# Ασύρματη ασφάλεια και location-based services : Ένα νέο μοντέλο ηλεκτρονικών υπηρεσιών για την διαχείριση εφοδιαστικών αλυσίδων.

του

**Ζήση-Γεωργίου Γκουτσίδη**

---

Διπλωματική Εργασία

που Υποβάλλεται στο

**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Η/Υ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ**

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ**

Προς

Εκπλήρωση των Απαιτήσεων Απόκτησης

Προπτυχιακού Τίτλου Σπουδών

---

Επιβλέποντες Καθηγητές: **Δρ. Κωνσταντίνος Κούτσικος**

**Δρ. Ηλίας Χούστης**

Ιανουάριος 2007

# Περιεχόμενα ii


**1 Εισαγωγή**

1.1 Γενικό Υπόβαθρο .....1

1.2 Βασικός Τομέας της διπλωματικής ..... 4

1.3 Ερευνητικοί Στόχοι ..... 5

1.4 Αποτελέσματα ..... 6

1.5 Σύντομη Περιγραφή των Κεφαλαίων ..... 7

**2 Συναφές Ερευνητικό Έργο 10**

2.1 Ορισμοί .....10

2.1.1 Κινητό Ηλεκτρονικό Επιχειρείν (m-business) .....10

2.1.2 Κινητή Δύναμη (mobile force)..... 11

2.1.3 Διαχείριση στόλου (fleet Management) .....11

2.1.4 Εικονικό Ιδιωτικό Δίκτυο (virtual private network-VPN)..... 11

2.1.5 Secure Socket Layer (SSL).....12

2.1.6 Internet Protocol Security (IPsec).....13

2.2 Κινητή Επιχείρηση & ηλεκτρονικό εμπόριο (mobile Business, E-business)..14

2.2.1 Ασύρματη ασφάλεια της ηλεκτρονικής επιχείρησης (Wireless Security for E-business)..... 15

2.2.2 Ασύρματη ασφάλεια location based υπηρεσιών..... 15

2.3 Επισκόπηση υπό ενότητας .....16

2.4 Ενσύρματα Δίκτυα-Διαδίκτυο (Internet-VPN)..... .....18

2.4.1 Χειρισμοί Ασφαλείας σε περιβάλλον Internet.....19

2.4.1.1 Αναγνώριση και αυθεντικοποίηση.....19

2.4.1.2 Εξουσιοδότηση (Authorization).....21

2.4.1.3 Εμπιστευτικότητα (Confidentiality).....21

2.4.1.4 Ακεραιότητα (Integrity).....21

2.4.1.5 Μη αποποίηση ευθύνης (Non-repudiation).....22

2.4.1.6 Διαθεσιμότητα (Availability).....22
2.4.1.7 Έλεγχος Πρόσβασης (Access Control).....22
2.4.2 Απειλές και κίνδυνοι της ασφάλειας σε περιβάλλον διαδικτύου.....23
2.4.3 Προβλήματα ασφαλείας στο TCP/IP.....25
2.4.3.1 Επιθέσεις Άρνησης Υπηρεσίας (Denial of Service).....26
2.4.3.2 Επιθέσεις Μεταμφίεσης (Spoofing).....26
2.4.3.3 Επιθέσεις Παρακολούθησης (Sniffing).....28
2.4.3.4 Πειρατεία Συνόδου (Session Hijacking).....29
2.4.3.5 Επιθέσεις «σπασίματος» συνθηματικών .....29
2.4.4 Μηχανισμοί Ασφαλείας του πρωτοκόλλου TCP/IP και λύσεις.....30
4.2.4.1 Ασφάλεια από την πλευρά του εξυπηρετητή.....32
4.2.4.2 Ασφάλεια από την πλευρά του χρήστη.....34
4.2.4.3 Άλλες λύσεις ασφαλείας.....33
2.5 Χαρακτηριστικά Φορητών Συσκευών.....35
2.5.1 Τα χαρακτηριστικά του ασυρμάτου πρωτοκόλλου εφαρμογής (GPRS-WAP).....36
2.5.2 Οι απαιτήσεις και απειλές ασφαλείας .....37
2.5.3 Επιθέσεις κατά της ασφάλειας στα ασύρματα δίκτυα.....38
2.5.4 Τρόποι προστασίας των φορητών συσκευών.....39
2.5.5 Ασφάλεια WAP.....43
2.6 Αρχιτεκτονικές location based.....45
2.7 Αρχιτεκτονικές VPN.....46
2.7.1 Συγκρίνοντας MPLS VPNs & IPSec VPNs και μια τους συνδυαστική προσέγγιση.....46
2.7.2 Ασφαλή εικονικά δίκτυα σε βάθος.....49
2.7.3 Σύγκριση IPSec vs SSL.....50
2.8 Μια προσέγγιση στο ηλεκτρονικό εμπόριο-Ανάλυση διαδικασίας.....52

**3 Εφαρμόζοντας τα μοντέλα (ανάλυση διαδικασίας) για την ανάπτυξη μια νέας ηλεκτρονικής υπηρεσίας. 54**

3.1 Επισκόπηση αξίας (Value Viewpoint)....54

3.1.1 Ιεραρχία Αξίας (Value Hierarchy)....57

3.1.2 Γράφημα συναλλαγών αξίας (Value Exchange Graph)....61

3.2 Επισκόπηση διαδικασίας (Process Viewpoint)....61

3.2.1 Ιεραρχία επιχειρηματικών διαδικασιών ....61

3.2.2 Ιεραρχία Στόχων (Task Hierarchy)....63

3.2.3 Ροή Διαδικασίας (Interleaved Process Flow 1)....64

3.2.4 Βήμα διαδικασίας (Process Step 1)....65

3.2.5 Ροή Διαδικασίας (Interleaved Process Flow 2)....67

3.2.6 Βήμα διαδικασίας (Process Step 2)....70

3.2.7 Βήμα διαδικασίας (Process Step 3)....73

**4 Ανάλυση των θεμάτων Ασφαλείας και προτεινόμενες λύσεις 75**

4.1 Επισκόπηση κεφαλαίου....75

4.2 Ηλεκτρονική υπηρεσία: Ενσύρματα Δίκτυα, Προβλήματα και Μηχανισμοί Ασφαλείας....75

4.2.1 Ιεραρχία Αξίας: ανάλυση θεμάτων ασφαλείας και προβλήματα....76

4.2.2 Γράφημα συναλλαγών αξίας: ανάλυση θεμάτων ασφαλείας και Προβλήματα....77

4.2.3 Ιεραρχία Επιχειρηματικών Διαδικασιών: ανάλυση θεμάτων ασφαλείας και Προβλήματα....79

4.2.4 Ιεραρχία Στόχων: ανάλυση θεμάτων ασφαλείας και Προβλήματα...80

4.2.5 Λοιπά διαγράμματα: ανάλυση θεμάτων ασφαλείας και Προβλήματα ....80

4.3 Ηλεκτρονική υπηρεσία: Ασύρματα Δίκτυα, Προβλήματα και Μηχανισμοί Ασφαλείας....82

4.3.1 Ιεραρχία Αξίας: ανάλυση θεμάτων ασφαλείας και προβλήματα....82

4.3.2 Γράφημα συναλλαγών αξίας: ανάλυση θεμάτων ασφαλείας και Προβλήματα.....84
4.3.3 Ιεραρχία Επιχειρηματικών Διαδικασιών: ανάλυση θεμάτων ασφαλείας και Προβλήματα.....84
4.3.4 Ιεραρχία Στόχων: ανάλυση θεμάτων ασφαλείας και Προβλήματα...86
4.3.5 Λοιπά διαγράμματα: ανάλυση θεμάτων ασφαλείας και Προβλήματα .....86

**5 Συμπεράσματα και μελλοντικές επεκτάσεις** **89**

**Βιβλιογραφία**

**92**

# Κεφάλαιο 1

# Εισαγωγή

## 1.1 Γενικό Υπόβαθρο

Με τον όρο εφοδιαστικές αλυσίδες νοούνται όλες οι διεργασίες και οι επιχειρήσεις που συμμετέχουν στην προετοιμασία της μεταφοράς και στη χερσαία μεταφορά εμπορευμάτων από τον τόπο παραγωγής μέχρι το σημείο παράδοσης τους [25]. Οι Location Based Services είναι το σύνολο των τεχνολογιών και συστημάτων το οποίο επιτρέπει σε μια επιχείρηση να έχει τον πλήρη έλεγχο των οχημάτων. Ο τρόπος λειτουργίας ενός τέτοιου συστήματος αποσκοπεί στην βελτιστοποίηση επιχειρηματικών διαδικασιών.

