη
Συσκευές	Φυσικά στοιχεία
Διακομιστές	Φυσικά στοιχεία

Το πρώτο, απλούστερο και πιο σημαντικό στοιχείο σε ένα προσωπικό δίκτυο αλλά και σε οποιαδήποτε περίπτωση ηλεκτρονικής, κινητής και διαδικτυακής ασχολίας εμπλακεί ένας χρήστης, είναι η ταυτότητα του, το ποιος είναι. Η έννοια της ταυτότητας είναι στενά συνδεδεμένη με τις προσωπικές πληροφορίες. Οι προσωπικές πληροφορίες περιλαμβάνουν μια ευρεία συλλογή από δεδομένα σχετικά με το χρήστη, και κυμαίνονται από βασικές μέχρι υψηλά προσωπικές και εξεζητημένες. Είναι γεγονός ότι τα Προσωπικά Δίκτυα εξορισμού έχουν μια μεγάλη συλλογή προσωπικών πληροφοριών, στις οποίες περιλαμβάνονται:

- **πληροφορίες ταυτοποίησης** για κάθε σύστημα που ο χρήστης συμμετέχει και γίνεται εξακρίβωση ταυτότητας (π.χ. εξουσιοδοτημένη χρήση υπηρεσίας, web banking, ηλεκτρονική αλληλογραφία ψηφιακά υπογεγραμμένη)
- **προσωπικές προτιμήσεις** για χρήση με εφαρμογές και υπηρεσίες με δυνατότητες προσωποποίησης (*personalisation*) (π.χ. επαγγελματική κατάσταση, σπορ, χόμπι, αλλεργίες, προτιμήσεις διατροφής)

- **συγκείμενη πληροφορία** (*context*) σχετικά με το χρήστη και τις δυναμικές εναλλαγές κατάστασης, για χρήση σε υπηρεσίες και εφαρμογές με επίγνωση κατάστασης (*context-awareness*) (π.χ. τοποθεσία, διάθεση, τρέχουσα απασχόληση και άλλες πληροφορίες κατάστασης)

Οι πληροφορίες αυτές είναι χρήσιμες προκειμένου να κατηγοριοποιηθούν οι χρήστε σε ομάδες κοινών ενδιαφερόντων μέσα σε μια κοινότητα, και να γίνεται πιο ακριβής και καλύτερη παροχή προσωποποιημένων υπηρεσιών με επίγνωση κατάστασης [6]. Ωστόσο, οι χρήστες δεν είναι πάντα θετικοί στο να δίνουν τα προσωπικά τους δεδομένα, όποια και αν είναι αυτά. Από την άλλη, υπάρχουν και οι απειλές επιθέσεων προκειμένου να αποκτηθούν οι προσωπικές πληροφορίες και να χρησιμοποιηθούν με δυσάρεστο για τον τρόπο χρήστη (π.χ. ανεπιθύμητες διαφημίσεις, spam κ.α.). Είναι λοιπόν προφανές ότι η ταυτότητα και προφίλ του χρήστη αποτελούν πολύ σημαντικά περιουσιακά στοιχεία.

Σύμφωνα με τα σενάρια, είναι προφανές ότι και οι ίδιες οι υπηρεσίες είναι επίσης σημαντικότατα περιουσιακά στοιχεία σε έναν συνασπισμό. Παραδείγματα τέτοιων υπηρεσιών μπορεί να είναι από απλές υπηρεσίες εκτύπωσης, μέχρι και υπηρεσίες αποθήκευσης πληροφορίας, ιατρικές υπηρεσίες εκτάκτου ανάγκης κ.α. Επίσης, αναγνωρίζοντας τη σημασία της συνδεσιμότητας, τα αποθέματα δικτύου επίσης είναι περιουσιακό στοιχείο, το οποίο απειλείται από παράνομη χρήση και περιορισμό των αποθεμάτων , καθώς και από κακόβουλες επιθέσεις και δικτυακές επιθέσεις όπως π.χ. distributed denial-of-service (DDoS) [7]. Τέλος λαμβάνονται υπόψη και τα φυσικά στοιχεία, οι συσκευές και η υποδομή που απαρτίζουν ένα PN καθώς και αυτά πέραν της ίδιας της χρηματικής αξίας αγοράς, φέρουν πιθανόν επιπλέον πολύτιμα αποθέματα μέσα τους όπως απόρρητα αρχεία και πιστοποιητικά.

Βάσει αυτής της ανάλυσης περιουσιακών στοιχείων, που ορίζει το τι πρέπει να προστατευτεί, αναγνωρίζονται οι «εχθροί» και τι τελικά απειλεί τα στοιχεία αυτά και εξάγονται οι απαιτήσεις ασφαλείας για τα περιβάλλοντα συνασπισμών PN-F. Η σχετική ανάλυση ακολουθεί στην επόμενη παράγραφο.

3.4. Απαιτήσεις ασφαλείας και απειλές

Η διατήρηση της ασφάλειας των Προσωπικών Δικτύων αποτελεί ένα πεδίο – πρόκληση για την έρευνα. Διανεμημένες και συνεργατικές αρχιτεκτονικές, συχνά ομότιμες P2P (*Peer-to-peer*) –η πιο διαδεδομένη λύση για τέτοια δίκτυα – απαιτούν λύσεις ασφαλείας που να υποστηρίζουν μεγάλη ικανότητα κλιμάκωσης (*scalability*), ευλυγισία και πάνω από όλα να εγγυώνται ένα λογικό επίπεδο ασφάλειας και άμυνας ενάντια στης απειλές της ιδιωτικότητας του χρήστη. Επιπλέον, τα PN όντας ανθρωποκεντρικά (*user-centric*) πρέπει να προσφέρουν μεγάλη δυνατότητα επιλογών, προσωποποίησης και προσαρμοστικότητας, ενώ παράλληλα δεν πρέπει να απαιτούν ειδικές τεχνικές γνώσεις από αυτόν. Θα λέγαμε ότι υπάρχει δηλαδή μια άνευ όρων προσφορά λειτουργικότητας στο χρήστη, η οποία όμως έχει το κόστος της όσον αφορά τις απαιτήσεις ασφαλείας και αυτόνομης διαχείριση του δικτύου.

Καταρχήν, οι απαιτήσεις ασφαλείας που ισχύουν γενικά για ένα σύστημα επικοινωνιών ισχύουν επίσης και για τα Προσωπικά Δίκτυα [8], δηλαδή:

- Ταυτοποίηση - *Authentication*
- Εμπιστευτικότητα - *Confidentiality*
- Ακεραιότητα - *Integrity*

- Μη-αποκήρυξη - *Non-repudiation*
- Έλεγχος πρόσβασης - *Access-control*
- Διαθεσιμότητα - *Availability*

Σε υψηλό επίπεδο, ο στόχος είναι να καταλήξουμε σε ένα περιβάλλον όπου οι ανταλλαγές μηνυμάτων και διαδικασίες θα εκτελούνται ασφαλώς από άκρη σε άκρη. Η ασφάλεια επομένως των δεδομένων πρέπει να διασφαλίζεται τόσο κατά τη μεταφορά τους μέσω σχετικών πρωτοκόλλων, λαμβάνοντας και υπόψη παρουσία ενδιάμεσων μεσολαβητών, όσο και κατά την αποθήκευση τους. Ακολουθεί η ανάλυση των γενικών απαιτήσεων ασφαλείας για τα Προσωπικά Δίκτυα.

Η ταυτοποίηση απαιτείται προκειμένου να επαληθευτούν σε κάθε συναλλαγή οι παρουσιαζόμενες ταυτότητες των εμπλεκόμενων μερών. Κατά την ανακάλυψη υπηρεσιών, πρέπει κάθε οντότητα (τερματικό, υπηρεσία, διακομιστές) να είναι σε θέση να αναγνωρίσουν με αξιόπιστο τρόπο τις οντότητες με τις οποίες επικοινωνούν. Σε πολλές περιπτώσεις, υπάρχει και η ανάγκη της αμοιβαίας ταυτοποίησης (*mutual authentication*), ακόμη και αν θεωρητικά μόνο το ένα μέρος ουσιαστικά επωφελείται της υπηρεσίας. Για παράδειγμα, έστω ότι θέλουμε να στείλουμε ένα έγγραφο για εκτύπωση σε έναν απομακρυσμένο εκτυπωτή δικτύου. Η ταυτοποίηση του χρήστη απαιτείται για να αποφασιστεί ότι όντως δικαιούται να επωφεληθεί της υπηρεσίας εκτύπωσης. Η ταυτοποίηση του εκτυπωτή όμως απαιτείται προς αποφυγή της περίπτωσης που μία κακόβουλη οντότητα παριστάνει την νόμιμη υπηρεσία με σκοπό να κλέψει τα έγγραφα που θα στείλει ο χρήστης.

Σαν επόμενο λογικό βήμα, έρχεται το σύστημα εξουσιοδότησης και ελέγχου πρόσβασης στα αποθέματα. Ουσιαστικά απαιτείται ένας μηχανισμός που ελέγχει τις προνόμια, δικαιώματα ή περιορισμοί συνδέονται με τη ταυτότητα προέλευσης της αίτησης για συγκεκριμένο απόθεμα. Αυτοί οι κανόνες τίθενται συνήθως από έμπειρους διαχειριστές, που αποφασίζουν για τη πρόσβαση που παρέχεται σε κάθε απόθεμα. Είναι σαφές ότι το αντίστοιχο σύστημα του προσωπικού δικτύου πρέπει να είναι όσο το δυνατόν αυτοδιαχειριζόμενο αλλά και να λαμβάνει υπόψη τις επιλογές του χρήστη-ιδιοκτήτη μέσω όσο το δυνατόν απλούστερων και φιλικών διεπαφών.

Η εμπιστευτικότητα και ακεραιότητα αφορούν κυρίως την ασφάλεια της επικοινωνίας. Ακόμη και όταν υπάρχει έλεγχος πρόσβασης, κακόβουλοι χρήστες μπορεί να παρακολουθούν και να υποκλέπτουν δεδομένα σε διαύλους επικοινωνίας, ή ακόμα και ενεργητικά να επιτεθούν για να την καταλάβουν. Αφενός ευαίσθητα δεδομένα δεν πρέπει σε καμία περίπτωση να αποκαλύπτονται σε αυτούς (εμπιστευτικότητα), αλλά ούτε και να επιτρέπουμε την αλλοίωση τους με κάποιο τρόπο (ακεραιότητα). Για το σκοπό αυτό απαιτείται κρυπτογράφηση των δεδομένων και χρήση συστημάτων ψηφιακών υπογραφών, όπως θα αναλυθεί και στις προτεινόμενες λύσεις.

Οι υπηρεσίες και οι κατάλογοι αποθεμάτων μπορεί να είναι επίσης στόχος επιθέσεων, τόσο σε επίπεδο εφαρμογής όσο και σε επίπεδο δικτύου (π.χ. DoS). Επομένως απαιτείται προστασία τόσο υψηλού επιπέδου, μέσω κάποιου συστήματος ελέγχου πρόσβασης, όσο και χαμηλότερο, με χρήση firewalls και IDS (*Intrusion Detection System* – σύστημα εντοπισμού εισβολής). Η δε παρακολούθηση όμως της κίνησης και λειτουργίας μιας υπηρεσίας, θα πρέπει να γίνεται με τρόπο ώστε να μην θίγεται η ιδιωτικότητα των χρηστών της υπηρεσίας.

Όσον αφορά τις διεπαφές δικτύου, αφενός πρέπει να υπάρχει συνοχή μεταξύ της εκάστοτε δυναμικής κατάστασης δικτύου και της ασφάλειας στο επίπεδο εφαρμογών: δηλαδή οι ρυθμίσεις ιδιωτικότητας να τηρούνται αδιάκοπα καθώς ο χρήστης μεταβαίνει από δίκτυο σε δίκτυο. Επιπλέον, οι πληροφορίες δικτύου που αφορούν τη δομή του και τις τεχνολογίες που χρησιμοποιούνται είναι και αυτές πολύ χρήσιμες πληροφορίες για πιθανές επιθέσεις και εύρεση αδύναμων σημείων. Για αυτό το λόγο και αυτές οι πληροφορίες πρέπει να προστατεύονται και να υπάγονται στο μοντέλο ιδιωτικότητας.

Η μη-αποκήρυξη είναι ένας μηχανισμός ασφαλείας που προστατεύει το ένα μέρος μιας συναλλαγής από ψευδή άρνηση της συναλλαγής από το άλλο μέρος (π.χ. άρνηση ηλεκτρονικής πληρωμής ή παραγγελίας). Οι σχετικές τεχνικές παρέχουν αξιόπιστες ψηφιακές αποδείξεις που μπορούν να δοθούν σε ένα τρίτο μέρος (π.χ. δικαστήριο) που θα επιλύσει τη διαμάχη. Συνήθως για τους σκοπούς αυτούς χρησιμοποιούνται οι ψηφιακές υπογραφές.

Από τη πλευρά του χρήστη τώρα, υπάρχει η απαίτηση της ιδιωτικότητας. Η ιδιωτικότητα παραμένει ίσως η πιο σημαντική πλευρά της ασφάλειας στα πλαίσια του ανθρωποκεντρικού προσωπικού δικτύου, καθώς είναι η εικόνα της ασφάλειας που αγγίζει άμεσα το χρήστη [9]. Οι απαιτήσεις ιδιωτικότητας προκύπτουν από τις ανάγκες ιδιωτικότητας του χρήστη – οι οποίες μερικές φορές έρχονται σε αντίθεση με τις ανάγκες χρήστη σχετικά με τη λειτουργικότητα και το κόστος- καθώς και σχετικούς κανονισμούς και νομοθεσίες [10][11]. Οι σχετικές οδηγίες για την ιδιωτικότητα καλύπτουν 4 βασικές περιοχές:

- **Ενημέρωση**: ο χρήστης πρέπει να είναι ενήμερος ανά πάσα στιγμή για το είδος ης πληροφορίας που συλλέγεται για αυτόν, τη χρήση της καθώς και τη διάθεση σε τυχόν τρίτα μέρη.
- **Επιλογή**: ο χρήστης πρέπει να έχει την επιλογή διάθεσης ή όχι των δεδομένων του.
- **Πρόσβαση**: ο χρήστης πρέπει να έχει πρόσβαση στη πληροφορία που αποθηκεύεται για αυτόν και να έχει το δικαίωμα ανά πάσα στιγμή να την τροποποιεί ή και να την σβήνει.
- **Ασφάλεια**: λογικά μέτρα πρέπει να ισχύουν ώστε να προστατεύεται (τεχνικά και επιχειρησιακά) τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση.

Όποτε είναι δυνατό, χρήση εναλλακτικών μεθόδων ταυτοποίησης ή ανωνυμίας θα ενίσχυε την ιδιωτικότητα του συστήματος. Σε περιπτώσεις όπου απαιτούνται δεδομένα από το χρήστη στα πλαίσια π.χ. μιας υπηρεσίας, ο χρήστης θα πρέπει να ελέγχει τις πολιτικές ιδιωτικότητας του παρόχου της υπηρεσίας, ώστε να αντιλαμβάνεται τι ζητείται από αυτόν και πως θα χρησιμοποιηθεί. Ιδανικά ο χρήστης θα πρέπει να διαφημίζει τις προτιμήσεις ιδιωτικότητας που έχει και να διαφημίζονται με τη σειρά τους σε αυτόν μόνο κατάλληλες υπηρεσίες. Εφόσον ο πάροχος αποκτήσει προσωπικά δεδομένα, σχετικοί πιστοποιημένοι μηχανισμοί ασφαλείας πρέπει να υπάρχουν ώστε να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή των δεδομένων. Σε περίπτωση ειδικά χρήσης δεδομένων θέσης του χρήστη, σε γενικές γραμμές επιβάλλεται να ενημερώνεται ο χρήστης ότι θα γίνει εντοπισμός της θέσης του και να δίνει τη συγκατάθεση του. Ακόμη και αν ο χρήστης επιβεβαιώσει μια φορά, πρέπει η λειτουργία επιβεβαίωσης να συνεχίζει. Επιπλέον οι σχετικοί διακομιστές αποθήκευσης γεωγραφικών στοιχείων, σε περίπτωση που για στατιστικούς λόγους αποθηκεύουν π.χ. τις θέσεις των πελατών τους, αυτό θα πρέπει να

γίνεται με τρόπο που το αποσυνδέει από τη ταυτότητα τους, να είναι δηλαδή η γεωγραφική θέση ουσιαστικά ανώνυμη.

Πέραν των γενικών απειλών και απαιτήσεων, τα Προσωπικά Δίκτυα έχουν και μοναδικά στοιχεία που σίγουρα θα ελκύσουν επιθέσεις και το ενδιαφέρον κακόβουλων ανθρώπων. Έτσι πρέπει να ληφθούν υπόψη:

- Η μοναδικότητα της ψηφιακής ταυτότητας για όλο το δίκτυο είναι εξαιρετικά πρακτικό αλλά αυξάνει επίσης και την αξία της στα μάτια των κακόβουλων ανθρώπων
- Εξορισμού τέτοια δίκτυα φέρουν ευαίσθητα προσωπικά δεδομένα, χρηματοοικονομικά και άλλα πολύτιμα (από υλική αλλά και ψυχική σκοπιά) δεδομένα καθώς και υψηλά προσωποποιημένες και συχνά κρίσιμες υπηρεσίες, όπως π.χ. υπηρεσία επειγόντων ιατρικών περιστατικών
- Τα PN αναμένεται να είναι εν μέρει αυτό-οργανούμενα, φιλικά στο χρήστη και διαχειριζόμενα από απλούς χρήστες. Ο «φιλικός» διαχειριστής δικτύου για να παραπονεθούμε, πιθανόν να μην υπάρχει!
- Επίγνωση κατάστασης, διεισδυτικές εφαρμογές και υψηλή προσωποποίηση. Όλο και μεγαλύτερο κομμάτι της ζωής μας θα είναι ψηφιακό και «πάνω από το σύρμα»
- Κινητικότητα Χρήστη σε Ετερογενή δίκτυα και με χρήση ετερογενών από άποψης δυνατοτήτων συσκευών ενώ υπάρχει ανάγκη για έλεγχο πρόσβασης και ασφάλεια, παντού και πάντα

Ακολουθούν οι σκέψεις σχετικά με δύο τεχνικές ταυτοποίησης που έχουν δεχθεί αρκετή κριτική, για διαφορετικούς λόγους η κάθε μία: **κωδικοί** και **βιομετρικά** δεδομένα.

Οι **κωδικοί** είναι ο πιο διαδεδομένος τρόπος να ταυτοποιηθεί ένας χρήστης σε ένα σύστημα. Στο προσωπικό δίκτυο πρέπει να ληφθεί υπόψη ο ετερογενής χαρακτήρας των δικτύων και των συσκευών. Επιπλέον το PN-F αποτελεί ένα συνασπισμό τέτοιων συνόλων. Τεχνικές ενιαίας εισόδου στο δίκτυο, *Single-Sign-On (SSO)*, είναι επιθυμητές αλλά και αρκετά πολύπλοκες στην εφαρμογή. Ο χρήστης εξάλλου δεν θα πρέπει να χρειάζεται αρκετούς κωδικούς προκειμένου να χρησιμοποιεί τις διάφορες προσωπικές υπηρεσίες μέσα σε ένα PN. Αν ίσχυε αυτό θα καταλήγαμε είτε στο να ξεχνιούνται συχνά κωδικοί, είτε να χρησιμοποιείται ο ίδιος σε όλα τα συστήματα, είτε να χρησιμοποιούνται υπερβολικά απλοί και ευάλωτοι κωδικοί. Η αλήθεια είναι ότι ο λεγόμενος «ανθρώπινος παράγοντας» [12] έχει πολύ κακό ιστορικό χρήσης κωδικών. Οι άνθρωποι ξεχνάνε τους κωδικούς τους, χρησιμοποιούνε προφανείς κωδικούς ή τους σημειώνουν σε κοινή θέα σε κάποιο τετράδιο. Επιπλέον, με τη πρώτη ευκαιρία δε θα διστάσουν να το μοιραστούν με τον άγνωστο «διαχειριστή δικτύου» που τους τον ζητάει με e-mail (*Phishing, κοινωνική μηχανική - social engineering*). Επομένως και προκειμένου να προστατευτεί το προσωπικό δίκτυο από αυτόν που οι ειδικοί ασφάλειας λένε ως «χειρότερο εχθρό», δηλαδή από τον ίδιο το χρήστη, η χρήση κωδικών πρέπει να ελαχιστοποιείται.

Ο κόσμος συχνά ανησυχεί και πλέκει περίεργα σενάρια στο μυαλό του όταν ακούει για συστήματα ασφαλείας βασισμένα στα **βιομετρικά δεδομένα** [13]. Και πολύ καλά κάνει. Το PN είναι ένα δίκτυο που εξορισμού ανήκει σε ένα συγκεκριμένο άνθρωπο. Αν γινόταν χρήση βιομετρικών δεδομένων όπως δακτυλικών αποτυπωμάτων ή σάρωσης της ίριδας, τα δίκτυα αυτά θα είχαν να αντιμετωπίσουν επιθέσεις αρπαγής τέτοιων κρίσιμων δεδομένων, η

ένταση και τεχνογνωσία των οποίων θα ήταν ανάλογη της κοινωνικής θέσης που θα κατείχε ο ιδιοκτήτης του δικτύου. Επιπλέον η καθημερινή και εκτεταμένη χρήση των Προσωπικών Δικτύων εντείνει αυτές τις απειλές. Τέλος, οπως συχνά λέγεται, ο χαμένος κωδικός αντικαθίσταται. Όμως η προοπτική κλοπής βιομετρικών δεδομένων είναι πραγματικά ζοφερή. Με αυτή τη λογική, η χρήση βιομετρικών δεδομένων αποκλείεται στα πλαίσια των Προσωπικών Δικτύων.

Απειλές

Για να οριστούν και αξιολογηθούν καταλλήλως οι απειλές, πρέπει να αναγνωριστούν ανάλογα και οι πηγές απειλών. Σύμφωνα με τον Stoneburner [14] οι πηγές απειλών κατατάσσονται στις εξής τρεις κατηγορίες: φυσικές, ανθρώπινες και περιβαλλοντικές. Οι φυσικές αναφέρονται σε φυσικές καταστροφές που μπορεί να προκαλέσουν φθορά στις συσκευές και στην υποδομή του Προσωπικού Δικτύου. Οι ανθρώπινες απειλές πηγάζουν από γεγονότα τα οποία άμεσα ή έμμεσα προκαλούν άνθρωποι, όπως ακούσια κακή χρήση του συστήματος ή εσκεμμένες πράξεις εναντίον του. Τέλος, οι περιβαλλοντικές έχουν να κάνουν με αποτυχία των τεχνητών εγκαταστάσεων που περιβάλλουν το δίκτυο, π.χ. τροφοδοσίας ρεύματος, μόλυνση, πλημμύρα λόγω βλάβης στα υδραυλικά κ.α. Πέραν αυτής της γενικής ανάλυσης, ειδικές απειλές για τα PN και PN-F πρέπει να αναγνωριστούν και να ληφθούν υπόψη.

Οι γενικές απαιτήσεις ασφαλείας εξάγονται για να αντιμετωπίσουν παραδοσιακές απειλές και επιθέσεις όπως: Denial of Service (DoS), Man-in-the-Middle, Message Alteration, Eavesdropping, Spoofing, Replay και Phishing επιθέσεις [7][15]. Είναι όμως τα ειδικά χαρακτηριστικά ενός συστήματος, που αναπόφευκτα μαζί με ειδικά πλεονεκτήματα, του δίνουν και ειδικές αδυναμίες, και το κάνουν ευάλωτο σε νέες προσαρμοσμένες επιθέσεις εναντίον του. Όπως θα αναλυθεί παρακάτω, χρησιμοποιώντας τις ειδικές συνθήκες που αναφέρθηκαν παραπάνω για τα Προσωπικά Δίκτυα, ένας κακόβουλος χρήστης μπορεί να αποκτήσει αρκετά ευκολότερα πρόσβαση και με χαμηλό κόστος εκμεταλλευόμενος π.χ. την αφέλεια ή αμέλεια του μέσου χρήστη του PN (ο γνωστός ανθρώπινος παράγοντας). Ο δρόμος για πολύτιμα δεδομένα και υπηρεσίες είναι αρκετά ευκολότερος σε αυτή τη περίπτωση.

Λόγω της φύσης και των ειδικών χαρακτηριστικών των Προσωπικών Δικτύων, οι σχετικές με τον άνθρωπο απειλές είναι μακράν και οι πιο σημαντικές. Οι απειλές μπορεί να προέλθουν από αμέλεια ή αφέλεια του ίδιου του ιδιοκτήτη, μέσω μελών PN-F με π.χ. συσκευές που έχουν διαφθαρεί ή από εξωτερικούς κακόβουλους χρήστες που είτε εξαπολύουν απευθείας επιθέσεις στην ασφάλεια και την ιδιωτικότητα του συστήματος είτε υποκλέπτουν πληροφορίες «στήνοντας αυτί» στου διαύλους επικοινωνίας μιας PN-F.

Προσπαθώντας να αναγνωρίσουμε τις ιδιαίτερες απειλές, συμπληρώνουμε την εξής λίστα:

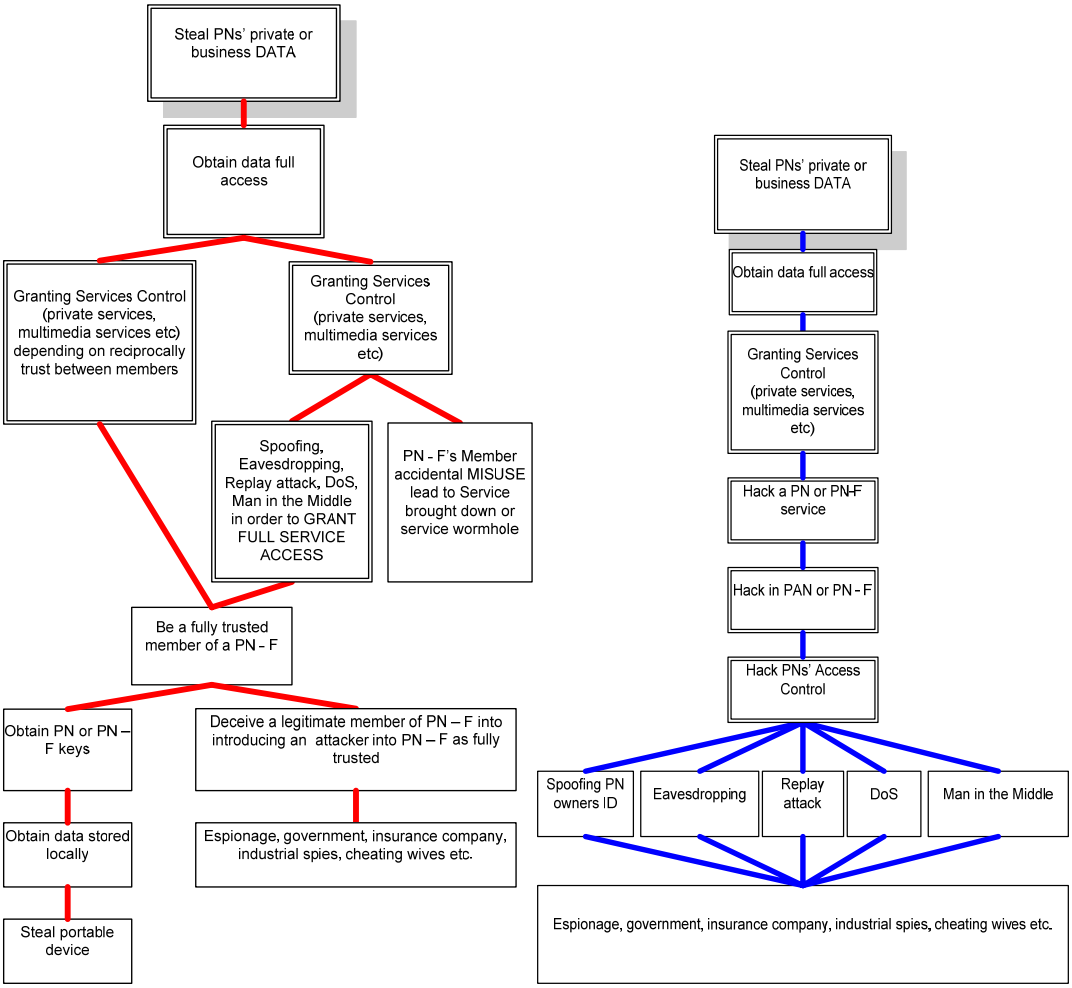
- Πλαστογραφία αναγνωριστικών για να αποκτηθεί πρόσβαση σε προσωπικά δεδομένα (*Spoofing*)
- Ωτακουστές (*Eavesdropping*) εις βάρος μελών συνομοσπονδίας
- Κλοπή ταυτότητας PN
- DoS στον διακομιστή σχηματισμού συνασπισμών
- Μη επιθυμητή αποκάλυψη πληροφορίας

- Κοινωνική Μηχανική – *Social Engineering*

Τα σημεία εισόδου για πιθανές επιθέσεις στο PN-F είναι συνήθως σε κεντρικές διαχειριστικές οντότητες. Ακόμη και όταν η επίθεση δεν αφορά άμεσα αυτές τις οντότητες, η σχετική κίνηση πρέπει να περάσει από αυτούς συνήθως. Επομένως το κύριο σημείο αποτυχίας θα πρέπει να θεωρηθεί ο διαχειριστής συνασπισμών.

Όσον αφορά τα αδύναμα σημεία (*vulnerabilities*), αυτά μπορεί να προκύψουν από αδύναμους κωδικούς, ατέλειες στο λογισμικό (*bugs*), ιούς, με script ή SQL injections, ή με κακόβουλα προγράμματα που εγκαταστήσαμε εν αγνοία μας. Αυτά μπορούν να αντιμετωπιστούν με συχνές ανανεώσεις και διορθώσεις του λογισμικού, κατάλληλες ρυθμίσεις και φυσικά, με επαγρύπνηση. Αυτό βέβαια προϋποθέτει σωστή και πλήρη ανάλυση απειλών ώστε να είμαστε ενήμεροι για το ποια είναι τα αδύναμα σημεία στο σύστημα μας και να είμαστε σε σχετική «επιφυλακή».

Στα Προσωπικά Δίκτυα όμως, η πλευρά στην οποία οφείλουμε να στρέψουμε τη προσοχή μας είναι αυτή που εμπλέκει τον ανθρώπινο παράγοντα. Για παράδειγμα, μια κινητή συσκευή, που αποτελεί ένα σημαντικό κόμβο του PN, μπορεί κατά γενική ομολογία να κλαπεί εύκολα και να επιτραπεί έτσι στο κλέφτη να αποκτήσει πρόσβαση σε προσωπικά δεδομένα και υπηρεσίες, ακόμη και αν αυτές δεν είναι στη συσκευή αλλά σε κάποιο άλλο μέρος του PN του οποίου τα πιστοποιητικά είναι πλέον στα χέρια του κλέφτη [16]. Εξάλλου, σε μια πρώιμη ανάλυση απειλών .που έγινε νωρίς στα πλαίσια της διατριβής μου [17], κατασκευάστηκαν ενδεικτικά τα δένδρα επίθεσης για την επίτευξη ενός κακόβουλου στόχου στο PN: την κλοπή συγκεκριμένα απόρρητων επαγγελματικών δεδομένων. Στο ένα δένδρο ακολουθήθηκαν μέθοδοι παραδοσιακών επιθέσεων κατά των αποθεμάτων και στοιχείων του δικτύου, ενώ στο άλλο δένδρο έγιναν επιθέσεις κατά του ανθρώπινου παράγοντα (*κοινωνική μηχανική, κλοπή συσκευής*). ΄Όπως φαίνεται και στην Εικόνα 11, η μεν παραδοσιακή οδός απαιτεί ειδική τεχνογνωσία και εξοπλισμό σε αρκετές περιπτώσεις από τον επιτιθέμενο. Η εκμετάλλευση του ανθρώπινου παράγοντα έρχεται με μηδενικό σχεδόν κόστος.(ειδικά στη περίπτωση κοινωνικής μηχανικής) και τεχνογνωσία. Το μόνο που απαιτείται είναι η απροσεξία, αμέλεια ή αφέλεια ή συνδυασμός αυτών από πλευράς χρηστών PN.



Εικόνα 11 – Σύγκριση δένδρων επίθεσης κλοπής επαγγελματικών δεδομένων μέσω (αριστερά) αποτυχίας ανθρώπινου παράγοντα και (δεξιά) τυπικών επιθέσεων κατά των στοιχείων του δικτύου

Συνοψίζοντας τα αδύναμα σημεία, κατασκευάζεται η λίστα από αδυναμίες του συστήματος σε σχέση με τις προαναφερθείσες απειλές:

- Φυσική ασφάλεια κινητών και φορητών συσκευών (είτε από αμέλεια του χρήστη, είτε από στοχευόμενη κίνηση κλέφτη).
- Αδύναμη ή ανύπαρκτη κρυπτογράφηση στο δίαυλο επικοινωνίας, προκειμένου να εξασφαλιστεί ασφαλής μεταφορά πληροφορίας (π.χ. πάνω από Bluetooth).
- Ανυπαρξία κεντρικών υποδομών ασφαλείας (π.χ. έλεγχου πρόσβασης, υποδομής δημοσίου κλειδιού *public key infrastructure - PKI*, IDS κ.α.) σε ορισμένες περιοχές προσωπικού δικτύου, λόγων περιορισμένων αποθεμάτων σε επίπεδο πρωτοκόλλου επικοινωνίας και συσκευών
- DoS στον διαχειριστή συνασπισμών κατά τη φάση σχηματισμού PN-F
- Πρόβλημα ιδιωτικότητας στη φάση σχηματισμού PN-F: κατά τη διάρκεια των διαπραγματεύσεων η αποστολή των προφίλ συμμετοχής είναι επώνυμη και μη αναστρέψιμη διαδικασία
- Κακή διαχείριση ρυθμίσεων ιδιωτικότητας και σχετική αδιαφορία χρηστών για το θέμα, μπορεί να οδηγήσει σε αποκάλυψη πληροφορίας

- Διάθεση προσωπικής πληροφορίας και πληροφορίας κατάστασης από τους παροχείς υπηρεσιών σε τρίτους
- Αδύναμοι κρυπτογραφικά κωδικοί
- Αφέλεια Χρήστη προς Πλαστοπροσωπίες (χρήστες)
- Αφέλεια Χρήστη προς Phishing (υπηρεσίες).
- Αμέλεια φύλαξης συσκευών και σωστού κλειδώματος (ψηφιακού και αναλογικού…)

Προκειμένου να αντιμετωπιστούν τα παραπάνω ευάλωτα σημεία, η απαραίτητη υποδομή και εφαρμογές ασφαλείας πρέπει να ενσωματωθούν στην υποδομή ή αρχιτεκτονική του PN και PN-F. Στην επόμενη παράγραφο εξετάζεται τι παρέχεται από τις υπάρχουσες λύσεις.

3.5. Αντιμετωπίζοντας τις απειλές: υπάρχουσες λύσεις και υπόβαθρο ασφαλείας για τα Προσωπικά Δίκτυα

Έχοντας αναλύσει τις απειλές και τους κινδύνους, σε αυτό το υποκεφάλαιο παρουσιάζονται λύσεις που είτε μειώνουν τη πιθανότητα υλοποίησης μιας απειλής, είτε αμβλύνουν τις επιπτώσεις στο σύστημα. Στα πλαίσια των Προσωπικών Δικτύων οι λύσεις πρέπει να είναι εστιασμένες στο χρήστη και τη διασφάλιση της ιδιωτικότητας, λαμβάνοντας υπόψη τον ανθρώπινο παράγοντα. Καθώς η ασφάλεια του συστήματος είναι τόσο ισχυρή όσο ο πιο αδύναμος κρίκος της, οι λύσεις πρέπει να καλύπτουν το PN από άκρη σε άκρη, και σε όλα τα στρώματα.

Καταρχήν, τα PN είναι προστατευμένα από επιθέσεις στο στρώμα δικτύου με χρήση σύγχρονων μηχανισμών δικτυακής προστασίας όπως firewalls, IDS και ασφαλών υποκείμενων διαύλων επικοινωνίας (π.χ. τεχνολογίες εικονικού ιδιωτικού δικτύου, *Virtual Private Network - VPN*). Αυτοί οι μηχανισμοί ουσιαστικά αποτελούν το υπόβαθρο ασφαλείας που από πάνω τους πρέπει να προστατευτούν και σε επίπεδο εφαρμογής οι υπηρεσίες, οι εφαρμογές και οι ίδιοι οι χρήστες. Στόχος είναι μια ολοκληρωμένη διαστρωματική (cross-layer) λύση ασφαλείας για τα PN και PN-F.

Ένα βασικό θέμα σε κάθε σύστημα ασφαλείας είναι η αρχικοποίηση των σχέσεων εμπιστοσύνης. Σε αυτά τα πλαίσια προτάθηκε η ιδέα της αποτύπωσης (*imprinting*) [3]. Η αποτύπωση ορίζεται ως η διαδικασία κατά την οποία δύο κόμβοι που δεν έχουν σχέση εμπιστοσύνης εκ των προτέρων μεταξύ τους, συστήνονται ο ένας στον άλλον με το σκοπό της εγκαθίδρυσης μακροπρόθεσμης σχέσης εμπιστοσύνης, και τυπικά απαιτεί γεωγραφική εγγύτητα. Ένα παράδειγμα είναι η διαδικασία αποτύπωσης που χρησιμοποιούν συσκευές Bluetooth αλλά το συγκεκριμένο πρωτόκολλο είναι ευρέως γνωστό ότι περιέχει γνωστές αδυναμίες και τρωτά σημεία. Η λύση είναι λοιπόν να οριστεί ένα πρωτόκολλο αποτύπωσης που βασίζεται σε δυνατότερους αλγόριθμους ασφαλείας και να προσαρμοστεί σε όλες τις ασύρματες τεχνολογίες. Στή [16] περιγράφεται ένα πρωτόκολλο αποτύπωσης βασισμένο στην ανταλλαγή Diffie-Hellman. Η διαδικασία γίνεται κάτω από την άμεση επίβλεψη του χρήστη, που μεταφέρει χειροκίνητα ένα μικρό άθροισμα ελέγχου (βασισμένο στα δημόσια κλειδιά των συσκευών) μεταξύ των δύο συσκευών που αποτυπώνονται.

Ως αποτέλεσμα της αποτύπωσης οι ομότιμοι προσωπικοί πλέον κόμβοι αποκτούν ένα κοινό μακροπρόθεσμο κλειδί μεταξύ τους, Ο κύριος στόχος της διαδικασίας αποτύπωσης

είναι να παρέχει τα κλειδιά που θα επιτρέψουν την ασφαλή επικοινωνία κατά την ασύρματη μετάδοση της πληροφορίας. Ωστόσο, το κλειδί αυτό μπορεί να χρησιμοποιηθεί για να παράγει επιπλέον κλειδιά για χρήση στα διάφορα στρώματα, συμπεριλαμβανομένου των υπηρεσιών. Τέλος η χρήση της αποτύπωσης ανταποκρίνεται και στην απαίτηση της ελάχιστης χρήσης κωδικών που αναφέρθηκε πριν.

Όπως είδαμε, ο έλεγχος πρόσβασης είναι βασική απαίτηση για ένα σύστημα προκειμένου να θεωρηθεί ασφαλές. Στη [19], παρουσιάστηκε μία ασφαλής βασισμένη σε INS/Twine πρωτόκολλα αρχιτεκτονική ανακάλυψης υπηρεσιών, ειδικά σχεδιασμένη για Προσωπικά Δίκτυα και για λειτουργία P2P. Σε αυτή την αρχιτεκτονική, εξαρτήματα έλεγχου πρόσβασης και βάσεις προφιλ ασφαλείας σχεδιάστηκαν με τέτοιο τρόπο, ώστε να λειτουργούν με διανεμημένο τρόπο σε όλο το προσωπικό δίκτυο. Συγκεκριμένα, διασυνδεδεμένες οντότητες διαχείρισης της πρόσβασης πάνω από το δίκτυο επικάλυψης δρουν εντός της εμβέλειας τους, πέραν της οποίας μια ομότιμη οντότητα αναλαμβάνει. Με αυτό τον τρόπο επιτυγχάνεται έλεγχος πρόσβασης παντού και ανά πάσα στιγμή στο δίκτυο των PN.

Είναι σαφές, ότι σε επίπεδο δικτύου, τα όποια κενά στην ασφάλεια αφορούν κυρίως την αδυναμία -από πλευράς αποθεμάτων- των συσκευών και συγκεκριμένων πρωτοκόλλων επικοινωνίας, Σε αυτά τα πλαίσια κινούνται ελαφριοί αλγόριθμοι κρυπτογράφησης κατάλληλοι για κινητές συσκευές ή αρχιτεκτονικές βασισμένες σε μεσολαβητές (proxy). Σε επίπεδο εφαρμογής όμως, γίνεται φανερή η έλλειψη μηχανισμών ασφαλείας που αφενός να προσαρμόζονται και οι ίδιοι στις καταστάσεις, αφετέρου να εξασφαλίζουν ολοκληρωμένα την ιδιωτικότητα τόσο της προσωπικής όσο και συγκείμενης πληροφορίας. Επιπλέον, και ειδικά στα πλαίσια των συνασπισμών Προσωπικών Δικτύων η παραδοχή για εγγύτητα είναι αρκετά περιοριστική ενώ διαπιστώνεται και ζήτημα ιδιωτικότητας στη φάση σχηματισμού PN-F: κατά τη διάρκεια των διαπραγματεύσεων, καθώς η αποστολή των προφίλ συμμετοχής είναι επώνυμη και μη αναστρέψιμη διαδικασία. Επομένως η εγκαθίδρυση εμπιστοσύνης σε συνασπισμό PN-F με μηδενικές βάσεις αποτελεί πρόκληση.

3.6. Συμπεράσματα

Σε αυτό το κεφάλαιο εξετάστηκαν οι γενικές αλλά και ειδικές απαιτήσεις ασφαλείας και ιδιωτικότητας, με βάση τα σενάρια χρήσης Προσωπικών Δικτύων και συνασπισμών Προσωπικών Δικτύων. Η προσέγγιση αυτή αρμόζει στα πλαίσια του ανθρωποκεντρικού χαρακτήρα και σχεδίασης που διέπουν αυτά τα δίκτυα. Στη συνέχεια εξετάστηκε τί πρέπει να προστατευτεί, από τί απειλείται και ποιες είναι οι υπάρχουσες λύσεις αλλά και προτάσεις της έρευνας σχετικά.

Τέλος, αναγνωρίζονται οι απαιτούμενες ελλείψεις οι οποίες ουσιαστικά εκκίνησαν την έρευνα της διδακτορικής μου διατριβής. Διαπιστώθηκαν αδυναμίες τόσο στη φάση σχηματισμού των συνασπισμών και την εγκαθίδρυση εμπιστοσύνης, καθώς η αποστολή των προφίλ συμμετοχής είναι επώνυμη και μη αναστρέψιμη διαδικασία. Το δε πρωτόκολλο σχηματισμού κάνει την παραδοχή ότι ο ιδιοκτήτης γνωρίζει είτε διευθύνσεις δικτύου είτε υπηρεσιών που αντιστοιχούν στα μέλη του συνασπισμού, είτε ότι τα μέλη έδωσαν αυτές τις πληροφορίες απλόχερα. Επιπλέον, σε επίπεδο εφαρμογής γίνεται φανερή η έλλειψη μηχανισμών ασφαλείας που αφενός να προσαρμόζονται και οι ίδιοι στις καταστάσεις, αφετέρου να εξασφαλίζουν ολοκληρωμένα την ιδιωτικότητα τόσο της προσωπικής όσο και συγκείμενης πληροφορίας. Και στις δύο περιπτώσεις η χρήση και τα υπάρχοντα μοντέλα

πληροφορίας θέτουν προβλήματα ιδιωτικότητας καθώς συνδέουν τις πληροφορίες ταυτοποίησης με τα προσωπικά δεδομένα και τη συγκείμενη πληροφορία.

3.7. *Ειδική ορολογία κεφαλαίου*

Ελληνικός όρος / φράση	Αγγλικός όρος / φράση
Αμοιβαία ταυτοποίηση	Mutual authentication
Ανθρωποκεντρικός	User-centric
Διαστρωματική	Cross-layer
Διεπαφή	Interface
Δίκτυο επικάλυψης	Overlay network
Εικόνικό ιδιωτικό δίκτυο	Virtual Private Network - VPN
Επίγνωση κατάστασης	Context-awareness
Ιδιωτικό δίκτυο προσωπικής περιοχής	Private Personal Area Network – P-PAN
Κλιμάκωση	Scalability
Κοινωνική μηχανική	Social engineering
Μη-αποκήρυξη	Non-repudiation
Ομότιμη αρχιτεκτονική	P2P (Peer-to-peer) architecture
Περιουσιακά στοιχεία	Assets
Προσωπικού Δικτύου	Personal Network - PN
Προσωποποίηση	Personalisation
Συγκείμενη πληροφορία	Context
Συνασπισμός Προσωπικών Δικτύων	Personal Networks Federation – PN-F
Ταυτοποίηση	Authentication
Υποδομή δημοσίου κλειδιού	Public key infrastructure -PKI
Ωτακουστές	Eavesdropping

3.8. *Βιβλιογραφικές Αναφορές*

[1] Niemegeers, I.G., & Heemstra de Groot, S. (2002). From Personal Area Networks to Personal Networks: A user oriented approach. Journal on Wireless and Personal Communications, 22, 175-186.

[2] Lo, A., Jacobsson, M., Prasad, V. & Niemegeers, I.G. (2006). "Personal Networks: An Overlay Network of Wireless Personal Area Networks and 3G Networks", presented at the Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose California.

[3] Cook, D.J., Youngblood, M., Heierman, E.O., Gopalratnam, K., Rao, S., Litvin, A. & Khawaja, F. (2003). "MavHome: an agent-based smart home", Proceedings of the First International Conference Pervasive Computing and Communications 2003, Dallas, Texas.

[4] Intille, S.S. (2002). Designing a home of the future, IEEE Pervasive Computing, 1, 2, 76-82.

[5] IST-MAGNET Beyond Public Deliverable D1.4.2 "Defining Usability of PN Services", 2008, available from Internet: http://magnet.aau.dk/public+deliverables/BeyondWP1

[6] Patrikakis, Ch. Z., Voulodimos, A.S., Nikolakopoulos, I.G. (2008). "PLASMA: Personalized Location Aware Services over Mobile Architectures", presented at the 1st International Conference on PErvasive Technologies Related to Assistive Environments (PETRA 08), July 2008, Athens, Greece.

[7] Patrikakis C., Masikos M., Zouraraki O., (2004). "Distributed Denial of Service Attacks", Internet Protocol Journal, Cisco Systems, vol. 7, issue 4, pp 13 – 35.

[8] Schneier, B. (1996). "Applied Cryptography", John Wiley & Sons, 1996.

[9] Mark Ackerman, Trevor Darrell, and Daniel J. Weitzner, "Privacy In Context", MIT/Lab for Computer Science 2001.

[10] Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"

[11] [Federal Trade Commission, "PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE", May 2000.

[12] Bruce Schneier, "Secrets & Lies: Digital Security in a Networked World", 2000.

[13] Liu, S. Silverman, M. , Johns Hopkins Univ., MD; "A practical guide to biometric security technology", appears in: IT Professional, Publication Date: Jan/Feb 2001 Volume: 3, Issue: 1, On page(s): 27-32, 2001

[14] Stoneburner G., Goguen A., Feringa A., "Risk Management Guide for Information Technology Systems", Recommendations of the National Institute of Standards and Technology, July 2002

[15] Anderson, R. (2001). "Security Engineering", John Wiley & Sons, 2001.

[16] Politis, C., Nyberg, K., Mirzadeh, S., Masmoudi, K., Afifi, H., Floriou, J., Prasad, N.R. (2005). "Personal Network Security Architecture", International Wireless

Summit 2005, Wireless Personal Multimedia Communications'05, September 18-22, Aalborg, Denmark.

[17] Dimitris M. Kyriazanos and Michalis G. Argyropoulos, "Personal Networks: Security Risks and Solutions", submitted and accepted for oral presentation on the FITCE 45TH Congress "Telecom Wars: The return of the Profit", 30/8/2006 – 2/9/2006.

[18] Dimitris M. Kyriazanos, John Williams Floroiu et al, "MAGNET Personal Network Security Model: Trust Establishment, Policy Management and AAA Infrastructure", WWRF15 Meeting, Paris, France, December 2005

[19] Kyriazanos, D.M., Louati, W., Genet, M.G., Zeghlache, D., Argyropoulos, M., and Patrikakis, Ch.Z. (2006). "An Architecture for Secure Wide-Area Service Discovery in Personal Peer-to-Peer Networks", IST Mobile & Wireless Communications Summit, Mykonos Greece.

4. Εγκαθίδρυση Σχέσεων Εμπιστοσύνης με Ανώνυμη και Ασφαλή Ανταλλαγή Πληροφοριών πάνω από Προσωπικά Δίκτυα

4.1. Εισαγωγή

Προκειμένου οι χρήστες να συμμετάσχουν σε οποιοδήποτε σύστημα, πρέπει καταρχήν να το εμπιστεύονται. Επιπλέον, για να πειστούν οι χρήστες να εμπιστευτούν τις καθημερινές τους ασχολίες και τις σχετικές προσωπικές πληροφορίες σε ένα Προσωπικό Δίκτυο, είναι φανερό το πόσο επιτακτική είναι αυτή η ανάγκη για εμπιστοσύνη στο σύστημα. Στα πλαίσια του PN ο χρήστης έχει πρόσβαση σε τεχνολογία αιχμής προκειμένου να γίνεται απομακρυσμένη χρήση διαφόρων συσκευών και υπηρεσιών οπουδήποτε στο δίκτυο, εκθέτοντας με αυτό τον τρόπο στο μεταξύ την απαραίτητη προσωπική πληροφορία. Σκοπός των μηχανισμών ιδιωτικότητας και ανωνυμίας να αποκρύπτουν την πληροφορία αυτή, ή να την αποσυσχετίζουν από το χρήστη, και επομένως να την καθιστούν σε κάθε περίπτωση άχρηστη για κακόβουλους σκοπούς. Η διασφάλιση της ιδιωτικότητας στα Προσωπικά Δίκτυα είναι επομένως σημαντική και -όπως αναλύθηκε και στο προηγούμενο κεφάλαιο- συνδέεται με ακόμη πιο αυστηρές απαιτήσεις ασφαλείας από ότι σε άλλα συστήματα. Σχετικές λύσεις και προτεινόμενες αρχιτεκτονικές ανωνυμίας μελετήθηκαν στην [24] και απορρίφτηκαν είτε επειδή βασίζονται σε απαιτούμενες σύνθετες υποδομές, είτε σε σύνθετα μοντέλα εμπιστοσύνης και πολιτικών ασφαλείας που δεν είναι κατάλληλα για το ανθρωποκεντρικό και διανεμημένο περιβάλλον του PN, όπως π.χ. πρωτόκολλα και κανονισμοί ασφαλείας που εφαρμόζονται εύκολα στο εταιρικό περιβάλλον. Υπάρχουσες λύσεις ανωνυμίας που βασίζονται σε σύνθετη διανεμημένη εξόρυξη δεδομένων (*data mining*) επίσης είναι εκτός πεδίου του PN και PN-F περιβάλλοντος [12].

Η εφαρμογή μηχανισμών ανωνυμίας φέρει ιδιαίτερες σχεδιαστικές αλλά και κοινωνικές δυσκολίες όπως εξηγήθηκε και στην [9]. Η πρόταση που παρουσιάζεται σε αυτό το κεφάλαιο λαμβάνει υπόψη τις σχετικές προκλήσεις και απαιτήσεις, είτε είναι ειδικές για τα PN είτε γενικές. Με αυτό τον τρόπο είναι εφαρμόσιμη τόσο στο περιβάλλον του Προσωπικού Δικτύου αλλά αποτελεί και μια γενική λύση.

Τα PN φέρουν ευαίσθητα προσωπικά δεδομένα, όπως αριθμούς πιστωτικών καρτών, πληροφορίας υγείας καθώς και άλλα πολύτιμα δεδομένα. Εξορισμού τα PN είναι συνδέουν έναν συγκεκριμένο άνθρωπο με μια ευρεία συλλογή συσκευών, υπηρεσιών και αποθεμάτων του συστήματος. Αν μια συσχέτιση ενός χρήστη με ένα συγκεκριμένο απόθεμα του PN αποκαλυφτεί, τότε αποκάλυψη και άλλων συσχετίσεων μπορεί να ακολουθήσει, τερματίζοντας έτσι το δικαίωμα του χρήστη στην ιδιωτικότητα. Οι μηχανισμοί ανωνυμίας, που θα αποσυσχετίζουν την ταυτότητα του χρήστη κατά το δυνατόν στις καθημερινές του συναλλαγές, είναι απαραίτητοι στα Προσωπικά Δίκτυα. Επιπλέον, τα PN αποτελούνται από διανεμημένα και διασυνδεδεμένα δίκτυα ετερογενών συσκευών και διεπαφών, επομένως οι σύνθετες κεντρικοποιημένες υποδομές δεν μπορούν να θεωρηθούν δεδομένες ανά πάσα στιγμή. Τέτοιες υποδομές μπορεί να μην υπάρχουν κατά παραγγελία και επίσης εξαρτώνται από τη διαθεσιμότητα δημοσίων δικτύων. Επομένως κάθε προτεινόμενο μοντέλο οφείλει να υποστηρίζει και λειτουργία με ομότιμη επικοινωνία (*Peer-to-peer, P2P communication*) μεταξύ των οντοτήτων. Τέλος, τα Προσωπικά Δίκτυα πρέπει να είναι όσο το δυνατόν αυτοδιαχειριζόμενα, φιλικά στο χρήστη και εύκολο να διαχειριστούν και από έναν απλό

χρήστη χωρίς ιδιαίτερες τεχνικές γνώσεις. Οπότε οι κατάλληλες προτάσεις δεν πρέπει να επιβάλλουν σύνθετα καθήκοντα διαχείρισης στον χρήστη.

Σε αυτά τα πλαίσια και ικανοποιώντας τις σχετικές απαιτήσεις, προτείνεται η λύση της ασφαλούς και ανώνυμης ανταλλαγής προσωπικής πληροφορίας μεταξύ των συμμετεχόντων σε ένα συνασπισμό Προσωπικών Δικτύων PN-F κατά την ευαίσθητη φάση της εγκαθίδρυσης εμπιστοσύνης, ώστε να διασφαλίζεται η ιδιωτικότητα σε όλη τη διαδικασία. Η λύση περιλαμβάνει καταρχήν ένα καινοτόμο μοντέλο αποσυσχέτισης της ταυτότητας του χρήστη από τις προτιμήσεις και λοιπές προσωπικές του πληροφορίες, έτσι ώστε η ανταλλαγή των πληροφοριών αυτών και η αντιστοίχιση των προφίλ χρήστη κατά την αρχικοποίηση ενός PN-F να γίνεται ανώνυμα. Επίσης προβλέπονται οι σχετικοί μηχανισμοί κρυπτογράφησης και πρωτόκολλα ασφαλείας, ώστε να θωρακίζεται ο προτεινόμενος μηχανισμός κατά των υποκλοπών (*eavesdropping*).

Με αυτό τον τρόπο η προτεινόμενη λύση διασφαλίζει την ιδιωτικότητα μέσω ανωνυμίας κατά την ανταλλαγή προσωπικής πληροφορίας, ενώ ενσωματώνονται και μηχανισμοί για εντοπισμό και αντιμετώπιση κακόβουλης συμπεριφοράς, καθώς και θωράκιση απέναντι σε επιθέσεις κατά του συστήματος. Ακολουθεί η αναλυτική περιγραφή της πρότασης και η σχετική μελέτη αντοχής σε απειλές και επιθέσεις. Τέλος, η πρόταση αξιολογείται τόσο για την δυνατότητα εφαρμογή της μέσω ενδεικτικής υλοποίησης που έγινε όσο και σε σύγκριση με σχετικές υπάρχουσες λύσεις.

4.2. Προτεινόμενη λύση διασφάλισης της ιδιωτικότητας με ανωνυμία της ανταλλασσόμενης πληροφορίας

Καταρχήν πρέπει να αναγνωριστούν οι βάσεις και οι συνθήκες υπό τις οποίες λαμβάνει χώρα η εγκαθίδρυση μιας συνομοσπονδίας PN-F.

Προκειμένου να σχηματιστεί μια συνομοσπονδία Προσωπικών Δικτύων, μέρος της πληροφορίας που αποτελεί την προσωπική πληροφορία του χρήστη πρέπει να ανταλλαχθεί μεταξύ χρηστών Προσωπικών Δικτύων, έτσι ώστε να αποφασιστεί ποιοι θα συμμετάσχουν στη συνομοσπονδία. Γι αυτό το σκοπό η πληροφορία χωρίζεται σε δυο ομάδες: δεδομένα ταυτοποίησης και δεδομένα προσωπικών προτιμήσεων και κατάστασης.

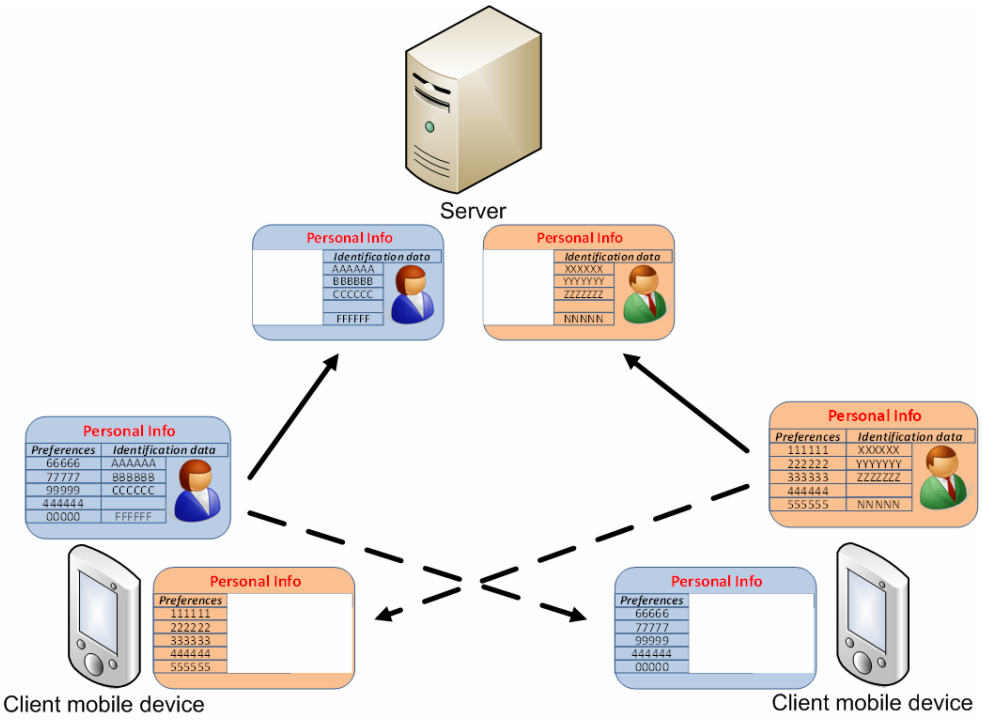
- *Τα δεδομένα ταυτοποίησης* αποτελούνται από όλη την πληροφορία που απαιτείται για να αναγνωριστεί ο χρήστης, μαζί με όλα τα δεδομένα τα οποία εισάγονται σε μηχανισμούς αυθεντικοποίησης και ελέγχου πρόσβασης. Π.χ.: όνομα χρήστη, ταυτότητα εγγραφής υπηρεσίας κ.α.

- *Οι προσωπικές προτιμήσεις και δεδομένα κατάστασης* περιέχουν πληροφορίες όπως προσωπικές προτιμήσεις και κατάστασης, και μπορεί να χρησιμοποιηθούν ως εισαγωγή σε μηχανισμό αναζήτησης και ομαδοποίησης χρηστών ώστε να στηθεί μια συνομοσπονδία Προσωπικών Δικτύων [13]. Π.χ.: επαγγελματική κατάσταση και ενδιαφέροντα, ασχολίες ελεύθερου χρόνου καθώς και πληροφορίες επίγνωσης κατάστασης όπως η τοποθεσία του χρήστη ακόμα και η διάθεση του.

Προκειμένου να διασφαλίσουμε την ιδιωτικότητα της πληροφορίας που ανταλλάσσεται κατά το στήσιμο μιας συνομοσπονδίας Προσωπικών Δικτύων, οι δυο διαφορετικές ομάδες προσωπικών δεδομένων χειρίζονται διαφορετικά: τα δεδομένα ταυτοποίησης

χρησιμοποιούνται για να αυθεντικοποιηθεί ο χρήστης και να αποκτήσει πρόσβαση, χωρίς να συνδέεται με τα δεδομένα προσωπικών προτιμήσεων και κατάστασης που εντωμεταξύ χρησιμοποιούνται στο ταίριασμα των προφίλ χρήστη. Όταν η αυθεντικοποίηση επιτευχθεί και τα ανώνυμα προφίλ ομαδοποιηθούν, τα κομμάτια αυτά μπορεί να ενωθούν για να δώσουν ένα σύνολο πληροφορίας που έχει νόημα προκειμένου να στηθεί το PN-F. Αυτό μπορεί να δοθεί με ομότιμο τρόπο, με απευθείας ανταλλαγή πληροφορίας μεταξύ των χρηστών (Εικόνα 12).

Χωρίζοντας λοιπόν την προσωπική πληροφορία σε δύο ομάδες επιτυγχάνεται η δυνατότητα ανώνυμης αποστολής πληροφορίας απαραίτητης για το σχηματισμό σχέσεων εμπιστοσύνης. Εξασφαλίζεται ιδιωτικότητα καθώς οι προσωπικές πληροφορίες αφαιρούνται ουσιαστικά από τα δεδομένα ταυτοποίησης καθώς και ανωνυμία, καθώς οι πληροφορίες ταυτοποίησης επίσης αφαιρούνται κατά την ανταλλαγή των υπόλοιπων προσωπικών πληροφοριών. Είναι δε μια σημαντική απαίτηση ασφαλείας κατά το σχηματισμό PN-F, καθώς δεν είναι γνωστό εκ των προτέρων αν μπορούμε να εμπιστευθούμε ή αν γνωρίζουμε όλα τα υποψήφια μέλη της συνομοσπονδίας.



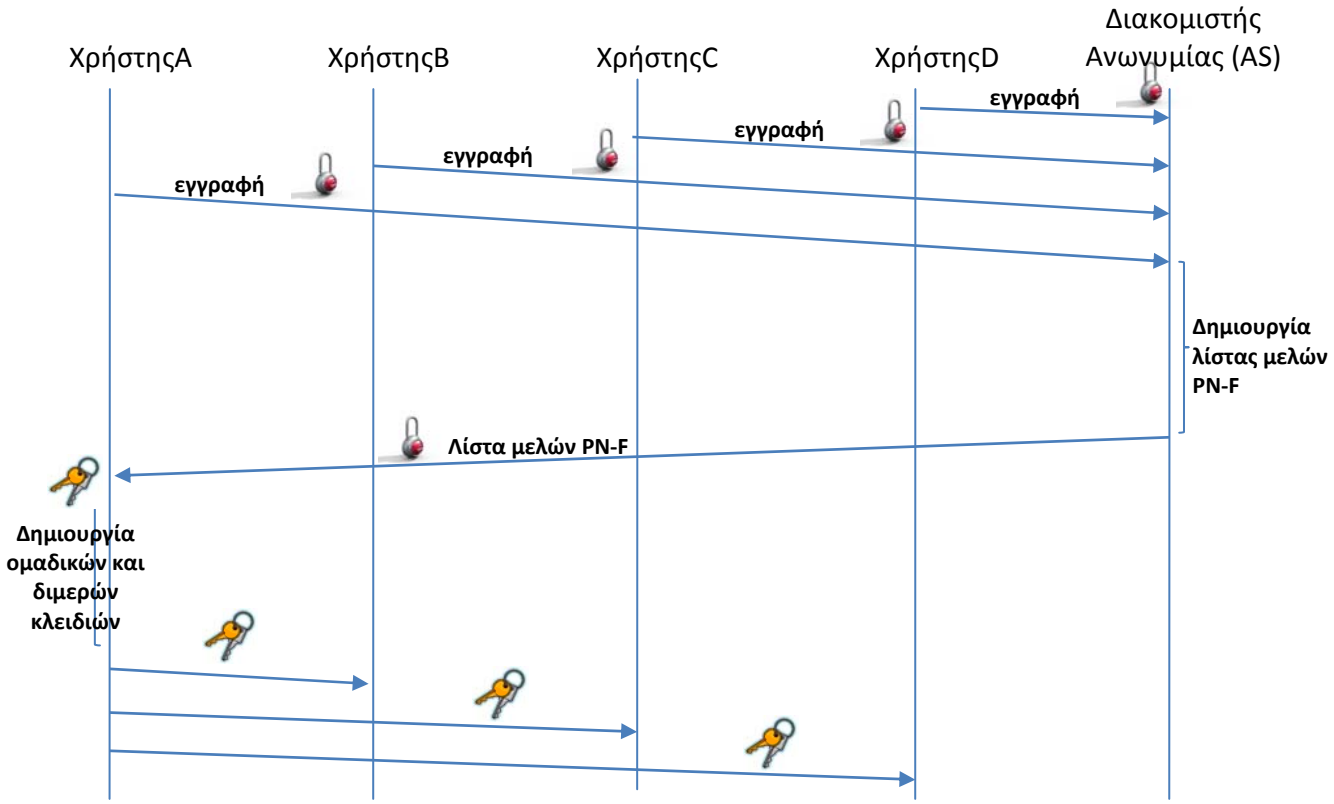
Εικόνα 12 - Αποσυσχετίζοντας τις προσωπικές προτιμήσεις από τα δεδομένα ταυτοποίησης

Το μοντέλο εμπιστοσύνης

Στο προτεινόμενο μοντέλο, αρχικά όλες οι σχέσεις εμπιστοσύνης μεταξύ των χρηστών και μιας κεντρικής οντότητας υπεύθυνης για την επιλογή των ομότιμων μελών μιας PN-F εγκαθίστανται μέσω μιας κατάλληλης διανομής και διαχείρισης κλειδιών. Ονομάσαμε την κεντρική οντότητα Εξυπηρετητή Ανωνυμίας (Anonymising Server – AS), και μπορεί να θεωρηθεί ως τρίτο εμπιστευόμενο μέρος. Προκειμένου να ξεπεραστούν προβλήματα διανομής κλειδιών και έλλειψη προϋπαρχόντων συνθηκών ασφαλείας (συνήθης περίπτωση σε αυτοοργανούμενες περιπτώσεις), το μοντέλο επωφελείται από την κρυπτογραφία δημοσίου κλειδιού [17], ένα ασυμμετρικό σχήμα που χρησιμοποιεί ένα ζεύγος κλειδιών: το δημόσιο, που κρυπτογραφεί δεδομένα και δεν είναι κρυφό, και ένα αντίστοιχο ιδιωτικό, το οποίο χρησιμοποιείται για την αποκρυπτογράφηση και είναι μυστικό. Προκειμένου να εγκαθιδρυθεί εμπιστοσύνη, τα ακόλουθα βήματα ακολουθούνται σύμφωνα με την πρόταση:

- Κάθε χρήστης εγγράφεται στον AS. Αυτό βασίζεται είτε σε ανταλλαγή κλειδιών είτε με μια απλή αυθεντικοποίηση με κωδικό πρόσβασης. Το αποτέλεσμα είναι ότι ο χρήστης αυθεντικοποιείται η επικοινωνία με τον AS είναι ασφαλής.

- Ο χρήστης μπορεί πλέον να δηλώσει ενδιαφέρον για να συμμετάσχει ή να δημιουργήσει κάποιο PN-F. Το αν θα γίνει δεκτός ή όχι εξαρτάται από τις πολιτικές ασφαλείας του εκάστοτε PN-F (π.χ. δημόσιες συνομοσπονδίες, κωδικός πρόσβασης, απαίτηση για πρόσκληση/εισιτήριο).



Εικόνα 13 – Εγκαθιδρώντας την υποδομή εμπιστοσύνης

- Ο AS παρέχει σε όλους τους εγγεγραμμένους χρήστες μια λίστα με όλα τα πιθανά μέλη της PN-F. Χρησιμοποιώντας υποδομή δημοσίου κλειδιού (Public Key Infrastructure -

PKI), οι χρήστες μπορούν να εκδώσουν ένα ομαδικό κλειδί για χρήση επικοινωνίας στα πλαίσια της PN-F. Αυτό μπορεί να γίνει είτε ομότιμα και αποκεντροποιημένα (ξεκινώντας από τον χρήστη δημιουργό και χρησιμοποιώντας μη ιεραρχικό PKI π.χ. PGP) είτε κεντρικά με χρήση μιας Αρχής Πιστοποιητικών. Οι χρήστες μπορούν επίσης να ανταλλάξουν κλειδιά μεταξύ τους έτσι ώστε να επιτραπεί ασφαλής απευθείας επικοινωνία μεταξύ τους σε μετέπειτα στάδια. Και πάλι PKI χρησιμοποιείται για αυτή τη περίπτωση.

Με αυτό το τρόπο η λεγόμενη υποδομή εμπιστοσύνης έχει στηθεί (Εικόνα 13).Τώρα οι χρήστες μπορούν να προχωρήσουν στο σχηματισμό μιας PN-F ακολουθώντας τα εξής βήματα:

- Κάθε χρήστης κρυπτογραφεί ανάλογα με την εφαρμογή το σχετικό κομμάτι από το Προφίλ του (π.χ. προσωπικές προτιμήσεις, κατάσταση) χρησιμοποιώντας το ομαδικό κλειδί. Επομένως το περιεχόμενο αμέσως γίνεται μυστικό όσον αφορά τον AS, καθότι δεν ανήκει στην ομάδα και επομένως δε κατέχει το σχετικό μυστικό κλειδί.

- Οι χρήστες αυθεντικοποιούνται, καταθέτουν τη κρυπτογραφημένη πληροφορία Προφίλ στον AS, ο οποίος τηρεί έναν πίνακα όπου αντιστοιχίζονται οι χρήστες με το αντίστοιχο κρυπτο-κείμενο.

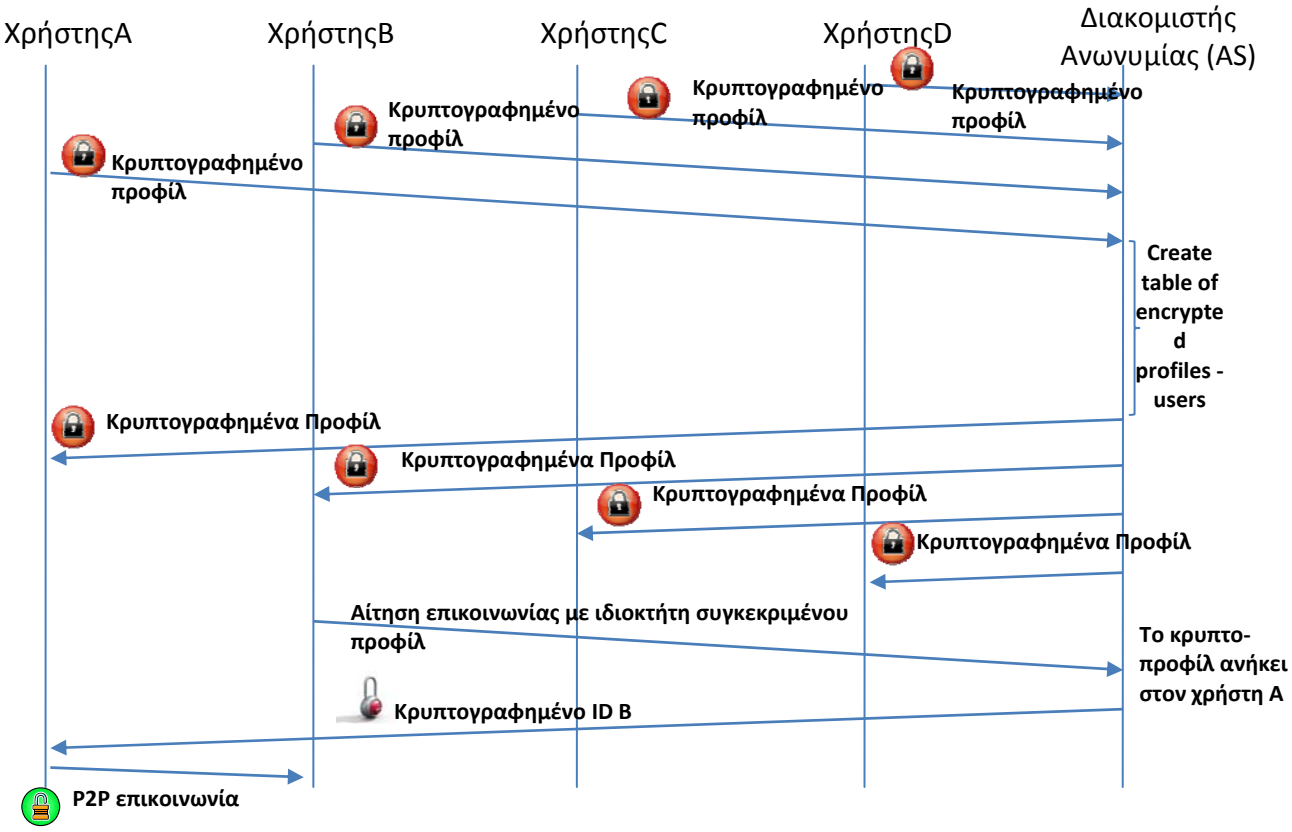
- Ο AS παρέχει το σύνολο των κρυπτο-κειμένων σε όλους τους χρήστες μέσα στην ομάδα, χωρίς όμως να παρέχει την αντιστοιχία στους χρήστες. Με αυτό το τρόπο τα κείμενα παραμένουν ανώνυμα.

- Όλοι οι χρήστες μπορούν να αποκρυπτογραφήσουν τα κρυπτο-κείμενα χρησιμοποιώντας το ομαδικό ιδιωτικό κλειδί. Παρόλ' αυτα η ιδιωτικότητα διαφυλάσσεται καθώς τα δεδομένα παρέχονται ανώνυμα. Έτσι για μέγεθος N μίας ομάδας, κάθε χρήστης μπορεί απλώς να ξέρει ότι τα δεδομένα ανήκουν σε κάποιο από τα υπόλοιπα N-1 μέλη.

- Ο χρήστης Β μέσω μιας κατάλληλης γραφικής διεπαφής επιλέγει ένα συγκεκριμένο προφίλ και ζητεί από τον AS να ξεκινήσει επικοινωνία P2P με τον άγνωστο προς το παρόν χρήστη.

- Ο AS συμβουλεύεται τον πίνακα του και βρίσκει ότι ο ζητούμενος χρήστης είναι ο Α. Ο AS προωθεί την αίτηση του χρήστη Β στον Α ενεργώντας σαν «μεσίτης» - proxy. Ο AS μπορεί να ενεργεί στο εξής και μέχρι το επόμενο βήμα ως ιδιωτικός μεσίτης για αμφίδρομη ανώνυμη επικοινωνία μεταξύ του Α και του Β με μόνα σημεία αναγνώρισης και αναφοράς τα ανώνυμα κομμάτια πληροφορίας προφίλ.

- Σε αυτό το τελικό βήμα, ο χρήστης Α (ή αμφότεροι οι Α και Β) μπορεί να αποφασίσει να «συστηθεί» (συστηθούν) και αποκαλυφθεί (αποκαλυφθούν) βάσει προσωπικής επιλογής, πολιτικών ασφαλείας ή κάποιου πρωτοκόλλου εφαρμογής. Η επικοινωνία και αλληλεπίδραση θα είναι στο εξής καθαρά P2P.