Στο *σχήμα 1* αναπαριστάται το γενικό υπόβαθρο. Ο τρισδιάστατος κύβος υποδηλώνει τις τρεις διαφορετικές αλλά συσχετιζόμενες έννοιες που αφορούν την ανάπτυξη της ηλεκτρονικής υπηρεσίας:


***Σχήμα 1:*** *Γενικό υπόβαθρο*

- **Εφοδιαστικές αλυσίδες:** όπως έχει προαναφερθεί οι επιχειρήσεις ελέγχουν, με τις τεχνολογίες και τα συστήματα, τα οχήματα τους και τη γενικότερη διαδικασία της μεταφοράς των προϊόντων.
- **Location Based Services:** είναι ένα φάσμα υπηρεσιών που προκύπτει από τις τεχνολογίες των γεωγραφικών συστημάτων (GIS) και GPS. Οι LBS παρέχουν πληροφορίες σε «κινητούς χρήστες».
- **Ασφάλεια:** ακεραιότητα των στοιχείων και εμπιστευτικότητα των προσωπικών δεδομένων.

Οι λειτουργίες της αλυσίδας εφοδιασμού μπορούν να χωριστούν σε δύο κατηγορίες: α) τον προγραμματισμό και β) την εκτέλεση. Η πρώτη κατηγορία συμπεριλαμβάνει διαδικασίες όπως η πρόβλεψη ζήτησης, ο προγραμματισμός προμηθειών υλικών και παραγωγής, ο προγραμματισμός αναγκών διανομής, καθώς επίσης και προγραμματισμός συνεχούς ανεφοδιασμού. Η δεύτερη κατηγορία είναι πιο επικεντρωμένη σε διαδικασίες όπως η παρακολούθηση παραγωγής, παρακολούθηση αποθέματος, οργάνωση αποθήκης, διανομή, συλλογή συσκευασιών (Reverse Logistics).

Οι Location Based Services αποτέλεσαν τα τελευταία χρόνια πεδίο έρευνας και μελέτης προκειμένου να βοηθήσουν τα αποτελέσματα αυτών των ερευνών, τους πάροχους κινητών υπηρεσιών να εμπλουτίσουν τις υπηρεσίες τους., αυξάνοντας τα έσοδά τους και μειώνοντας ταυτοχρόνως τα έξοδα τους. Επιπροσθέτως οι LBS παρέχουν εξατομικευμένες υπηρεσίες στον πελάτη που βασίζονται κάθε φορά στην τρέχουσα τοποθεσία του. Καθώς η εποχή μας χαρακτηρίζεται από σημαντικές τηλεπικοινωνιακές εξελίξεις, αυτού του είδους οι υπηρεσίες ανοίγουν νέους ορίζοντες για την παροχή καινοτόμων υπηρεσιών προστιθέμενης αξίας. Εκτός των άλλων, οι υπηρεσίες αυτές υποστηρίζουν real- time εξακρίβωση θέσης (positioning) των χρηστών μεγάλης ακρίβειας προκειμένου αυτοί να έχουν πρόσβαση στην πληροφορία

που τους ενδιαφέρει (π.χ κατάσταση μεταφοράς προϊόντων) με ασφάλεια, μέσω κινητών συσκευών (PDA,GPS, …)

Τα τελευταία χρόνια παρατηρείται ένα αυξανόμενος ρυθμός επένδυσης στην τρίτη διάσταση του κύβου (δηλ. στη Ασφάλεια). Δίνεται έμφαση στο πως τα στοιχεία δεν θα αλλοιωθούν και τα προσωπικά δεδομένων δεν θα «υποκλαπούν» από κακόβουλες επιθέσεις. Επομένως καταλήγουμε στο συμπέρασμα πως οι νέες τεχνολογίες δικτύων, τηλεπικοινωνιών και κατανεμημένων συστημάτων είναι οι αρωγοί στο σχηματισμό της ηλεκτρονικής υπηρεσίας.

## 1.2 Βασικός Τομέας της Διπλωματικής

Στα πλαίσια αυτής της διπλωματικής εργασίας διαπραγματευόμαστε :

- Τα μοντέλα (ανάλυση των διαδικασιών) για την ανάπτυξη μιας ηλεκτρονικής υπηρεσίας. Με βάση τα μοντέλα αυτά θα προσδιορίσουμε με τις ανάγκες που θα έχουν οι πολίτες, που χρησιμοποιούν την εν λόγω ηλεκτρονική υπηρεσία .
- Υπό το πρίσμα των μοντέλων διαδικασιών αναδεικνύουμε τα προβλήματα που προκύπτουν από αυτά και συμβάλουμε καταλυτικά στην έννοια της ΑΣΦΑΛΕΙΑΣ.

Κατά τη συγγραφή της εργασίας προέκυψαν μερικά θεμελιώδη ερωτήματα :

- Πώς θα έπρεπε να «σχεδιαστούν» τα μοντέλα των λειτουργικών διαδικασιών ενός οργανισμού που κατανέμονται στα ασύρματα δίκτυα.;
- Εφόσον σχεδιάστηκαν τα μοντέλα των διαδικασιών, πώς θα δείξουμε το πως πηγάζουν τα προβλήματα στις εφαρμογές του διαδικτύου και ασύρματου δικτύου;
- Κατά την παροχή πληροφοριακών συστημάτων, έπρεπε να χρησιμοποιηθεί ο μηχανισμός του δικτύου VPN ή ο κάποιος άλλος μηχανισμός;

## 1.3 Ερευνητικοί Στόχοι

Η διπλωματική έχει τους ακόλουθους ερευνητικούς στόχους :

- Εφαρμογή μεθοδολογίας σχεδιασμού των λειτουργικών διαδικασιών στην ανάπτυξη νέων ηλεκτρονικών υπηρεσιών με βάση τις υποδομές τις κινητής και ασύρματης επικοινωνίας.
- Κριτική ανάλυση των θεμάτων ασφαλείας που προκύπτουν.
- Σχεδιασμός σχετικών λύσεων όσο αναφορά την τεχνολογική υποδομή.

## 1.4 Αποτελέσματα

Από την υπάρχουσα διπλωματική, πετύχαμε το εξής : 1) να παρουσιάσουμε ένα αντιπροσωπευτικό παράδειγμα, ανάπτυξης μιας ηλεκτρονικής υπηρεσίας με την υποστήριξη των τεχνολογιών των ενσύρματων και ασυρμάτων υποδομών. Χρησιμοποιήσαμε τις λειτουργικές διαδικασίες του οργανισμού ΕΛ.Γ.Α και περιγράψαμε στο έπακρο τα μοντέλα των διαδικασιών (δηλαδή την *Ιεραρχία Αξίας-Value hierarchy, το Γράφημα Συναλλαγών Αξίας-Value Exchange Graph, την Ιεραρχία επιχειρηματικών διαδικασιών-Business Process Hierarchy, την Ιεραρχία Στόχων-Task Hierarchy, καθώς με τις Ροές διαδικασιών με τα αντίστοιχα βήματα διαδικασιών).* Ο ΕΛ.Γ.Α είναι ο γεωργικός ασφαλιστικός οργανισμός που καλύπτει και αποζημιώνει ζημιές από ζημιογόνα αίτια.[1] 2) αναδείξαμε κάποιες στρατηγικές επιλογές (λύσεις ή μηχανισμούς ασφαλείας σε υπαρκτά προβλήματα, που ευδοκιμούν στο διαδίκτυο ή σε κινητές και ασύρματες εφαρμογές) για άλλες Επιχειρήσεις. Οι λύσεις από τα υπαρκτά προβλήματα, επιδεικνύονται συνοπτικά στο πίνακα που ακολουθεί

| ***ΕΦΑΡΜΟΓΗ*** | ***ΠΡΟΒΛΗΜΑΤΑ*** | ***ΛΥΣΕΙΣ*** |
|---|---|---|
| ***Ενσύρματα Δίκτυα*** | 1)Επιθέσεις παρακολούθησης (Sniffing) και ανιχνεύσεις,<br>2) Άρνηση εξυπηρέτησης (Denial of Service),<br>3) Επιθέσεις μεταμφίεσης (Spoofing),<br>4) Επιθέσεις «σπασίματος» συνθηματικών,<br>5) Υποκλοπές δεδομένων. | 1) Μηχανισμοί IPsec και SLL,<br>2) Χρήση κρυπτογραφημένων passwords και στοιχείων,<br>3) Παροχή πιστοποιητικών,<br>4) Δικτυακά συστήματα ανιχνεύσεις εισβολέων. |

[1] *Τα ζημιογόνα αίτια είναι: το χαλάζι, ο παγετός, η ανεμοθύελλα, η πλημμύρα, ο καύσωνας, οι υπερβολικές ή ακραίες βροχοπτώσεις, το χιόνι, οι ζημιές από την θάλασσα.*

| | | |
|---|---|---|
| ***Ασύρματα Δίκτυα*** | 1)Επιθέσεις ενάντια της αυθεντικοποίησης & κρυπτογράφησης, 2)Επιθέσεις εναντίων των passwords στα Access Points, 3) Επιθέσεις παρεμβολής παρασίτων, 4)Επιθέσεις παρακολούθησης της κίνησης. | 1) Δίκτυα VPN με τη υποστήριξη του IPSec 2)Ψηφιακά πιστοποιητικά, 3)Μηχανισμούς κρυπτογράφησης, 4)Προτεινόμενα Ασφαλή σχέδια . |

3) Κατά συνέπεια με τις στρατηγικές επιλογές έχουμε υλοποιήσει ένα ΑΣΦΑΛΕΣ σύστημα e-business.

Κατά την διεκπεραίωση της διπλωματικής εργασίας, προέκυψαν μερικές ενδιαφέρουσες περιπτώσεις για *μελλοντική έρευνα*:

- Στα δίκτυα υλοποίησης VPN, να προστεθεί η παράμετρος της φωνής και να ερευνηθεί εκ νέου τι είδους προβλήματα μπορεί να εμφανιστούν. Παράλληλα θα πρέπει να μελετηθεί τι μηχανισμούς ασφαλείας μπορεί να παρέχουμε με ένα τέτοιο ευαίσθητο προσωπικό δεδομένο που είναι η φωνή.

## 1.5 Σύντομη περιγραφή των κεφαλαίων

Στο Κεφάλαιο 1 παρουσιάζονται τα εισαγωγικά θέματα της υπάρχουσας διπλωματικής εργασίας. Στην ενότητα 1.1 έχουμε ένα συνδυασμό από γενικές περιγραφές που αφορούν το υπόβαθρο της εργασίας. Η ενότητα 1.2 παρουσιάζει το εξειδικευμένο αντικείμενο που διαπραγματεύεται η εργασία. Η ενότητα 1.3 αναφέρεται στους ερευνητικούς στόχους, οι οποίοι απαντούν στο ερώτημα «τι πετύχαμε» με την αποπεράτωση της διπλωματικής. Και η ενότητα 1.4 περιέχει περιληπτικά τα συμπεράσματα.

Το Κεφάλαιο 2 αφορά το συναφές ερευνητικό έργο. Γίνονται αναφορές σε : 1) θέματα ασφαλείας (προβλήματα, απειλές ή και κινδύνους), 2) μηχανισμούς ασφαλείας που βρίσκουν εφαρμογές σε ενσύρματα δίκτυα (διαδίκτυο) είτε σε ασύρματα δίκτυα (GPRS και VPN). Τόσο τα θέματα ασφαλείας αλλά και τόσο οι μηχανισμοί ασφαλείας προκύπτουν μέσα από τα μοντέλα των διαδικασιών της ηλεκτρονικής υπηρεσίας. Επίσης το συγκεκριμένο κεφάλαιο περιγρέφονται αρχιτεκτονικές ασφάλειας που θα χρησιμοποιηθούν σε παρακάτω κεφάλαια.

Το Κεφάλαιο 3 ασχολείται με την περιγραφή μοντέλων σχεδιασμού διαδικασιών, ώστε να αναπτυχθεί μια ηλεκτρονική υπηρεσία. Τα μοντέλα των διαδικασιών είναι: 1) η Ιεραρχία Αξίας, 2) το Γράφημα Συναλλαγών Αξίας, 3) η Ιεραρχία Επιχειρηματικών Διαδικασιών, 4) η Ιεραρχία Στόχων, 5)οι Ροές Διαδικασιών και 6) τα βήματα διαδικασιών. Στόχος μας είναι να συνδέσουμε αυτές τις επιχειρησιακές διαδικασίες με τις καταναλωτικές ανάγκες των χειριστών. Στην προκειμένη περίπτωση χρησιμοποιήσουμε τις διαδικασίες του οργανισμού ΕΛ.Γ.Α και πρέπει να αναπτυχθεί ένα σύστημα ώστε να στοχεύει στην αυτοματοποίηση και στη εκτίμησης ζημίας.

Στο Κεφάλαιο 4 θα μελετήσουμε λεπτομερειακά τα θέματα ΑΣΦΑΛΕΙΑΣ που προκύπτουν κατά το σχεδιασμό διαδικασιών ηλεκτρονικών υπηρεσιών (Κεφάλαιο 3).

Αναλυτικά στην ενότητα 4.2 μελετώνται τα θέματα ασφαλείας (προβλήματα, απειλές ή και κινδύνους) και οι μηχανισμοί ασφαλείας σε εφαρμογή του διαδικτύου, στην ενότητα 4.3 μελετώνται τα θέματα ασφαλείας (προβλήματα, απειλές ή και κινδύνους) και οι μηχανισμοί ασφαλείας σε εφαρμογή του δικτύου υλοποίησης VPN με τα ασύρματα πρωτόκολλα εφαρμογής GPRS.

Στο Κεφάλαιο 5 η διατριβή ολοκληρώνεται με τη καταγραφή γενικών συμπερασμάτων καθώς και μερικά ζητήματα για μελλοντική έρευνα.

# Κεφάλαιο 2

# Συναφές ερευνητικό έργο

## 2.1 Ορισμοί

### 2.1.1 Κινητό Ηλεκτρονικό Επιχειρείν ( m-business)

Ο όρος «κινητό Ηλεκτρονικό επιχειρείν (m-business) αναφέρεται σε ένα ευρύ φάσμα εφαρμογών που συσχετίζονται με την ασύρματη δικτύωση, τις ασύρματες τηλεπικοινωνίες και περιλαμβάνουν από την επικοινωνία και τις υπηρεσίες πληροφόρησης μέσω ασύρματης συσκευής, μέχρι τις καταναλωτικές συναλλαγές και στις κινητές επιχειρηματικές εφαρμογές.

Ο Επιστημονικός χώρος του Κινητού Ηλεκτρονικού Επιχειρείν είναι ένας χώρος τεχνολογικής και επιχειρηματικής αιχμής αλλά και υψίστου ακαδημαϊκού ενδιαφέροντος σε ευρωπαϊκή αλλά και σε παγκόσμια κλίμακα.

Ως μια πολυδιάστατη περιοχή αποτελείται από τέσσερις βασικούς επιστημονικούς άξονες :

- Τεχνολογίες
- Εφαρμογές και υπηρεσίες
- Κοινωνικοοικονομικές επιπτώσεις
- Επιχειρηματικά μοντέλα

### 2.1.2 Κινητή Δύναμη (Mobile Force)

Η Κινητή Δύναμη (Mobile Force) είναι μια εφαρμογή που εκμεταλλεύεται τόσο τις δυνατότητες των δικτύων και τα δίκτυα κινητής τηλεφωνίας GP όσο και αυτές των «έξυπνων» ψηφιακών βοηθών (Personal Data Assistants-PDA). Αποτελείται από μια

σειρά υποσυστημάτων που καθιστούν δυνατή την αυτοματοποίηση όλων των διαδικασιών ανάπτυξης αγοράς.