Εικόνα 14 - Ολοκληρώνοντας το στήσιμο της Συνομοσπονδίας Προσωπικών Δικτύων

Η Εικόνα 14 παρουσιάζει την παραπάνω διαδικασία. Το προτεινόμενο μοντέλο υποθέτει ότι τα κλειδιά ανταλλάσσονται ασφαλώς μέσω σχετικών μηχανισμών ανταλλαγής κλειδιών και επομένως δεν ασχολείται με το σχετικό πρόβλημα. Άλλωστε, υπάρχουν ήδη πρωτόκολλα και λύσεις διαχείρισης κλειδιών που παρέχονται προκειμένου να ικανοποιηθούν ειδικές απαιτήσεις στα Προσωπικά Δίκτυα και στους συνασπισμούς Προσωπικών Δικτύων, όπως το πρωτόκολλο σχηματισμού PAN και η CPFP [31], τα οποία θεωρούμε ότι εφαρμόζονται και εδώ.

Αναφέροντας την εμπιστοσύνη

Προκειμένου να αναγνωριστούν οι κακόβουλοι χρήστες και να απαγορευτεί η πρόσβαση τους, είναι απαραίτητος ένας μηχανισμός αναφοράς κακής συμπεριφοράς. Αυτός ο μηχανισμός βασίζεται στις αναφορές που παρέχει ο κάθε χρήστης σχετικά με τα επίπεδα εμπιστοσύνης που έχει με κάθε ομότιμο μέλος που συμμετέχει σε ένα συνασπισμό PN-F. Οι αναφορές παρέχονται με το πέρας μιας PN-F συνόδου (*session*), και είναι δύο τύπων: Θετικές και Αρνητικές. Το σύνολο των θετικών και αρνητικών αναφορών χαρακτηρίζουν τον χρήστη και γίνονται αναπόσπαστο μέρος της προσωπικής του πληροφορίας και προτιμήσεων, όπως αυτές περιγράφτηκαν και χρησιμοποιήθηκαν προηγουμένως. Το επίπεδο εμπιστοσύνης λοιπόν διαχειρίζεται ο διακομιστής ανωνυμίας, το οποίο επισυνάπτει στις προσωπικές πληροφορίες προτιμήσεων και κατάσταση κατά τη διάρκεια της αντιστοίχισης προφίλ στην εγκαθίδρυση του PN-F.

Ο μηχανισμός που χρησιμοποιείται για τον ορισμό του επιπέδου εμπιστοσύνης κάθε χρήστη βασίζεται στην ιδέα της διανεμημένης φήμης (*distributed reputation*) [14] και είναι ο εξής:

- Κάθε χρήστης έχει μια βάση αναφοράς εμπιστοσύνης, υλοποιημένη σαν μία ουρά FIFO (First In – First Out) που κρατάει έναν πεπερασμένο αριθμό των πιο πρόσφατων αναφορών για αυτών από άλλους χρήστες.

- Κάθε χρήστης ξεκινά έχοντας ένα επίπεδο εμπιστοσύνης ίσο με το μηδέν. Κάθε αριθμός μεγαλύτερος του μηδενός υποδεικνύει θετική βαθμολόγηση, με το ανώτατο να είναι ίσο με τον μέγιστο αριθμό των αναφορών στην ουρά.

- Κάθε αριθμός μικρότερος του μηδενός, υποδεικνύει αρνητική βαθμολόγηση με το ελάχιστο αντίστοιχα με τον αντίθετο του μέγιστου.

- Μια αρνητική βαθμολόγηση δεν αποκλείει απαραίτητα τον χρήστη από συμμετοχή στο PN-F. Αν όμως το επίπεδο εμπιστοσύνης φτάσει μια προκαθορισμένη ως ελάχιστη τιμή, τότε ο χρήστης αποκλείεται (*banned*) από το συνασπισμό για συγκεκριμένη χρονική περίοδο, μετά το πέρας της οποίας του επιτρέπεται να εισέλθει ξανά, με μόλις μία αρνητική αναφορά εμπιστοσύνης λιγότερη (ώστε να είναι ακριβώς μία πάνω από το ελάχιστο).

- Ο χρήστης θα πρέπει να ξανανέβει με τη συμπεριφορά του την κλίμακα εμπιστοσύνης, ενώ με το πρώτο κρούσμα κακής συμπεριφοράς θα βρεθεί πάλι εκτός συνασπισμού.

Μέσω αυτού του μηχανισμού, ο συνασπισμός μπορεί να αναγνωρίζει αυτόνομα ποιοι χρήστες φέρονται κακόβουλα ή απλά ανεύθυνα και τελικά να τους περιθωριοποιεί, μέχρι του σημείου που να τους αποκλείει εξολοκλήρου από την ομάδα. Όντας ανθρωποκεντρικό το σύστημα, συμπεριλήφθηκε και ένας μηχανισμός «συγχώρεσης» ο οποίος επιτρέπει σε χρήστες να εισέρχονται εκ νέου και με οριακά επίπεδα εμπιστοσύνης στον συνασπισμό, τον οποίο και θα μπορούν να συνεχίσουν να χρησιμοποιούν αν εγκαταλείψουν την βλαπτική ή προσβλητική συμπεριφορά τους. Φυσικά, υπάρχουν θέματα κακόβουλης εκμετάλλευσης αυτού του μηχανισμού, μέσω π.χ. μιας επίθεσης φήμης, αλλά αυτά προβλέπονται και αντιμετωπίζονται από τις προτεινόμενες λύσεις του επόμενου υποκεφαλαίου.

4.3. Διασφάλιση ανωνυμίας και ιδιωτικότητας, ασφάλεια και ανθεκτικότητα ενάντια σε επιθέσεις

Ο σχεδιασμός της προτεινόμενης λύσης έγινε έχοντας κατά νου τρεις ειδικές ανάγκες: την ανάγκη για ανωνυμία (ειδικά όσον αφορά την διαχείριση της πληροφορίας από το διακομιστή ανωνυμίας), την ανάγκη για ιδιωτικότητα και ασφάλεια για την ανταλλασσόμενη πληροφορία (ειδικά πληροφορίας προσωπικής φύσης) και τέλος την ανάγκη ανθεκτικότητας ενάντια σε πιθανές επιθέσεις.

Διασφαλίζοντας την ανωνυμία

Όταν η ανωνυμία είναι στόχος, η ανάγκη για ταυτοποίηση και ελέγχου πρόσβασης παρουσιάζεται ως αντίθετη δύναμη. Από τη μία πλευρά οι προσωπικές πληροφορίες του χρήστη πρέπει να τηρηθούν ανώνυμες, από την άλλη η ανάγκη εγκατάστασης ενός μηχανισμού ελέγχου πρόσβασης απαιτεί την χρήση κάποιων στοιχείων ταυτοποίησης του χρήστη. Στη πρόταση, ο διαχωρισμός των δεδομένων ταυτοποίησης και ελέγχου πρόσβασης από τις υπόλοιπες προσωπικές πληροφορίες και πληροφορίες κατάστασης, καθώς και η διαφορετική διαχείριση αυτών των δύο κατηγοριών, διασφαλίζει ότι οι προσωπικές πληροφορίες δεν αποκαλύπτονται κατά την εγκαθίδρυση του συνασπισμού PN-F παρά μόνο όταν ομότιμα οι χρήστες μεταξύ τους επικοινωνήσουν κατά βούληση και το επιλέξουν. Αυτό επιτυγχάνεται μέσω της κρυπτογράφησης των προσωπικών πληροφοριών χρησιμοποιώντας ομαδικά κλειδιά, διαθέσιμα μόνο στους ομότιμους χρήστες, ενώ από την άλλη οι πληροφορίες ταυτότητας, αλλά όχι το προσωπικό περιεχόμενο, είναι διαθέσιμο μόνο στο διακομιστή. Το προτεινόμενο μοντέλο διασφαλίζει ότι τα δύο αυτά μέρη πληροφορίας παραμένουν ασυσχέτιστα κατά την διαδικασία εγκαθίδρυσης PN-F, και ότι συνδέονται μόνο εφόσον δύο χρήστες επιθυμούν να εκκινήσουν μια σύνοδο συνασπισμού.

Επιπλέον, η ανωνυμία αναιρείται καταρχήν για το χρήστη που εκκινεί την αίτηση συνόδου PN-F, ελαχιστοποιώντας με αυτό τον τρόπο τη πιθανή απόπειρα απάτης με χρήση αυτόματων πρακτόρων (*agents*). Το μοντέλο ανωνυμίας επιτρέπει στο χρήστη που δέχεται την πρόσκληση να αξιολογήσει τα δεδομένα του άλλου χρήστη, να έχει και κάποια επικοινωνία πρώτα αν το επιθυμεί (π.χ. μέσω ανταλλαγής μηνυμάτων κειμένου), προτού προχωρήσει στην άρση της ανωνυμίας του. Με αυτό τον τρόπο αυτόματα προγράμματα που προσπαθούν να πλαστοπροσωπήσουν χρήστες και να συλλέξουν προσωπικά δεδομένα μπορούν να αναγνωριστούν και να αποφεχθούν.

Διασφαλίζοντας την ιδιωτικότητα και την ασφάλεια της ανταλλασσόμενης πληροφορίας

Το θέμα της διασφάλισης της ιδιωτικότητας και της ασφάλειας επιλαμβάνεται με τη χρήση πιστοποιητικών και κρυπτογράφησης της ανταλλασσόμενης πληροφορίας μέσω εργαλείων ασύμμετρης κρυπτογραφίας. Η χρήση προσωπικών πιστοποιητικών για το κάθε χρήστη για την επικοινωνία με τον διακομιστή ανωνυμίας, και ομαδικών πιστοποιητικών ανά σύνοδο διαφυλάσσουν όλη την πληροφορία κατά την διαδικασία εγκαθίδρυσης PN-F ενάντια σε επιθέσεις κατά της ιδιωτικότητας και ασφάλειας. Όσον αφορά την ανταλλαγή πληροφορίας από εκεί και πέρα, και πάλι η κρυπτογράφηση μπορεί να εφαρμοστεί, ένα τα μέρη που επικοινωνούν αισθάνονται ότι είναι απαραίτητο.

Διασφαλίζοντας την ανθεκτικότητα ενάντια στις επιθέσεις

Ένα σημαντικό θέμα που έπρεπε να αντιμετωπιστεί κατά τον ορισμό του προτεινόμενου μοντέλου είναι και αυτό των πιθανών επιθέσεων. Στη περίπτωση συνασπισμού χρηστών, μια συνήθης επίθεση είναι η λεγόμενη «επίθεση φήμης» [15][14], κατά την οποία ο επιτιθέμενος (ή επιτιθέμενοι) προσπαθεί να βλάψει την φήμη του θύματος μέσα στο συνασπισμό. Προσπαθώντας να αναγνωριστούν οι δυνατοί τρόποι με τους οποίος μια τέτοια επίθεση μπορεί να πραγματοποιηθεί, προέκυψαν δύο διαφορετικές εκδοχές.

Πρώτον, όταν ένας κακόβουλος χρήστης επιχειρεί να βλάψει την φήμη των άλλων χρηστών με το να καταθέτει συνεχώς αρνητικές αναφορές για αυτούς εσκεμμένα. Αυτό μπορεί να ανιχνευτεί εύκολα με παρακολούθηση του ιστορικού αναφορών του χρήστη. Στη δεύτερη εκδοχή, έχουμε συγχρονισμένη επίθεση πολλών χρηστών ενάντια σε έναν, όπου όλοι οι επιτιθέμενοι τον αναφέρουν ως κακόβουλο προκειμένου να του ρίξουν το επίπεδο εμπιστοσύνης και να τον πετάξουν έξω από το σύστημα. Και πάλι η επίθεση αυτή μπορεί να ανιχνευτεί (και ο χρήστης να αναγνωριστεί ως μη κακόβουλος) καθώς στην περίπτωση επίθεσης, οι επιτιθέμενοι θα είναι αυτοί που θα επιχειρούν να εκκινήσουν σύνοδο PN-F με το θύμα σε σύντομο χρονικό διάστημα (ένας πραγματικά κακόβουλος χρήστης θα είχε λίγες πιθανότητες να επιτεθεί απλά περιμένοντας τους άλλους να συνδεθούν μαζί του, και θα έπρεπε το προφίλ του να αντιστοιχεί με έναν μεγάλο αριθμό άλλων προφίλ ώστε να ενδιαφερθούν να επικοινωνήσουν μαζί του).

Επιπλέον, ο AS γνωρίζει ποιος κατέθεσε πιο κρυπτο-κείμενο, χωρίς φυσικά να μπορεί να αποκρυπτογραφήσει τη σχετική πληροφορία. Αν οι χρήστες αναφέρουν ότι κάποιο κρυπτο-κείμενο έχει κακόβουλες διαθέσεις στον AS, τότε αυτός θα γνωρίζει τον υπεύθυνο και θα μπορεί να δράσει αναλόγως, π.χ. με το να ανακαλέσει τα σχετικά πιστοποιητικά και αποκλείσει τον χρήστη από το συνασπισμό. Καθώς ο διακομιστής είναι το κεντρικό σημείο επιβολής πολιτικών ασφαλείας (*central policy enforcement point*), ο αποκλεισμός θα ίσχύσει αμέσως, ανεξαρτήτως από το πόσοι χρήστε είναι στην εμβέλεια της επικοινωνίας εκείνη τη στιγμή. Από την άλλη πλευρά, η κεντρικοποιημένη προσέγγιση μπορεί να γίνει ευάλωτη σε σενάρια μοναδικού σημείου αποτυχίας (*Single Point of Failure - SPOF*). Ωστόσο αυτό το ευάλωτο σημείο μπορεί να αντιμετωπιστεί εφόσον ισχύσουν οι εξής απαιτήσεις ασφαλείας:

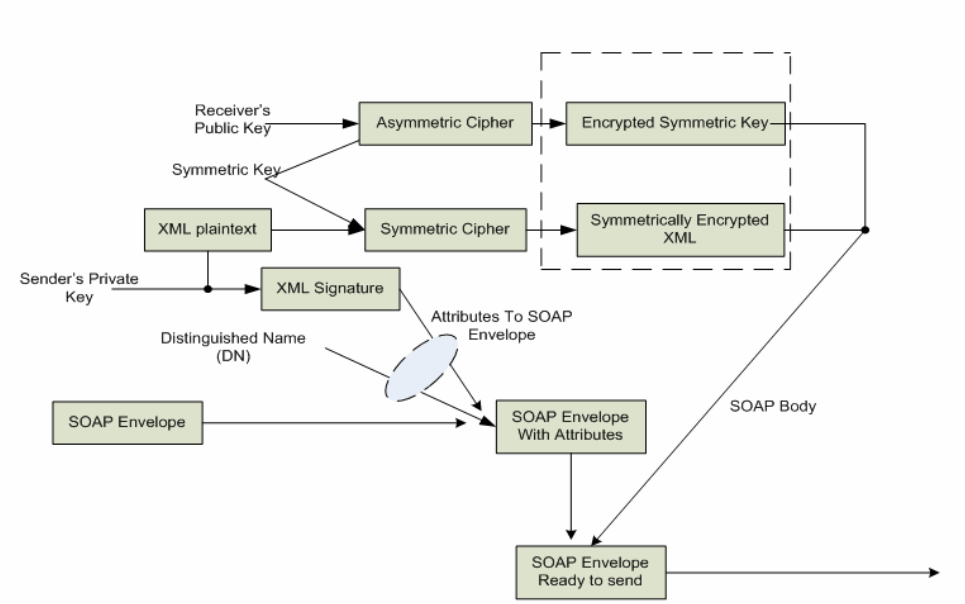
- Ο διακομιστής ανωνυμίας βρίσκεται σε ασφαλές μέρος, από φυσικής και δικτυακής άποψης.
- Υπάρχουν σύγχρονοι προστατευτικοί μηχανισμοί ασφαλείας, όπως ένα σύστημα ανίχνευσης εισβολής (*Intrusion Detection System - IDS*) και ένα υπόβαθρο ασφαλών διαύλων επικοινωνίας (π.χ. SSL, IPsec) με τον AS, που θα απέτρεπαν επιθέσεις όπως man-in-the-middle, DoS, D-DoS και άλλες δικτυακές επιθέσεις [13]. Όταν αυτό το υποστηρικτικό υπόβαθρο ασφαλείας λείπει, θα πρέπει αυτό να γίνεται γνωστό ώστε να αποθαρρύνεται η χρήση κρίσιμων εφαρμογών και υπηρεσιών σε αυτές τις περιοχές, μειώνοντας έτσι τις νόμιμες αιτήσεις υπηρεσίας, και την πιθανότητα επομένως ενός DoS.

4.4. Υλοποίηση και επίδειξη εφαρμογής

Σε αυτό το τμήμα παρουσιάζουμε εν συντομία μια πρακτική υλοποίηση του προτεινόμενου μοντέλου ανωνυμίας. Η υλοποίηση βασίζεται σε υποδομή δημοσίων κλειδιών, πιστοποιητικά X.509 και κρυπτογραφία βασισμένη σε βιβλιοθήκες Java. Η χρήση των πιστοποιητικών χρειάζεται για να γίνει η διαχείριση εμπιστοσύνης. Δηλαδή, χάρη στους μηχανισμούς που παρέχονται από τα PKI και πιστοποιητικά X.509 [17][18], κάθε οντότητα είναι ικανή να πιστοποιεί την εγκυρότητα της ταυτότητας άλλων οντοτήτων, ενεργώντας έτσι σαν έμπιστο τρίτο μέρος - Trusted Third Party (TTP) όταν δύο οντότητες επιχειρήσουν να εγκαταστήσουν μια σχέση εμπιστοσύνης. Στη περίπτωση μιας τυπικής ιεραρχικής PKI τέτοιες οντότητες είναι κεντρικά σημεία που όλοι εμπιστεύονται, γνωστά σαν Αρχές Πιστοποιητικών - Certificate Authorities (CAs). Στη μη ιεραρχική περίπτωση, κάθε οντότητα μπορεί να ενεργεί σαν TTP κατά περίπτωση, όποτε και είναι γνωστή ως έμπιστος εισηγητής - Trusted Introducer για τις οντότητες αυτές. Στο προτεινόμενο μοντέλο, ο AS ενεργεί σαν CA ενώ οι χρήστες μπορούν επίσης να ενεργούν σαν Trusted Introducers όταν θελήσουν να διανέμουν δημόσια κλειδιά μεταξύ τους ή να επικοινωνήσουν με P2P τρόπο.

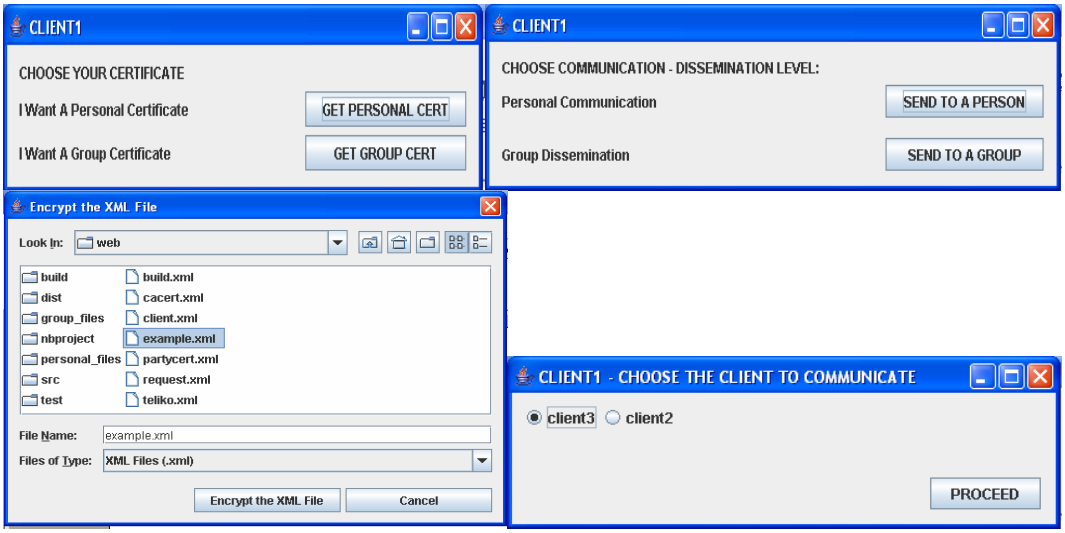
Εφόσον λυθούν τα θέματα εμπιστοσύνης, η ιδιωτικότητα διασφαλίζεται με κρυπτογράφηση και εξουσιοδοτημένη αποκρυπτογράφηση με χρήση του δημοσίου και ιδιωτικού κλειδιού αντίστοιχα. Η υλοποίηση έγινε με χρήση ανοιχτών βιβλιοθηκών κρυπτογραφίας Java [19][21]. Εφόσον η υλοποίηση στοχεύει στο να αποδείξει την πρακτική εφαρμογή της ιδέας (proof-of-concept) χρησιμοποιήθηκε ο διαδεδομένος Triple DES αλγόριθμος κρυπτογράφησης. Σε περιπτώσεις όπου οι επιδόσεις αποτελούν απαίτηση, η υλοποίηση μπορεί να βασιστεί σε έναν γρηγορότερο αλγόριθμο, όπως το Advanced Encryption Standard (AES) [20], διάδοχο του Triple DES.

Όσον αφορά τους μηχανισμούς διαχείρισης και ανταλλαγής πληροφορίας προφίλ, η υλοποίηση βασίστηκε σε XML (eXtensible Mark-up Language) τεχνολογίες. Δηλαδή όλη η πληροφορία αποθηκεύεται σε μορφή XML, ενώ τα XML μηνύματα ανταλλάσσονται με χρήση του σχετικού πλαισίου που παρέχεται από την SOAP[22]. Οι μηχανισμοί κρυπτογράφησης που περιέγραψα παραπάνω εφαρμόζονται στο κείμενο XML προτού εγκλειστεί σε ένα φάκελο SOAP και σταλεί «πάνω από το σύρμα» (Εικόνα 15). Επίσης κρυπτογραφώντας το αρχικό κείμενο με χρήση του ιδιωτικού κλειδιού ισοδυναμεί με το να υπογράφεται ηλεκτρονικά, δηλαδή ο παραλήπτης είναι σε αυτή τη περίπτωση σίγουρος για την ταυτότητα του αποστολέα.

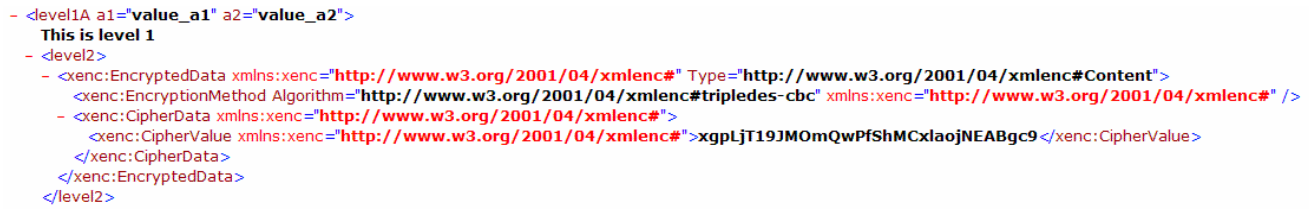


Εικόνα 15 - Κρυπτογράφηση και υπογραφή XML κειμένου για επικοινωνία

Η υλοποίηση περιλαμβάνει ένα σύνολο απλών στοιχείων γραφικής διεπιφάνειας χρήστη (*Graphical User Interface - GUI*) για την έκδοση προσωπικών και ομαδικών πιστοποιητικών καθώς και την εγκαθίδρυση ασφαλούς XML επικοινωνίας με χρήση κρυπτογραφικών μεθόδων που υλοποιούν τους μηχανισμούς ασφαλείας ενός τυπικού PKI. Στην Εικόνα 16 παρουσιάζεται μια σύνθεση από τα σχετικά GUIs ενώ στην Εικόνα 17 παρατίθεται ένα επιλεκτικά κρυπτογραφημένο XML, όπου το περιεχόμενο ενός συγκεκριμένου στοιχείου κρυπτογραφείται κατά τις προτιμήσεις ιδιωτικότητας του χρήστη (στο παράδειγμα το στοιχείο "level2").



Εικόνα 16 – Σύνθεση GUIs για την αρχικοποίηση των πιστοποιητικών και την έναρξη ασφαλούς μεταφοράς XML



Εικόνα 17 – Δείγμα επιλεκτικά κρυπτογραφημένου αρχείου XML

4.5. Αξιολόγηση της πρότασης σε σχέση με υπάρχοντα πλαίσια και λύσεις

Πρόσφατα, και προς την κατεύθυνση της παροχής ανωνυμίας και πλήρους ιδιωτικότητας στο επίπεδο εφαρμογής, προτάθηκε η ιδέα της εικονικής ταυτότητας (*Virtual Identity - VID*) από το ερευνητικό πρόγραμμα Daidalos [23]. Η σχετική ιδέα όμως είναι μια λύση για διαχείριση της ιδιωτικότητας παρά μια λύση επιβολής της, που είναι και ο στόχος της λύσης που προτείνεται σε αυτό το κεφάλαιο. Επομένως η ιδέα του VID που υιοθετήθηκε και από το πρόγραμμα MAGNET BEYOND είναι συμπληρωματική λύση και όχι επικαλυπτόμενη, καθώς θα επιτρέψει το σύστημα διαχείρισης της ταυτότητας και των πολιτικών ασφαλείας να λειτουργεί ομαλά, όταν οι σχετικοί μηχανισμοί θα αποκρύπτουν δεδομένα και θα αποσυσχετίζουν την ταυτότητα στις συναλλαγές. Οι σχεδιαστικές προσαρμογές αυτής της συνεργασίας αναλύθηκαν στη [30].

Είναι προφανές ότι το προτεινόμενο μοντέλο ανωνυμίας είναι καλά προσαρμοσμένο ώστε να επιτυγχάνει ανώνυμή δημοσίευση πληροφορίας από έναν προς πολλούς (one-to-many). Υπό αυτή την έννοια είναι πιο αποδοτικό σε ένα περιβάλλον συνομοσπονδίας PN-F, και πιο κατάλληλο από σχετικές λύσεις ανώνυμων καναλιών σημείου προς σημείου όπως π.χ. οι λύσεις Freedom [25] και Mixmaster Remailer [26].

Επιπλέον, το προτεινόμενο μοντέλο παρέχει ανωνυμία τόσο για τους καταναλωτές όσο και για τους παραγωγούς της πληροφορίας, προσφέροντας έτσι ενισχυμένη ιδιωτικότητα σε σχέση με μεσολαβητικές υπηρεσίες φυλλομετρητή (*browser proxy services*) όπως το Anonymizer [27], που δεν παρέχει καμία προστασία για τους παραγωγούς της πληροφορίας ενώ τα logs των υπηρεσιών επίσης θέτουν σε κίνδυνο την ιδιωτικότητα των καταναλωτών της πληροφορίας. Στη περίπτωση μας παραγωγοί και καταναλωτές προστατεύονται από το μεν γεγονός ότι τα προφίλ είναι κρυφά από τον διακομιστή AS, ενώ τα προφίλ είναι ανώνυμα όσον αφορά τους χρήστες. Σε περίπτωση «θεωρίας συνωμοσίας», όπου ένας χρήστης θα συνεργαζόταν με ή θα ξεγελούσε έναν AS ή το αντίστροφο προκειμένου να αποκτήσει πρόσβαση σε όλα τα κομμάτια της πληροφορίας μαζί, αυτό θα αποτελούσε παραβίαση του πρωτοκόλλου λειτουργίας που θα πρέπει να ανιχνευτεί, μπλοκαριστεί και να αναφερθεί από αυτόνομους παρεμβατικούς μηχανισμούς ασφαλείας, όπως π.χ. μια προσαρμοσμένη λύση IDS.

Προκειμένου να γίνει σύγκριση της πρότασης με λύσεις διανεμημένης ανταλλαγής ανώνυμης πληροφορίας, όπως το Freenet[28], πρέπει να αξιολογηθούν τα υπέρ και τα κατά του να υπάρχει μια κεντρική οντότητα (AS) και της αποκεντροποιημένης, Peer-to-Peer λύσης. Οι κεντρικές οντότητες δέχονται κριτική ότι είναι ευάλωτες σε σενάρια αποτυχίας του κεντρικού σημείου. Ωστόσο, τα κεντρικά σημεία μπορεί να προστατεύονται και πολύ καλύτερα από τον μέσο χρήστη και την συσκευή του. Συγκεκριμένα αντίμετρα ασφαλείας που αμβλύνουν το ευάλωτο αυτό σημείο παρουσιάστηκαν σε προηγούμενο υποκεφάλαιο.

Επιπλέον, σε περιπτώσεις που συγκεκριμένη πληροφορία αποθηκεύεται σε συγκεκριμένους διακομιστές, η απλή κακόβουλη παρακολούθηση της κίνησης από και προς τον διακομιστή, μπορεί επίσης να οδηγήσει σε χρήσιμα συμπεράσματα και να θέσει σε κίνδυνο την ιδιωτικότητα των χρηστών. Αν κάποιος προσπαθούσε να το αντιμετωπίσει αυτό με το να αποθηκεύει στον κάθε διακομιστή όλη τη πληροφορία, αυτό θα είχε προβλήματα κλιμάκωσης. Στη πρόταση που παρουσιάστηκε αυτά τα προβλήματα αντιμετωπίζονται ως εξής: για τη μεν κλιμάκωση, η πληροφορία πρέπει να διανέμεται στους διακομιστές που βρίσκονται διάσπαρτοι μέσα στη συνομοσπονδία, όπως ήδη αναφέρθηκε. Ωστόσο, οι διασυνδεδεμένοι διακομιστές δεν θα βρίσκονταν σε απευθείας σύνδεση με τους χρήστες ανά πάσα στιγμή, αλλά η σύνδεση θα γίνεται μέσω μεσολαβητή διακομιστή (*proxy*) ο οποίος θα αναθέτει δυναμικά έναν από τους διαθέσιμους διακομιστές ανωνυμίας, αντιμετωπίζοντας με αυτό τον τρόπο την απειλή της παρακολούθησης της κίνησης ενός διακομιστή.

Τώρα που προτάθηκαν λύσεις για τα υποτιθέμενα μειονεκτήματα, παρουσιάζονται και τα πλεονεκτήματα του προτεινόμενου μοντέλου στο ειδικό περιβάλλον των PN και PN-F [10]:

Καταρχήν, η καινοτόμος πρόταση χρήσης μοντέλου διαχωρισμού της πληροφορίας ταυτότητας από τις προσωπικές πληροφορίες και πληροφορίες συγκειμένου, η οποία αποτελεί ισχυρή προστασία της ταυτότητας και διευκολύνει την ανωνυμία, μη εμποδίζοντας τη λειτουργικότητα, ενώ διευκολύνει ιδιαίτερα την δυναμική εφαρμογή κανόνων πολιτικής ακόμη και σε περιπτώσεις ανωνυμίας.

Επίσης, στο προτεινόμενο πλαίσιο δεν απαιτείται από τον εκάστοτε κόμβο του χρήστη να έχει αρκετά υπολογιστικά αποθέματα ώστε να δημιουργεί τα δικά του κλειδιά. Ο διακομιστής μπορεί να ενεργεί σαν μια τυπική CA και μεσολαβητή για όλες τις διεργασίες κρυπτογράφησης και αποκρυπτογράφησης, που έχουν υψηλές απαιτήσεις σε υπολογιστικά αποθέματα. Καθώς αυτό είναι εκτός του πεδίου ενδιαφέροντος, το κύριο όφελος από τον AS είναι ότι επιβάλλει πραγματική ανωνυμία κατά την ανταλλαγή της πληροφορίας σε όλα τα στρώματα. Τα κρυπτο-προφίλ εγγυώνται την ανωνυμία στο στρώμα εφαρμογής, ενώ η χρήση του διακομιστή για τη διανομή και αρχική διαχείριση τους κρύβει και την υπόλοιπη πληροφορία που θα μπορούσε να χρησιμοποιηθεί για να συνδεθεί ένας συγκεκριμένος χρήστης: π.χ. μέσω διευθύνσεων MAC και IP συσκευών χρήστη. Οι διανεμημένες λύσεις ανταλλαγής πληροφορίας σε γενικές γραμμές μειονεκτούν σε αυτό το θέμα και γενικά λειτουργούν μόνο στο στρώμα εφαρμογής.

Επιπλέον, με την οντότητα του διακομιστή ανωνυμίας, η προτεινόμενη λύση αντιδρά θετικά στην κλιμάκωση σε θέματα διαχείρισης της πληροφορίας και επεξεργασίας της, καθώς αυτά βαραίνουν τον διακομιστή και όχι τους χρήστες. Καθώς η κοινότητα των χρηστών θα μεγάλωνε, το φορτίο θα διανεμόταν σε πολλές οντότητες AS παρά στους χρήστε, που από ένα συγκεκριμένο επίπεδο ανάπτυξης της κοινότητας θα ήταν αδύνατον να χειριστούν πιστοποιητικά όλης της κοινότητας. Αυτό είναι ιδιαίτερα σημαντικό στο περιβάλλον των PN και PN-F, όπου δεν αναμένουμε από τους χρήστες να εκτελούν πολύπλοκα καθήκοντα διαχείρισης ή να είναι ειδικοί στο χειρισμό μηχανισμών ασφαλείας.

Τέλος, το μοντέλο μας έχει οφέλη και από επιχειρηματικής σκοπιάς, καθώς η οντότητα του διακομιστή ανωνυμίας θα μπορούσε να ανήκει σε έναν έμπιστο και πιστοποιημένο

πάροχο υπηρεσιών. Υπό αυτή την έννοια, το προτεινόμενο μοντέλο επιτρέπει την παροχή ανώνυμης και ιδιωτικής ανταλλαγής πληροφορίας σαν μια συνδρομητική υπηρεσία.

4.6. Συμπεράσματα και μελλοντικές επεκτάσεις

Το θέμα της εγκαθίδρυσης εμπιστοσύνης, αποφεύγοντας παράλληλα την έκθεση προσωπικής πληροφορίας που μπορεί να χρησιμοποιηθεί για κακούς σκοπούς είναι αρκετά σημαντικό και παρουσιάζει αρκετές ερευνητικές προκλήσεις. Όταν πρέπει να εκτελεστούν συναλλαγές με άγνωστους χρήστες και ειδικά όταν το προφίλ χρήστη συμπεριλαμβάνεται στην ανακάλυψη και αντιστοίχιση ομότιμων χρηστών, ο κίνδυνος έκθεσης της προσωπικής πληροφορίας είναι υψηλός (όπως π.χ. σε περιπτώσεις επιθέσεων κοινωνικής μηχανικής).

Σε αυτό το κεφάλαιο, παρουσιάστηκε ένα μοντέλο ανωνυμίας βασισμένο στον διαχωρισμό της πληροφορίας ταυτότητας χρήστη από τις λοιπές πληροφορίες κατάστασης και προτιμήσεων, προκειμένου να αντιμετωπιστεί ο κίνδυνος έκθεσης που προαναφέρθηκε. Το μοντέλο μπορεί να εφαρμοστεί πάνω από Προσωπικά Δίκτυα και συνδυάζει την ανωνυμία της προσωπικής πληροφορίας χρήστη που χρησιμοποιείτο στην ανακάλυψη και αντιστοίχιση ομότιμων χρηστών, με κρυπτογράφηση του περιεχομένου που ανταλλάσσεται έτσι ώστε τρίτα μέρη που εμπλέκονται προκειμένου να υποστηρίξουν τη διαδικασία να μην μπορούν να συνδέσουν το προσωπικό περιεχόμενο με την ταυτότητα του χρήστη. Η ολοκληρωμένη λύση που προτείνεται είναι ανθεκτική στις επιθέσεις και επίσης προσφέρει ανίχνευση κακόβουλων συμπεριφορών και χαρακτηρισμό των χρηστών αναλόγως βάσει μηχανισμού αναφορών συμπεριφοράς και εμπιστοσύνης. Επίσης παρουσιάστηκε μια ενδεικτική υλοποίηση για την αξιολόγηση της δυνατότητας εφαρμογής ενώ έγινε και αξιολόγηση με σύγκριση των υπαρχουσών τεχνικών και λύσεων.

Μελλοντικές Επεκτάσεις

Το προτεινόμενο μοντέλο έχει σχεδιαστεί ώστε να ενσωματωθεί στην πρωτότυπη πλατφόρμα PN και PN-F [6]. Για αυτό το σκοπό, συγκεκριμένα στοιχεία και υποδομές πρέπει να παρέχουν συγκεκριμένες απαραίτητες λειτουργίες και να γίνουν συγκεκριμένες επιλογές και ρυθμίσεις, με τις κυριότερες να είναι:

- Επιλογή του μοντέλου PKI. Η επιλογή ιεραρχικού ή μη μοντέλου (π.χ. PGP) που θα προσαρμοστεί στη λύση πρέπει να αποφασιστεί. Προς το παρόν, υλοποιήθηκε ένα ενδεικτικό PKI με χρήση CA που χρησιμοποιείται στη διανομή πιστοποιητικών για το σχηματισμό PN-F. Σε περίπτωση δικτύων με περισσότερο P2P και ad-hoc φύση, μη ιεραρχικά πιστοποιητικά θα πρέπει να υποστηριχθούν, αναθέτοντας ρόλο έμπιστου εισηγητή (*trusted introducers*) σε συγκεκριμένους χρήστες. Αυτό θα μπορούσε να βασιστεί σε μηχανισμό φήμης ή μέσω μιας απλής εφαρμογής κοινωνικής δικτύωσης (*social networking application*).

- Ενσωμάτωση του διακομιστή ανωνυμίας AS στο μοντέλο οντοτήτων του PN: ο διακομιστής ανωνυμίας δεν είναι ουσιαστικό μέρος της PN ή PN-F πλατφόρμας καθώς είναι ένα σύνολο από κεντρικές υπηρεσίες που παρέχονται από ένα έμπιστο τρίτο μέρος. Εναλλακτικά, στη περίπτωση της PGP, κάθε μέλος του PN-F θα μπορεί να δρα σαν TTP αν έχει σχετική εξουσιοδότηση, και να παρέχει τις υπηρεσίες του AS σε όλο το PN-F.