Με την Κινητή δύναμη (Mobile Force) για παράδειγμα οι πωλητές μιας εταιρίας τροφίμων αποστέλλουν άμεσα (On-Line) στο εταιρικό δίκτυο τις παραγγελίες που λαμβάνουν στα διάφορα σημεία πώλησης. Με τον τρόπο αυτό, ενημερώνεται μέσα σε ελάχιστα δευτερόλεπτα η αποθήκη και ξεκινά αμέσως η προετοιμασία και η αποστολή της νέας παραγγελίας. Η μείωση του χρόνου παραγγελίας και παράδοσης και γενικότερα η απλοποίηση της εφοδιαστικής αλυσίδας αποτελεί έναν από τους βασικούς στόχους όλων των εταιρειών που διανέμουν ανάλογης φύσης προϊόντα.

### 2.1.3 **Διαχείριση στόλου** (Fleet Management)

Διαχείριση στόλου (Fleet Management) καλείται το σύνολο των τεχνολογιών και των συστημάτων το οποίο επιτρέπει σε μία επιχείρηση να έχει πλήρη έλεγχο των οχημάτων της. Ο τρόπος λειτουργίας ενός τέτοιου συστήματος αποσκοπεί στη βελτιστοποίηση αρκετών επιμέρους επιχειρηματικών διαδικασιών, στο διαχειριστικό έλεγχο και κατά συνέπεια, στη μείωση του κόστους και την καλύτερη κατανομή των πόρων της επιχείρησης.

### 2.1.4 **Εικονικό ιδιωτικό δίκτυο** (Virtual Private Network-VPN)

Ένα Ιδεατό Δίκτυο (Virtual Private Network-VPN) είναι ένα περιβάλλον επικοινωνίας στο οποίο η πρόσβαση ελέγχεται με τέτοιο τρόπο ώστε να επιτρέπει συνδέσεις μεταξύ μελών μιας ορισμένης περιοχής ενδιαφέροντος.

Η έννοια της Ιδεατής σημαίνει ότι κάθε φορά τα δεδομένα που αποστέλλονται μπορεί να ακολουθούν διαφορετική διαδρομή μέχρι να φτάσουν στον προορισμό τους. Εκτός από την έννοια του Ιδεατού υπάρχει και ή έννοια της κρυπτογράφησης που χαρακτηρίζει τη λειτουργία ενός VPN. Η κρυπτογράφηση αφορά τη μετατροπή του εκάστοτε μηνύματος σε μια μορφή που είναι δύσκολο ή αδύνατον να κατανοηθεί από κάποιον τρίτο εκτός από τον δέκτη.

Η υλοποίηση ενός VPN πρέπει να υποστηρίζει τα χαρακτηριστικά:

- Διαθεσιμότητα (Availability)
- Έλεγχος (Control)
- Συμβατότητα (Compatibility)
- Ασφάλεια (Security): Εδώ αναφερόμαστε σε όλες τις ενέργειες που εκτελούνται από τα στοιχεία του VPN, όπως για παράδειγμα είναι η διαδικασία κρυπτογράφησης των δεδομένων ή η διαδικασία πιστοποίησης των χρηστών του δικτυού.
- Διαλειτουργικότητα (Interoperability)
- Αξιοπιστία (Reliability)
- Πιστοποίηση δεδομένων και χρηστών (Data and User authentication)
- Nonrepudiation

### 2.1.5 Secure Socket Layer (SSL)

Υλοποιώντας ασφάλεια πάνω από το επίπεδο μεταφοράς (Transport Layer) μπορούμε να παρέχουμε προστασία σε όλες τις εφαρμογές που χρησιμοποιούν το επίπεδο αυτό. Έχουμε δύο μηχανισμοί έχουν αναπτυχθεί πάνω σ'αυτό το επίπεδο: το *Secure Socket Layer* (SSL) *και το Transport Layer Security* (TLS). Το SSL παρέχει αξιόπιστη end-to-end ασφαλή υπηρεσία. Το SSL δεν είναι ένα πρωτόκολλο αλλά δύο επίπεδα πρωτοκόλλων, όπως φαίνεται παρακάτω.

| **SSL Handshake Protocol** | **SSL Change Cipher Spec Protocol** | **SSL Alert protocol** | **HTTP** |
|---|---|---|---|
| **SSL Record Protocol** | | | |
| **TCP** | | | |
| **IP** | | | |

Το SSL Record Protocol παρέχει βασικές υπηρεσίες ασφαλείας σε διάφορα πρωτόκολλα υψηλότερων επιπέδων, όπως το HTTP. Τα τρία πρωτόκολλα υψηλότερων επιπέδων ορίζονται ως μέρη του SSL και υποστηρίζουν τη διαχείριση του SSL

ανταλλαγών: το Handshake Protocol, το Change Cipher Spec Protocol και το Alert Protocol.

Οι διαδικτυακές επικοινωνίες προστατεύονται καθώς επιτυγχάνεται :

- Επικύρωση της ταυτότητας του Εξυπηρετητή (Server) (ή και του πελάτη)
- Μυστικότητα χρησιμοποιώντας κρυπτογράφηση δεδομένων.
- Ακεραιότητα δεδομένων.
- Αυθεντικοποιήση του Εξυπηρετητή ή και του πελάτη μέσω των ψηφιακών πιστοποιητικών.

### 2.1.6 Internet Protocol Security (IPsec)

Το Internet Protocol Security (IPsec) είναι ένα σύνολο πρωτοκόλλων ανοιχτών προδιαγραφών για τη διασφάλιση του απόρρητου των επικοινωνιών. Το IPsec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο και παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη λύσεων ασφαλείας σε ένα δίκτυο. Αξίζει να σημειωθεί πως τα πρωτόκολλα του IPsec χρησιμοποιούνται για την υλοποίηση Εικονικών Ιδιωτικών Δικτύων (VPNs)

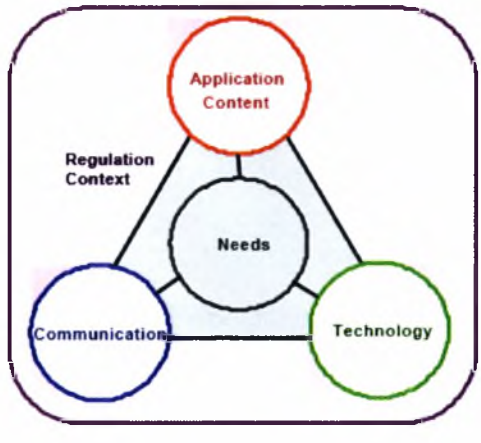
Οι υπηρεσίες ασφαλείας που προσφέρει το IPsec είναι οι ακόλουθες :

- Περιορισμός πρόσβασης. Αποτρέπει τη μη εξουσιοδοτημένη χρήση ενός πόρου.
- Πιστοποίηση. Εξασφαλίζει την πιστοποίηση της προέλευσης των δεδομένων. Δηλαδή την διαβεβαίωση ότι τα δεδομένα ήρθαν από τον αρχικό παραλήπτη χωρίς παραποίηση.
- Εμπιστευτικότητα. Το IPsec προστατεύει από την παράνομη αποκάλυψη όλα τα δεδομένα των ανώτερων επιπέδων εφαρμόζοντας κρυπτογράφηση.

- Ακεραιότητα. Το IPsec υποστηρίζει δύο μορφές ακεραιότητας , την ακεραιότητα του κάθε πακέτου και την προστασία από την πολλαπλή αποστολή των ίδιων πακέτων.

## 2.2 Κινητή επιχείρηση και ηλεκτρονικό εμπόριο (Mobile Business and E-business)

Η κινητή επιχείρηση είναι μια νέα ελπιδοφόρος επιχείρηση που δημιουργείται από την εμφάνιση των ασύρματων δικτύων δεδομένων. Υπάρχουν μερικές στρατηγικές αβεβαιότητες, όπου ένας μεγάλος αριθμός χειριστών δοκιμάζει διάφορες στρατηγικές προσεγγίσεις για να τοποθετηθεί στην ευνοϊκότερη θέση στο σύστημα αξίας. Σκοπός είναι να εφαρμοστούν τα επιχειρησιακά πρότυπα προκειμένου να γίνουν κατανοητές, οι στρατηγικές προσεγγίσεις αυτών των χειριστών.




***Σχήμα 2:*** *Mbusiness framework*

Στο κέντρο μιας κινητής επιχείρησης είναι οι χρήστες, οι οποίοι έχουν κινητικότητα σχετική με τις ανάγκες τους. Προκειμένου να εκπληρωθούν αυτές οι ανάγκες, χρειαζόμαστε τρία απαραίτητα και συμπληρωματικά χαρακτηριστικά: *επικοινωνία* (συμπεριλαμβανομένου διαφορετικά δίκτυα που παρέχουν τη μετάδοση ), *τεχνολογία* (που συντίθεται ικανότητα από όλο απαραίτητο υλικό, συμπεριλαμβανομένου του εξοπλισμού δικτύων, κινητές συσκευές και πλατφόρμες)

και οι *υπηρεσίες* (συμπεριλαμβανομένων των εφαρμογών, του περιεχομένου και της υποστήριξης υπηρεσίας). Αυτά τα χαρακτηριστικά περιορίζονται από τους κανονισμούς και τα κοινωνικά πλαίσια. [12],[13]

### 2.2.1 Ασύρματη ασφάλεια της ηλεκτρονικής επιχείρησης (Wireless Security for e-business)

Σε τέτοιες υπηρεσίες η ασφάλεια είναι ένα μεγάλο ζήτημα που πρέπει να δώσουμε την μεγαλύτερη προσοχή. Είναι σημαντικό να προστατέψουμε την ακεραιότητα των στοιχείων. Η επικύρωση των χρηστών θα πρέπει να γίνεται με την χρήση ψηφιακών πιστοποιητικών [3].

### 2.2.2 Ασύρματη ασφάλεια location based υπηρεσιών (Wireless Security for Location Based Services)

Οι Location Based υπηρεσίες (LBS) είναι ένα ευρύ φάσμα υπηρεσιών που προκύπτουν από τις τεχνολογίες γεωγραφικών συστημάτων πληροφοριών-Geographical Information System (GIS) και από τα Παγκόσμια συστήματα προσδιορισμού θέσης-Global Positioning System (GPS). Οι LBS είναι ικανές να παρέχουν χωρικές πληροφορίες σε κινητούς χρήστες. [14],[4]. Γενικά, ένα ασύρματο σύστημα επικοινωνιών αποτελείται από τρία κύρια συστατικά: Mobile Switching Centres (Msc) ή κεντρικός εξοπλισμός επεξεργασίας, οι σταθμοί βάσεων και τα μικροτηλέφωνα χρηστών. Οι σταθμοί βάσεων είναι οι "συνδέσεις" μεταξύ του Msc και των μικροτηλεφώνων. Ένας σταθμός βάσεων διαχειρίζεται ένα κύτταρο μέσα σε ένα ασύρματο δίκτυο τηλεφωνίας, που περιέχει πολλά κινητά μικροτηλέφωνα. Ο σταθμός βάσεων περιλαμβάνει χαρακτηριστικά μια μονάδα ελέγχου, έναν ράδιο εξοπλισμό σταθμών βάσεων και μια κεραία. Τα κινητά μικροτηλέφωνα μπορούν να είναι τηλέφωνα κυττάρων ή μικρές φορητές συσκευές υπολογισμού γνωστά ως προσωπικοί ψηφιακοί βοηθοί (PDA). Ένα κινητό μικροτηλέφωνο αποτελείται από έναν έλεγχο/μια μονάδα διεπαφών, έναν πομποδέκτη και ένα σύστημα κεραιών. Ενώ οι LBS

υπόσχονται κέρδη αποδοτικότητας και αποτελεσματικότητας, η χρήση τους επίσης προκύπτει από τα θεμελιώδη ζητήματα μυστικότητας.

Ένα τέτοιο ζήτημα είναι η *ασύρματη μυστικότητα*. Οι κινητές υπηρεσίες πρέπει να συμμορφωθούν με τους νόμους προστασίας των δεδομένων. Εδώ οι χρήστες γνωρίζουν λιγότερο ότι αποκαλύπτουν τις ιδιωτικές πληροφορίες. Στη χειρότερη περίπτωση, η θέση του κινητού συνδρομητή θα μπορούσε να καθοριστεί χωρίς τη γνώση του ατόμου. Το γεγονός ότι τα άτομα μπορούν να μην γνωρίζουν τις ιδιωτικές πληροφορίες που αποκαλύπτουν είναι ένα πρόβλημα που έχει συχνάσει τις υπηρεσίες διαδικτύου για κάποιο χρόνο [11],[6].

## 2.3 Θέματα Ασφαλείας, Προβλήματα και λύσεις

Σε αυτό το χωρίο του κεφαλαίου θα επιχειρήσουμε να εστιάσουμε εμπεριστατωμένα στα θέματα ασφαλείας, αλλά και σε προβλήματα και απειλές που προκύπτουν από τα διαγράμματα της συγκεκριμένης υπηρεσίας. Όταν λέμε «θέματα ασφαλείας» εννοούμε τις απειλές ενός πληροφοριακού συστήματος (ΠΣ) με δυνητικό κίνδυνο την μη εξουσιοδοτημένη πρόσβαση, την αποκάλυψη πληροφοριών, την χρήση, την κλοπή ή την καταγραφή των πόρων των συστήματος.

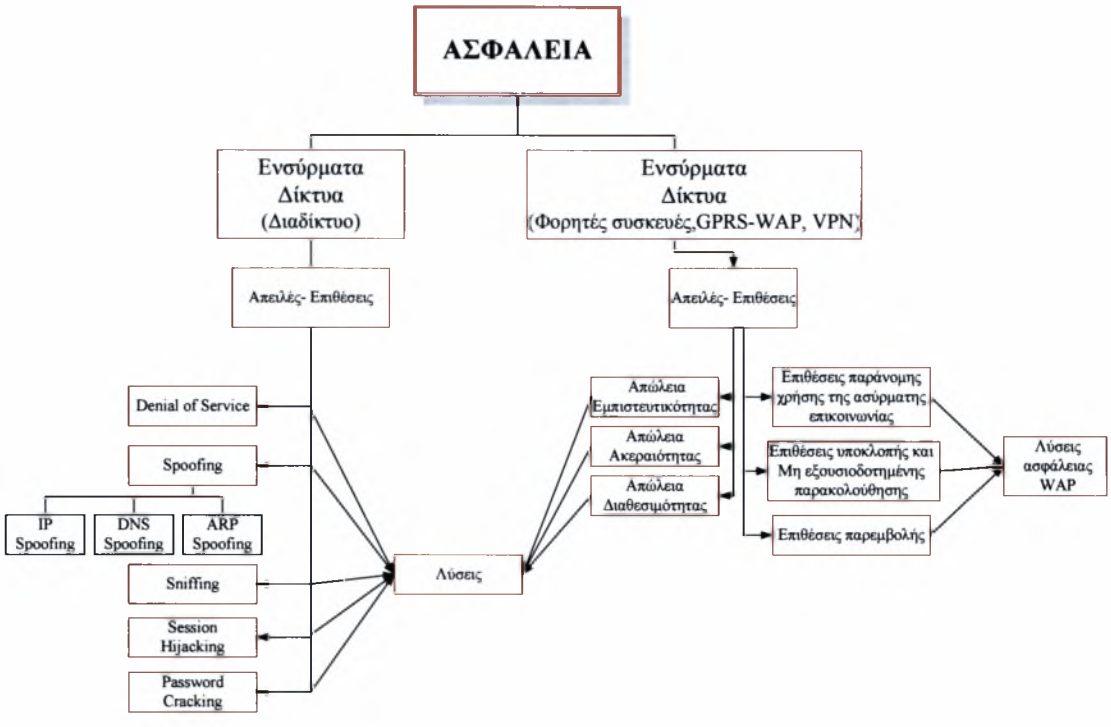
Ανάλογα με τους πόρους ενός ΠΣ, δηλαδή το υλικό (hardware), το λογισμικό (software) και τα δεδομένα (data), διακρίνουμε τα ακόλουθα είδη απειλών:

- Υποκλοπή (Interception): κάποιο μη-εξουσιοδοτημένο μέρος έχει καταφέρει να αποκτήσει προσπέλαση σε ένα τμήμα του συστήματος. Για παράδειγμα η υποκλοπής γραμμής με σκοπό την απόκτηση δεδομένων. Πρόκειται για απειλή κυρίως κατά της εμπιστευτικότητας.
- Μεταβολή (Modification): κάποιο μη-εξουσιοδοτημένο μέρος δεν έχει καταφέρει να αποκτήσει πρόσβαση αλλά επιπλέον παραποιεί το λογισμικό ή τα δεδομένα. Για παράδειγμα η τροποποίηση ενός προγράμματος από έναν ιό. Πρόκειται για απειλή κατά της ακεραιότητας.
- Πλαστογραφία (Fabrication): είναι απειλή αποκλειστικά ενάντια στα δεδομένα του συστήματος και συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος εισάγει

επιπρόσθετα – παραποιημένα δεδομένα σε ένα ΠΣ. Πρόκειται για απειλή κατά της ακεραιότητας και της διαθεσιμότητας του συστήματος.

- Πλαστοπροσωπία (Impersonation): Οι πληροφορίες πηγαίνουν σε ένα πρόσωπο που παριστάνει το νόμιμο αποδέκτη. Χρησιμοποιείται ο όρος προσποίηση (spoofing) για τη περιγραφή της κατάστασης όπου κάποιος ή κάτι επιχειρεί να φανεί σαν κάποιος ή κάτι άλλο.
- Διακοπή (Interruption): ένα μέρος του συστήματος γίνεται μη-διαθέσιμο ή άχρηστο ή χάνεται εντελώς. Για παράδειγμα είναι το σβήσιμο προγραμμάτων ή αρχείων. Πρόκειται κυρίως για απειλή κατά της διαθεσιμότητας του συστήματος. Ο όρος άρνηση εξυπηρέτησης (Denial of Service) περιγράφει συνήθως μια επιτυχημένη επίθεση διακοπής. Δηλαδή είναι αντίθετος του όρου διαθεσιμότητα.
- Παρουσίαση Πληροφοριών (Information Browsing): η αποκάλυψη ευαίσθητων πληροφοριών σε μη εξουσιοδοτημένους χρήστες, είτε πρόκειται για νόμιμους χρήστες είτε για κάποιους επίδοξους εισβολής.
- Κατάχρηση (Misuse): η χρήση των πληροφοριακών αγαθών αλλά και των υπόλοιπων πόρων για σκοπούς διαφορετικούς από αυτούς που έχουν προκαθοριστεί.
- Διαστρέβλωση (Penetration): οι προσπάθειες ενός χρήστη που παρανομεί, να μεταμφιεστεί σαν ένας χρήστες με εξουσιοδοτήσεις τέτοιες ώστε να μπορεί να κλέψει πληροφορίες ή να εκμεταλλευτεί υπηρεσίες ή να εκκινήσει συναλλαγές που προκαλούν οικονομικές απώλειες ή δυσχέρειες σε ένα δίκτυο.
- Παραποίηση (Tampering): οι πληροφορίες παραμένουν ανέγγιχτες, αλλά παραβιάζεται η εμπιστευτικότητα τους, όπως για παράδειγμα η καταγραφή μια ιδιωτικής συζήτησης [22].

Εφόσον καταγράψαμε επιφανειακά τις κατηγορίες των απειλών θα επιδιώξουμε στην συνέχεια της υπό ενότητας του κεφαλαίου να αναλύσουμε τα θέματα ασφαλείας, συνάμα με τα προβλήματα ή και τους κινδύνους που βρίσκουν εφαρμογές είτε σε ενσύρματα δίκτυα (internet) είτε σε ασύρματα δίκτυα (GPRS και VPN), πάντα υπό το πρίσμα κάποιων χαρακτηριστικών (όπως φαίνεται στο παρακάτω ιεραρχικό σχήμα).




***Σχήμα 3:*** *Επισκόπηση υπό ενότητας*

## 2.4 Ενσύρματα Δίκτυα-Διαδίκτυο (Internet-VPN)

Σήμερα με τον όρο διαδίκτυο εννοούμε το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων (Net of Nets) που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP, ενώ μπορεί να βρίσκονται εγκατεστημένα σε κάθε γωνιά του πλανήτη. Το πρωτόκολλο TCP/IP (Transmission Control Protocol / Internet Protocol), λοιπόν είναι αυτό που κατά κανόνα χρησιμοποιείται ως η προσυμφωνημένη μέθοδος επικοινωνίας και μεταγωγής δεδομένων στο Internet. Βασίζεται στη λογική του «πακέτου»: στο κόμβο του αποστολέα το μήνυμα μετάδοσης τεμαχίζεται σε μικρά τμήματα σταθερού μεγέθους τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου. Κάθε πακέτο μεταφέρει ζωτικά στοιχεία για τη δρομολόγηση του (για παράδειγμα η διεύθυνση προορισμού του) και ακολουθεί τη δική του διαδρομή μέσα στο δίκτυο. Στον κόμβο του παραλήπτη τα πακέτα συναρμολογούνται για να σχηματιστεί το αρχικό μήνυμα.

Εννοείται πως όλη η διαδικασία προϋποθέτει ότι κάθε υπολογιστής στο διαδίκτυο έχει τη δική του διεύθυνση επικοινωνίας (IP address).

Στα Πληροφοριακά Συστήματα, το διαδίκτυο προσφέρει δυνατότητες διασυνδεσιμότητας ολοκλήρωσης και επεκτασιμότητας. Επίσης αυξάνει σημαντικά τα προβλήματα προστασίας και διαθεσιμότητας των πληροφοριών. Επειδή η ασφάλεια είναι η πρώτη προτεραιότητα για τις επιχειρήσεις, για το λόγο αυτό κάθε ΠΣ που συλλέγει , αποθηκεύει, μεταδίδει πληροφορίες και παρέχει υπηρεσίες μέσου του διαδικτύου θα πρέπει να εφαρμόσει μια πολιτική ασφαλείας ικανή να εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα αυτών.

### 2.4.1 Χειρισμοί Ασφαλείας σε περιβάλλον Internet

Υπάρχουν διάφορες τεχνικές που μπορούν να εφαρμοστούν ώστε να επιτευχθεί η ασφάλεια των πληροφοριών που είναι αποθηκευμένες σε ένα σύστημα και μεταδίδονται στο διαδίκτυο. Οι χειρισμοί ασφαλείας κινούνται στις παρακάτω κατευθύνσεις :

- Έλεγχος αυθεντικότητας (Authentication)
- Εξουσιοδότηση (Authorization)
- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Μη αποποίηση ευθύνης (Non-Repudiation)
- Διαθεσιμότητα (Availability)
- Έλεγχος Προσπέλασης (Access Control)

#### 2.4.1.1 Αναγνώριση και αυθεντικοποίηση

Η αναγνώριση και η αυθεντικοποίηση είναι η διαδικασία προσδιορισμού μιας οντότητας (χρήστη, εφαρμογής η Η/Υ) και η απόδειξη της γνησιότητας της ταυτότητας που ισχυρίζεται ότι είναι. Η αυθεντικοποίηση είναι η βασική υπηρεσία ασφαλείας καθώς παρεμποδίζει την εμφάνιση μιας οντότητας ως μια άλλη εξασφαλίζοντας τη γνησιότητας ενός μηνύματος, τη νομιμότητα ενός χρήστη ή αποστολέα και την

εγκυρότητα ενός υπολογιστή. Η εφαρμογή της αποτελεί τη βάση για να επιτευχθεί έλεγχος πρόσβασης, εκχώρησης προνομίων και αρμοδιοτήτων, εφαρμογή συνυπευθυνότητα και πολιτική μη αποποίησης μιας πράξης.