- Ενσωμάτωση κατάλληλων πολιτικών ιδιωτικότητας και ανωνυμίας στο μοντέλο του PN, ώστε να υποστηρίζεται η ανώνυμη ανταλλαγή πληροφορίας προφίλ και επίγνωσης

κατάστασης. Ο AS εξασφαλίζει ότι το περιεχόμενο που ανταλλάσσεται δεν μπορεί να συσχετιστεί με μια πραγματική ταυτότητα χρήστη. Επομένως απαιτείται κάποιο σχήμα Εικονικής ταυτότητας ή Ψευδώνυμου μέσα στο PN-F [23]. Με δεδομένους τους μηχανισμούς ανταλλαγής εικονικών ταυτοτήτων, προφίλ και πληροφορίας επίγνωσης κατάστασης [16], απαιτούνται πολιτικές ιδιωτικότητας που να προσαρμόζονται στο ψευδώνυμο ή στην εικονική ταυτότητα. Δηλαδή, προκειμένου να υποστηρίξουν το προτεινόμενο μοντέλο, οι μηχανισμοί ανταλλαγής προφίλ και πληροφορίας επίγνωσης κατάστασης απαιτούν κατάλληλες πολιτικές ανωνυμίας και όχι επεκτάσεις και τροποποιήσεις στις λειτουργικότητες.

4.7. Ειδική ορολογία κεφαλαίου

Ελληνικός όρος / φράση	Αγγλικός όρος / φράση
Αρχή Πιστοποιητικών	Certificate Authority - CA
Γραφικής Διεπιφάνεια Χρήστη	Graphical User Interface - GUI
Διακομιστής	Server
Διανεμημένη φήμη	Distributed reputation
Εικονική ταυτότητα	Virtual Identity - VID
Έμπιστο τρίτο μέρος	Trusted Third Party - TTP
Έμπιστοι εισηγητές	Trusted Introducers
Εξόρυξη δεδομένων	Data minining
Εφαρμογής κοινωνικής δικτύωσης	social networking application
Μεσίτης, μεσολαβητής	Proxy
Μεσολαβητικές υπηρεσίες φυλλομετρητή	browser proxy services
Μοναδικό σημείο αποτυχίας	Single Point of Failure
Ομότιμη επικοινωνία	Peer-to-peer, P2P communication
Ομότιμος χρήστης	Peer user
Πράκτορες	Agents
Σημείο επιβολής πολιτικών ασφαλείας	policy enforcement point
Σύνοδος	Session
Σύστημα ανίχνευσης εισβολής	Intrusion Detection System - IDS
Υποδομή δημοσίου κλειδιού	Public Key Infrastructure - PKI

4.8. Βιβλιογραφικές Αναφορές

[1] Niemegeers, I.G., Heemstra de Groot, S. (2002). From Personal Area Networks to Personal Networks: A user oriented approach. Journal on Wireless and Personal Communications, 22, 175-186.

[2] Lo, A. Jacobsson, M., Prasad, V., Niemegeers, I.G. (2006). Personal Networks: An Overlay Network of Wireless Personal Area Networks and 3G Networks. Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose California.

[3] Cook, D.J., Youngblood, M., Heierman, E.O., Gopalratnam, K., Rao, S., Litvin, A., Khawaja, F. (2003). MavHome: an agent-based smart home. PerCom 2003: Pervasive Computing and Communications 2003 conference, Dallas, Texas.

[4] Intille, S.S. (2002). Designing a home of the future. IEEE Pervasive Computing, 1, 2, 76-82.

[5] Seigneur, J-M., Farrell, S., Jensen, C., Gray, E., Chen, Y. (2003).Towards security auto-configuration for smart appliances. Smart Objects Conference, Grenoble, France.

[6] Kyriazanos, D., Argyropoulos, M., Sanchez, L., Lanza, J., Alutoin, M., Hoebeke, J., Patrikakis, C. (2006). Overview of a personal network prototype. IEC ANNUAL REVIEW OF COMMUNICATIONS, 59, 521-534.

[7] Niemegeers, I. G., Heemstra De Groot, S. M. (2005). FEDNETS: Context-Aware Ad-hoc Network Federations. Springer Wireless Personal Communcations Journal, 33, 3-4, 305-318.

[8] Javaid, U., Meddour, D., Rasheed, E., Ahmed, T. (2007). A Profile-Based Network Layer Architecture for Personal Ubiquitous Environments. VTC2007: Vehicular Technology Conference 2007, Dublin, Ireland.

[9] Dingledine, R., Mathewson, N., Syverson, P. (2007). Deploying Low-Latency Anonymity: Design Challenges and Social Factors. IEEE Security & Privacy Magazine, 5, 5, 83-87.

[10] Kyriazanos, D., Argyropoulos, M. (2006). Personal Networks: Security Risks and Solutions. 45th FITCE Congress: Telecom Wars, Athens Greece.

[11] Kyriazanos, D., Stassinopoulos, G., Prasad N. (2006). Ubiquitous Access Control and Policy Management in Personal Networks. Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose California.

[12] Jiang, W., Clifton Ch. (2006). A secure distributed framework for achieving k-anonymity. The International Journal on Very Large Data Bases, 15, 4, 316-333.

[13] Persson, P., Younghee, J. (2005). Nokia sensor: from research to product. DUX'05: Designing for User Experiences Conference, San Francisco California.

[14] Kinateder, M., Rothermel K. (2003). Architecture and Algorithms for a Distributed Reputation System. First International Conference on Trust Management, Heraklion, Greece.

[15] Levy, E. (2004). Criminals Become Tech Savvy. IEEE Security and Privacy Magazine, 2, 2, 65-68.

[16] Stango, A., Kyriazanos, D., Prasad, N. (2007 December). An Architecture for securing context in federation Personal Networks, WPMC '07, Jaipur India.

[17] PGP 6.5.1 documentation, Introduction to Cryptography. (n. d.), Retrieved September 10, 2007 from http://www.pgpi.org/doc/pgpintro.

[18] Adams, C., Farrell, S. (1999). RFC 2510: Internet X.509 Public Key Infrastructure: Certificate Management Protocols.

[19] Hook, D. (2005). Beginning Cryptography with Java: WROX/Wiley.

[20] Sterbenz, L. (2000). Performance of the AES Candidate Algorithms in Java. Third AES Conference, New York.

[21] Java cryptography and C# cryptography resources, Home of open source libraries of the Legion of the Bouncy Castle. (n.d.) Retrieved October 5, 2007 from http://www.bouncycastle.org.

[22] W3C SOAP Specifications. (n.d.) (2007). Retrieved October 5, 2007 from http://www.w3.org/TR/soap/

[23] Chen, Z. (2007). A Scenario for Identity Management in Daidalos. CNSR '07: Fifth Annual Conference on Communication Networks and Services Research, New Brunswick, Canada.

[24] Jacobsson M., Niemegeers, I. (2005). Privacy and Anonymity in Personal Networks. IEEE PerCom 2005, 3rd Int'l Conf. on Pervasive Computing and Communications, Kauai Island, Hawaii.

[25] L. Cottrell (2000). Frequently asked questions about Mixmaster remailers. http://www.obscura.com/~loki/remailer/mixmaster-faq.html

[26] Zero-Knowledge Systems, http://www.zks.net/.

[27] Anonymizer, http://www.anonymizer.com/.

[28] Clarke, I., Sandberg, O., Brandon, W., Hong, T. W. (2001). Freenet: A Distributed Anonymous Information Storage and Retrieval System. In Designing Privacy Enhancing Technologies. International Workshop on Design Issues in Anonymity and Unobservability. New York: Springer.

[29] Politis, C., Nyberg, K., Mirzadeh, S., Masmoudi, K., Afifi, H., Floroiu, J., Prasad, N. R. (2005). Personal Network Security Architecture. International Wireless Summit, Wireless Personal Multimedia Communications'05, Aalborg, Denmark.

[30] WP4 "Security and Privacy" Group, IST Project MAGNET BEYOND Public Deliverable D4.4.2 "Solutions for Identity Management, Trust Model and Privacy for PNs"

[31] WP4 "Security and Privacy" Group, IST Project MAGNET BEYOND Public Deliverable D4.2.2 "Final PN key management solution and Cryptographic techniques"

5. Διαχείριση Ασφάλειας με Επίγνωση Κατάστασης και Προστασία Προσωπικής και Συγκείμενης Πληροφορίας

5.1. *Εισαγωγή*

Προκειμένου να υποστηριχθεί η επίγνωση κατάστασης (context awareness) και η σχετική δυναμική προσαρμογή των υπηρεσιών, οι εφαρμογές και τα στοιχεία δικτύου σε ένα PN και PN-F, η χρήση της συγκείμενης πληροφορίας (context) είναι απαραίτητη. Ο γενικός ορισμός της συγκείμενης πληροφορίας που χρησιμοποιείται είναι:

> ***Συγκείμενη πληροφορία*** *είναι κάθε πληροφορία που μπορεί να χρησιμοποιηθεί για να χαρακτηρίσει την κατάσταση μιας οντότητας. Η οντότητα είναι ένας άνθρωπος, ένα μέρος ή αντικείμενο που εμπλέκεται στην αλληλεπίδραση μεταξύ ενός χρήστη και μίας εφαρμογής, συμπεριλαμβανομένου του χρήστη και της εφαρμογής.* [1]

Είναι σαφές ότι τέτοια πληροφορία είναι απαραίτητη προκειμένου να επιτευχθεί η επιθυμητή προσαρμοστικότητα των υπηρεσιών και εφαρμογών.

Στο [2] αναγνωρίστηκαν δύο κατηγορίες πληροφορίας, τα συγκείμενα δεδομένα και η συγκείμενη πληροφορία. Η λογική ήταν να διαχωριστεί η ωμή πληροφορία που συλλέγεται από διάφορες πηγές ή άλλα υποσυστήματα από την επεξεργασμένη πληροφορία που διανέμεται και χρησιμοποιείται από εφαρμογές με επίγνωση κατάστασης.

- **Συγκείμενα Δεδομένα**: Τα ωμά, ακατέργαστα δεδομένα που λαμβάνονται απευθείας από τη πηγή, π.χ. έναν αισθητήρα, ένα στατιστικό πρόγραμμα στο στρώμα δικτύου, ένα αρχείο κ.α. Αυτά τα δεδομένα μπορούν να περιγραφούν με χρήση οποιασδήποτε αυθαίρετης μορφής δεδομένων (*data format*). Οι διαφορετικοί τύποι δεδομένων των οποίων γίνεται χρήση στο MAGNET Beyond μπορούν να βρεθούν στο [2].
- **Συγκείμενη Πληροφορία**: Επεξεργασμένα δεδομένα σε μια κοινή ή πρότυπη μορφή αναπαράστασης, προσαρμοσμένα στο μοντέλο πληροφορίας του συστήματος, ελεγμένα για συνοχή, περιλαμβάνουν μετα-δεδομένα (*meta-data*) κτλ. Η συγκείμενη πληροφορία μπορεί επίσης να προκύψει από άλλη συγκείμενη πληροφορία. Η πληροφορία τυποποιείται σε συγκεκριμένη μορφή και γενικά είναι επεξεργάσιμη και χρήσιμη για όλα τα στοιχεία του συστήματος που λειτουργούν με επίγνωση κατάστασης.

Ωστόσο, προκειμένου να γίνει καλύτερη χρήση της συγκείμενης πληροφορίας, θα πρέπει να λάβουμε υπόψη ότι διαφορετικοί χρήστες έχουν και διαφορετική άποψη για το πώς οι εφαρμογές πρέπει να αντιδρούν. Για αυτό το λόγο, τα προφίλ χρήστη χρησιμοποιούνται για να καθοριστεί πως θα χρησιμοποιείται η συγκείμενη πληροφορία. Επιπλέον, διαχωρίζεται η συγκείμενη πληροφορία από τα προφίλ χρήστη [3]σύμφωνα με τον ορισμό του ETSI:

> ***Προφίλ Χρήστη****: το σύνολο των σχετικών με το χρήστη πληροφοριών, προτιμήσεις, κανόνες και ρυθμίσεις, που επηρεάζουν το πώς ο χρήστης αντιλαμβάνεται τα τερματικά, τις συσκευές και τις υπηρεσίες.* [4]

Το προφίλ χρήστη λοιπόν αποτελεί μια τρίτη κατηγορία πληροφορίας και χρησιμοποιείται στην διεργασία προσωποποίησης (personalisation) των στοιχείων του συστήματος.

Αν και τα προφίλ χρήστη και η συγκείμενη πληροφορία διαχωρίζονται στη πρόταση που παρουσιάζεται, οι δύο κατηγορίες πληροφορίας μοιράζονται κοινά χαρακτηριστικά που κάνει εφικτό τον παρόμοιο χειρισμό στη περίπτωση της διανομής της πληροφορίας. Στο πρόγραμμα MAGNET Beyond, ένα ολοκληρωμένο πλαίσιο διαχείρισης συγκείμενης πληροφορίας (Secure Context Management Framework – SCMF) σχεδιάστηκε με γενικό τρόπο, ώστε να επιτρέπει την αποθήκευση και τη γενική πρόσβαση και στα προφίλ χρήστη. Σε αυτό το κεφάλαιο παρουσιάζεται καταρχήν το πλαίσιο και η αρχιτεκτονική που προέκυψε, καθώς και πως αυτή συλλέγει, διατηρεί και διανέμει την συγκείμενη πληροφορία αλλά και τα προφίλ χρήστη στο διανεμημένο περιβάλλον των Προσωπικών Δικτύων και των PN-Fs.

Με βάση αυτή την αρχιτεκτονική, παρουσιάζεται η πρόταση του Διαχειριστή Ασφαλείας με Επίγνωση Κατάστασης (Context Aware Security Manager - CASM), ο οποίος αφενός αποτελεί μια εφαρμογή με επίγνωση κατάστασης, λαμβάνοντας τροφή από το πλαίσιο SCMF, αλλά ταυτόχρονα αποτελεί και μια ολοκληρωμένη λύση προστασίας τόσο της συγκείμενης πληροφορίας όσο και των προφίλ χρήστη. Με αυτό τον τρόπο η πρόταση έχει τα εξής καινοτόμα χαρακτηριστικά:

- Διαχωρίζει τη συγκείμενη πληροφορία πλήρως από την προσωπική πληροφορία αλλά και την πληροφορία ασφαλείας όπως πολιτικές και κανόνες πρόσβασης, οδηγώντας σε ένα δυναμικό, εύκολα επεκτάσιμο και συνεργατικό μοντέλο. Κάθε κατηγορία πληροφορίας χειρίζεται από διαφορετική οντότητα διαχείρισης (context – διαχειριστής context SCMF, ασφάλεια – CASM, προφίλ χρήστη – διαχειριστής προφίλ SCMF)
- Επιτρέπει την προσωποποίηση της ασφάλειας, λαμβάνοντας υπόψη τις ιδιαίτερες προτιμήσεις του χρήστη όπως αυτές εκφράζονται στο σχετικό προφίλ. Με αυτό τον τρόπο η συμπεριφορά του συστήματος ασφάλειας και ο τρόπος αντίδρασης στις διάφορες καταστάσεις αλλάζει δυναμικά ανάλογα των προσωπικών προτιμήσεων.
- Είναι μέρος ενός γενικού πλαισίου διαχείρισης πληροφορίας με επίγνωση κατάστασης, και επομένως εναρμονισμένο με τις υπηρεσίες και τις εφαρμογές επίγνωσης κατάστασης που προστατεύει.
- Είναι εφαρμόσιμο σε πραγματική πλατφόρμα, όπως αυτή αναπτύχθηκε στα πλαίσια του προγράμματος MAGNET Beyond, και δεν αποτελεί απλώς ένα γενικό πλαίσιο αλλά μια ολοκληρωμένη λύση για ασφάλεια και έλεγχο πρόσβασης με επίγνωση κατάστασης.

Ακολουθεί η περιγραφή της Ασφαλούς Αρχιτεκτονικής Προσωπικής και Συγκείμενης Πληροφορίας καθώς και του Διαχειριστή Ασφαλείας με Επίγνωση Κατάστασης ενώ στο τέλος γίνεται σύγκριση με άλλες σχετικές προτάσεις, πλαίσια και λύσεις.

5.2. Ασφαλής Αρχιτεκτονική Διαχείρισης Συγκείμενης Πληροφορίας

Οι κύριες απαιτήσεις που πρέπει να ανταποκρίνεται η SCMF για να λειτουργεί στα πλαίσια των συνασπισμένων Προσωπικών Δικτύων παρουσιάζονται στο [6][5]και οδήγησαν στην αρχιτεκτονική που περιγράφεται σε αυτό το υποκεφάλαιο.

Ο πυρήνας του SCMF αποτελείται από ένα σύνολο στοιχείων (components) σε σύμπνοια με τις γενικές απαιτήσεις, που προσδίδουν την επιθυμητή λειτουργικότητα στο πλαίσιο, δηλαδή [6][5]:

- Παροχή αποδοτικής και ενιαίας πρόσβασης στη συγκείμενη πληροφορία κάνοντας την ανάπτυξη στοιχείων, υπηρεσιών και εφαρμογών με επίγνωση κατάστασης ευκολότερη.
- Επιτρέπει σε όλα τα στοιχεία, υπηρεσίες και εφαρμογές με επίγνωση κατάστασης να έχουν κοινή οπτική της συγκείμενης πληροφορίας.
- Να κρύβουν όλα τα ειδικά με την υλοποίηση ζητήματα προς έναν τερματικό (*client*) σχετικά με τα ωμά δεδομένα και την διαχείριση, διανομή και ανακάλυψη της συγκείμενης πληροφορίας.

Εσωτερική δομή αρχιτεκτονικής

Σε αυτή τη παράγραφο περιγράφεται εν συντομία η εσωτερική δομή της αρχιτεκτονικής, αποσαφηνίζοντας που έγκειται η κάθε διαφορετική λειτουργικότητα. Λεπτομέρειες της δομής και της εσωτερικής ροής πληροφορίας μπορούν να βρεθούν στο [2]. Η λειτουργία κάθε στοιχείου καθώς και η αλληλεπιδράσεις μεταξύ τους θα παρουσιαστούν.

Παρατηρώντας την Εικόνα 18, βλέπουμε ότι ο πυρήνας της αρχιτεκτονικής αποτελείται από έναν Πράκτορα (Context Agent) που βρίσκεται σε κάθε κόμβο στο PN και περιέχει μεταξύ άλλων τα εξής:

- Context Access Manager (CAM) - Διαχειριστής Συγκείμενης Πληροφορίας
- Processing & Storage (P & S) – Επεξεργασία & Αποθήκευση
- Context Aware Security Manager (CASM) - Διαχειριστής Ασφαλείας με Επίγνωση Κατάστασης

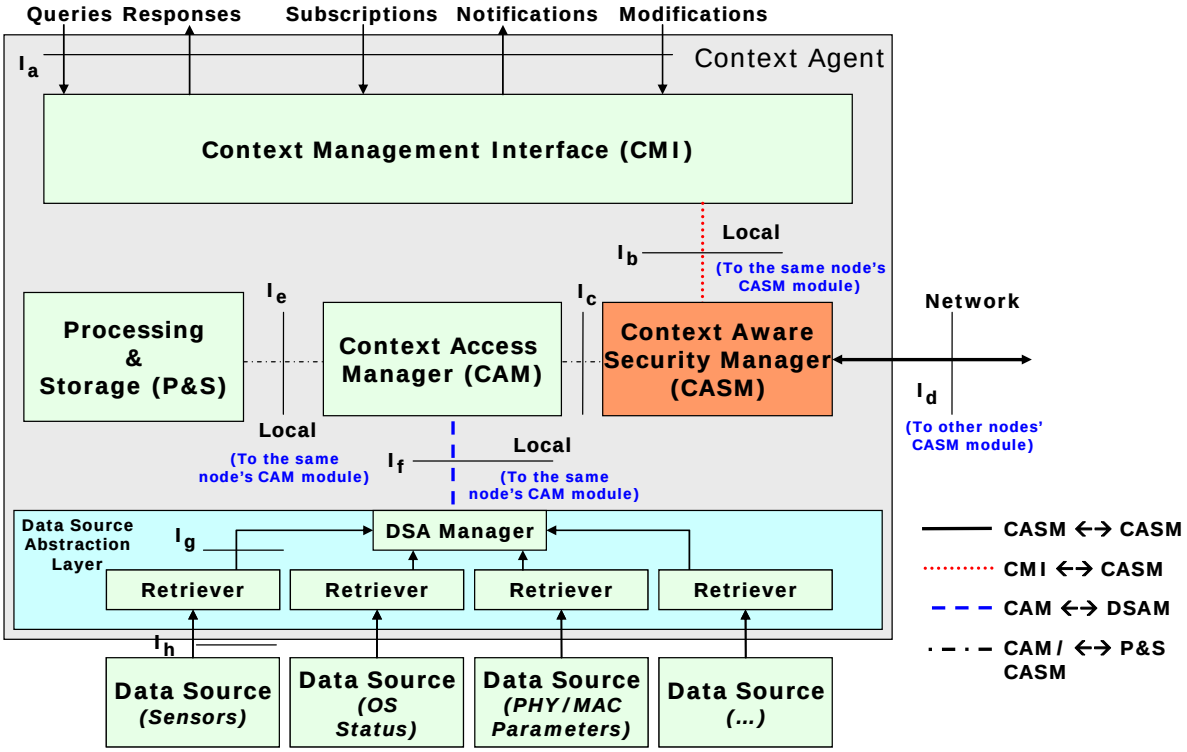
Αυτά τα εξαρτήματα αναλαμβάνουν τη διαχείριση της συγκείμενης πληροφορίας που λαμβάνεται από το Data Source Abstraction Layer (DSA) – Στρώμα Απόσπασης Πηγών Δεδομένων και χειρίζονται τα ερωτήματα που έρχονται από άλλα τοπικά στοιχεία επίγνωσης κατάστασης καθώς και άλλους απομακρυσμένους κόμβους.

Ξεκινώντας από την βάση της Εικόνα 18, όλες οι πηγές συγκείμενων δεδομένων δίνουν την πληροφορία τους στα αντίστοιχα εξαρτήματα ανάκτησης δεδομένων χρησιμοποιώντας την διεπαφή Ih. Αυτά τα εξαρτήματα είναι μικρά στοιχεία λογισμικού που επιτρέπουν την αλληλεπίδραση μεταξύ των πηγών δεδομένων και του CAM ως εξής:

- Με τυποποιημένες διεπαφές, δηλαδή τις I_h και I_g,

- Τον DSA Manager και τη διεπαφή I_f που περιλαμβάνει λειτουργία για σύγχρονη και ασύγχρονη ανάκτηση. Επίσης, ο CAM ενημερώνεται κάθε φορά που ένα εξάρτημα ανάκτησης κάνει εκκίνηση, γίνεται διαθέσιμο ή εξαφανίζεται.

Ο CAM κρατάει τους δείκτες του ποια συγκείμενη πληροφορία είναι διαθέσιμη που, δηλαδή είτε από τις τοπικές πηγές δεδομένων μέσω της διεπαδής If, από το P&S module μέσω της διεπαφής Ie, ή από άλλους κόμβους του PN μέσω πρόσβασης στο δίκτυα διαμέσου της διεπαφής Id. Όλες οι αιτήσεις για πληροφορία ελέγχονται μέσα στον CAM ώστε να βρεθεί κάθε φορά η βέλτιστη πηγή της πληροφορίας. Σε περίπτωση που ζητηθούν τιμές, ο CAM θα προωθήσει την αίτηση στη σχετική πηγή και θα επιστρέψει τη τιμή που θα λάβει από τη πηγή. Σε περίπτωση που ζητηθεί η θέση της πληροφορίας, ο CAM μπορεί να επιστρέψει επιτόπου τον σχετικό δείκτη. Επιπλέον, ο CAM είναι ικανός να αλληλεπιδρά με απομακρυσμένα CAM (δηλαδή μέσα σε άλλους κόμβους) προκειμένου να ανταλλάσσει και να ανανεώνει πληροφορίες σχετικά με ποια συγκείμενη πληροφορία διατίθεται σε κάθε κόμβο και να μπορεί να την διαθέσει ανά πάσα στιγμή.



Εικόνα 18 – Αρχιτεκτονική Πράκτορα Διασφάλισης Προσωπικής και Συγκείμενης Πληροφορίας

Το P&S εξάρτημα είναι υπεύθυνο για:

- Την αποθήκευση συγκείμενης πληροφορίας που δεν μπορεί να βρεθεί απευθείας από την πηγή, ή απλώς για λόγους τήρησης cache και για συνολικά πιο αποδοτική λειτουργία.
- Την επεξεργασία συγκείμενης πληροφορίας, π.χ. για την εξαγωγή υψηλότερου επιπέδου συγκείμενης πληροφορίας όπως την τρέχουσα κατάσταση του χρήστη ή συγκεκριμένα μετα-δεδομένα όπως η διάθεση.

Το αποθηκευτικό κομμάτι εξασφαλίζει ότι όλη η προφίλ και συγκείμενη πληροφορία που παρέχεται από το χρήστη, καθώς και η εξαγόμενη ή μη πληροφορία συγκειμένου είναι

αποθηκευμένη για γρήγορη μελλοντική χρήση αλλά και για εξαγωγή ιστορικών, συνηθειών κ.α.

Η Context Management Interface (CMI) – Διεπαφή Διαχείρισης Συγκείμενης Πληροφορίας βρίσκεται στη κορυφή του Πράκτορα. Η CMI χειρίζεται την αλληλεπίδραση μεταξύ των στοιχείων επίγνωσης κατάσταση και του SCMF (με τα εσωτερικά του δηλαδή στοιχεία), με σκοπό την ανάκτηση συγκείμενης πληροφορίας. Αυτές οι αλληλεπιδράσεις γίνονται βάσει ορισμένης γλώσσας πρόσβασης συγκείμενης πληροφορίας (Context Access Language -CALA) πάνω από τη διεπαφή επικοινωνίας Ia [2]. Αυτή η διεπαφή υποστηρίζει τόσο σύγχρονη όσο και ασύγχρονη πρόσβαση στη πληροφορία. Επομένως, το εξάρτημα αυτό εστιάζει στην μορφή των ερωτημάτων και την μετατροπή της εισόδου/εξόδου σύμφωνα με τον ορισμό του CALA.

Η ιδιωτικότητα και η ασφάλεια είναι κρίσιμα ζητήματα όταν χειρζόμαστε την προσωπική και τη συγκείμενη πληροφορία, καθώς υπάρχουν πολλές κακόβουλες εφαρμογές για τόσο ευαίσθητα και ιδιωτικά δεδομένα. Επίσης ο ίδιος ο χρήστης δεν επιθυμεί να κοινοποιεί παρά συγκεκριμένα δεδομένα, σε συγκεκριμένους ανθρώπους και ίσως μόνο σε συγκεκριμένες καταστάσεις και συνθήκες. Σε αυτά τα ζητήματα έρχεται να δώσει λύση ο Διαχειριστής Ασφάλειας με Επίγνωση Κατάστασης CASM, ο οποίος είναι ένα αυτόνομο στοιχείο σχεδιασμένο εντός του SCMF. Η θέση του CASM στην αρχιτεκτονική είναι τέτοια ώστε όλη η εισερχόμενη και εξερχόμενη πληροφορία από τον κόμβο να χρειάζεται να περάσει μέσω αυτού του στοιχείου. Αυτό εξασφαλίζει ότι όλη η πληροφορία και τα αιτήματα είναι ταυτοποιημένα, εξουσιοδοτημένα και καταγεγραμμένα, ενώ όποια πληροφορία βγαίνει προς τα έξω ανταποκρίνεται στις επιθυμίες και απαιτήσεις ιδιωτικότητας του ιδιοκτήτη. Στην επόμενη παράγραφο ακολουθεί η περιγραφή του CASM, οι λειτουργίες του καθώς και οι αλληλεπιδράσεις με τα άλλα στοιχεία της αρχιτεκτονικής.

5.3. Διαχειριστής ασφάλειας με επίγνωση κατάστασης

Ο Διαχειριστής Ασφαλείας (CASM) είναι μέρος της SCMF. Σχεδιάστηκε ενσωματώνοντας λειτουργίες AAA (Authentication, Authorisation, Accounting) [7] με τις εξής εξελιγμένες δυνατότητες ασφαλείας:

- Αναγνώριση και Ταυτοποίηση - Authentication / Identification
- Έλεγχο Πρόσβασης και Εξουσιοδότηση - Authorization/ Access control, βάσει των πολιτικών ασφαλείας
- Επιβολή ιδιωτικότητας και σχετικών πολιτικών
- Διαχείριση ασφαλείας και εμπιστοσύνης
- Καταγραφή των συναλλαγών – Accounting

Αποτελείται όπως θα περιγραφεί και παρακάτω από τις λογικές οντότητες των διαχειριστών ασφαλείας, ιδιωτικότητας και εμπιστοσύνης, που είναι υπεύθυνες για τις σχετικές αποφάσεις στο PN βάσει των πληροφοριών όλων των κατηγοριών για το περιβάλλον, τις εμπλεκόμενες οντότητες και τη θέση τους και τις υπηρεσίες ή πληροφορίες που ζητούνται. Λόγω των διεπαφών με το προφίλ χρήστη, το SCMF αλλά και τη βάση πολιτικών ασφαλείας του ίδιου του CASM (ή μιας εξωτερικής μηχανής πολιτικών ασφαλείας) οι προσωπικές επιλογές και προτιμήσεις, η κατάσταση και συγκείμενη

πληροφορία αλλά και οι ρυθμίσεις ασφαλείας όπως αυτές εκφράζονται στις πολιτικές, ελέγχονται και χρησιμοποιούνται συνολικά για κάθε απόφαση. Με αυτό τον τρόπο ο Διαχειριστής εκτελεί προσαρμοστική και δυναμική διαχείριση ασφάλειας με επίγνωση κατάστασης, διασφαλίζοντας τις σχετικές συναλλαγές πληροφορίας, εφαρμογών και υπηρεσιών. Η προσαρμοστικότητα και ευλυγισία υποστηρίζονται με τον ορισμό και χρήση διαφορετικών επιπέδων για την ασφάλεια, την ιδιωτικότητα και την εμπιστοσύνη για τις εμπλεκόμενες οντότητες και συνθήκες μίας συναλλαγής. Τα διαφορετικά αυτά επίπεδα ασφάλειας, ιδιωτικότητας και εμπιστοσύνης προσαρμόζονται στις αντίστοιχες πολιτικές και ρυθμίσεις ασφαλείας του PN, τις προσωπικές προτιμήσεις ιδιωτικότητας του χρήστη καθώς και τις εκάστοτε τεχνικές παραμέτρους σε όλα τα στρώματα του δικτύου (πρωτόκολλα επικοινωνίας, ύπαρξη και ισχύς ασφαλούς καναλιού, δυνατότητες συσκευής κ.α.)

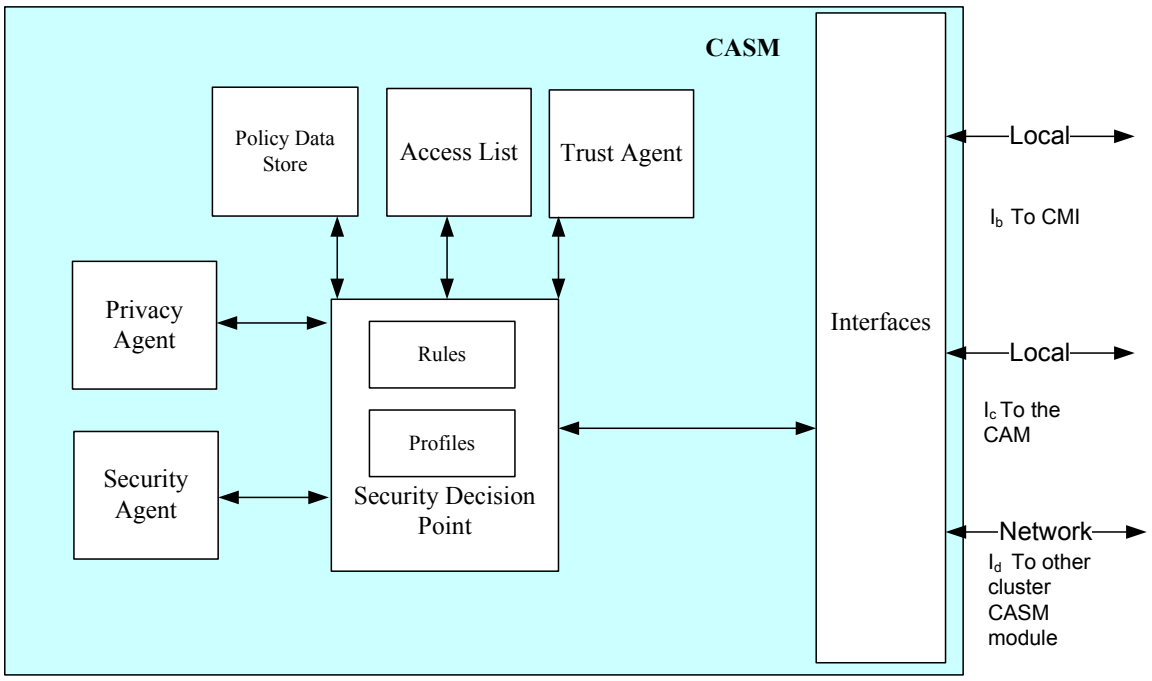
Συνοπτικά τα ωφέλιμα χαρακτηριστικά του Διαχειριστή Ασφαλείας είναι τα εξής:

- Λειτουργεί σαν σημείο εφαρμογής πολιτικών ασφαλείας, διασφαλίζοντας την ιδιωτικότητα πληροφοριών προφίλ χρήστη και συγκείμενης πληροφορίας
- Συνδέεται με ομότιμες τέτοιες οντότητες διαχείρισης σε όλο το προσωπικό δίκτυο, παρέχοντας πλήρη κάλυψη σε όλο το δίκτυο
- Βασίζεται σε ανοιχτές τεχνολογίες και πρότυπα καθώς και τεχνολογίες XML, επιτρέποντας δυναμική εφαρμογή νέων πολιτικών και επεκτασιμότητα
- Παρέχει μια ενιαία διεπαφή για όλες τις εφαρμογές και υπηρεσίες που χρησιμοποιούν προσωπικά δεδομένα και συγκείμενες πληροφορίες, και χάριν στο SCMF, δρα και ο ίδιος ως μια εφαρμογή επίγνωσης κατάστασης στα ίδια πλαίσια
- Λαμβάνει υπόψη τον ανθρωποκεντρικό χαρακτήρα των Προσωπικών Δικτύων, ενσωματώνοντας στις πολιτικές και αποφάσεις ασφαλείας την πληροφορία προφίλ χρήστη και τις προσωπικές προτιμήσεις, όπως αυτές εκφράζονται με την έννοια της σημαίας ιδιωτικότητας (privacy flags)
- Έχει επίγνωση κατάστασης ασφαλείας, οι οποίες, χωριζόμενες σε τρία επίπεδα ασφαλείας (Χαμηλό, Μέσο, Υψηλό) οδηγούν και σε δυναμική εφαρμογή διαφορετικού συνόλου πολιτικών ασφαλείας
- Συνεργάζεται με μηχανισμούς φήμης και μοντέλα εμπιστοσύνης, ενσωματώνοντας το επίπεδο εμπιστοσύνης για κάθε εμπλεκόμενη οντότητα σε μια συναλλαγή
- Υποστηρίζει το μηχανισμό ανωνυμίας που προτάθηκε επίσης στη διατριβή, φροντίζοντας ώστε η πληροφορία που δημοσιεύεται να μην οδηγεί σε άμεση ή έμμεση αποκάλυψη της ταυτότητας

Ακολουθεί αναλυτική περιγραφή της δομής και των λειτουργιών του CASM, συμπεριλαμβανομένου και του μοντέλου πληροφοριών ασφαλείας, όπως αυτό ενσωματώνεται στις πολιτικές και τους κανόνες πρόσβασης.

5.4.1 Δομή CASM και μοντέλο πληροφορίας ασφαλείας

Η θέση του CASM στην αρχιτεκτονική παρουσιάστηκε στην Εικόνα 18 ενώ στην Εικόνα 19 παρουσιάζεται σε υψηλό επίπεδο τα στοιχεία που τον απαρτίζουν και που εκτελούν τις λειτουργίες διαχείρισης της ασφάλειας, ιδιωτικότητας και εμπιστοσύνης στα Προσωπικά Δίκτυα και συνασπισμούς αυτών.



Εικόνα 19 – Εσωτερική δομή Διαχειριστή Ασφαλείας για ασφάλεια, ιδιωτικότητα και διαχείριση εμπιστοσύνης

Ακολουθεί η περιγραφή καθενός από τα εσωτερικά στοιχεία.

Πράκτορας Ασφάλειας - Security Agent

Ο Πράκτορας Ασφαλείας εξασφαλίζει την εμπιστευτικότητα και ακεραιότητα των δεδομένων κατά τους κανόνες του αντίστοιχου προφίλ ασφαλείας. Επίσης υλοποιεί την ταυτοποίηση προέλευσης των δεδομένων κατόπιν της οποίας ο Πράκτορας Εμπιστοσύνης - Trust Agent ενημερώνεται για τα αποτελέσματα της εξακρίβωσης ταυτοποίησης.

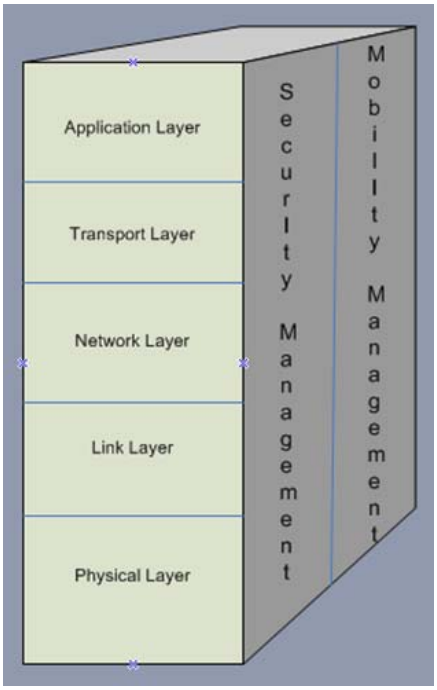
Ο ρόλος του Πράκτορα Ασφαλείας είναι συνδεδεμένος με την αναγνώριση και ταυτοποίηση της προέλευσης των δεδομένων ενώ η ταυτοποίηση και αναγνώριση ταυτότητας (authentication) συμβαίνει στον Πράκτορα Εμπιστοσύνης προκειμένου να αποδοθεί το σχετικό επίπεδο εμπιστοσύνης.