Η αυθεντικοποίηση σε περιβάλλον δικτύων υπολογιστών βασίζεται σε ένα ή περισσότερα από τέσσερα παρακάτω κριτήρια:

- Από κάτι που κατέχει ο χρήστης.
- Από κάτι που γνωρίζει (συνθηματικά)
- Από προσωπικά χαρακτηριστικά
- Από κάτι που προσδιορίζει τη θέση (internet διεύθυνση)

Η πιο απλή μορφή αυθεντικοποίησης βασίζεται στην τεχνική των συνθηματικών (passwords) ενώ οι ισχυρές τεχνικές στηρίζονται σε κρυπτογραφικά συστήματα.

Σε περιβάλλον διαδικτύου η αναγνώριση και ο προσδιορισμός της ταυτότητας ενός χρήστη (ή υπολογιστή) διαφοροποιείται γιατί αρκετές φορές οι συναλλασσόμενες οντότητες δεν γνωρίζονται μεταξύ τους και δεν μπορούν έτσι να αποδείξουν ότι είναι πράγματι αυτές που ισχυρίζονται ότι είναι. Διακρίνουμε τρεις κατηγορίες αυθεντικοποίησης :

- ***Μονόδρομη αυθεντικοποίηση*** (one-way-authentication) κατά την οποία ο χρήστης δικτύου πρέπει να γνωστοποιήσει την ταυτότητα του στον υπολογιστή που πρέπει να χρησιμοποιήσει, ώστε να του επιτραπεί η προσπέλαση σε αυτόν.
- ***Αμφίδρομη αυθεντικοποίησης*** (two-way-authentication) κατά την οποία και ο χρήστης και ο υπολογιστής πρέπει να γνωστοποιήσουν ο ένας στον άλλο τις ταυτότητες τους.
- ***Αμφίδρομη αυθεντικοποίησης μέσω τρίτης έμπιστης πηγής*** (two-way authentication using trusted third party) κατά την οποία μια τρίτη οντότητα Τρίτη Έμπιστη Πηγή (ΤΕΠ) διευκολύνει τη διαδικασία αυθεντικοποίησης με την παροχή των αναγκαίων πληροφοριών-πιστοποιητικών για κάθε εμπλεκόμενο χρήστη. Απαραίτητη προϋπόθεση είναι η αποδοχή του από τα όλα τα εμπλεκόμενα μέρη, καθώς η ΤΕΠ κατέχει και διαχειρίζεται

πληροφορίες, η αποκάλυψη και τροποποίηση των οποίων συνεπάγεται την υπονόμευση του συστήματος ασφαλείας.

### 2.4.1.2 **Εξουσιοδότηση** (Authorization)

Ο έλεγχος προσπέλασης δικτύων υπολογιστών περιλαμβάνει όλους τους τυπικούς μηχανισμούς ελέγχου που διατίθενται από τα λειτουργικά συστήματα και τα συστήματα βάσεων δεδομένων καθώς και στις επεκτάσεις των ελέγχων αυτών για την προστασία των συνδέσεων μεταξύ των κόμβων ενός δικτύου και των δεδομένων που διακινούνται μέσω αυτών. Οι έλεγχοι προσπέλασης στα δεδομένα και τους υπολογιστικούς πόρους του δικτύου πρέπει να περιλαμβάνουν κάποια διαδικασία αυθεντικοποίησης του χρήστη που καθορίζεται από το επιθυμητό επίπεδο ασφαλείας.

### 2.4.1.3 **Εμπιστευτικότητα** (Confidentiality)

Εξασφάλιση της εμπιστευτικότητας στο διαδίκτυο σημαίνει ότι οι πληροφορίες που είναι αποθηκευμένες αποκαλύπτονται μόνο σε εξουσιοδοτημένους χρήστες και επιπλέον δεν απειλούνται από μη εξουσιοδοτημένη αποκάλυψη κατά την μεταφορά τους. Η έννοια της εμπιστευτικότητας των δεδομένων που διακινούνται μέσω διαδικτύου μπορεί να εφαρμοστεί καθ' ολοκληρία ή σε ένα τμήμα τους. Η επιβολή της εμπιστευτικότητας στο Internet γίνεται μέσα από πολιτικές ελέγχου πρόσβασης σε συνδυασμό με την χρήση κρυπτογραφίας και τεχνολογιών Εικονικών Ιδιωτικών Δικτύων.

### 2.4.1.4 **Ακεραιότητα** (Integrity)

Η εξασφάλιση της ακεραιότητας δεδομένων στο Internet σημαίνει ότι δεν έχουμε μετατροπή, διαγραφή και δημιουργία δεδομένων από μη εξουσιοδοτημένους χρήστες (ή με παράνομο τρόπο) κατά την μεταφορά τους ή την αποθήκευση τους. Στο διαδίκτυο για παράδειγμα είναι σημαντικό ο παραλήπτης ενός μηνύματος να είναι σίγουρος ότι το μήνυμα που έλαβε δεν έχει παραποιηθεί κατά την μεταφορά του. Ο μηχανισμός που χρησιμοποιείται ευρέως για την εξασφάλιση της ακεραιότητας των

δεδομένων κατά την μεταφορά τους είναι ψηφιακές υπογραφές, ενώ τα λειτουργικά συστήματα και τα συστήματα Βάσεων Δεδομένων είναι υπεύθυνα για την ακεραιότητα των δεδομένων κατά την αποθήκευσης τους.

### 2.4.1.5 **Μη αποποίηση ευθύνης** (Non-Repudiation)

Η προστασία από την μη-ανάληψη ενός αποστολέα ότι αυτός έστειλε συγκεκριμένα δεδομένα (Non-Repudiation of origin), καθώς και από την άρνηση ενός παραλήπτη ότι παρέλαβε κάποια δεδομένα (Non-Repudiation of delivery). Χρησιμοποιούνται οι μηχανισμοί υποστήριξης ψηφιακών πιστοποιητικών. Οι αρχές πιστοποίησης (Certification Authorities) αναλαμβάνουν την ευθύνη, ως τρίτα έμπιστα μέρα για την δημιουργία του απαραίτητου κλίματος εμπιστοσύνης μεταξύ των συμμετεχόντων μερών.

### 2.4.1.6 **Διαθεσιμότητα** (Availability)

Με την διασφάλιση της διαθεσιμότητας οι υπηρεσίες είναι διαθέσιμές και χωρίς καθυστέρηση στις εξουσιοδοτημένες οντότητες. Έτσι οι εξουσιοδοτημένες χρήστες δεν πρέπει να αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης όταν επιθυμούν να προσπελάσουν τις υπηρεσίες και τους πόρους που έχουν δικαίωμα. Η διαθεσιμότητα υπηρεσιών και πόρων σε περιβάλλον διαδικτύου απειλείται από την εξαπόλυση επιθέσεων τύπου «πλημμύρας» (SYN). Στόχος της επίθεσης αποτελεί ο εξυπηρετητής-παροχέας των υπηρεσιών και η μέθοδος που ακολουθείται είναι ο βομβαρδισμός τους με τεράστιο όγκο πληροφοριών που το καθιστούν εκτός λειτουργίας.

### 2.4.1.7 **Έλεγχος Πρόσβασης** ( Access Control)

Η προστασία ενάντια σε μη-εξουσιοδοτημένη χρήση των πόρων, είτε είναι υλικό, είτε λογισμικό, είτε είναι δεδομένα. Μηχανισμοί όπως είναι οι λίστες ελέγχου προσπέλασης (Access Control Lists-ACLs) και οι ετικέτες ασφάλεια, χρησιμοποιούνται για τον περιορισμό στη προσπέλαση των πόρων. Γενικότερα υποστηρίζουν πολιτικές ασφαλείας που παρέχουν μια πολλαπλών επιπέδων και διαφοροποιημένη προσπέλαση

πόρων στους χρήστες ανάλογα με το επίπεδο εμπιστοσύνης που μπορούν αυτοί να τεκμηριώσουν.