Οι μηχανισμοί ασφαλείας που εφαρμόζονται εξαρτώνται από τις απαιτήσεις ασφαλείας της επικοινωνίας αλλά και τις αλλαγές στην κατάσταση (π.χ. αλλαγή στη θέση, ή μεταφορά πιο ευαίσθητων προσωπικών δεδομένων). Η προσαρμοστικότητα των μηχανισμών του CASM εξασφαλίζεται από τον Πράκτορα Ασφαλείας, ο οποίος αναθέτει το κατάλληλο Επίπεδο Ασφαλείας για την επικοινωνία και κατάσταση σε τρία πιθανά επίπεδα: Χαμηλό, Μέσο και Υψηλό. Ανάλογα με το επίπεδο επιτρέπεται και η πρόσβαση σε υπηρεσίες και δεδομένα διαφορετικής σημαντικότητας. Αναλυτικά:

- *Χαμηλό* – παρέχονται δημόσιες υπηρεσίες και επιτρέπεται ανταλλαγή μη ευαίσθητων και ασήμαντων δεδομένων. Σε αυτό το επίπεδο τα δεδομένα ανταλλάσσονται ως απλό κείμενο, δεν υπάρχει ασφαλής δίαυλος επικοινωνίας και κάποια σχετική υποδομή ασφαλείας. Επιπλέον η θέση των εμπλεκόμενων κόμβων κρίνεται ως μη ασφαλής. Π.χ. Συναλλαγή πάνω από ανοιχτό, δημόσιο δίκτυο wi-fi σε μια καφετέρια.

- *Μέσο* – η επικοινωνία απαιτεί κάποια βασική προστασία, ακόμη και αν τα δεδομένα που ανταλλάσσονται δεν είναι ευαίσθητα. Σε αυτό το επίπεδο υπάρχει μια τυπική υποδομή ασφαλείας, όπως π.χ. κάποιο απλό σύστημα login με κωδικό, δίαυλος με ασθενή κρυπτογράφηση ή ένα firewall. Επίσης η θέση βρίσκεται σε έναν σχετικά ελεγχόμενο χώρο. Π.χ. συναλλαγή πάνω από Bluetooth με PIN, συναλλαγή πάνω από το τοπικό δίκτυο του γραφείου.
- *Υψηλό* – παρέχεται προνομιούχος πρόσβαση σε σημαντικές υπηρεσίες ή/και ανταλλαγή ευαίσθητων προσωπικών δεδομένων. Π.χ. ύπαρξη ισχυρών ασφαλών διαύλων (π.χ. IPSec), ψηφιακών πιστοποιητικών και υπογραφών (PKI, PGP [8]) και ισχυρών αλγορίθμων κρυπτογράφησης. Αυτό το επίπεδο έχει υψηλές απαιτήσεις σε δικτυακά και υπολογιστικά αποθέματα.

Ο καθορισμός του επιπέδου ασφαλείας βασίζεται στην προσφερόμενη συγκείμενη πληροφορία από τον SCMF και συγκρίνεται με τις απαιτήσεις και τους κανόνες πρόσβασης που συνδέονται με την ζητηθείσα πληροφορία, εφαρμογή ή υπηρεσία ανάλογα τη σημαντικότητα τους. Ουσιαστικά, το επίπεδο ασφαλείας εκφράζει την επίγνωση της κατάστασης από τον CASM, καθώς λαμβάνει υπόψη του της πηγές συγκείμενης πληροφορίας από όλα τα στρώματα του δικτύου, καθώς και πληροφορίες θέσεις από πηγές διαχείρισης της κίνησης του χρήστη (mobile management) όπως εικονογραφείται στην Εικόνα 20.



Εικόνα 20 – Σχέτική θέση διαχείρισης ασφάλειας (security management) με τα πρωτόκολλα σε όλα τα στρώματα (layers) και τη διαχείριση κινητικότητας (mobility management)

Πράκτορας Εμπιστοσύνης - Trust Agent

Οι μηχανισμοί εγκαθίδρυσης εμπιστοσύνης χρησιμοποιούνται για να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση ή τον είσοδο ψευδών και βλαπτικών για το σύστημα στοιχείων από π.χ. φαινομενικά νόμιμους κόμβους που ελέγχονται για κάποιο λόγο από κακόβουλους όπως σε περίπτωση κλοπής. Η εγκαθίδρυση της εμπιστοσύνης μπορεί να βασίζεται στην ταυτοποίηση, στους ρόλους χρήστη, στη συμπεριφορά και στην αξιοπιστία των δεδομένων.

Επομένως, για να λειτουργήσουν οι μηχανισμοί αυτοί απαιτείται συνεργασία με τυπικούς μηχανισμούς authentication και ελέγχου πρόσβασης.

Ο CASM είναι επίσης υπεύθυνος για την εγκαθίδρυση εμπιστοσύνης μεταξύ των μερών που επικοινωνούν. Αυτό είναι καθήκον του Πράκτορα Εμπιστοσύνης, ο οποίος είναι υπεύθυνος για τη διαχείριση των σχέσεων εμπιστοσύνης και των σχετικών λιστών πρόσβασης. Τα πιστοποιητικά και κλειδιά διαμοιράζονται κατά τον σχηματισμό του συνασπισμού Προσωπικών Δικτύων [15] και από εκεί και πέρα ο Πράκτορας Εμπιστοσύνης διαχειρίζεται την εμπιστοσύνη που συνδέεται με το καθένα.

Τα επίπεδα εμπιστοσύνης ορίζονται ως εξής:

- *Άγνωστο* – για οντότητες που εισέρχονται στο PN/PN-F και ζητούν πρόσβαση σε κάποια υπηρεσία ή πληροφορία για πρώτη φορά (διαδικασία πρόσκλησης).
- *Μη έμπιστα* – για οντότητες που για οποιοδήποτε λόγο τους έχει αφαιρεθεί το δικαίωμα πρόσβασης (*black list*) και ας είχαν εισέλθει στο παρελθόν. Εδώ περιλαμβάνονται οντότητες που τους έχουν ανακληθεί τα πιστοποιητικά ή που ο χρήστης έχει κηρύξει ως ανεπιθύμητες.
- *Έμπιστα* – για οντότητες που έχουν προσκληθεί στο PN και διαθέτουν τα απαραίτητα έγκυρα πιστοποιητικα, π.χ. ένα κοινό κλειδί.
- *Μερικώς Έμπιστα* – ένα ενδιάμεσο επίπεδο εμπιστοσύνης που εξυπηρετεί κυρίως στο να δίνονται περισσότερες διαχειριστικές επιλογές και να υποστηρίζονται μοντέλα εμπιστοσύνης όπως η PGP που το υποστηρίζουν. Για οντότητες που διαθέτουν μέρος των απαιτούμενων πιστοποιητικών (π.χ. μια μόνο συστατική υπογραφή στο πιστοποιητικό τους αντί για τρεις).

Πράκτορας Ιδιωτικότητας - Privacy Agent

Συνήθως η ιδιωτικότητα κατανοείται ως ανωνυμία του αποστολέα και του παραλήπτη. Ωστόσο, πληροφορίες για την επικοινωνία μπορεί να εξαχθούν και από άλλες παραμέτρους, όπως την κίνηση του δικτύου ή τα πρότυπα της κίνησης, το μέγεθος των μηνυμάτων, το χρόνο και τη θέση κ.α. Εν συντομία, η ιδιωτικότητα μπορεί να παραβιαστεί και παρακολουθώντας έναν κόμβο για συγκεκριμένο χρόνο, αναγνωρίζοντας τον χρήστη που χρησιμοποιεί έναν συγκεκριμένο κόμβο και αποκτώντας πρόσβαση σε δεδομένα ενάντια στη θέληση του ιδιοκτήτη.

Επομένως οι ακόλουθες πλευρές του ζητήματος της ιδιωτικότητας ελήφθησαν υπόψη:

- *Διασφάλιση ιδιωτικότητας της πληροφορίας*, δηλαδή αποτροπή αποκάλυψης προσωπικής πληροφορίας σε κακόβουλους, δίνοντας πληροφορίες μόνο σε έμπιστες και εξουσιοδοτημένες οντότητες (ελεγχόμενη αποκάλυψη πληροφορίας).
- *Διατήρηση ανωνυμίας* για χρήστες σε συγκεκριμένα σενάρια και περιπτώσεις. Δηλαδή, η κατάσταση του να είναι ο χρήστης μη αναγνωρίσιμος μέσα σε ένα σύνολο χρηστών ή συνασπισμού PN-F. Η ανωνυμία επίσης επηρεάζει την ιδιωτικότητα της θέσης, καθώς αυτή επίσης αποκρύπτεται σε περιπτώσεις ανωνυμίας.
- *Διασφάλιση ιδιωτικότητας θέσης*, δηλαδή η απόκρυψη από κακόβουλους χρήστες της τρέχουσας ή παλιότερης θέσης ενός κόμβου.

Ο Πράκτορας Ιδιωτικότητας είναι υπεύθυνος για να αποφασίσει αν τα δεδομένα θα αποκαλυφθούν, ή αν θα δοθούν ανώνυμα σε περιπτώσεις που εμπλέκεται ομάδα χρηστών, ενεργοποιώντας μηχανισμούς όπως π.χ. ο μηχανισμός ανωνυμίας που προτείνεται στη παρούσα διατριβή. Για αυτό το σκοπό γίνεται χρήση σημαιών επιπέδου ιδιωτικότητας που εκφράζουν την προσωπική επιλογή του χρήστη όσον αφορά την ιδιωτικότητα των δεδομένων του. Οι διαθέσιμες σημαίες είναι:

- *«ελεύθερη πρόσβαση»* - παροχή των δεδομένων χωρίς περαιτέρω έλεγχο ή επιβεβαίωση, κατάλληλο για δημόσια ή ασήμαντα δεδομένα.
- *«έλεγχος κανόνων πρόσβασης και τρέχουσας κατάστασης»* - εδώ διατάσσεται ο έλεγχος των προφίλ της οντότητας που κάνει την αίτηση και γίνεται σύγκριση με τις πολιτικές ασφαλείας και κανόνες πρόσβασης. Σε αυτή τη φάση επίσης ελέγχεται η σχετική συγκείμενη πληροφορία για την κατάσταση και το επίπεδο ασφαλείας που χαρακτηρίζει την συναλλαγή. Το τελευταίο βήμα είναι ικανό να οδηγήσει σε εξαίρεση των στατικών κανόνων ασφαλείας, π.χ. όταν ένας έμπιστος χρήστης προσπαθεί να αποκτήσει πρόσβαση πάνω από μη ασφαλή πρωτόκολλα επικοινωνίας. Το τελευταίο αποτελεί και την κύρια λειτουργία επίγνωσης κατάστασης του CASM.
- *«απαιτείται επιβεβαίωση χρήστη»* - ο χρήστης ερωτάται κάθε φορά να επιτρέψει την πρόσβαση στα δεδομένα ο ίδιος μέσω κατάλληλου GUI. Αν ο χρήστης δεν είναι διαθέσιμος (π.χ. offline) τότε αυτόματα απορρίπτεται η σχετική αίτηση πρόσβασης, όντας η ασφαλέστερη επιλογή.
- *«απαγορευμένη πρόσβαση»* - τα δεδομένα δεν αποκαλύπτονται σε καμία αίτηση, ούτε γίνεται χρήση τους σε οποιαδήποτε υπηρεσία, ανεξαρτήτως πιστοποιητικών. Για πολύ ευαίσθητα δεδομένα που ο ιδιοκτήτης θέλει να έχει αποκλειστική τοπική πρόσβαση.

Σημείο Αποφάσεων Ασφαλείας – Security Decision Point

Ο κύριος στόχος του CASM είναι να παρέχει εξουσιοδότηση προσπέλασης σύμφωνα με τις πολιτικές ασφαλείας και την συγκείμενη πληροφορία. Αυτό εκτελείται στο Σημείο Αποφάσεων Ασφαλείας (ΣΑΑ). Η πολιτική ασφάλειας είναι γενικά ένας κανόνας ή σύνολο κανόνων που αποτελείται από ένα σύνολο ορισμένων τιμών, σύνολα τιμών ή μιας ακτίνας τιμών για παραμέτρους που προβλέπονται από τα προφίλ ασφάλειας. Το ΣΑΑ περιλαμβάνει ένα σύνολο κανόνων και παραμέτρων ασφαλείας, που χρησιμοποιούνται στις αποφάσεις πολιτικής. Με τη σωστή εφαρμογή των πολιτικών σε ταχτοποιημένες αιτήσεις, πραγματοποιείται ο έλεγχος πρόσβασης. Στο ΣΑΑ, έχουν προβλεφτεί τα προφίλ του κόμβου-συσκευής, υπηρεσίας και εφαρμογής, χρήστη και κατάστασης. Αυτά περιέχουν όλη την απαραίτητη πληροφορία που αντιστοιχεί στις παραμέτρους ασφαλείας που ελέγχει ο CASM. Στα πλαίσια των σεναρίων Προσωπικών Δικτύων, όπως αυτά καταστρώθηκαν στο MAGNET Beyond, παρουσιάζονται τα προφίλ, οι ρόλοι των χρηστών, οι τοποθεσίες και οι γενικές κατηγορίες ευαίσθητων δεδομένων στον Πίνακας 2.

Πίνακας 2 – Ρόλοι χρηστών και ευαίσθητα προσωπικά δεδομένα

Προφίλ οντοτήτων σε χρήση	Ρόλος Πηγής Δεδομένων	Ρόλος Παραλήπτη Δεδομένων	Τοποθεσία	Γενικές κατηγορίες ευαίσθητων προσωπικών δεδομένων
• Χρήστης • Κόμβος (συσκευή) • Κατάσταση • Υπηρεσία (εφαρμογή)	• Ασθενής • Μέλος Οικογένειας • Σύζυγος • Γονέας • Υπάλληλος • Συνεργάτης • Φίλος • Χρήστης	• Ιατρός • Μέλος Οικογένειας • Προϊστάμενος • Συνεργάτης • Παιδί • Σύζυγος • Φίλος • Άγνωστος	• Σπίτι • Γραφείο • Νοσοκομείο • Αυτοκίνητο • Δημόσιος χώρος • Άγνωστος	*Ταυτότητα Χρήστη* *Ιατρικό Ιστορικό Ιατρικά Δεδομένα* *Οικονομικά Στοιχεία* *Στοιχεία Επαφής* *Θέση*

Ο τρέχων ρόλος ανατίθεται στον χρήστη είτε από τον ίδιο είτε αυτόματα ελέγχοντας τη συγκείμενη πληροφορία και τις συνήθειες του χρήστη. Πέραν των προεπιλεγμένων κανόνων ασφαλείας, ο χρήστης μπορεί να αλλάξει τους κανόνες πρόσβασης στη πληροφορία μέσω κατάλληλου διαχειριστικού εργαλείου, όπως επίσης μπορεί να αλλάξει και το απαιτούμενο επίπεδο ασφαλείας. Παραδείγματα των κανόνων παρουσιάζονται στον Πίνακας 3.

Πίνακας 3 – Παραδείγματα κανόνων και αντίστοιχων επιπέδων ασφαλείας

ID Κανόνα	Θέση Προορισμού	Ρόλος Παραλήπτη Δεδομένων	Θέση Πηγής	Τρέχων Ρόλος Πηγής	Κανόνες πρόσβασης	Απαιτούμενο Επίπεδο Ασφάλειας
Pt01	Νοσοκομείο	Ιατρός	Σπίτι	Ασθενής	Ναι (ιατρική κατάσταση), Όχι για τα υπόλοιπα δεδομένα	Χαμηλο
Pt02	Νοσοκομείο	Ιατρός	Νοσοκομείο	Ασθενής	Ναι (ιατρική κατάσταση, ιστορικό, ιατρικά δεδομένα), Επιβεβαίωση χρήστη (διεύθυνση), Όχι για τα υπόλοιπα δεδομένα	Μέσο
Em02	Γραφείο	Προϊστάμενος	Γραφείο	Υπάλληλος	Ναι (Θέση), Όχι για τα υπόλοιπα δεδομένα	Μέσο
Pt03	Σπίτι	Παιδί	Γραφείο	Γονέας	Ναι (Θέση) Ναι (Ιατρική Κατάσταση), Όχι για τα υπόλοιπα δεδομένα	Μέσο
Us01	Δημόσιος Χώρος	Άγνωστος	Σπίτι	Χρήστης	Όχι για όλα τα δεδομένα	Υψηλό

Οι παραπάνω κανόνες εφαρμόζονται βάσει των πληροφοριών και παραμέτρων που διατίθενται από τα προφίλ των εμπλεκόμενων οντοτήτων. Ακολουθεί η περιγραφή των σχετικών προφίλ ασφαλείας.

5.4.2 Προφίλ ασφάλειας και χρήστη

Όπως είδαμε ο CASM είναι ένα εξάρτημα που τροφοδοτείται από προφίλ διαφόρων οντοτήτων. Τα προφίλ παρέχουν δομημένη πληροφορία για όλα τα στοιχεία του PN και PN-F καθώς και για νοερές οντότητες: Χρήστες, Συσκευές, Υπηρεσίες, Καταστάσεις καθώς και ρόλους αλλά και Προσωπικά Δίκτυα και συνασπισμούς. Η πληροφορία αυτή επίσης συνοδεύεται από τις σχετικές παραμέτρους και πολιτικές ασφαλείας, πάνω στις οποίες βασίζεται ο έλεγχος πρόσβασης.

Τα *προφίλ χρήστη* φέρουν όλα τα χαρακτηριστικά των χρηστών καθώς και σχετικές παραμέτρους και δεδομένα ασφαλείας:

- Πληροφορίες χρήστη: η ταυτότητα, οργανισμός, ρόλος, ιδιότητες μέλους, ενδιαφέροντα, προτιμήσεις, στοιχεία επαφής, ιατρικά δεδομένα κ.α.
- Κλειδιά και πιστοποιητικά από συσκευές και συνασπισμούς όπου έχει προηγηθεί η διαδικασία εγκαθίδρυσης εμπιστοσύνης (π.χ. κλειδια PFP για την είσοδο στο PN ως προσωπικός κόμβος [15]).
- Υπηρεσίες: πληροφορίες για συνδρομές σε υπηρεσίες, προτιμήσεις, πληροφορίες χρήσης, εξόφλησης κ.α.
- Επίπεδα εμπιστοσύνης: κάθε χρήστης διαθέτει μια συλλογή από πιστοποιητικά από οντότητες με τις οποίες έχει αλληλεπιδράσει στο παρελθόν. Η ιεραρχία που δίνει ο χρήστης σε αυτά τα πιστοποιητικά είναι το λεγόμενο μοντέλο εμπιστοσύνης, σύμφωνα με το οποίο κάθε οντότητα έχει ένα συγκεκριμένο επίπεδο εμπιστοσύνης.
- Πληροφορίες μέλους συνασπισμών Προσωπικών Δικτύων και σχετικά πιστοποιητικά.

Ανάλογα περιγραφικά προφίλ υπάρχουν και για τις υπόλοιπες οντότητες στο προσωπικό δίκτυο καθώς και για νοερές οντότητες όπως η Κατάσταση. Βάσει των παραμέτρων που παρέχονται σε κάθε προφίλ οντότητας, τα Προφιλ Πολιτικών Ασφαλείας αφού έχουν αρχικοποιήσει το σύνολο των κανόνων πρόσβασης προχωρούν στη λήψη αποφάσεων ασφαλείας. Η διαχείριση των πολιτικών στην επικράτεια του συνασπισμού των Προσωπικών Δικτύων επιτυγχάνεται με την μετάδοση της ανανεωμένης πληροφορίας από τον διαχειριστή με χρήστη της πλατφόρμας διαχείρισης πληροφορίας SCMF που περιγράφτηκε πριν. Για αυτό το λόγο αναπτύχθηκε ένα εργαλείο μέσω του οποίου ο διαχειριστής μπορεί να τροποποιεί ή να δημιουργεί νέους κανόνες ασφαλείας, και να διατάσσει την ενημέρωση όλων των διαχειριστών ασφαλείας πάνω από το ενιαίο προσωπικό υπερ-δίκτυο (*overlay network*).

Ακολουθεί μια ανάλυση των Προφίλ ασφάλειας:
Προφίλ Ασφάλειας:

Οντότητα: Χρήστης

Ιδιότητα: Ταυτότητα χρήστη
Πεδίο: Εικονικές ταυτότητες/Ψευδώνυμα
Πεδίο: Ρόλος
Πεδίο: Επίπεδο Εμπιστοσύνης

Οντότητα: Συσκευή
Ιδιότητα: ID Συσκευής
Ιδιότητα: Banned (ναι/όχι)
Πεδίο: Επίπεδο Εμπιστοσύνης

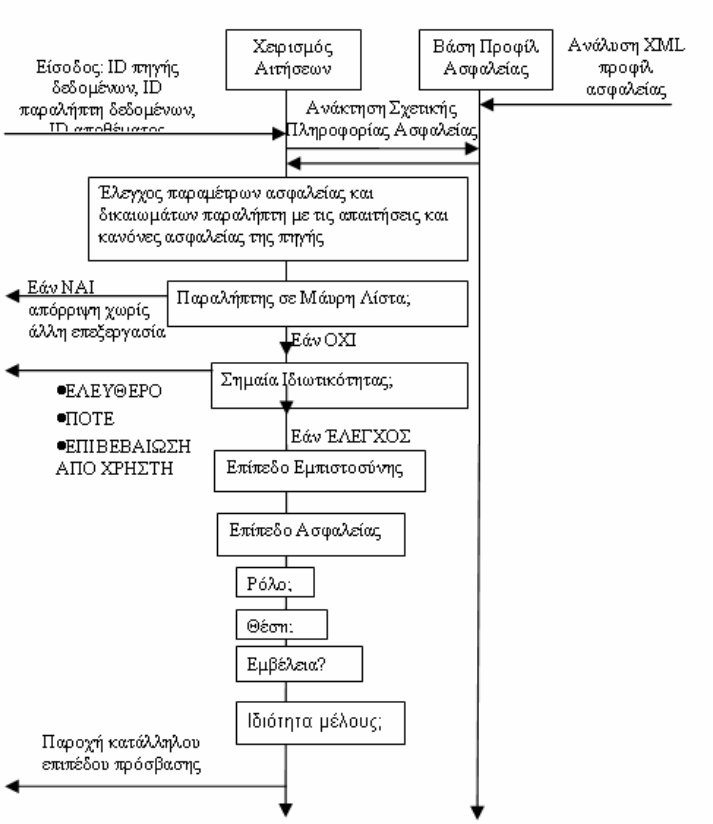
Οντότητα: Απόθεμα
Επιλογή: Υπηρεσία
Ιδιότητα: ID Υπηρεσίας
Ιδιότητα: Σημαία Ιδιωτικότητας
(ΕΛΕΥΘΕΡΑ/ΕΛΕΓΧΟΣ/ΕΠΙΒΕΒΑΙΩΣΗ/ΠΟΤΕ)

Επιλογή: Προσωπική και Συγκείμενη Πληροφορία
Ιδιότητα: ID Πληροφορίας
Ιδιότητα: Σημαία Ιδιωτικότητας
(ΕΛΕΥΘΕΡΑ/ΕΛΕΓΧΟΣ/ΕΠΙΒΕΒΑΙΩΣΗ/ΠΟΤΕ)

Οντότητα: PN-F
Πεδίο: ID Συνασπισμού, περιγραφή
Πεδίο: PN-F λίστα μελών

5.4.3 Διάγραμμα ροής αλγορίθμου ασφαλείας

Το ακόλουθο διάγραμμα ροής (Εικόνα 21) παρουσιάζει τη λειτουργία του αλγορίθμου λειτουργίας του CASM, με τις λειτουργίες να αντιστοιχούν στους ελέγχους από τα διάφορα στοιχεία του CASM όπως αυτά παρουσιάστηκαν στη προηγούμενη παράγραφο.



Εικόνα 21 – Διάγραμμα ροής για τον αλγόριθμο λειτουργίας του διαχειριστή ασφάλειας

5.4.4 Διεπαφές

Όπως είδαμε έχει γίνει πρόβλεψη ώστε ο Διαχειριστής Ασφάλειας να αλληλεπιδρά με μηχανισμούς του υπόβαθρου ασφαλείας και άλλα εξωτερικά στοιχεία, όπως π.χ. ένα μηχανισμό φήμης, πέραν των εσωτερικών στοιχείων του SCMF. Η εντός του SCMF λειτουργία καθώς και οι αλληλεπιδράσεις με ενδεικτικά εξωτερικά στοιχεία παρουσιάζονται από την Εικόνα 22 εώς και Εικόνα 27.

Ο CASM παρέχει διεπαφές βασισμένες σε:

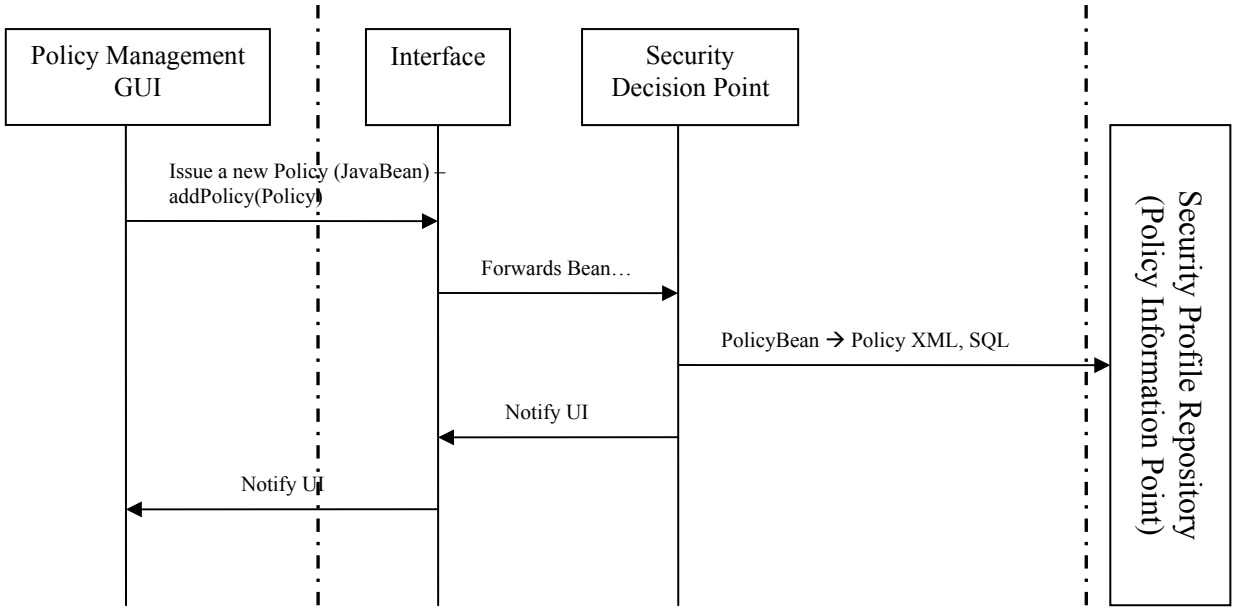
- XML-RPC: Απομακρυσμένη κλήση διαδικασιών με χρήση XML
- SOAP messaging [10]: πρωτόκολλο ανταλλαγής κειμένων XML
- JavaBeans [11]: μια αντικειμενοστρεφής λύση για την διαχείριση σε Java όλων των σχετικών οντοτήτων

Ο CASM έχει σχεδιαστεί να αλληλεπιδρά με:

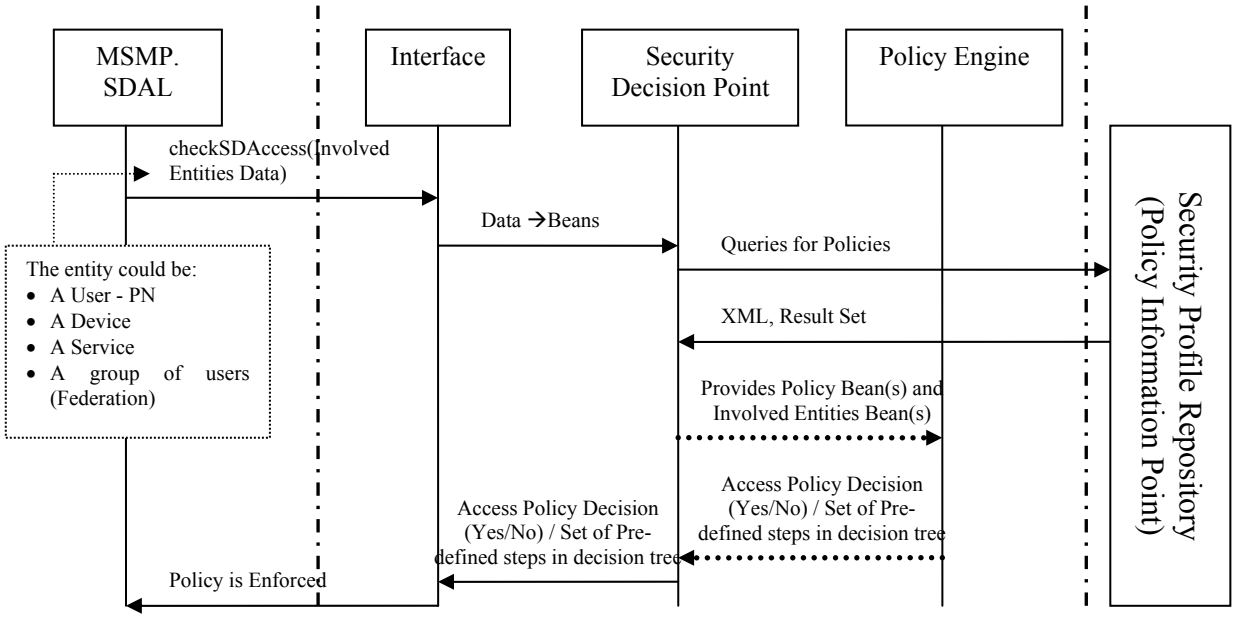
- Πλαίσιο διαχείρισης πολιτικών - Policy Management Framework: επιτρέποντας την διαχείριση πολιτικών σε όλο το PN.
- Πλατφόρμα Ανακάλυψης Υπηρεσιών - MAGNET Service Management Platform, MSMP: για έλεγχο ανακάλυψης και πρόσβασης σε υπηρεσίες [5].
- Διαχειριστή Συνομοσπονδιών - Federation Manager: για διασφάλιση των συναλλαγών σχηματισμού και διαχείρισης συνομοσπονδιών.
- Intra - Secure Context Management Framework (SCMF): για επιβολή ιδιωτικότητας και ανωνυμίας κατά τη χρήση προσωπικής και συγκείμενης πληροφορίας.

- Πιστοποιημένο Πρωτόκολλο Σχηματισμού PAN - Certified PAN Formation Protocol (CPFP): για ανάκληση κλειδιών και πιστοποιητικών [15].
- Με μια εξωτερική μηχανή πολιτικής - Policy Engine, PE: σε περίπτωση που χρησιμοποιείται κάποιο σύνθετο εξωτερικό πλαίσιο πολιτικών, Αυτό είναι χρήσιμο σε περιπτώσεις συνασπισμών και τομέων ασφαλείας με διαφορετικά πλαίσια πολιτικών ασφαλείας, οπότε και μια εξωτερική μηχανή πολιτικών μπορεί να δράσει σαν μεσολαβητής - “policy broker”.

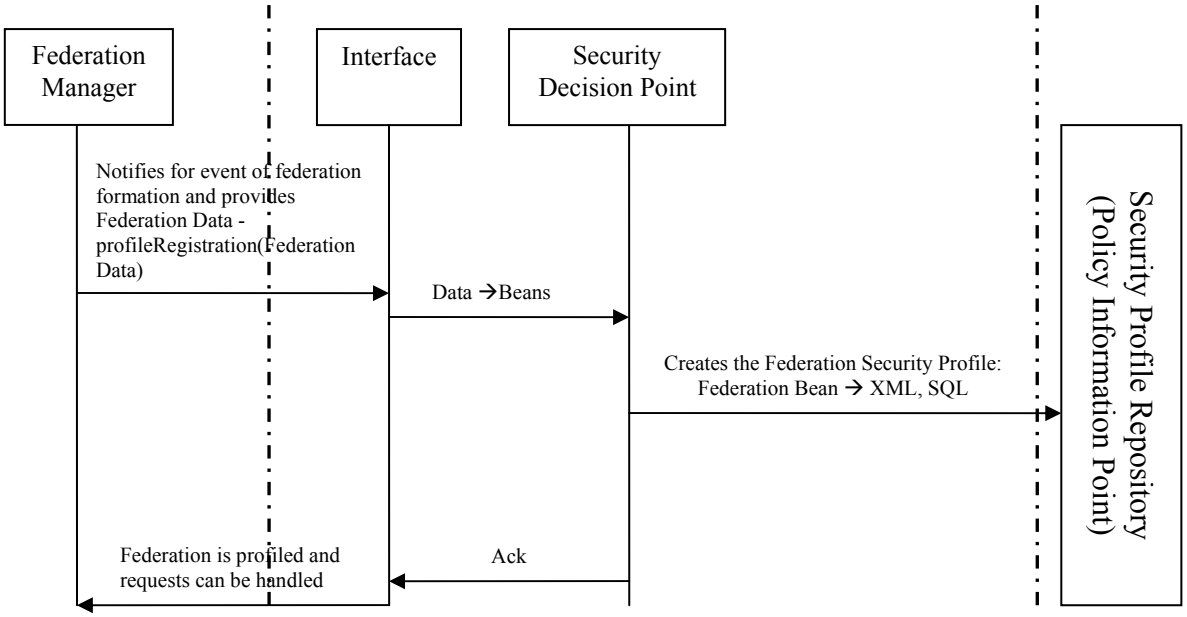
Ακολουθούν τα διαγράμματα ροής των σχετικών αλληλεπιδράσεων μεταξύ του διαχειριστή ασφάλειας και των εξωτερικών ή εσωτερικών στοιχείων. Ο CASM είναι αποδομημένος στα εσωτερικά του στοιχεία, ενώ έχει συμπεριληφθεί και περίπτωση policy broker όπως αναφέρθηκε πριν.



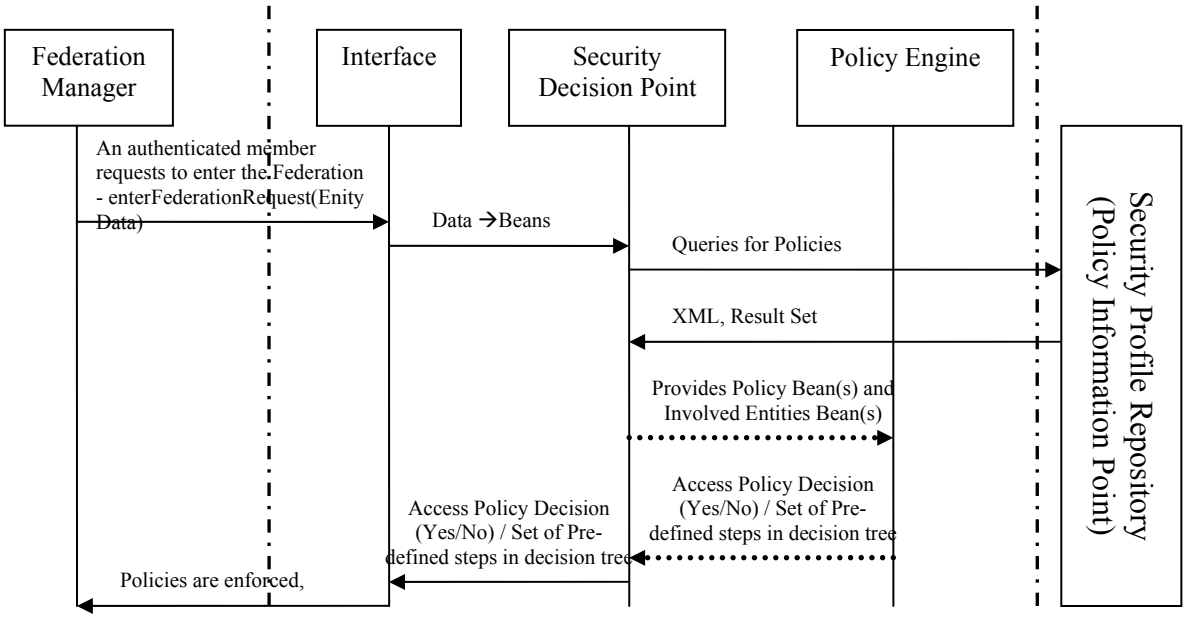
Εικόνα 22 – Διαχείριση Πολιτικών Ασφαλείας



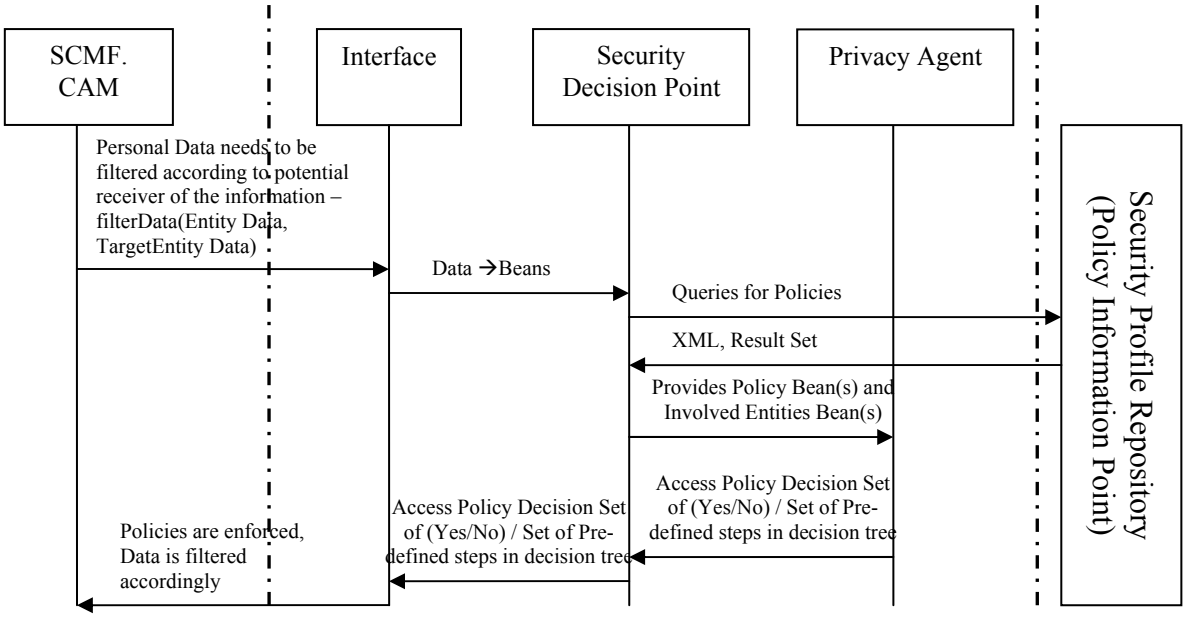
Εικόνα 23 – Έλεγχος πρόσβασης υπηρεσιών (διεπαφή με τη πλατφόρμα διαχείρισης υπηρεσιών PN MSMP [2])



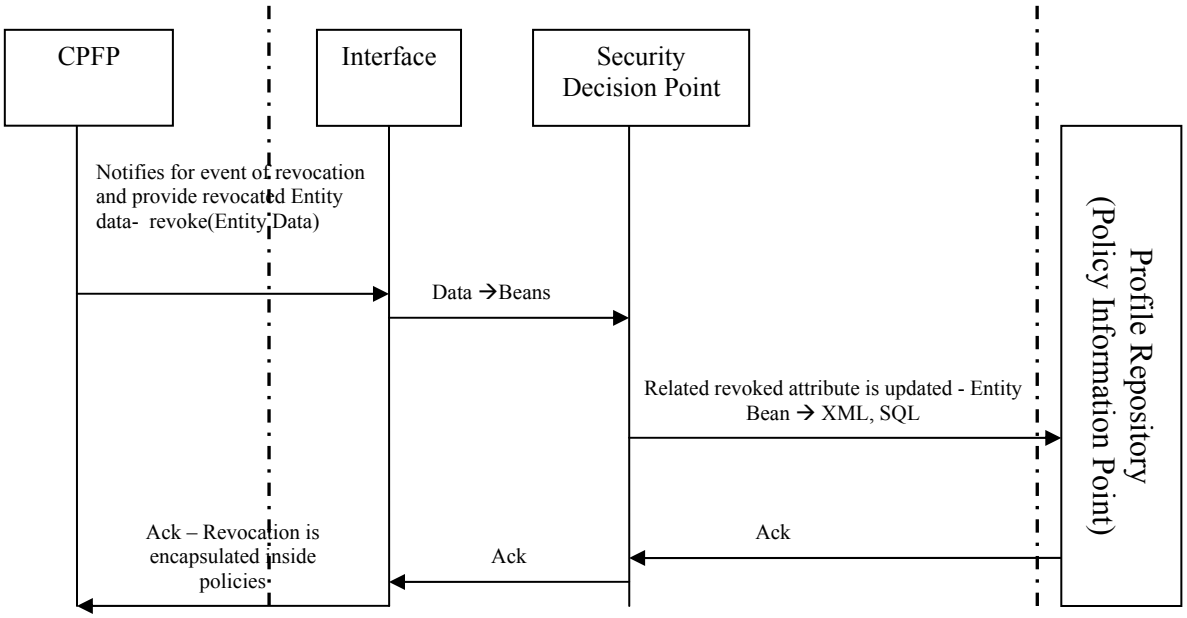
Εικόνα 24 - Σύσταση νέου συνασπισμού PN-F



Εικόνα 25 – Νέο μέλος στο συνασπισμό



Εικόνα 26 – Επιβολή κανόνων ιδιωτικότητας



Εικόνα 27 – Επιβολή ανάκλησης πιστοποιητικών

5.4.5 Πρωτόκολλα και πλατφόρμες υλοποίησης

Ο Διαχειριστής Ασφάλειας είναι ένα εξάρτημα ασφαλείας που βρίσκεται στο στρώμα εφαρμογής αλλά επίσης πρέπει να είναι σε θέση να επικοινωνήσει και με πρωτόκολλα και πρότυπα σε χαμηλότερα στρώματα. Σε αυτό το μέρος περιγράφονται συνοπτικά οι επιλογές που έγιναν για την υλοποίηση του CASM στα πλαίσια της πλατφόρμας Προσωπικού Δικτύου MAGNET [12].

Για την αναπαράσταση και αποθήκευση των δεδομένων se προφίλ ασφαλείας επιλέχθηκε η XML καθώς είναι ένα ανοιχτό και ανεξάρτητο πρότυπο, το οποίο έχει διαδοθεί ευρέως τα τελευταία χρόνια σε όλες τις λύσεις διαχείρισης και ανταλλαγής δεδομένων μεταξύ εφαρμογών. Η δομή της XML προσφέρει ένα αποδοτικό και επεκτάσιμο τρόπο αναπαράστασης των δεδομένων, ενώ αποτελεί τη βάση και για πολλά πρότυπα, όπως το πρότυπο γλώσσας ελέγχου πρόσβασης XACML [13].

Στα επιπλέον οφέλη της χρήσης της XML συγκαταλέγεται η ευκολία μετατροπής τους με χρήση XSL. Η εύκολη μετατροπή τους είναι πλεονέκτημα σε περιπτώσεις που χρειαστούν αλλαγές προκειμένου να στηθούν διεπαφές και να υπάρχει διαλειτουργικότητα και με άλλους εξωτερικούς μηχανισμούς πληροφορίας προφίλ. Η ακεραιότητα και η ιδιωτικότητα των προφίλ εξασφαλίζεται από μηχανισμούς κρυπτογράφησης και ψηφιακής υπογραφή XML αρχείων, χρησιμοποιώντας σχετικές ανοικτές βιβλιοθήκες κρυπτογραφίας για εφαρμογή ψηφιακών υπογραφών και 3DES αλγορίθμου [14].

Η ανάλυση και επεξεργασία των προφίλ ασφαλείας και του διαχειριστή ασφαλείας έγιναν με χρήση της ανοικτής Java πλατφόρμας και των σχετικών ανοικτών βιβλιοθηκών ανάλυσης XML JAXP. Επιπλέον των πλεονεκτημάτων της ανοικτής πλατφόρμας, ο αντικειμενοστρεφής χαρακτήρας της Java την καθιστά ιδανική για την μετατροπή των οντοτήτων του PN σε αντικείμενα Java. Επίσης, και καθώς ο CASM είναι μια δικτυακή εφαρμογή, η υλοποίηση ωφελήθηκε και από την δικτυακές δυνατότητες της πλατφόρμας.

Όσον αφορά τις πολλές διεπαφές του CASM με εσωτερικούς και εξωτερικούς μηχανισμούς, επιλέχθηκε το –βασισμένο σε XML- διαδεδομένο πρωτόκολλο ανταλλαγής XML μηνυμάτων SOAP σε συνδυασμό με JavaBeans τα οποία χρησιμοποιούνται για την μετατροπή των οντοτήτων σε πρότυπα αντικείμενα Java τα οποία αφενός επειδή είναι πρότυπα χρησιμεύουν ιδιαιτέρως στις διεπαφές με άλλα στοιχεία, και αφετέρου οργανώνουν καλύτερα τις σύνθετες και πολύπλοκες δομές που μπορεί να προκύψουν στα πλαίσια ενός Προσωπικού Δικτύου.

5.4. Αξιολόγηση πρότασης σε σύγκριση με υπάρχουσα πλαίσια και λύσεις

Έχουν ήδη γίνει αρκετές προσπάθειες και προσεγγίσεις ώστε να συμπεριληφθεί η συγκείμενη πληροφορία στα παραδοσιακά μοντέλα ελέγχου πρόσβασης, ειδικά για διεισδυτικά περιβάλλοντα (*pervasive environments*) και πανταχού παρόντος υπολογισμού αρχιτεκτονικών (*ubiquitous computing*). Στο [21] δόθηκε ο βασικός ορισμός ενός συστήματος ελέγχου πρόσβασης με επίγνωση κατάστασης. Ωστόσο η εργασία ήταν σε βασικά επίπεδα, υποστήριζε μόνο ενδεικτικά το πεδίο του χρόνου και τη θέση όσον αφορά τον ορισμό της κατάστασης και επίσης στερούταν βασικών στοιχείων στο μοντέλο ελέγχου πρόσβασης όπως ομάδες, ιεραρχία των οντοτήτων και των κανόνων και επίλυση συγκρούσεων. Στο [25] προτάθηκαν γράφοι για την μοντελοποίηση πολιτικών ασφαλείας με επίγνωση κατάστασης. Ουσιαστικά προτείνονται προσαρμοσμένα δένδρα απόφασης που διακλαδίζονται ανάλογα με τη συγκείμενη πληροφορία. Αν και εκφραστικός τρόπος παρουσίασης των πολιτικών, η διαχείριση τους αντιμετωπίζει σοβαρό πρόβλημα πολυπλοκότητας.

Πολλοί ερευνητές ασχολούνται με την προσθήκη επίγνωσης κατάστασης στο RBAC (Role Based Access control) μοντέλο, δηλαδή στον έλεγχο πρόσβασης βασισμένο σε

ρόλους [16]. Ο Zhang πρότεινε ένα δυναμικό έλεγχο πρόσβασης με επίγνωση κατάστασης για διεισδυτικές εφαρμογές [19]. Σε αυτή τη πρόταση περιλαμβάνονται δύο μηχανές κατάστασης: μια μηχανή κατάστασης ρόλων για το χρήστη, και μια μηχανή κατάστασης κανόνων για κάθε ρόλο. Αλλαγές στην κατάσταση εκκινούν μεταβάσεις στις μηχανές. Ο Zhang πέτυχε έτσι λειτουργία που επηρεάζεται από τη συγκείμενη πληροφορία ωστόσο μπορούσε να υποστηρίξει περιορισμένες αλλαγές στο συγκείμενο τις οποίες έπρεπε και να προβλέψει στο προγραμματισμό των μηχανών κατάστασης. Επίσης στη συγκεκριμένη πρόταση ήταν εκτός πεδίου ενδιαφέροντος η δυνατότητα πρακτικής χρήσης στις εφαρμογές, παρουσιάζοντας ουσιαστικά μόνο τις βασικές έννοιες και ιδέες. Την ιδέα προχώρησαν τελικά παραπέρα οι συγγραφείς του [17], έχοντας έναν πράκτορα παρακολούθησης κατάστασης και πίνακες ελέγχου κατάστασης που χαρτογραφούν τις πιθανές καταστάσεις και τιμές συγκείμενης πληροφορίας με τους ρόλους του χρήστη και την ενεργοποίηση/απενεργοποίηση τους. Με αυτό τον τρόπο κάθε φορά που υπήρχε αλλαγή στη κατάσταση, ανάλογα ο πίνακας ενεργοποιεί και απενεργοποιεί συγκεκριμένους ρόλους για το χρήστη. Και πάλι πρόβλημα σε αυτή τη πρόταση αποτελούν οι περιορισμοί των πινάκων ελέγχων κατάστασης σε περιπτώσεις ειδικά υψηλής ανάλυσης της συγκείμενης πληροφορίας. Επίσης, η προσέγγιση του να συνδέεται η συγκείμενη πληροφορία με ρόλους και ανάλογα να επιτυγχάνεται δυναμικός έλεγχος πρόσβασης, απαιτεί δύσκολο διαχειριστικό καθήκον για τους ρόλους χρήστη. Και πάλι η εφαρμογή παραμένει θέμα εκτός ενδιαφέροντος για τους συγγραφείς. Είναι γεγονός ότι ειδικά στο ανθρωποκεντρικό περιβάλλον των Προσωπικών Δικτύων τέτοια μοντέλα είναι προβληματικά λόγω διαχειριστικής δυσκολίας. Πάλι στο μοντέλο RBAC προτάθηκε και η δυναμική αλλαγή κανόνων βάσει χαρακτηριστικών του χρήστη [22], βάζοντας κατά κάποιο τρόπο την προσωπική πληροφορία στο μοντέλο ελέγχου πρόσβασης. Ωστόσο και σύμφωνα με τον ορισμό του ETSI για τη συγκείμενη πληροφορία, η πρόταση αυτή δεν υποστηρίζει κατά τα άλλα επίγνωση κατάστασης.

Πέραν του RBAC μοντέλου, υπάρχει και το εστιασμένο στους κανόνες Provision-Based Access Control (PBAC) [24], που αφορά έλεγχο πρόσβασης με ενέργειες πρόληψης. Δηλαδή πέραν του κλασσικής απάντηση αποδοχής η απόρριψης ο κανόνας μπορεί να περιέχει και την απαίτηση ο χρήστης να προβεί σε προληπτικές ενέργειες προκειμένου να ανταπεξέλθει στον κανόνα πρόσβασης. Οι συγγραφείς εύστοχα ενσωματώνουν τη συγκείμενη πληροφορία στις ομαδικές ιεραρχίες του μοντέλου PBAC, θέτοντας συνθήκες ομάδος σχετικές με τη συγκείμενη πληροφορία. Διαφορετική κατάσταση θα θέσει τους χρήστες σε διαφορετική θέση της ιεραρχίας και επομένως θα αλλάξει την πρόσβαση. Ωστόσο η πρόταση δε διαχωρίζει την συγκείμενη πληροφορία από το μοντέλο πληροφορίας του ελέγχου πρόσβασης και την περιορίζει στις συγκεκριμένες συνθήκες εισόδου στις ομάδες. Έτσι δεν υπάρχει ευλυγισία στη θέσπιση κανόνων πρόσβασης βάσει συγκείμενης πληροφορίας.

Σύμφωνα με τα παραπάνω, το μοντέλο διαχείρισης ασφάλειας που προτείνεται στη διατριβή έχει τα εξής πλεονεκτήματα:

- Ενσωματώνει στις πολιτικές και αποφάσεις ασφαλείας την πληροφορία προφίλ χρήστη και τις προσωπικές προτιμήσεις, όπως αυτές εκφράζονται με την έννοια της σημαίας ιδιωτικότητας (privacy flags), λαμβάνοντας υπόψη τον ανθρωποκεντρικό χαρακτήρα των Προσωπικών Δικτύων
- Διαχωρίζει πλήρως τους τρεις τύπους πληροφορίας: παράμετροι ασφαλείας και κανόνες, προσωπική πληροφορία και συγκείμενη πληροφορία, δίνοντας έτσι ευλυγισία στη θέσπιση κανόνων ασφαλείας βασισμένων στη συγκείμενη πληροφορία

- Αποτελεί το διαχειριστή ασφαλείας μιας ολοκληρωμένης πλατφόρμας διαχείρισης συγκείμενης πληροφορίας δίνοντας του πρόσβαση σε ένα πλούσιο, ανεξάρτητο και πλήρες μοντέλο οντολογιών συγκείμενης πληροφορίας.
- Έχει ενσωματώσει στη σχεδίαση του σχετικές μελέτες απαιτήσεων χρήστη σχετικά με την επιθυμητή λειτουργικότητα και χρηστικότητα στα πλαίσια της εφαρμογής σε πραγματική ubiquitous πλατφόρμα, όπως είναι τα Προσωπικά Δίκτυα

5.5. Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκε μια ολοκληρωμένη πρόταση διαχείρισης ασφάλειας με επίγνωση κατάστασης. Ο μηχανισμός και το σχετικό μοντέλο πληροφορίας αποτελεί μέρος της ευρύτερης Ασφαλούς Αρχιτεκτονικής Προσωπικής και Συγκείμενης Πληροφορίας.

Συγκεκριμένα ο Διαχειριστής Ασφάλειας:

- Λειτουργεί σαν σημείο εφαρμογής πολιτικών ασφαλείας, διασφαλίζοντας την ιδιωτικότητα πληροφοριών προφίλ χρήστη και συγκείμενης πληροφορίας
- Συνδέεται με ομότιμες τέτοιες οντότητες διαχείρισης σε όλο το προσωπικό δίκτυο, παρέχοντας πλήρη κάλυψη σε όλο το δίκτυο
- Βασίζεται σε ανοιχτές τεχνολογίες και πρότυπα καθώς και τεχνολογίες XML, επιτρέποντας δυναμική εφαρμογή νέων πολιτικών και επεκτασιμότητα
- Παρέχει μια ενιαία διεπαφή για όλες τις εφαρμογές και υπηρεσίες που χρησιμοποιούν προσωπικά δεδομένα και συγκείμενες πληροφορίες, και χάριν στο SCMF, δρα και ο ίδιος ως μια εφαρμογή επίγνωσης κατάστασης στα ίδια πλαίσια
- Λαμβάνει υπόψη τον ανθρωποκεντρικό χαρακτήρα των Προσωπικών Δικτύων, ενσωματώνοντας στις πολιτικές και αποφάσεις ασφαλείας την πληροφορία προφίλ χρήστη και τις προσωπικές προτιμήσεις, όπως αυτές εκφράζονται με την έννοια της σημαίας ιδιωτικότητας (privacy flags)
- Έχει επίγνωση κατάστασης ασφαλείας, οι οποίες, χωριζόμενες σε τρία επίπεδα ασφαλείας (Χαμηλό, Μέσο, Υψηλό) οδηγούν και σε δυναμική εφαρμογή διαφορετικού συνόλου πολιτικών ασφαλείας
- Συνεργάζεται με μηχανισμούς φήμης και μοντέλα εμπιστοσύνης, ενσωματώνοντας το επίπεδο εμπιστοσύνης για κάθε εμπλεκόμενη οντότητα σε μια συναλλαγή
- Υποστηρίζει το μηχανισμό ανωνυμίας που προτάθηκε επίσης στη διατριβή, φροντίζοντας ώστε η πληροφορία που δημοσιεύεται να μην οδηγεί σε άμεση ή έμμεση αποκάλυψη της ταυτότητας

Τέλος, η πρόταση του διαχειριστή ασφαλείας αξιολογήθηκε σε σύγκριση με άλλες σχετικές προτάσεις, πλαίσια και λύσεις και βρέθηκε να έχει σημαντικά πλεονεκτήματα, ειδικά στα πλαίσια των Προσωπικών Δικτύων.

5.6. *Ειδική ορολογία κεφαλαίου*

Ελληνικός όρος / φράση	**Αγγλικός όρος / φράση**
Διαλειτουργικότητα	Interoperability
Διαχείριση κινητικότητας	Mobility management
Διαχείριση πολιτικών	Policy management
Διαχείρισης ασφάλειας	Security management
Διεισδυτικά περιβάλλοντα	Pervasive environments
Διεπαφή	Interface
Έλεγχος πρόσβασης	Access control
Ενιαίο υπερ-δίκτυο	Overlay network
Εξουσιοδότηση	Authorisation
Επίγνωση κατάστασης	Context-awareness
Καταγραφή	Accounting
Πανταχού παρόντος υπολογισμού	Ubiquitous computing
Πολιτικές ασφαλείας	Security policies
Πράκτορας Ασφάλειας	Security Agent
Προφιλ χρήστη	User profile
Στρώματα	Layers
Συγκείμενο	Context
Ταυτοποίηση	Authentication
Τερματικό	Client

5.7. *Βιβλιογραφικές αναφορές*

[1] K. Dey, "Providing Architectural Support for Building Context-Aware Applications", PhD thesis, Georgia Inst. Tech., USA, Nov. 2000.

[2] IST-027396 MAGNET/WP2.3/DUT/D2.3.1/PU/001/15.01.2007, "Specification of PN networking and security components", January 2007.

[3] IST-027396 MAGNET/B/WP1.2/DTU/D1.2.1/R/PU/001/02.10.2006, "The conceptual structure of user profiles", September 2006.

[4] Human factors (HF); User profile management, ETSI Guide, EG 202 325 v1.1.1, Oct. 2005, available from Internet: http://webapp.etsi.org/action/PU/20051018/eg_202325v010101p.pdf.

[5] IST-027396 MAGNET/B/WP1/Task1/D1.1.1, "MAGNET System and Pilot Service Design Specifications**",** June 2007.

[6] M. Bauer, R. L. Olsen, M. Jacobsson, L. Sanchez, J. Lanza, M. Imine, N. Prasad, "Context Management Framework for MAGNET Beyond", 15th IST Mobile & Wireless Summit Communications Summit, Myconos, Greece, June 2006.

[7] IST-027396 MAGNET/WP4.1/WMC/D4.1.3, "The extended secure architecture - Final", 2008.

[8] Ross Anderson, *Security Engineering*. Wiley. ISBN 0-471-38922-6.

[9] IST-027396 MAGNET/WP4.2/UNIS/D4.2.1/PU/001/15.12.2006, "First solutions for implementation of Key Management and Crypto techniques", Dec. 2006.

[10] Online SOAP Tutorial available at: http://www.w3schools.com/soap/default.asp

[11] Javabeans Technology Overview, APIs and documentation available at: http://java.sun.com/javase/technologies/desktop/javabeans/index.jsp

[12] Dimitris M. Kyriazanos, Michael Argyropoulos, Luis Sanchez, Jorge Lanza, Mikko Alutoin, Jeroen Hoebeke and Charalampos Z. Patrikakis, "Overview of a Personal Network Prototype", IEC Annual review of telecommunications vol. 59, 2007

[13] OASIS eXtensible Access Control Markup Language (XACML) open standard: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[14] A lightweight cryptography open API for Java and C#. available online at: http://www.bouncycastle.org].

[15] WP4 "Security and Privacy" Group, IST Project MAGNET BEYOND Public Deliverable D4.2.2 "Final PN key management solution and Cryptographic techniques"

[16] David F. Feraiolo, D.Richard Kuhn, Ramaswamy Chandramouli, Role-Based Access Control, Artech House, INC, 2003

[17] Young-Gab Kim, Chang-Joo Mon, Dongwon Jeong, Jeong-Oog Lee, Chee-Yang Song and Doo-Kwon Baik, "Context-Aware Access Control Mechanism for Ubiquitous Applications", Advances in Web Intelligence, Lecture Notes in Computer Science, Volume 3528/2005, 2005

[18] Amir Reza Masoumzadeh, Morteza Amini and Rasool Jalili, "Context-Aware Provisional Access Control", Lecture Notes in Computer Science, Information Systems Security , Volume 4332/2006, 2006

[19] Zhang, G., Parashar, M.: Context-aware dynamic access control for pervasive applications. In: Communication Networks and Distributed Systems Modeling and Simulation Conference, San Diego, USA, 2004

[20] M. J. Covington, W. Long, S. Srinivasan, A. K. Dey, M. Ahamad, G.D. Abowd, Securing Context-aware Applications Using Environment Roles, In proceedings of SACMAT'01, May 2001

[21] Han, W., Zhang, J., Yao, X.: Context-sensitive access control model and implementation. In: Fifth International Conference on Computer and Information Technology (CIT 2005), Shanghai, China, IEEE Computer Society 757–763, 2005

[22] Al-Kahtani, M.A., Sandhu, R.S.: A model for attribute-based user-role assignment. In: 18th Annual Computer Security Applications Conference (ACSAC 2002), Las Vegas, NV, USA, IEEE Computer Society (2002) 353–364

[23] Michael J. Covington, Prahlad Fogla, Zhiyuan Zhan, Mustaque Ahamad, "A Context-Aware Security Architecture for Emerging Applications," *Computer Security Applications Conference, Annual*, pp. 249, 18th Annual Computer Security Applications Conference (ACSAC '02), 2002.

[24] Kudo, M.: Pbac: Provision-based access control model. International Journal of Information Security 1(2) (2002) 116–130

[25] Kouadri Most´efaoui, G., Br´ezillon, P.: Modeling context-based security policies with contextual graphs. In: 2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), Orlando, FL, USA, IEEE Computer Society 28–32, 2004.

6. Μεθοδολογία Ανάλυσης Απειλών για Αξιολόγηση και Σχεδίαση Ενίσχυσης Ασφάλειας Προσωπικών Δικτυων

6.1. Εισαγωγή

Όπως είδαμε στα τελευταία χρόνια η μεγάλη διάδοση των νέων τεχνολογιών και του Διαδικτύου αύξησε περαιτέρω τις ανάγκες για ασφάλεια, καθώς τα δίκτυα επικοινωνιών μεταφέρουν όλο και περισσότερη πληροφορία ενώ ένα μεγάλο μέρος αυτής είναι πολύτιμο ή και εμπιστευτικό. Για αυτό το λόγο απαιτείται προστασία τόσο από τους εαυτούς μας σε περίπτωση αμέλειας όσο και από κακοπροαίρετους που προσελκύονται στα πλαίσια ηλεκτρονικών πταισμάτων αλλά και κακουργημάτων.

Η ασφάλεια λοιπόν είναι οι διαδικασίες και συστήματα με τα οποία τα ψηφιακά περιουσιακά μας στοιχεία προστατεύονται, από εσωτερικές και εξωτερικές απειλές. Επίσης, κάθε δίκτυο για να μπορέσει να λειτουργήσει και να αποδώσει όπως έχει σχεδιαστεί πρέπει να προστατευτεί από απειλές και να προστατεύει αντίστοιχα τα τρωτά του σημεία. Σε αυτά τα πλαίσια είναι ουσιώδης για κάθε σύστημα *η ανάλυση απειλών*, η διαδικασία δηλαδή αναγνώρισης των απειλών, που περιλαμβάνει (α) την κατανόηση του πως πιθανοί «εχθροί» μπορούν να εκμεταλλευτούν αδυναμίες του συστήματος για να επιτύχουν τους σκοπούς τους [1], και (β) την εύρεση και εφαρμογή κατάλληλων αντίμετρων. Η διαδικασία αυτή είναι απαραίτητη επομένως για την προδιαγραφή ολοκληρωμένων και στεγανών απαιτήσεων ασφαλείας κατά τη σχεδίαση ενός συστήματος, έτσι ώστε να συμπεριληφθούν όλοι οι απαραίτητοι μηχανισμοί ασφαλείας που θα προστατεύσουν το σύστημα. Επιπλέον όταν η σωστή αξιολόγηση των απειλών και των ευάλωτων σημείων εφαρμόζεται σε υπάρχον σύστημα, γίνεται δυνατή η (επαν)εκτίμηση της ασφάλειας του συστήματος, η ιεράρχηση των απειλών καθώς και η εξαγωγή ενός βέλτιστου σχεδίου ενίσχυσης της ασφάλειας, δεδομένων συγκεκριμένων πόρων. Ωστόσο η σωστή «μέτρηση» της ασφάλειας αποτελεί πρόκληση για την έρευνα, ελλείψει κάποιας κοινά αποδεκτής πρότυπης διαδικασίας και μέθοδος μέτρησης και εκτίμησης ρίσκου. Επιπλέον στο πολυσύνθετο και ανθρωποκεντρικό περιβάλλον των Προσωπικών Δικτύων η ανάγκη για μια ολιστική προσέγγιση στην αξιολόγηση της ασφάλειας με ενσωμάτωση του ανθρώπινου παράγοντα θέτει επιπλέον απαιτήσεις όπως θα δούμε παρακάτω.

Σε αυτά τα πλαίσια, προτείνεται μια καινοτόμος ολοκληρωμένη μεθοδολογία ανάλυσης απειλών και σχεδίασης ενίσχυσης ασφαλείας η οποία προσφέρει μοναδικά για το χώρο των προσωπικών επικοινωνιών τρόπο:

- αξιολόγηση της ασφάλειας στο σύνολο της (global security evaluation) και όχι μόνο επί μέρους μηχανισμών ή στρωμάτων
- ανάλυση πολύ-βηματικών επιθέσεων (multi-step attacks) και σχέσεων μεταξύ απειλών
- ενσωμάτωση του Ανθρώπινου Παράγοντα στις απειλές (αμέλεια, κοινωνική μηχανική κ.α.)

6.2. Σχετικές με το θέμα υπάρχουσες λύσεις και έρευνα

Η έρευνα στο θέμα της ανάλυσης απειλών χρίζει ωρίμανσης καθώς υπάρχουν λίγες εφαρμόσιμες τεχνικές που να βοηθούν μια τυποποιημένη διαδικασία ανάλυσης απειλών, ενώ οι περισσότερες από αυτές συνδέονται μόνο με την ασφάλεια του λογισμικού. Επιπλέον, οι υπάρχουσες επιλογές δεν ενσωματώνουν τη μοντελοποίηση των απειλών - την διαδικασία δηλαδή της αναγνώρισης και καταγραφής των απειλών του συστήματος – με την μεθοδολογία ανάλυσης. Οι Swiderski και Snyder [2], για παράδειγμα περιγράφουν εκτενώς το μοντέλο απειλών αλλά δεν παρέχουν τη μέθοδο για να οριστεί η αξία του περιουσιακού στοιχείου, δεν εκτελείται ανάλυση ρίσκου και επίσης αφορά μόνο εφαρμογές λογισμικού. Αποκλειστικά για τη φάση εξαγωγής απαιτήσεων εφαρμογών λογισμικού, έχει προταθεί μια στοχο-κεντρική προσέγγιση στη [3]. Η μοντελοποίηση απειλών [4] χρησιμοποιείται επίσης σαν βήμα προς την ολοκλήρωση των απαιτήσεων ασφαλείας, και η διαδικασία επεκτείνεται ώστε να ταιριάζει σε πολύπλοκα, δικτυωμένα συστήματα. Ο χαρακτηρισμός ενός συστήματος επιτυγχάνεται μέσω διαγράμματα ροών δεδομένων (Data Flow Diagrams), μέσω μοντέλο δικτύου [4] ή διαγράμματος αρχιτεκτονικής υψηλού επιπέδου [5] ανάλογα με το σύστημα, εφαρμογή ή δίκτυο. Οι συγγραφείς του [4] ασχολούνται επίσης με τη διαχείριση του ρίσκου και την άμβλυνση των απειλών. Σε αρχιτεκτονικές λογισμικού οι απειλές μοντελοποιούνται επίσης σε περιπτώσεις κακής χρήσης και αμέλειας [6]. Σε αυτή τη περίπτωση, χρησιμοποιήθηκαν τα UML διαγράμματα ακολουθίας για να περιγράψουν την διαδικασία αποφάσεων και ενεργειών που θα οδηγήσουν σε προβληματική κατάσταση ή σε εκμετάλλευση του συστήματος, καθώς επίσης και για να αξιολογηθεί η αρχιτεκτονική και οι περιορισμοί που μπορούν να επιβληθούν για να αμβλυνθούν οι απειλές. Ένα πλαίσιο για μοντέλο απειλών σε Προσωπικά Δίκτυα παρουσιάστηκε στο [1], με μια αρχική γενική μεθοδολογία ενώ δεν συμπεριλαμβάνονται τεχνικές άμβλυνσης απειλών. Μια άλλη πρακτική λύση παρέχεται από τις PTA Technologies [7], και περιλαμβάνει ένα εργαλείο λογισμικού που βοηθάει τους υπευθύνους ανάπτυξης λογισμικού στο να αξιολογούν το ρίσκο στη ασφάλεια του συστήματος και να κατασκευάζουν πολιτικές μείωσης ρίσκου για τα συστήματα τους. Το εργαλείο αυτό είναι ικανό να κάνει πλήρη ανάλυση απειλών, ωστόσο τα τρωτά σημεία δεν βαθμολογούνται/ιεραρχούνται ενώ οι τελικές τιμές για τις απειλές αντιστοιχούν σε χρηματικές απώλειες – ένα αμφιλεγόμενο κριτήριο. Ειδικά στα ανθρωποκεντρικά Προσωπικά Δίκτυα το ηθικό κόστος και η ψυχική οδύνη σε περίπτωση αποτυχίας της ασφάλειας του συστήματος πρέπει οπωσδήποτε να συμπεριληφθούν στην ανάλυση. Τέλος, το Common Vulnerability Scoring System (CVSS – κοινό σύστημα βαθμολόγησης ευάλωτων σημείων) [8] παρέχει ένα πρότυπο σύστημα βαθμολόγησης ευάλωτων σημείων και αξιολόγησης αδυναμιών συστημάτων και πρωτοκόλλων πληροφορικής και επικοινωνιών αλλά δεν παρέχεται αξιολόγηση απειλών ούτε σχετική μεθοδολογία ανάλυσης. Το CVSS έχει χρησιμοποιηθεί στο παρελθόν για να παρέχει αρχικές τιμές σε πολύπλοκους αλγόριθμους [12] που παρέχουν επί μέρους αξιολόγηση της ασφάλειας της λειτουργίας ενός δικτύου.

Η πρόταση που παρουσιάζεται σε αυτό το κεφάλαιο βελτιώνει τις υπάρχουσες τεχνικές ενσωματώνοντας την μοντελοποίηση απειλών με την ανάλυση και διαχείριση, χρησιμοποιώντας μια καινοτόμο ολιστική προσέγγιση ώστε να αναλυθεί το σύστημα στο σύνολο του (χρήστες, εφαρμογές, δίκτυα και τεχνολογίες/πρωτόκολλα), παρέχοντας μια μεθοδολογία έγκυρη για δίκτυα και εφαρμογές, και κατάλληλη για αξιολόγηση ασφαλείας στο σύνολο της (global security evaluation). Επιπλέον, ενσωματώνει τον Ανθρώπινο Παράγοντα, εστιάζοντας στις ενέργειες εσωτερικών και εξωτερικών χρηστών, τεχνικές ή μη, όπως π.χ. σε περιπτώσεις επιθέσεων κοινωνικής μηχανικής.

Η πρόταση προβλέπει τη χρήση των UML διαγραμμάτων περιπτώσεων χρήσης μαζί με UML διαγράμματα ακολουθίας για να προκύψει η συνολική εικόνα του συστήματος και να αναλυθεί το τεχνικό υπόβαθρο που υπάρχει σε κάθε περίπτωση χρήσης. Τα διαγράμματα περίπτωσης χρήσης επιτρέπουν την περιγραφή του τι μπορεί να κάνει το σύστημα, καλύπτοντας όλες τις λειτουργίες που βρίσκονται στα σενάρια από την οπτική γωνία του χρήστη, ενώ τα διαγράμματα ακολουθίας επεκτείνουν αυτή την εικόνα συμπεριλαμβάνοντας όλες τις οντότητες που εμπλέκονται στο σύστημα. Μια αρχική εφαρμογή της προτεινόμενης μεθοδολογίας έγινε στη περίπτωση σχηματισμού συνασπισμού Προσωπικών Δικτύων, κατά την εργασία μου στο ερευνητικό πρόγραμμα MAGNET BEYOND [9], κατά την ευαίσθητη από πλευράς ασφαλείας φάση αρχικοποίησης δηλαδή των σχέσεων μεταξύ Προσωπικών Δικτύων προκειμένου να χρησιμοποιηθούν κοινοί πόροι (υπηρεσίες, περιεχόμενο).

Από την εφαρμογή αυτή έγινε φανερό ότι ήταν δύσκολο να ιεραρχηθούν βάσει κάποιας ποσοτικοποίησης οι απειλές και οι αδυναμίες ενός τόσο σύνθετου και ολοκληρωμένου συστήματος όπως είναι οι συνομοσπονδίες Προσωπικών Δικτύων. Σε αυτό συντελούν η έλλειψη μεθόδου μέτρησης ασφάλειας καθώς και η σύνθετη και ευαίσθητη φύση της ασφάλειας [10]. Προκειμένου να λυθεί το πρόβλημα αυτό, η πρόταση μας ενισχύεται με την ιδέα της συνδυαστικής μεθοδολογίας βαθμολόγησης απειλών και αδυναμιών, συνδυάζοντας τα δέντρα επίθεσης με το πρότυπο σύστημα βαθμολόγησης CVSS.

Σε αυτή τη πρόταση μελετήθηκε και η κριτική που δέχονται τα δέντρα επίθεσης για (i) την αδυναμία να μοντελοποιήσουνε κύκλο και (ii) την πολυπλοκότητα και δυσκολία διαχείρισης για πολύπλοκα συστήματα και σενάρια επίθεσης. Όσον αφορά το πρώτο μειονέκτημα, αντισταθμίζεται ουσιαστικά από το σχεδιαστικό πλεονέκτημα της δενδρικής δομής, που επιτρέπει μια σαφή αναπαράσταση της αλληλεξάρτησης κάθε κατάστασης/βήματος μέσα στο δέντρο – ένα σύνηθες μειονέκτημα σε άλλες μη δενδρικές αναπαραστάσεις. Άλλωστε τα δέντρα επίθεσης έχουν χρησιμοποιηθεί με επιτυχία στην αναγνώριση και αναπαράσταση απειλών στη βιβλιογραφία [11][12]. Γενικότερα, και προκειμένου να αποφθεχθούν τα προβλήματα μοντελοποίησης και δύσκολης ανάγνωσης πολύπλοκων δένδρων επίθεσης που αναφέρθηκαν, στο τελικό μοντέλο οι απειλές δεν καταγράφονται και αναλύονται ως αλληλουχία διαδικασιών αλλά βάσει της τελικής κατάστασης, του στόχου δηλαδή της «επίθεσης». Επίσης για την απλούστευση πολύπλοκων δέντρων τεχνικές απλοποίησης και κλαδέματος μπορούν να εφαρμοστούν όπως στην [11].

Σε αυτά τα πλαίσια, η πρόταση εφαρμόζει μια προσέγγιση γύρω από το χρήστη και τις περιπτώσεις χρήσης, εστιάζοντας στις ενέργειες του χρήστη (νόμιμες ή κακοπροαίρετες) παρά στα δίκτυα και στα επί μέρους κομμάτια του συστήματος. Επιπλέον, τα δέντρα χρησιμοποιούνται για να δείχνουν την συνέπεια της κάθε ενέργειας του χρήστη (εξάρτηση μιας κατάστασης με άλλη), ενώ ένα επίπεδο επικινδυνότητας συνδέεται με κάθε κατάσταση, χρησιμοποιώντας το CVSS για την ποσοτική αξιολόγηση όλων των κόμβων του δένδρου. Επιπλέον, η προτεινόμενη χρήση του CVSS κρατά το δέντρο ενημερωμένο και ρεαλιστικό όσον αφορά την προσπάθεια και την τεχνογνωσία που απαιτεί η κάθε επίθεση, σε σχέση με προτάσεις που βασίζονται στη γεωμετρία του δέντρου επίθεσης [11]. Ο απώτερος στόχος της πρότασης είναι να οδηγήσει σε ένα αρχής KISS (Keep it Short and Simple – κράτα το σύντομο και απλό) αυτόνομο βοηθητικό εργαλείο διαχείρισης ασφάλειας, χρήσιμο τόσο για έναν έμπειρο διαχειριστή συστήματος, έναν αναλυτή ασφαλείας καθώς και τον απλό χρήστη ενός Προσωπικού Δικτύου.

Στη συνέχεια ακολουθεί η πλήρης περιγραφή της προτεινόμενης μεθοδολογίας ανάλυσης απειλών.

6.3. Προτεινόμενη μεθοδολογία ανάλυσης απειλών

Η ανάλυση απειλών είναι η διαδικασία αναγνώρισης, καταγραφής και άμβλυνσης των απειλών ασφαλείας ενός συστήματος, και μπορεί να διαχωριστεί σε τρεις κύριες φάσεις: μοντελοποίηση απειλών (*threats modeling*), χαρτογράφηση περιουσιακών στοιχείων (*assets mapping*) και φάση κατασκευής σχεδίου άμβλυνσης απειλών (*building a mitigation plan*). Η προτεινόμενη μεθοδολογία ουσιαστικά παρέχει τυποποιημένες διαδικασίες για κάθε φάση της ανάλυσης μαζί με μια νέα προσέγγιση στην αποδόμηση και ανάλυση του συστήματος.

Κατά τη μοντελοποίηση απειλών αξιολογείται και καταγράφεται τεκμηριωμένα κάθε πιθανός κίνδυνος ασφαλείας που συνδέεται με ένα στοιχείο του συστήματος. Σε αυτή τη φάση απαιτείται κατανόηση των στόχων μιας πιθανής επίθεσης στο σύστημα, λαμβάνοντας υπόψη και ποια είναι τα περιουσιακά στοιχεία που στοχεύονται. Με αυτό τον τρόπο απαριθμούνται οι απειλές και επίσης ανακαλύπτονται τα τρωτά σημεία και οι αδυναμίες του συστήματος. Η μοντελοποίηση απειλών είναι ιδιαιτέρως χρήσιμη στη πρώιμη φάση σχεδίασης και ανάπτυξης ενός συστήματος, θέτοντας τις καλές βάσεις για ένα εξαρχής ασφαλέστερο σύστημα. Καθώς οι εφαρμογές θα αναπτύσσονται και οι απαιτήσεις θα ορίζονται σε πιο μεγάλο βαθμό, η λίστα των απειλών και αδυναμιών θα ανανεώνεται ανάλογα και εφόσον είναι απαραίτητο.

Εικόνα 28 - Βήματα Ανάλυσης Απειλών

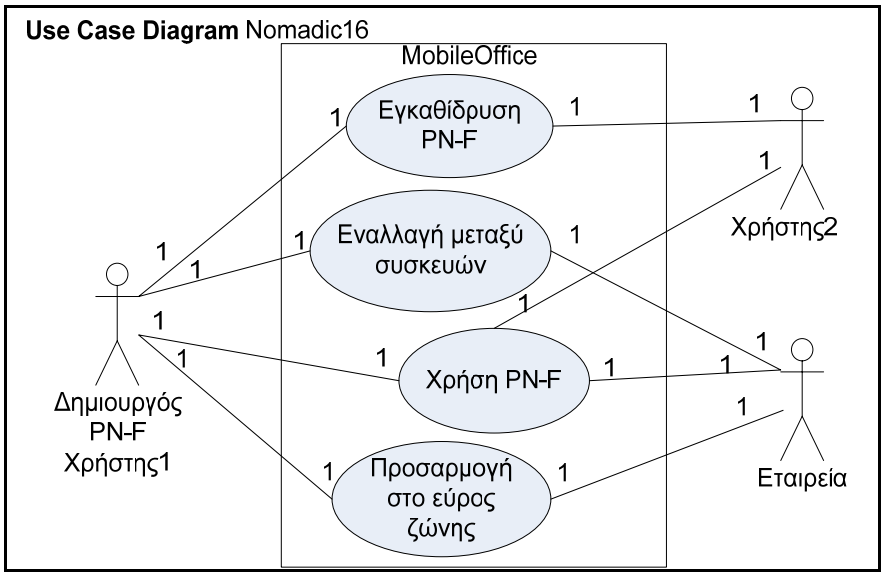
Η χαρτογράφηση απειλών περιλαμβάνει την καταγραφή όλων των απτών αλλά και άυλων περιουσιακών στοιχείων του συστήματος και την αναγνώριση των σχετικών σημείων εισόδου του συστήματος. Η αξία των στοιχείων αυτών είναι και η βάση για τον υπολογισμό του κινδύνου που συνδέεται με τη κάθε απειλή, καθώς και για την ιεράρχηση των αντίμετρων βάσει της προτεραιότητας που δίδεται στα στοιχεία. Συχνά είναι πιο πρακτικό

για τον αναλυτή να αναγνωρίζει τα στοιχεία του συστήματος μέσω της διαδικασίας ανάλυσης συγκεκριμένων απειλών, Για αυτό το λόγο μεταξύ των διαδικασιών χαρτογράφησης απειλών και απαρίθμησης απειλών είναι δυνατόν να υπάρχουν αναθεωρήσεις και να ισχύει μια επαναληπτική προσέγγιση (iterative approach).

Η τρίτη φάση της ανάλυσης απειλών είναι η κατασκευή του σχεδίου άμβλυνσης, δηλαδή η συνδυαστική επιλογή των πιο πιθανόν αντίμετρων από τη σχετική λίστα αντίμετρων για όλες τις απειλές και αδύναμα σημεία που έχουν καταγραφεί. Οι αναλυτές καλούνται να αποφασίσουν ποια από τα προτεινόμενα αντίμετρα θα συμπεριληφθούν στο τελικό σχέδιο άμβλυνσης ανάλογα με την εμπειρία τους. Προκειμένου να βοηθηθεί ο υπολογισμός της συνεισφοράς κάθε αντίμετρου στην άμβλυνση κινδύνων, ο αναλυτής καλείται να εκτιμήσει (α) το επίπεδο άμβλυνσης που κάθε αντίμετρο παρέχει αν ήταν το μόνο αντίμετρο που θα εφαρμοστεί και (β) το συνολικό επίπεδο άμβλυνσης που μπορεί να επιτευχθεί για έναν κίνδυνο από όλα τα αντίμετρα στο σχέδιο [7]. Το αποτέλεσμα αυτής της ανάλυσης είναι ένα σύνολο από αντίμετρα τα οποία αμβλύνουν στο βέλτιστο βαθμό τις απειλές που αναγνωρίστηκαν. Στην Εικόνα 28 παρουσιάζεται βήμα-βήμα η γενική μεθοδολογία που χρησιμοποιείται από τη πρόταση και προσαρμόστηκε ώστε να εξυπηρετεί της ανάγκες της αξιολόγησης ασφαλείας Προσωπικών Δικτύων – και όχι μόνο – στο σύνολο της. Ακολουθούν οι προτεινόμενες για τα Προσωπικά Δίκτυα μέθοδοι για κάθε βήμα της ανάλυσης.

Βήμα 1. Περιγραφή του Συστήματος: επισκόπηση δικτύου και περιπτώσεις χρήσης

Για την περιγραφή του συστήματος είναι απαραίτητο να κατανοηθούν κάθε στοιχείο αυτού και οι διασυνδέσεις μεταξύ τους, καθώς και να οριστούν τα σχετικά σενάρια και οι περιπτώσεις χρήσης (use cases).



Εικόνα 29 - UML διάγραμμα περίπτωσης χρήσης

Πίνακας 4 - Περιγραφικός πίνακας UML διαγράμματος περίπτωσης χρήσης

Όνομα Περίπτωσης	**Εγκαθίδρυση PN-F**
Γενικοί στόχοι	Συνεργασία, Ανακάλυψη υπηρεσίας

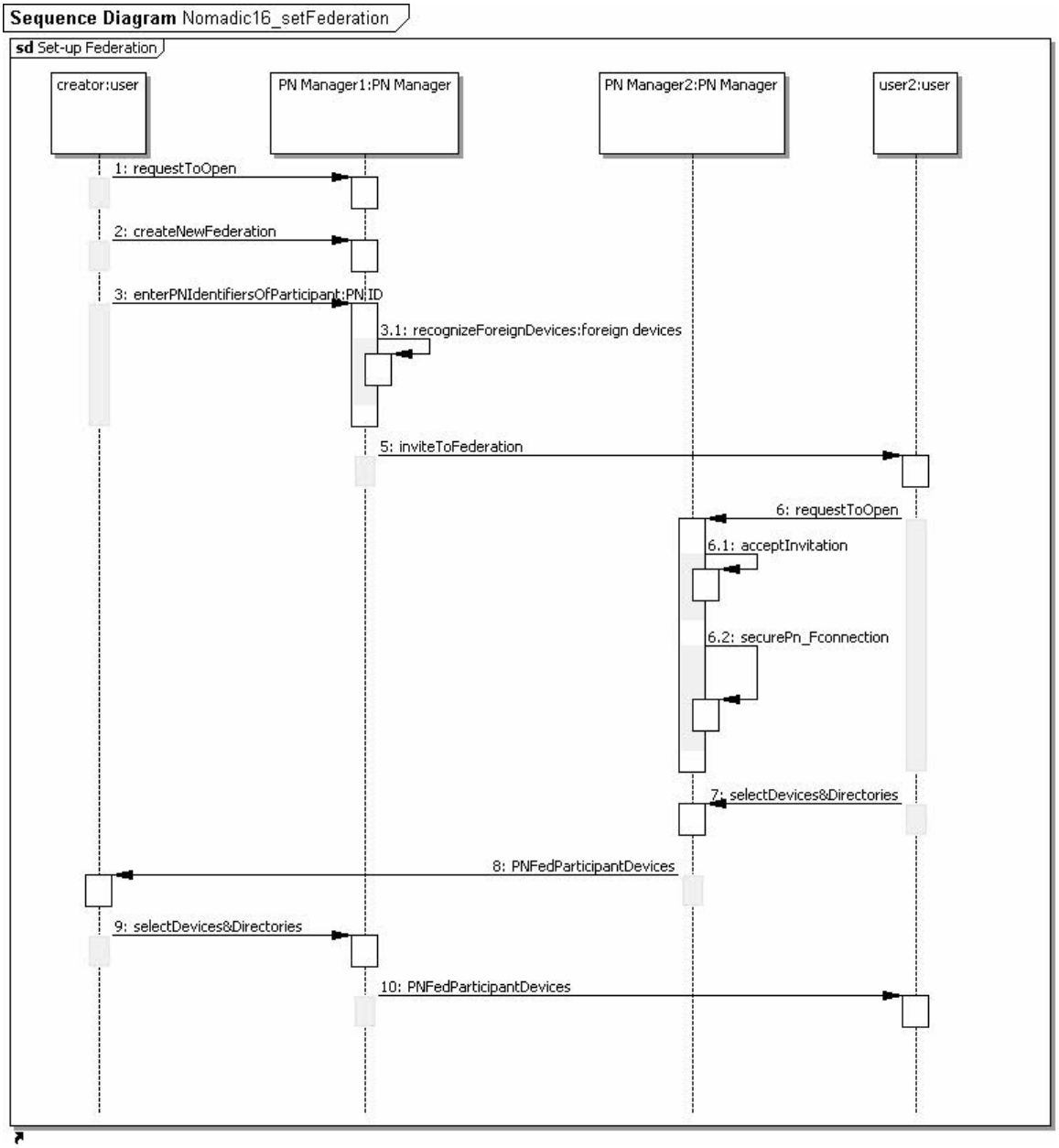
Προϋποθέσεις	Οι συμμετέχοντες έχουν φορητές συσκευές που έχουν MAGNET Air Interface/ WiFi/ UMTS δυνατότητες καθώς και γενικές εφαρμογές γραφείου. Οι συσκευές είναι συνδεδεμένες μεταξύ τους.
Συνθήκη επιτυχούς ολοκλήρωσης.	Ενα PN-F δημιουργήθηκε.
Συνθήκη Αποτυχίας	Δεν υπάρχει συνασπισμός.
Κύριοι συμμετέχοντες	Δύο συνάδελφοι (δημιουργός PN-F, χρήστης)
Δευτερεύοντες συμμετέχοντες	
Συνθήκη Έναρξης	Ο δημιουργός καλεί για συνασπισμό.
Κύρια Ροή	
1	Ο Χρήστης1 (δημιουργός) καλεί δημιουργία συνασπισμού επιλέγωντας το σχετική εντολή στη γραφική διεπιφάνεια του.
2	Η διεπιφάνεια ζητά για τα αναγνωριστικά των Προσωπικών Δικτύων που επιτρέπεται να συμμετάσχουν στον συνασπισμό.
3	Ο Χρήστης1 δίνει τα αναγνωριστικά των PNs για αυτόν και τον συνάδελφο του.
4	Ο Χρήστης1 ανοίγει τον διαχειριστή του PN του, ο οποίος προς το παρόν αναγνωρίζει σαν ξένη συσκευή την συσκευή του συναδέλφου του.
5	Χρησιμοποιώντας τον διαχειριστή PN ο δημιουργός διαλέγει τη συσκευή του Χρήστη2 και στέλνει πρόσκληση σε αυτήν για συμμετοχή στο συνασπισμό PN-F μέσω της εντολής του διαχειριστή PN: Πρόσκληση σε PN-F.
6	Ο Χρήστης2 ανοίγει τον διαχειριστή PN του και αποδέχεται την ληφθείσα πρόσκληση
7	Όταν ο διαχειριστής PN του Χρήστη2 δείξει ότι υπάρχει ασφαλής σύνδεση συνασπισμού PN-F μεταξύ των δυο Προσωπικών Δικτύων, ο Χρήστης2 ανοιγεί τον διαχειριστή

	καταλόγου και διαλέγει τις συσκευές και τους καταλόγους των συσκευών που θα διατεθούν για τον συνασπισμό. Οι συσκευές αυτές μπορεί να είναι το laptop και το PDA.
8	Ο Χρήστης2 στέλνει την πληροφορία στον δημιουργό με την εντολή του διαχειριστή: Συσκευές συμμετοχής PN-F.
9	Ο δημιουργός αντίστοιχα επιλέγει το PDA και το laptop και στέλνει την πληροφορία στον Χρήστη2 με την εντολή του διαχειριστή: Συσκευές συμμετοχής PN-F.
Επεκτάσεις	
7.1	Μη ασφαλής σύνδεση για τον συνασπισμό PN-F.
7.2	Κανένας συνασπισμός.

Για την πλήρη και αποδοτική περιγραφή των χαρακτηριστικών του συστήματος προτείνονται τα UML διαγράμματα περιπτώσεων χρήσης και οι σχετικοί περιγραφικοί πίνακες, καθώς επιτρέπουν τι περιγραφεί του τι μπορεί να κάνει το σύστημα, μέσω της αλληλεπίδρασης μεταξύ περιπτώσεων χρήσης και των συμμετεχόντων χρηστών και οντοτήτων. Η περιγραφή και ανάλυση της περίπτωσης χρήσης γίνεται σε έναν πίνακα που περιέχει όλη τη σχετική για το σύστημα πληροφορία, δηλαδή τους στόχους χρήσης, τις συσκευές και εμπλεκόμενες τεχνολογίες, την περιγραφή της κάθε εμπλεκόμενης οντότητας καθώς και τα στάδια που απαιτούνται για την ολοκλήρωση της περίπτωσης χρήσης. Στην Εικόνα 29 παρατίθεται παράδειγμα UML διαγράμματος περίπτωσης χρήσης για το σενάριο "Nomadic@work" όπως αυτό σχεδιάστηκε για την πλατφόρμα Προσωπικού Δικτύου MAGNET [9]. Στον Πίνακας 4 παρέχεται ο σχετικός περιγραφικός πίνακας για την περίπτωση χρήσης «Εγκαθίδρυση PN-F».

Βήμα 2. Ανάλυση του τεχνικού υπόβαθρου των περιπτώσεων χρήσης

Για να αναλυθεί η χρονική αλληλουχία εμπλοκής των συσκευών και των οντοτήτων σε κάθε περίπτωση χρήσης υιοθετείται η χρήση των UML διαγραμμάτων ακολουθίας όπως προτείνεται στη [1]. Το διάγραμμα ροής δείχνει τις αλληλεπιδράσεις μεταξύ των διαφόρων αντικειμένων οργανωμένες σε χρονική ακολουθία, όπως π.χ. στην Εικόνα 30 για την περίπτωση της εγκαθίδρυσης του συνασπισμού Προσωπικών Δικτύων. Η όψη της ακολουθίας περιγράφει τη συμπεριφορά του συστήματος κατά την εκτέλεση, και μπορεί να χρησιμοποιηθεί για να μοντελοποιήσει την συμπεριφορά του συστήματος αναπαριστώντας την υλοποίηση ενός σεναρίου περίπτωσης χρήσης. Εικονογραφούνται με αυτό τον τρόπο τα αντικείμενα που εμπλέκονται στο σενάριο και η σειρά ανταλλαγής μηνυμάτων μεταξύ των αντικειμένων. Με αυτό τον τρόπο γίνεται σαφές ποιες τεχνολογίες χρησιμοποιούνται σε κάθε συγκεκριμένο βήμα της περίπτωσης χρήσης και ποιος τις χρησιμοποιεί.



Εικόνα 30 - UML Διάγραμμα Ακολουθίας για την Εγκαθίδρυση PN-F

Βήμα 3. Αναγνώριση Περιουσιακών Στοιχείων - Υπαρχόντων

Σε αυτό το βήμα οτιδήποτε μπορεί να υποστεί φθορά ή να παραβιαστεί μέσα στο δίκτυο πρέπει να καθοριστεί. Τα περιουσιακά στοιχεία μπορεί να είναι απτά ή νοητικά, γενικά ή σχετικά με μια περίπτωση χρήσης. Τα στοιχεία αυτά και η προστασία τους είναι πολύ σημαντικά θέματα, καθώς είναι σύνηθες λάθος σε οργανισμούς να εστιάζονται στις απειλές και όχι στην προστασία των δικών τους υπαρχόντων, αφήνοντας έτσι τρωτά σημεία και αδυναμίες στο σύστημα [13].

Γενικά, τα υπάρχοντα σχετίζονται με συγκεκριμένες καταστάσεις και χρήστες, αλλά είναι επίσης δυνατόν να αναγνωριστούν και γενικά υπάρχοντα για ένα σύστημα όπως π.χ. το ID του ιδιοκτήτη των συσκευών. Με τη νέα προσέγγιση χρήσης διαγραμμάτων περιπτώσεων χρήσης και περιγραφικών πινάκων επιτρέπεται η αναγνώριση των γενικών και ειδικών περιουσιακών στοιχείων για κάθε περίπτωση χρήσης κατά την ανάλυση της. Σε αυτή τη φάση όλα τα υπάρχοντα απαριθμούνται και αποθηκεύονται σε έναν πίνακα ως εγγραφή με

συγκεκριμένο ID (μοναδικό αύξων αριθμό δηλαδή), όνομα και σύντομη περιγραφή, Στα επόμενα βήματα οι αναλυτές μπορούν να ανατρέξουν σε αυτό το πίνακα ξανά αν χρειαστεί και να τον ενημερώσουν σε περίπτωση που βρεθούν και άλλα υπάρχοντα κατά την ανάλυση. Στα πλαίσια της εφαρμογής της μεθοδολογίας σε πραγματική πλατφόρμα Προσωπικού Δικτύου στο ερευνητικό πρόγραμμα MAGNET BEYOND 108[23] παρατίθεται ένα δείγμα ενός τέτοιου πίνακα στον Πίνακας 5.

Πίνακας 5 - Δείγμα Περιουσιακών Στοιχείων Προσωπικού Δικτύου

ID	**Όνομα**	**Περιγραφή**
MM.1	Προσωπικά Δεδομένα	Προσωπικά Δεδομένα αποθηκευμένα σε συσκευές του PN-F που ο χρήστης χρησιμοποιεί
MM.2	Δεδομένα login χρήστη	Πιστοποιητικά στοιχεία χρήστη: κωδικοί και εικονικές ταυτότητες (Virtual Identities - VIDs)

Βήμα 4. Καθορίζοντας τις Απειλές

Χρησιμοποιώντας την πληροφορία που συλλέχθηκε μέχρι τώρα είναι δυνατόν να ξεκινήσει η αναγνώριση των απειλών και των πιθανών πηγών απειλών του συστήματος. Πηγή απειλών ορίζεται ως κάθε συγκυρία ή γεγονός με τη δυνατότητα να βλάψει ένα σύστημα. Σύμφωνα με την [14] οι πηγές απειλών ταξινομούνται σαν: φυσικές, ανθρώπινες και περιβαλλοντικές.

Αναλύοντας τις περιπτώσεις χρήσης, τις τεχνικές λειτουργίες και τα διαγράμματα ακολουθιών, είναι δυνατόν να αναγνωριστούν οι απειλές και οι πηγές απειλών. Στη συνέχεια οι απειλές θα πρέπει να συσχετιστούν με συγκεκριμένα υπάρχοντα και σημεία εισόδου. Το αποτέλεσμα αυτού του βήματος είναι ένα προφίλ απειλών σύμφωνα με αυτό που προτείνουν οι Swiderski και Snyder στη [2]. Στον πίνακα κάθε απειλή συσχετίζεται με ένα ID, ένα όνομα ή ταξινόμηση, τη πηγή της απειλής, τα υπάρχοντα που εμπλέκονται και τα σημεία εισόδου. Στα πλαίσια της εφαρμογής της μεθοδολογίας σε πραγματική πλατφόρμα Προσωπικού Δικτύου στο ερευνητικό πρόγραμμα MAGNET BEYOND 108[23] παρατίθεται ένα δείγμα ενός τέτοιου πίνακα στον Πίνακας 6 - Δείγμα Πίνακα Απειλών. Τέλος, οι απειλές αναλύονται για το κατά πόσον το σύστημα είναι ευάλωτο σε αυτές.

Πίνακας 6 - Δείγμα Πίνακα Απειλών Προσωπικού Δικτύου

ID	Περιγραφή	Όνομα (Ταξινόμηση)	Πηγή	Υπάρχοντα	Σημεία Εισόδου
T.N.1	Κατά την εισαγωγή ξένων συσκευών σε ένα συνασπισμό, αν δεν υπάρχει οπτική επαφή, κάποιος κακόβουλος μπορεί να προσποιηθεί ότι είναι συνάδελφος	Spoofing για πρόσβαση σε ιδιωτική πληροφορία	άνθρωπος	G1 IDs G3 access services	PN-F Manager (PDA ή laptop)
T.N.2	Πρόσληψη πρόσκλησης σε συνασπισμό από κάποιον που δεν είναι ο δημιουργός	Eavesdropping σε μέλη συνασπισμού	άνθρωπος	G2 profiles G6 reputation	PN-F Manager (PDA ή laptop

Βήμα 5. Καθορισμός Ευάλωτων Σημείων

Ο στόχος αυτού του βήματος είναι να αναπτυχθεί μια λίστα από ευάλωτα σημεία του συστήματος τα οποία θα μπορούσαν να εκμεταλλευθούν οι πηγές απειλών. Όταν όλες οι απειλές και τα σχετικά σενάρια έχουν περιγραφεί είναι δυνατόν να εξάγουμε τι εκμεταλλεύονται οι απειλές στο σύστημα μας. Σε αυτή τη διαδικασία συμπληρώνεται ένας πίνακας με τα κύρια πραγματικά ευάλωτα σημεία και τις αντίστοιχες απειλές που τα εκμεταλλεύονται σε περιπτώσεις χρήσης που αναλύθηκαν προηγουμένως. Κάθε ευάλωτο σημείο αποτελείται από ένα ID, περιγραφή, όνομα και αντίστοιχη απειλή, όπως π.χ. στον Πίνακας 7. Τα δένδρα επίθεσης που προτείνονται στη συνέχεια, επίσης μπορούν να χρησιμοποιηθούν για να δούμε αν το σύστημα καταρχήν είναι ευάλωτο στις αναγνωρισμένες απειλές.

Πίνακας 7 - Δείγμα Πίνακα Ευάλωτων Σημείων

ID	Περιγραφή	Όνομα	Αντίστοιχες Απειλές
V1	Ο χρήστης αφήνει τη συσκευή χωρίς να κάνει logout και ένας κακόβουλος την κλέβει.	Κακόβουλος αποκτά πρόσβαση στο PN	TN1 TN2 TN5
V2	Ο χρήστης δίνει προσωπικά στοιχεία χωρίς να ελέγξει ότι ο παραλήπτης είναι έμπιστος (trusted)	Ευπιστος χρήστης	TN4 TD1

Βήμα 6. Χαρτογράφηση Περιουσιακών Στοιχείων

Σε αυτό το βήμα η λίστα των υπαρχόντων που κατασκευάστηκε στο βήμα 3 ελέγχεται για την πληρότητα της. Είναι πολύ σημαντικό να καθοριστεί η αξία των υπαρχόντων αυτών καθώς και το ρίσκο που ο ιδιοκτήτης είναι διατεθειμένος να δεχτεί [1], και βάσει αυτών να τα ιεραρχήσουμε. Αυτό είναι ένα δύσκολο μέρος καθώς η αξία ενός στοιχείου είναι κάτι υποκειμενικό, προσωπικό και οι προτεραιότητες του καθενός είναι διαφορετικές. Ωστόσο

στη μεθοδολογία προτείνονται τρεις διαφορετικές τιμές-επίπεδα, σύμφωνα με τις οποίες μπορούν εύκολα και γρήγορα να καταταγούν τα περιουσιακά στοιχεία:

- *Υψηλή*, για υπάρχοντα που πρέπει να προστατευτούν σε υψηλά επίπεδα ασφαλείας και που: συνδέονται άμεσα με τον έλεγχο του συστήματος, με υπηρεσίες εξαιρετικά κρίσιμες για τη λειτουργία του συστήματος, συνδέονται με εξαιρετικά απόρρητες πληροφορίες ή έχουν μεγάλη χρηματική αξία.
- *Μέση*, για υπάρχοντα που συνδέονται με κοινές υπηρεσίας, όχι κρίσιμες αλλά σημαντικές και με μια πιθανόν μέση χρηματική αξία.
- *Χαμηλή,* για υπάρχοντα ελάσσονος σημασίας.

Οι τιμές ανατίθενται λαμβάνοντας υπόψη τα σενάρια, τις συγκεκριμένες περιπτώσεις χρήσης αλλά και τις προσωπικές προτιμήσεις του χρήστη. Στον Πίνακας 8 φαίνεται ένα μέρος σχετικού πίνακα χαρτογράφησης για Προσωπικά Δίκτυα.

Πίνακας 8 - Δείγμα Πίνακα Χαρτογράφησης Περιουσιακών Στοιχείων Προσωπικού Δικτύου

ID	**Όνομα**	**Περιγραφή**	**Τιμή**
A1	Δεδομένα login Χρήστη	Πιστοποιητικά στοιχεία χρήστη: κωδικοί και ηλεκτρονικές ταυτότητες.	Υψηλή
A2	Τραπεζικές Πληροφορίες	Πληροφορίες για τραπεζικούς λογαριασμούς και πιστωτικές κάρτες.	Υψηλή
A10	Πληροφορίες εργασίας αποθηκευμένα σε PN-F	Εργασιακή πληροφορία κοινοποιημένη σε PN-F	Μέση
A11	Πληροφορίες Επαφής	Τηλέφωνα, e-mail, διεύθυνση	Μέση
A20	Θέση	Θέση Χρήστη	Χαμηλή
A22	Προορισμός	Προορισμός Ταξιδιού	Χαμηλή

Βήμα 7. Διαχείριση Κινδύνου - Ρίσκου

Η διαχείριση κινδύνου και ρίσκου βοηθά στο να ισορροπούμε μεταξύ του τι είναι δυνατόν και τι είναι αποδεκτό.

Από τη λίστα απειλών και ευάλωτων σημείων είναι δυνατόν να εξαχθούν οι πληροφορίες για το ποιες απειλές έχουν το μεγαλύτερο δείκτη κινδύνου. Για να αξιολογηθεί ο κίνδυνος θα πρέπει να ληφθούν υπόψη το αντίκτυπο και η ζημιά στα υπάρχοντα και το σύστημα όταν η απειλή υλοποιηθεί, το μέγεθος των ευάλωτων σημείων και τη πιθανότητα υλοποίησης της απειλής. Στο 6.3 που ακολουθεί, η προτεινόμενη μέθοδος, βασισμένη σε βιομηχανικό πρότυπο, οδηγεί στη βαθμολόγηση και κατάταξη απειλών και ευάλωτων σημείων. Βάσει αυτής της αξιολόγησης, οι σχετικοί κίνδυνοι μπορεί να θεωρηθούν αποδεκτοί, να μεταφερθούν ή να αμβλυνθούν όπως προτείνεται στη [4].

Βήμα 8. Σχέδιο Άμβλυνσης

Το τελευταίο βήμα της ανάλυσης είναι η κατάστρωση ενός σχεδίου άμβλυνσης που περιλαμβάνει την επιλογή αντίμετρων. Σε αυτό το βήμα οι απειλές που επιλέγονται για άμβλυνση πρέπει να αντιμετωπιστούν από ένα ή περισσότερα αντίμετρα. Για τη σχεδίαση της άμβλυνσης είναι απαραίτητο να υπάρχει μια λίστα από αντίμετρα και η σχέση τους με ευάλωτα σημεία. Στη συνέχεια επιλέγεται ο πιο αποδοτικός συνδυασμός από αυτή τη λίστα.

Η σχετική απόφαση για το ποια προτεινόμενα αντίμετρα θα συμπεριληφθούν στο τελικό σχέδιο άμβλυνσης λαμβάνεται από τον αναλυτή.

Το αποτέλεσμα της διαδικασίας είναι ένα σύνολο από προτεινόμενα αντίμετρα που θα αμβλύνουν τις απειλές που αναγνωρίστηκαν. Καθώς η υλοποίηση όλων των αντίμετρων δεν είναι συνήθως δυνατή λόγω περιορισμών σε προϋπολογισμό, χρήμα και αποθέματα, ο στόχος μιας ευεργετικής ανάλυσης απειλών είναι να προτείνει τα πιο αποδοτικά αντίμετρα ενάντια στην αναγνωρισμένη απειλή [7].

Επομένως, όπως γίνεται φανερό, η ιεράρχηση των απειλών είναι το σημείο κλειδί για κάθε ανάλυση απειλών. Επιπλέον, η βαθμολόγηση των απειλών θα πρέπει αφενός να συμπεριλαμβάνει την υποκειμενική για κάθε σύστημα άποψη επί του αντίκτυπου κάθε υλοποιημένης απειλής στο σύστημα αλλά από την άλλη να είναι δυνατόν να εκφραστεί με τρόπο αποδεκτό και κατανοητό και από έναν εκτός συστήματος αναλυτή. Π.χ. στα Προσωπικά Δίκτυα, ο Ανθρώπινος Παράγοντας είναι ειδικά πηγή για πολλά ευάλωτα σημεία και επιπλέον χρειάζεται να ληφθεί ιδιαιτέρως υπόψη σε αυτό το ανθρωποκεντρικό περιβάλλον η προσωπική και ηθική αξία που έχει το κάθε περιουσιακό στοιχείο [24]. Για αυτό το λόγο προτείνεται η αξιολόγηση και ιεράρχηση απειλών βάσει του προτύπου CVSS και των δένδρων επίθεσης, όπως περιγράφεται στο υποκεφάλαιο που ακολουθεί.

6.4. Μετρικό σύστημα και μετρήσεις για ιεράρχηση απειλών και ευάλωτων σημείων

Όπως έγινε φανερό, η βαθμολόγηση και ιεράρχηση απειλών είναι μια πρόκληση για τους αναλυτές της ασφάλειας. Οι σχετικές λύσεις και έρευνα όπως καταγράφτηκαν στο υποκεφάλαιο 6.2 λύνουν επί μέρους και ανά περίπτωση το πρόβλημα δίδοντας είτε λύσεις που συνδέονται μόνο με το χρηματικό κόστος, είτε στατιστικές και πιθανολογικές τιμές, είτε λύσεις σχετικές με τη δύναμη των αλγορίθμων ασφαλείας. Όμως και παίρνοντας σα βάση το ολοκληρωμένο και ανθρωποκεντρικό περιβάλλον του Προσωπικού Δικτύου είναι ορατή η ανάγκη για:

- Αξιολόγηση και μέτρηση της ασφάλειας στο σύνολο της και σε όλα τα στρώματα, και όχι μόνο π.χ. σε αλγοριθμικό, δικτυακό επίπεδο
- Ενσωμάτωση και μέτρηση της απειλής του ανθρώπινου παράγοντα, π.χ. με τις σχετικές απειλές από κοινωνική μηχανική αλλά και του υποκειμενικού και ανθρώπινου χαρακτήρα στην αξία των υπαρχόντων
- Μετρήσεις και βαθμολογίες που να γίνονται κατανοητές από όλους τους αναλυτές και να εφαρμόζονται σε κάθε σύστημα
- Ανάλυση πολύ-βηματικών επιθέσεων (multi-step attacks) και σχέσεων μεταξύ απειλών

Γενικότερα, η έγκυρη μέτρηση της ασφάλειας ενός συστήματος είναι ένα δύσκολο αλλά απαραίτητο βήμα σε μια ανάλυση απειλών, προκειμένου να οριστεί με ακρίβεια η απόδοση των μηχανισμών ασφαλείας, καθώς και να ενισχυθεί η ασφάλεια με την ελαχιστοποίηση της έκθεσης σε σημαντικές απειλές και τρωτά σημεία. Γι αυτούς τους σκοπούς, οι ειδικοί της ασφάλειας πρέπει να μπορούν να ιεραρχήσουν τις απειλές που αφορούν ένα σύστημα, και επομένως χρειάζονται:

- Μια δομημένη εικόνα του πλαισίου ασφαλείας, η οποία θα περιέχει όλα τα τρωτά σημεία ενός συστήματος, τις σχέσεις μεταξύ τους, τις σχέσεις με τους μηχανισμούς ασφαλείας και με τα υπόλοιπα μέρη του συστήματος.
- Μια τυποποιημένη μέτρηση που να εκφράζει την σοβαρότητα και τον κίνδυνο (δηλαδή την πιθανότητα και ευκολία εκμετάλλευσης του τρωτού σημείου) κάθε τρωτού σημείου, και επομένως της σημαντικότητας της αντίστοιχης απειλής η οποία να μπορεί να εφαρμοστεί συνολικά σε κάθε σύστημα.

Για όλους τους παραπάνω λόγους, προτείνεται η συνδυαστική χρήση των Δένδρων Επίθεσης του Bruce Schneier [15] και του προτύπου γνωστού ως Common Vulnerability Scoring System (CVSS) [16][8].

Τα Δένδρα Επίθεσης αναπαριστούν τις επιθέσεις εναντίον ενός συστήματος σε μια δενδρική δομή, με το στόχο της επίθεσης να είναι ο κόμβος-ρίζα και οι διάφοροι τρόποι για να επιτευχθεί ο στόχος να ξεκινάνε από τους κόμβους φύλλα. Με αυτή τη δομή, είναι εφικτό να υπάρχουν πολλά δυνατά μονοπάτια σε μια επίθεση, μέσω εκμετάλλευσης διαφορετικών ευάλωτων σημείων και με διαφορετικές μεθόδους. Καταρχήν, για να χτιστεί η δομή του δέντρου χρειάζεται λεπτομερής και μεθοδική ανάλυση του συστήματος, των περιουσιακών του στοιχείων που πρέπει να προστατεύσουμε, τις απειλές που ελλοχεύουν και των ευάλωτων του σημείων. Σαν δεύτερο βήμα, τιμές θα πρέπει να ανατεθούν στους κόμβους του δέντρου ώστε να αξιολογηθούν και να ιεραρχηθούν τα μονοπάτια στο δέντρο, και να δοθεί ανάλογα προτεραιότητα στα αντίστοιχα αντίμετρα. Όταν ολοκληρωθεί αυτό το βήμα, τα βέλτιστα μονοπάτια για τις επιθέσεις αποκαλύπτονται, υπογραμμίζοντας έτσι τις προτεραιότητες στη σχεδίαση ενίσχυσης ασφάλειας του συστήματος. Καθώς οι επιθέσεις παρουσιάζουν μεγάλη ποικιλομορφία, η εύρεση σωστών και ακριβών μετρήσεων είναι ένα δύσκολο έργο. Π.χ. εξαιρετικά εξειδικευμένες και τεχνικά δύσκολες έως και πρακτικά αδύνατες επιθέσεις στον αλγόριθμο κρυπτογράφησης [17], επιθέσεις δικτύου όπως η Distributed Denial of Service, δηλαδή διανεμημένη άρνηση παροχής υπηρεσίας (DDoS) [18][19] καθώς και επιθέσεις κοινωνικής μηχανικής (social engineering attacks) ή απλώς αμέλειας χρήστη [20] είναι μερικές επιθέσεις που διαφέρουν σημαντικά σε ποιότητα και ποσότητα απαιτούμενων πόρων που απαιτούνται προκειμένου να πραγματοποιηθούν. Επιπλέον, καθώς κάθε σύστημα έχει τις δικές του απαιτήσεις ασφαλείας, η επίπτωση κάθε επίθεσης αλλάζει ανάλογα με την περίπτωση. Μια επίθεση DoS σε ένα τραπεζικό σύστημα σημαίνει σημαντική οικονομική ζημία, ενώ DoS σε ένα εξυπηρετητή chat απλώς θα εκνευρίσει στη χειρότερη μερικούς χρήστες. Είναι λοιπόν ορατή η ανάγκη για μια προτυποποιημένη μέτρηση, έτσι ώστε να υπάρξει μια κοινή, γενικά αποδεκτή και σταθερή άποψη για την αξιολόγηση της ασφάλειας. Για αυτό το λόγο, προτείνεται το πρότυπο CVSS ως η μέθοδος ανάθεσης τιμών στους κόμβους των Δένδρων Επίθεσης.

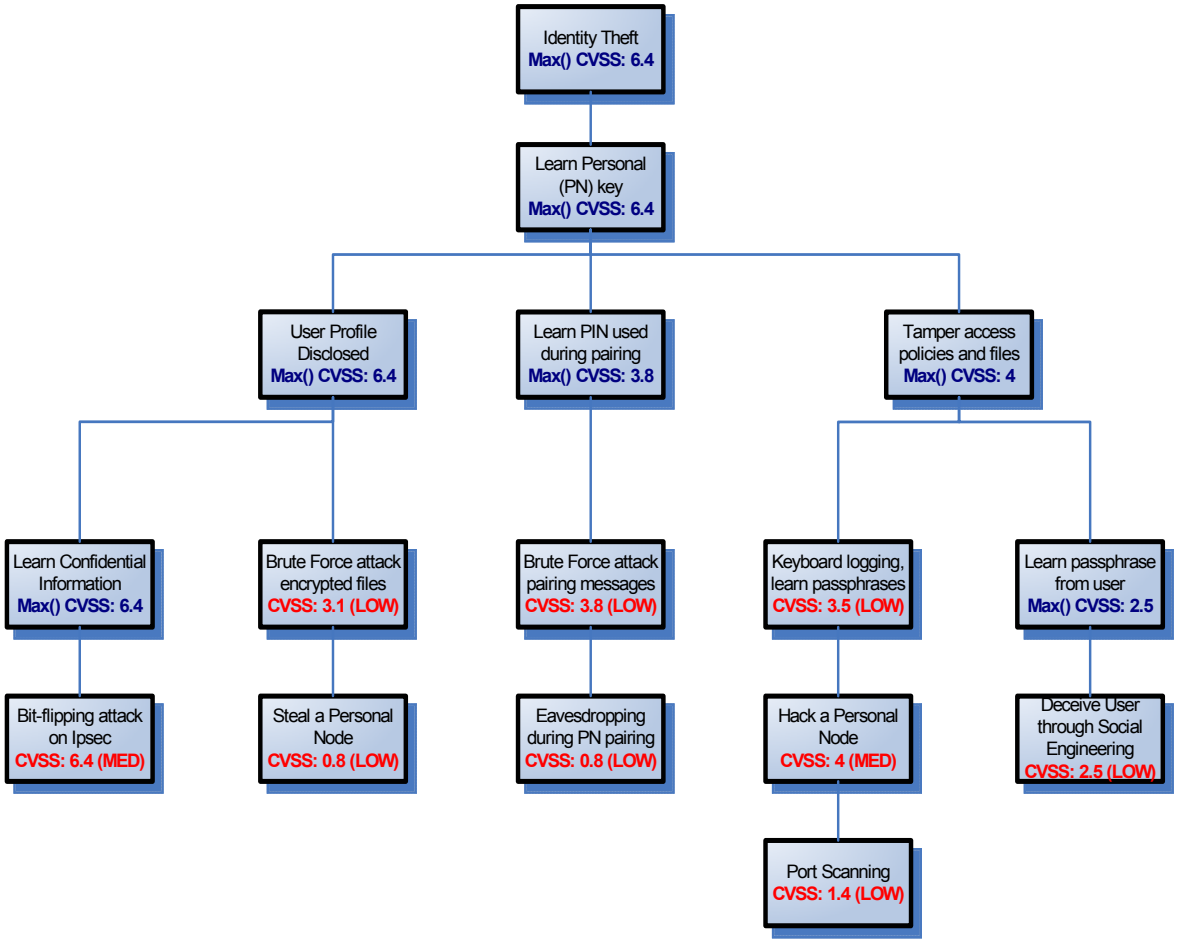
Το CVSS είναι ένα ανεξάρτητο και ανοιχτό βιομηχανικό πρότυπο, σχεδιασμένο να καταγράφει και να βαθμολογεί την σημαντικότητα ευάλωτων σημείων, καθώς και να βοηθά στο καθορισμό επειγόντων περιστατικών και προτεραιοτήτων στην αντιμετώπιση αυτών. Η αξιολόγηση του CVSS χωρίζει τα χαρακτηριστικά των ευάλωτων σημείων σε τρεις περιοχές:

- Βασική: για ιδιότητες που χαρακτηρίζουν άμεσα το τρωτό σημείο
- Χρονική - Συγκυριακή: για χαρακτηριστικά που αφορούν τη διάρκεια ζωής του τρωτού σημείου και την δυνατότητα εκμετάλλευσης
- Περιβαλλοντική: για χαρακτηριστικά που εξαρτώνται από συγκεκριμένες περιπτώσεις συστημάτων και από το περιβάλλον

Καθώς το CVSS παρέχει ένα ανοιχτό πλαίσιο για βαθμολόγηση ευάλωτων σημείων, οι ειδικοί ασφαλείας ανά τον κόσμο μπορούν να ανταλλάσσουν απόψεις και πληροφορίες

βάσει μιας κοινής μεθοδολογίας μέτρησης, και να σχηματίσουν με αυτό το τρόπο δημόσια δελτία ενημέρωσης με CVSS βαθμολογίες, από τα οποία ο καθένας μπορεί να αντλεί πληροφορία. Διαλέγοντας το CVSS για πλήρωση των τιμών των Δένδρων Επίθεσης, επωφελούμαστε από όλα τα στοιχεία αυτών των εργαλείων μέτρησης. Χρησιμοποιούμε δε το Δένδρο Επίθεσης για την περιγραφή της ασφάλειας του συστήματος συνολικά, και το CVSS για να παρέχουμε επί μέρους μετρήσεις για κάθε απειλή που συνδέετε σε κάθε κόμβο του Δένδρου.

Η χρήση του ανοιχτού προτύπου επιπλέον διευκολύνει την κατασκευή των Δένδρων, καθώς όλη η κοινότητα των ειδικών συνεισφέρει σε αυτό με την διαρκή ενημέρωση των δελτίων ενημέρωσης των CVSS βαθμολογιών.



Εικόνα 31 - Δένδρο επίθεσης κλοπής ταυτότητας

Για να γίνει καλύτερα κατανοητή η μεθοδολογία της μέτρησης της ασφάλειας με χρήση των CVSS Δένδρων Επίθεσης παρουσιάζεται ένα παράδειγμα στην Εικόνα 31, που αφορά κλοπή της ηλεκτρονικής ταυτότητας σε Προσωπικά Δίκτυα (PN) [21].

Το παράδειγμα εστιάζεται στο περιουσιακό στοιχείο «Ταυτότητα» ενός Προσωπικού Δικτύου. Όλες οι απειλές και τα τρωτά σημεία, καθώς και οι σχέσεις μεταξύ τους αναλύονται και το σχετικό Δένδρο Επίθεσης σχηματίζεται. Έπειτα, οι βαθμολογίες CVSS τοποθετούνται στους κόμβους, είτε υπολογισμένες από τις εξισώσεις των περιοχών του CVSS (βασική, χρονική, περιβαλλοντική), είτε απευθείας από δελτία ενημέρωσης και διαθέσιμες βάσεις δεδομένων «σεσημασμένων» ευάλωτων σημείων, όπως είναι για παράδειγμα η επίθεση Bit-flipping («στρίψιμο» ψηφίου) στο πρωτόκολλο IPsec (γνωστό τρωτό σημείο με τον κωδικό CVE-2005-0039 [22]). Οι τιμές που υπολογίζονται με τη βαθμολόγηση του CVSS φαίνονται με κόκκινο στο Δένδρο, και οι αντίστοιχοι κόμβοι συνδέονται άμεσα με την εκμετάλλευση κάποιου τρωτού σημείου και με το σχετικό κίνδυνο. Οι κόμβοι με μπλε χρώμα αντιστοιχούν στη περίπτωση συνέπειας από επιτυχημένη επίθεση και κληρονομούν τη μέγιστη βαθμολόγηση από όλους τους κόμβους παιδιά των. Όταν το δέντρο συμπληρωθεί με βαθμολογίες, η αξιολόγηση και ο σχεδιασμός βελτίωσης του συστήματος μπορεί να επιτευχθεί αναγνωρίζοντας τα μονοπάτια «τρωτότητας» που οδηγούν στις υψηλότερες βαθμολογίες. Με την ποσοτικοποίηση της απειλής χάρις στο CVSS, οι απειλές μπορούν να ιεραρχηθούν. Προκύπτει στο παράδειγμα ότι η μεγαλύτερη προτεραιότητα είναι η λήψη μέτρων για την bit-flipping επίθεση στο IPsec πρωτόκολλο.

Η επιπλέον αξία της χρήσης του δένδρου επίθεσης γίνεται προφανής κατά το σχεδιασμό βελτίωσης του συστήματος. Για παράδειγμα, βάσει μόνο της βαθμολογίας CVSS, το να «χακάρει» κάποιος έναν Προσωπικό Κόμβο είναι η δεύτερη κατά σειρά προτεραιότητα. Όμως, βάσει του δένδρου επίθεσης, η επίθεση αυτή είναι ουσιαστικά το δεύτερο βήμα μιας επίθεσης (σάρωση θύρας) με αρκετά χαμηλή βαθμολογία, κυρίως επειδή τα firewalls και η σωστές ρυθμίσεις ασφαλείας αντιμετωπίζουν αυτή την επίθεση σε πολύ μεγάλο βαθμό. Ακολουθώντας αυτή τη λογική, και πάντα σύμφωνα με τις πολιτικές ασφαλείας και απαιτήσεις του συγκεκριμένου συστήματος, οι διαχειριστές μπορούν να επιλέξουν ένα σχεδιασμό βελτίωσης που να ενισχύει κόμβους του Δένδρου με χαμηλότερη μεν βαθμολογία, αλλά που να είναι μέρος ενός πιο συνεκτικού μονοπατιού (όπως π.χ. το μονοπάτι της κοινωνικής μηχανικής), φοβούμενοι πιθανή δράση «ντόμινο».

6.5. Συμπεράσματα - Επεκτάσεις

Σε αυτό το κεφάλαιο προτάθηκε μια γενική μεθοδολογία η οποία ενσωματώνει τη μοντελοποίηση των απειλών με την ανάλυση απειλών με έμφαση στις ειδικές ανάγκες των Προσωπικών Δικτύων. Δηλαδή, στο ολοκληρωμένο περιβάλλον των Προσωπικών Δικτύων οι χρήστες κινούνται πάνω από διαφορετικά δίκτυα και τεχνολογίες, κάνοντας χρήση ποικίλων εφαρμογών και υπηρεσιών σε οποιοδήποτε σημείο και στιγμή. Επιπλέον τα Προσωπικά Δίκτυα είναι συστήματα σχεδιασμένα με ανθρωποκεντρικό τρόπο, λαμβάνοντας υπόψη τις προσωπικές προτιμήσεις αλλά και την υποκειμενικότητα του κάθε χρήστη. Για αυτό το λόγο, και δεδομένου ότι οι υπάρχουσες λύσεις αδυνατούν να εξυπηρετήσουν το σύνολο των αναγκών αυτών, η προτεινόμενη μεθοδολογία προσφέρει:

- Αξιολόγηση και μέτρηση της ασφάλειας στο σύνολο της, σε όλες τις περιπτώσεις χρήσης και σε όλα τα στρώματα, και όχι μόνο π.χ. σε αλγοριθμικό, δικτυακό επίπεδο
- Ενσωμάτωση και μέτρηση της απειλής του ανθρώπινου παράγοντα, π.χ. με τις σχετικές απειλές από κοινωνική μηχανική αλλά και του υποκειμενικού και ανθρώπινου χαρακτήρα στην αξία των υπαρχόντων
- Μετρήσεις και βαθμολογίες που να γίνονται κατανοητές από όλους τους αναλυτές και να εφαρμόζονται σε κάθε σύστημα και όχι μόνο σε ειδικά περιβάλλοντα (π.χ. οικονομικά μεγέθη για εταιρικά περιβάλλοντα)

Η μεθοδολογία χωρίζεται σε τρεις φάσεις: μοντελοποίηση απειλών, χαρτογράφηση υπαρχόντων και σχέδιο άμβλυνσης απειλών. Προς την ολιστική προσέγγιση αξιολόγησης προτείνεται μια νέα προσέγγιση αποδόμησης και ανάλυσης του συστήματος σε περιουσιακά στοιχεία χρησιμοποιώντας UML διαγράμματα περιπτώσεων χρήσης και ακολουθιών και ανάλυση σε περιγραφικούς πίνακες, Βάσει αυτών γίνεται η αναγνώριση των απειλών, σημείων εισόδου και ευάλωτων σημείων του συστήματος και ολοκληρώνεται η φάση μοντελοποίησης απειλών. Ακολουθεί η χαρτογράφηση απειλών προς το τελικό βήμα της διαχείρισης κινδύνου και της κατάστρωσης του σχεδίου άμβλυνσης. Σε αυτά τα βήματα, υπάρχει ανάγκη πρότυπης μεθοδολογίας βαθμολόγησης και ιεράρχησης των απειλών και ευάλωτων σημείων. Για αυτό το σκοπό προτάθηκε η συνδυαστική χρήση δένδρων επίθεσης με το σύστημα βαθμολόγησης CVSS η οποία παρέχει στον αναλυτή:

- Μια δομημένη και συνολική εικόνα του πλαισίου ασφαλείας, η οποία περιέχει όλα τα τρωτά σημεία ενός συστήματος, τις σχέσεις μεταξύ τους, τις σχέσεις με τους μηχανισμούς ασφαλείας και με τα υπόλοιπα μέρη του συστήματος.
- Μια τυποποιημένη μέτρηση που εκφράζει την σοβαρότητα και τον κίνδυνο (δηλαδή την πιθανότητα και ευκολία εκμετάλλευσης του τρωτού σημείου) κάθε τρωτού

σημείου, και επομένως της σημαντικότητας της αντίστοιχης απειλής η οποία να εφαρμόζεται συνολικά σε κάθε σύστημα.

Πέραν της ειδικής πρόνοιας για τα Προσωπικά Δίκτυα, η προτεινόμενη δουλειά είναι χρήσιμη για κάθε σύστημα που χρειάζεται αξιολόγηση της ασφάλειας του στο σύνολο της και μια ολοκληρωμένη ανάλυση απειλών, αξιολογώντας τις απειλές και ευάλωτα σημεία με μετρήσεις κατανοητές και μεταφέρσιμες από σύστημα σε σύστημα και αναλυτή σε αναλυτή. Σε τέτοια συστήματα, όπως και στη περίπτωση των Προσωπικών Δικτύων έμφαση δίνεται και στο χρήστη και τον Ανθρώπινο παράγοντα, που επιτυχώς ενσωματώνει η πρόταση. Η πρόταση αυτή επικυρώθηκε μέσω της εφαρμογής στην αναπτυχθείσα πλατφόρμα Προσωπικού Δικτύου στα πλαίσια του ερευνητικού προγράμματος MAGNET BEYOND.

Σαν μελλοντική επέκταση της εργασίας αυτής, είναι η επικύρωση της προσέγγισης και σε άλλα συστήματα πέραν των Προσωπικών Δικτύων καθώς και η ανάπτυξη ενός πρωτότυπου διαχειριστικού εργαλείου ασφαλείας που να χρησιμεύει στα πλαίσια διαχείρισης της ασφάλειας του συστήματος τόσο σε έναν έμπειρο διαχειριστή συστήματος, σε έναν αναλυτή ασφαλείας αλλά και στον απλό χρήστη ενός Προσωπικού Δικτύου.

6.6. Ειδική ορολογία κεφαλαίου

Ελληνικός όρος / φράση	Αγγλικός όρος / φράση
Απειλή	Threat
Διάγραμμα Ακολουθίας	Sequence Diagram
Διάγραμμα Περίπτωσης Χρήσης	Use Case Diagram
Διαχείριση κινδύνου, ρίσκου	Risk Management
Ευάλωτο σημείο, αδυναμία	Vulnerability
Κοινωνική Μηχανική	Social Engineering
Μοντελοποίηση Απειλών	Threat Modeling
Περιουσιακό Στοιχείο	Asset
Περίπτωση Χρήσης	Use Case
Πιστοποιητικά Χρήστη	User Credentials
Σχέδιο Άμβλυνσης (Απειλών)	Mitigation Plan
Χαρτογράφηση Περιουσιακών Στοιχείων	Asset Mapping

6.7. Βιβλιογραφικές Αναφορές

[1] N. R. Prasad “Threat Model Framework and Methodology for Personal Network”, Communication Systems Software and Middleware, COMSWARE 2007.

[2] F. Swiderski, W. Snyder, “Threat Modeling”, Microsoft Press 2004.

[3] E. Oladimeji, S. Supakkul and L. Chung, “Security Threat Modeling: A Goal-Oriented Approach,” Proc. SEA’06, Dallas, TX, Dec. 2006 pp. 178-185.

[4] S. Myagmar, A. Lee, and W. Yurcik, “Threat modeling as a basis for security requirements,” In Proceedings of the Symposium on Requirements Engineering for Information Security, Paris, Aug 2005.

[5] J.D. Meier, A. Mackman, M. Dunner, S. Vasireddy, and A. Murukan, “Improving Web Application Security: Threats and Countermeasures”, Microsoft Press, 2003.

[6] J. Pauli and D. Xu, "Threat-driven Architectural Design of Secure Information Systems", Proc. of the 7th International Conference on Enterprise Information Systems, ICEEIS 2005, Miami, FL, USA, May 2005

[7] Ygor Goldberg, “Practical Threat Analysis for the Software Industry”, http://www.securitydocs.com/library/2848.

[8] CVSS documentation, Forum of Incident Response and Security Teams, http://www.first.org/cvss/cvss-guide.html.

[9] http://www.ist-magnet.org/ MAGNET beyond/D4.4.2 “Analysis, Verification and Evaluation”, June 2008

[10] S. A. Butler, “Security attribute evaluation method: a cost-benefit approach”, Proceedings of the 24th ICSE, May 2002

[11] Indrajit Ray and Nayot Poolsapassit, “Using Attack Trees to Identify Malicious Attacks from Authorized Insiders”, Computer Security – ESORICS 2005, Lecture Notes in Computer Science, Volume 3679/2005, pp. 231-246, Springer Berlin / Heidelberg, 2005.

[12] Igor Kotenko and Mikhail Stepashkin, “Attack Graph Based Evaluation of Network Security”, Communications and Multimedia Security, Lecture Notes in Computer Science, Volume 4237/2006, pp. 216-227, Springer Berlin / Heidelberg, 2006

[13] J. Steven, G.Peterson, “Security lesson learned from Société Générale”, IEEE Security & Privacy, 2008.

[14] G. Stoneburner, A. Goguen, A. Feringa, “Risk Management Guide for Information Technology Systems”, Recommendations of the National Institute of Standards and Technology, July 2002.

[15] Schneier Bruce, "Attack Trees". Dr Dobb's Journal, v.24, n.12, December 1999, web source retrieved on 01-09-2008.

[16] Patriciu Victor-Valieriu, Priescu Iustin, Nicolaescu Sebastian, “Security Metrics for Enterprise Information Systems” Journal of Applied Quantitative Methods, JAQM, Vol 1, No. 2, Winter 2006.

[17] Bruce Schneier, Applied Cryptography, Second Edition. John Wiley & Sons, p. 151, 1996.

[18] Lee Garber, "Denial-of-Service Attacks Rip the Internet," Computer, vol. 33, no. 4, pp. 12-17, Apr., 2000.

[19] Mirkovic, J. and Reiher, P., "A taxonomy of DDoS attack and DDoS defense mechanisms", SIGCOMM Comput. Commun. Rev. 34, 2, April 2004.

[20] Gragg, David. "A Multi-Level Defense against Social Engineering." SANS Reading Room, March 13, 2003, URL: http://www.sans.org/rr/paper.php?id=920 (Aug 12, 2003).

[21] Kyriazanos, D., et Al., "Overview of a personal network prototype", Annual Review of Communications: Volume 59, p.521-534, Intl. Engineering Consortiu, 2007.

[22] Vulnerability Summary for CVE-2005-0039, http://web.nvd.nist.gov/view/vuln/search?execution=e1

[23] WP4 "Security and Privacy" group, MAGNET BEYOND Public Deliverable 4.4.2 "Analysis, Verification and Evaluation", June 2008

[24] Dimitris M. Kyriazanos and Michalis G. Argyropoulos, "Personal Networks: Security Risks and Solutions", submitted and accepted for oral presentation on the FITCE 45TH Congress "Telecom Wars: The return of the Profit", 30/8/2006 – 2/9/2006.

7. Συμπεράσματα και προοπτικές για μελλοντικές επεκτάσεις

Ακολουθεί η ανακεφαλαίωση των συμπερασμάτων της διατριβής καθώς και των προοπτικών για μελλοντικές επεκτάσεις. Η διατριβή ασχολήθηκε με το θέμα της διασφάλισης της ιδιωτικότητας σε Προσωπικά Δίκτυα με επίγνωση κατάστασης. Το περιβάλλον των Προσωπικών Δικτύων έθεσε ιδιαίτερες προκλήσεις για την έρευνα καθώς:

- Τα Προσωπικά Δίκτυα εξ' ορισμού εμπεριέχουν ευαίσθητα και πολύτιμα προσωπικά δεδομένα, όπως π.χ. ηλεκτρονικές ταυτότητες, αριθμούς πιστωτικών καρτών, πληροφορίες υγείας και άλλες πληροφορίες. Όντας υψηλά προσωποποιημένα, κάθε επίθεση στο δίκτυο απειλεί άμεσα την ηλεκτρονική ταυτότητα του προσώπου με το οποίο συνδέεται το δίκτυο.
- Οι προσωπικές πληροφορίες υπάρχουν προκειμένου ο χρήστης να επωφεληθεί από υψηλά προσωποποιημένες υπηρεσίες και εφαρμογές. Η χρήση της πληροφορίας όμως την καθιστά στόχο για επιθέσεις κατά του απορρήτου και της ιδιωτικότητας.
- Η μοναδικότητα της ψηφιακής ταυτότητας για όλο το Προσωπικό Δίκτυο είναι εξαιρετικά πρακτικό αλλά αυξάνει επίσης και την αξία της στα μάτια των κακόβουλων ανθρώπων
- Επίγνωση κατάστασης, διεισδυτικές εφαρμογές και υψηλή προσωποποίηση είναι στους στόχους των παρεχόμενων προσωπικών υπηρεσιών. Όλο και μεγαλύτερο κομμάτι της ζωής μας θα είναι ψηφιακό και «πάνω από το σύρμα», εκθέτοντας το σε μεγαλύτερο κίνδυνο
- Η υποστήριξη της κινητικότητας χρήστη σε ετερογενή δίκτυα και με χρήση ετερογενών από άποψης δυνατοτήτων συσκευών ενώ παράλληλα υπάρχει ανάγκη για έλεγχο πρόσβασης και ασφάλεια, παντού και πάντα. Από την άλλη πλευρά, οι υπάρχουσες παραδοσιακές λύσεις ασφαλείας είναι σχεδιασμένες για εφαρμογή σε εξειδικευμένο μέρος αυτών των δικτύων και συσκευών.
- Καθότι αποτελούνται από διανεμημένα αλληλοσυνδεόμενα δίκτυα, πολύπλοκες κετρικοποιημένες υποδομές και αρχιτεκτονικές δεν μπορούν να θεωρηθούν διαθέσιμες ανά πάσα στιγμή. Προσαρμοστικές αρχιτεκτονικές και μηχανισμοί θα πρέπει να είναι διαθέσιμοι είτε ως κύριοι μηχανισμοί είτε εναλλακτικά, στα πλαίσια υποστήριξης των παραδοσιακών μηχανισμών ασφαλείας.
- Τα Προσωπικά Δίκτυα αναμένονται να είναι όσο το δυνατόν φιλικά προς το χρήστη, με υψηλές δυνατότητες προσωποποίησης αλλά και συγχρόνως αυτόνομα σε μεγάλο βαθμό και εν μέρει αυτό-οργανούμενα και ικανά να τα διαχειριστούν απλοί χρήστες. Ο «φιλικός» διαχειριστής δικτύου για να παραπονεθούμε, πιθανόν να μην υπάρχει! Με αυτή την έννοια δεν θα πρέπει να θέτουν πολύπλοκα καθήκοντα διαχείρισης ασφαλείας στους απλούς καθημερινούς χρήστες τους.

Σε αυτά τα πλαίσια έρευνας η διδακτορική διατριβή παρουσίασε σημαντική συνεισφορά που εκφράζεται με τις εξής καινοτομίες:

- **Μηχανισμός ανωνυμίας βασισμένος στον καινοτόμο διαχωρισμό της πληροφορίας ταυτότητας χρήστη από τις λοιπές πληροφορίες κατάστασης**

και προσωπικών προτιμήσεων, για να διασφαλιστεί η ευαίσθητη από πλευράς ασφάλειας φάση εγκαθίδρυσης εμπιστοσύνης μεταξύ αγνώστων χρηστών. Το προτεινόμενο μοντέλο μπορεί να εφαρμοστεί πάνω από Προσωπικά Δίκτυα και συνδυάζει την ανωνυμία της προσωπικής πληροφορίας χρήστη που χρησιμοποιείτο στην ανακάλυψη και αντιστοίχιση ομότιμων χρηστών, με κρυπτογράφηση του περιεχομένου που ανταλλάσσεται έτσι ώστε τρίτα μέρη που εμπλέκονται προκειμένου να υποστηρίξουν τη διαδικασία να μην μπορούν να συνδέσουν το προσωπικό περιεχόμενο με την ταυτότητα του χρήστη. Η ολοκληρωμένη λύση που προτείνεται είναι ανθεκτική στις επιθέσεις και επίσης προσφέρει ανίχνευση κακόβουλων συμπεριφορών και χαρακτηρισμό των χρηστών αναλόγως βάσει μηχανισμού αναφορών συμπεριφοράς και εμπιστοσύνης. Επίσης παρουσιάστηκε μια ενδεικτική υλοποίηση για την αξιολόγηση της δυνατότητας εφαρμογής ενώ έγινε και αξιολόγηση με σύγκριση των υπαρχουσών τεχνικών και λύσεων. Μεσω της σύγκρισης βρέθηκαν τα εξής πλεονεκτήματα:

- Καταρχήν, η καινοτόμος πρόταση χρήσης μοντέλου διαχωρισμού της πληροφορίας ταυτότητας από τις προσωπικές πληροφορίες και πληροφορίες συγκειμένου, η οποία αποτελεί ισχυρή προστασία της ταυτότητας και διευκολύνει την ανωνυμία, μη εμποδίζοντας τη λειτουργικότητα, ενώ διευκολύνει ιδιαίτερα την δυναμική εφαρμογή κανόνων πολιτικής ακόμη και σε περιπτώσεις ανωνυμίας.
- Με την οντότητα του διακομιστή ανωνυμίας, η προτεινόμενη λύση αντιδρά θετικά στην κλιμάκωση σε θέματα διαχείρισης της πληροφορίας και επεξεργασίας της, καθώς αυτά βαραίνουν τον διακομιστή και όχι τους χρήστες.
- Το κύριο όφελος από τον διακομιστή ανωνυμίας είναι ότι επιβάλλει πραγματική ανωνυμία κατά την ανταλλαγή της πληροφορίας σε όλα τα στρώματα. Τα κρυπτο-προφίλ εγγυώνται την ανωνυμία στο στρώμα εφαρμογής, ενώ η χρήση του διακομιστή για τη διανομή και αρχική διαχείριση τους κρύβει και την υπόλοιπη πληροφορία που θα μπορούσε να χρησιμοποιηθεί για να συνδεθεί ένας συγκεκριμένος χρήστης: π.χ. μέσω διευθύνσεων MAC και IP συσκευών χρήστη. Οι διανεμημένες λύσεις ανταλλαγής πληροφορίας σε γενικές γραμμές μειονεκτούν σε αυτό το θέμα και γενικά λειτουργούν μόνο στο στρώμα εφαρμογής.

- **Ολοκληρωμένη λύση διαχείρισης ασφάλειας με επίγνωση κατάστασης για τα Προσωπικά Δίκτυα, για την προστασία της προσωπικής και συγκείμενης πληροφορίας**. Συγκεκριμένα ο Διαχειριστής Ασφάλειας λειτουργεί σαν σημείο εφαρμογής πολιτικών ασφαλείας, διασφαλίζοντας την ιδιωτικότητα πληροφοριών προφίλ χρήστη και συγκείμενης πληροφορίας, συνδέεται με ομότιμες τέτοιες οντότητες διαχείρισης σε όλο το προσωπικό δίκτυο, παρέχοντας πλήρη κάλυψη σε όλο το δίκτυο. Παρέχει μια ενιαία διεπαφή για όλες τις εφαρμογές και υπηρεσίες που χρησιμοποιούν προσωπικά δεδομένα και συγκείμενες πληροφορίες, και χάριν στο SCMF, δρα και ο ίδιος ως μια εφαρμογή επίγνωσης κατάστασης στα ίδια πλαίσια Λαμβάνει υπόψη τον ανθρωποκεντρικό χαρακτήρα των Προσωπικών Δικτύων, ενσωματώνοντας στις πολιτικές και αποφάσεις ασφαλείας την πληροφορία προφίλ χρήστη και τις προσωπικές προτιμήσεις, όπως αυτές εκφράζονται με την έννοια της σημαίας ιδιωτικότητας (privacy flags). Έχει

επίγνωση κατάστασης ασφαλείας, οι οποίες, χωριζόμενες σε τρία επίπεδα ασφαλείας (Χαμηλό, Μέσο, Υψηλό) οδηγούν σε δυναμική εφαρμογή διαφορετικού συνόλου πολιτικών ασφαλείας ανάλογα με τη συγκείμενη πληροφορία. Συνεργάζεται με μηχανισμούς φήμης και μοντέλα εμπιστοσύνης, ενσωματώνοντας το επίπεδο εμπιστοσύνης για κάθε εμπλεκόμενη οντότητα σε μια συναλλαγή. Υποστηρίζει το μηχανισμό ανωνυμίας που προτάθηκε επίσης στη διατριβή, φροντίζοντας ώστε η πληροφορία που δημοσιεύεται να μην οδηγεί σε άμεση ή έμμεση αποκάλυψη της ταυτότητας Τέλος, η πρόταση του διαχειριστή ασφαλείας αξιολογήθηκε σε σύγκριση με άλλες σχετικές προτάσεις, πλαίσια και λύσεις και βρέθηκε να έχει σημαντικά πλεονεκτήματα, ειδικά στα πλαίσια των Προσωπικών Δικτύων:

- Ενσωματώνει στις πολιτικές και αποφάσεις ασφαλείας την πληροφορία προφίλ χρήστη και τις προσωπικές προτιμήσεις, λαμβάνοντας υπόψη τον ανθρωποκεντρικό χαρακτήρα των Προσωπικών Δικτύων.
- Διαχωρίζει πλήρως τους τρεις τύπους πληροφορίας: παράμετροι ασφαλείας και κανόνες, προσωπική πληροφορία και συγκείμενη πληροφορία, δίνοντας έτσι ευλυγισία στη θέσπιση κανόνων ασφαλείας βασισμένων στη συγκείμενη πληροφορία αλλά και στη δυναμική εφαρμογή τους.
- Αποτελεί το διαχειριστή ασφαλείας μιας ολοκληρωμένης πλατφόρμας διαχείρισης συγκείμενης πληροφορίας δίνοντας του πρόσβαση σε ένα πλούσιο, ανεξάρτητο και πλήρες μοντέλο οντολογιών συγκείμενης πληροφορίας.
- Έχει ενσωματώσει στη σχεδίαση του σχετικές μελέτες απαιτήσεων χρήστη σχετικά με την επιθυμητή λειτουργικότητα και χρηστικότητα στα πλαίσια της εφαρμογής σε πραγματική ubiquitous πλατφόρμα, όπως είναι τα Προσωπικά Δίκτυα.

- **Αξιολόγηση ασφαλείας με έμφαση στον ανθρώπινο παράγοντα και ολική μοντελοποίηση της ασφάλειας του συστήματος με συνδυασμένη χρήση Δένδρων Επίθεσης και ανοιχτού πρότυπου αξιολόγησης απειλών (CVSS):** Η συγκεκριμένη πρόταση συνδυάζει μια δομημένη ολιστική άποψη του πλαισίου ασφαλείας, που να εμπεριέχει όλα τα τρωτά σημεία του συστήματος, τις σχέσεις μεταξύ τους και την αλληλεπίδραση με τους μηχανισμούς ασφαλείας, αν υπάρχουν με μια πρότυπη μέθοδος μέτρησης που να εκφράζει τη σοβαρότητα και το ρίσκο κάθε τρωτού σημείου, και επομένως την σημασία και τις πιθανότητες επιτυχίας της σχετικής απειλής. Προτείνεται μια νέα προσέγγιση αποδόμησης και ανάλυσης του συστήματος βασισμένη σε UML διαγράμματα περιπτώσεων χρήσης και ακολουθιών και ανάλυση σε περιγραφικούς πίνακες. Συνδέοντας το μοντέλο απειλών με την ανάλυση κινδύνων, προτείνεται συνδυασμός χρήσης των Δένδρων Επίθεσης του Bruce Schneier και του ανοιχτού προτύπου για βαθμολόγηση κοινών τρωτών σημείων (Common Vulnerability Scoring System - CVSS) μέσω μιας μεθοδολογίας έτσι ώστε να καλύπτεται ο ανθρώπινος παράγοντας και να υποστηρίζονται επιθέσεις σε περισσότερα βήματα. Η μεθοδολογία παρουσιάζει τα εξής πλεονεκτήματα σε σχέση με άλλες προτάσεις:
  - Αξιολόγηση και μέτρηση της ασφάλειας στο σύνολο της, σε όλες τις περιπτώσεις χρήσης και σε όλα τα στρώματα, και όχι μόνο π.χ. σε αλγοριθμικό, δικτυακό επίπεδο.

- Ενσωμάτωση και μέτρηση της απειλής του ανθρώπινου παράγοντα, π.χ. με τις σχετικές απειλές από κοινωνική μηχανική αλλά και του υποκειμενικού και ανθρώπινου χαρακτήρα στην αξία των στοιχείων και αποθεμάτων που απαρτίζουν το σύστημα.
- Μετρήσεις και βαθμολογίες που να γίνονται κατανοητές από όλους τους αναλυτές και να εφαρμόζονται σε κάθε σύστημα και όχι μόνο σε ειδικά περιβάλλοντα (π.χ. οικονομικά μεγέθη για εταιρικά περιβάλλοντα).

Οι καινοτομίες που προσφέρονται ουσιαστικά δημιουργούν μια ολοκληρωμένη λύση διασφάλισης της ιδιωτικότητας στα Προσωπικά Δίκτυα, καθώς και αξιολόγησης και ανάλυσης των απειλών κατά αυτής. Είναι δε σχεδιασμένες βάσει πραγματικής πλατφόρμας Προσωπικών Δικτύων, οπότε και εφαρμόσιμες στις σχετικές εφαρμογές και συστήματα που θα διαδοθούν στο μέλλον. Ακολουθούν οι προοπτικές για μελλοντικές επεκτάσεις της εργασίας της διατριβής.

7.1. Προοπτικές για μελλοντικές επεκτάσεις

Το καινοτόμο **μοντέλο διαχωρισμού της πληροφορίας ταυτότητας από τις προσωπικές πληροφορίες και πληροφορίες συγκειμένου**, χρίζει προτυποποίησης, τα οφέλη της οποίας θα είναι εξαιρετικά για την ερευνητική κοινότητα. Η κοινή όψη για το τί αποτελεί πληροφορία ταυτότητας και τί απλή προσωπική πληροφορία θα οδηγήσει σε καλύτερη σχεδίαση των αντίστοιχων πολιτικών ασφαλείας και μηχανισμών ιδιωτικότητας. Επιπλέον θα διευκολύνει την λειτουργία των υπηρεσιών σε περιπτώσεις όπου η ταυτότητα δεν είναι επιθυμητό να είναι γνωστή,

Το **προτεινόμενο μοντέλο ανωνυμίας** έχει σχεδιαστεί ώστε να ενσωματωθεί στην πρωτότυπη πλατφόρμα PN και PN-F. Για αυτό το σκοπό, συγκεκριμένα στοιχεία και υποδομές πρέπει να παρέχουν συγκεκριμένες απαραίτητες λειτουργίες και να γίνουν συγκεκριμένες επιλογές και ρυθμίσεις, με τις κυριότερες να είναι:

- Επιλογή του μοντέλου PKI. Η επιλογή ιεραρχικού ή μη μοντέλου (π.χ. PGP) που θα προσαρμοστεί στη λύση πρέπει να αποφασιστεί. Προς το παρόν, υλοποιήθηκε ένα ενδεικτικό PKI με χρήση CA που χρησιμοποιείται στη διανομή πιστοποιητικών για το σχηματισμό PN-F. Σε περίπτωση δικτύων με περισσότερο P2P και ad-hoc φύση, μη ιεραρχικά πιστοποιητικά θα πρέπει να υποστηριχθούν, αναθέτοντας ρόλο έμπιστου εισηγητή (*trusted introducers*) σε συγκεκριμένους χρήστες. Αυτό θα μπορούσε να βασιστεί σε μηχανισμό φήμης ή μέσω μιας απλής εφαρμογής κοινωνικής δικτύωσης (*social networking application*).

- Ενσωμάτωση του διακομιστή ανωνυμίας στις ομότιμες οντότητες του Προσωπικού Δικτύου: ο διακομιστής ανωνυμίας δεν είναι ουσιαστικό μέρος της πλατφόρμας καθώς είναι ένα σύνολο από κεντρικές υπηρεσίες που παρέχονται από ένα έμπιστο τρίτο μέρος. Εναλλακτικά, στη περίπτωση της PGP, κάθε μέλος του συνασπισμού θα μπορεί να δρα σαν έμπιστο τρίτο μέρος αν έχει σχετική εξουσιοδότηση, και να παρέχει τις υπηρεσίες του διακομιστή στα όμότιμα μέλη του συνασπισμού.

Για τον δε **προτεινόμενο διαχειριστή ασφάλειας με επίγνωση κατάστασης**, επίσης η εργασία προτυποποίησης του σύνθετου μοντέλου πληροφορίας ασφαλείας

που συνδέεται με όλες τις κατηγορίες: ταυτότητας, προσωπικές, συγκείμενο και παραμέτρους ασφαλείας θα ωφελήσει την μετέπειτα σχεδίαση αντίστοιχων συστημάτων, οδηγώντας σε ολοκληρωμένες λύσεις και διάδοση των τεχνικών διασφάλισης της ιδιωτικότητας.

Σαν μελλοντική επέκταση της εργασίας **ανάλυσης απειλών στα Προσωπικά Δίκτυα**, είναι η επικύρωση της προσέγγισης και σε άλλα συστήματα πέραν των Προσωπικών Δικτύων καθώς και η ανάπτυξη ενός πρωτότυπου διαχειριστικού εργαλείου ασφαλείας που να χρησιμεύει στα πλαίσια διαχείρισης της ασφάλειας του συστήματος τόσο σε έναν έμπειρο διαχειριστή συστήματος, σε έναν αναλυτή ασφαλείας αλλά και στον απλό χρήστη ενός Προσωπικού Δικτύου.