Τα δικαιώματα προσπέλασης είναι οι απαραίτητες πληροφορίες που συσχετίζουν ένα σύστημα πελάτη με ένα σύστημα πελάτη με ένα σύστημα διανομέα και καθορίζουν αν ο πελάτης θα αποκτήσει συγκεκριμένο τύπο προσπέλαση σε ένα συγκεκριμένο πόρο του διανομέα. Η ασφάλεια που προσφέρει ο έλεγχος πρόσβασης είναι μια αρκετά πολύπλοκη διαδικασία και μπορεί να εφαρμοστεί με διάφορους τρόπους, όπως συνθηματικά, ψηφιακές υπογραφές, firewalls.

### 2.4.2 Απειλές και κίνδυνοι της ασφάλειας σε περιβάλλον διαδικτύου

Υπάρχουν τρεις κύρια πεδία απειλών κατά της ασφαλείας πληροφοριών στο διαδίκτυο:

- *Αποθήκευση*, αναφέρεται στην προστασία των φυσικών θέσεων αποθήκευσης δεδομένων, οι οποίες μπορεί να είναι κατανεμημένες στο διαδίκτυο.
- *Πρόσβαση*, αφορά τον έλεγχο πρόσβασης των χρηστών στους πόρους του Πληροφοριακού Συστήματος (δεδομένα και συστήματα Η\Υ) και τον προσδιορισμό της ταυτότητας του χρήστη.
- *Μεταφορά*, συσχετίζεται με την προστασία των δεδομένων κατά την μεταφορά του μέσα στο διαδίκτυο.

Πιο αναλυτικά οι σημαντικότερες απειλές που πρέπει να εξετάσουμε προκειμένου να αναπτυχθεί ένα ασφαλές περιβάλλον στο διαδίκτυο, Παρουσιάζονται παρακάτω :

- Βλάβες συστατικών μερών (Component Failure). Έχει να κάνει με κακή σχεδίαση του υλικού/λογισμικού του ΠΣ με αποτέλεσμα την άρνηση εξυπηρέτησης (Denial of Service). Χαρακτηριστικό παράδειγμα αυτής της απειλής είναι η άρνηση εξυπηρέτησης ενός Web Server εξαιτίας της συμπλήρωσης των επιτρεπόμενων χρηστών.
- Παρακολούθηση των καναλιών επικοινωνίας (Monitoring of Communication Lines). Με την παρακολούθηση των καναλιών επικοινωνίας οι υποκλοπές

μπορούν να αποκτήσουν πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες παραβιάζοντας έτσι την ιδιωτικότητα (privacy).

- Πρόβλεψη του κοινού κλειδιού ( shared key guessing). Έναν κάποιος καταφέρει να υποκλέψει το κοινό κλειδί μια συμμετρικής κρυπτογράφησης επικοινωνίας, η συγκεκριμένη σύνοδος επικοινωνίας μπορεί να αποκρυπτογραφηθεί.
- Μη εξουσιοδοτημένη τροποποίηση των πληροφοριών κατά την μεταφορά (Unauthorized modification of information in transit). Πληροφορίες μπορούν να τροποποιηθούν κατά την μεταφορά τους και μάλιστα με τέτοιο τρόπο ώστε ο παραλήπτης να μην αντιληφθεί τις διενεργηθείσες μεταβολές.
- Παραποίηση Internet Διεύθυνσης (Forged Internet Addresses). Εάν δύο οντότητες στο διαδίκτυο εμπιστεύονται η μια την άλλη στο να ανταλλάσουν δεδομένα τότε είναι δυνατόν μια τρίτη οντότητα παραποιώντας την Internet διεύθυνση της να προσποιηθεί ότι είναι μια από τις «έμπιστες» οντότητες.
- Μεταμφίεση (Masquerade). Όταν ένας χρήστης υποκρίνεται ότι είναι κάποιος άλλος προκειμένου να αποκτήσει πρόσβαση σε πόρους για τους οποίους δεν έχει εξουσιοδότηση.
- Υποκλοπή συνθηματικού (Password Stealing). Όταν τα συνθηματικά πιστοποίησης των χρηστών σε ένα δημόσιο δίκτυο δεν διαβιβάζονται σε κρυπτογραφημένη μορφή, κάποιος μπορεί να τα κλέψει ( με την χρήση sniffer πρόγραμμα) και επομένως να αποκτήσει πρόσβαση σε πόρους που είναι διαθέσιμοι κανονικά μόνο στο νόμιμο ιδιοκτήτη.
- Μη εξουσιοδοτημένη πρόσβαση (Unauthorized Access). *Η μη εξουσιοδοτημένη πρόσβαση από μη νόμιμους χρήστες μπορεί να προκαλέσει μεταξύ άλλων την παράνομη αποθήκευση, αλλοίωση ή τροποποίηση στοιχείων παραβιάζοντας έτσι την ακεραιότητα και την εγκυρότητα των δεδομένων.*
- Κλοπή Ιδιωτικού Κλειδιού (Private key stealing). Με την κλοπή του ιδιωτικού κλειδιού μιας οντότητας, κάποιος μπορεί να αποκτήσει το ψηφιακό πιστοποιητικό της οντότητας με άμεση απειλή κατά της ασφάλειας των πληροφοριών για τις οποίες είναι υπεύθυνη.
- Άρνηση Εξυπηρέτησης (Denial of Service). Αυτή η απειλή έχει σαν αποτέλεσμα την μη διάθεση υπηρεσιών σε νόμιμους χρήστες. Η επίθεση

εξαπολύεται με την αποστολή μεγάλου όγκου μηνυμάτων (mails) σε μια συγκεκριμένη Internet διεύθυνση με συνέπεια να δημιουργούν προβλήματα χωρητικότητας δίσκου και να θέτουν υπηρεσίες εκτός λειτουργίας, ή με την παραγωγή ενός μεγάλου όγκου κυκλοφορίας μέσα στο δίκτυο («σκουπιδιών) που το καθιστούν τελικά μη διαθέσιμο.

Το διαδίκτυο ως μέσο ψηφιακής επικοινωνίας κρύβει έναν αριθμό από ορισμένους κινδύνους όπως :

- Έλλειψη εμπιστευτικότητας, αφού τα δεδομένα που διακινούνται είναι χωρισμένα σε πακέτα και μπορούν εύκολα να κλαπούν και να αποκαλυφθεί το περιεχόμενό τους.
- Έλλειψη μηχανισμών για την ταυτοποίηση των οντοτήτων (χρηστών) των συστημάτων.
- Έλλειψη αξιόπιστων μέσων για σύνδεση των IP διευθύνσεων με συγκεκριμένους υπολογιστές.
- Εκτεθειμένοι κωδικοί πρόσβασης. Τα περισσότερα συστήματα χρησιμοποιούν κωδικούς για την ταυτοποίηση των χρηστών, οι οποίοι τις περισσότερες φορές μεταφέρονται στο δίκτυο χωρίς να κρυπτογραφηθούν .

### 2.4.3 Προβλήματα ασφαλείας στο TCP/IP

Το Θεμελιώδες πρόβλημα της ασφάλειας πληροφοριακών συστημάτων στο διαδίκτυο είναι ότι το διαδίκτυο να είναι λειτουργικό περιβάλλον και όχι ασφαλές. Τα περισσότερα από τα προβλήματα ασφαλείας στο Internet είναι εγγενή, τα πιο χαρακτηριστικά παρουσιάζονται παρακάτω:

- Εύκολη παρακολούθηση και ανίχνευση. Όλες οι πληροφορίες που κινούνται με την μορφή πακέτων tcp/ip, μπορούν να παρακολουθήσουν εύκολα χρησιμοποιώντας ευρέως διαθέσιμο software (π.χ Sniffer). Αυτό είναι πάρα πολύ σημαντικό πρόβλημα μιας η πλειοψηφία των πληροφοριών που ανταλλάσσονται είναι μη κρυπτογραφημένες.

- Ευπαθείς Internet υπηρεσίες. Ένας αριθμός από τέτοιες υπηρεσίες δεν έχουν σχεδιαστεί να είναι ασφαλείς (π.χ. το ping) αποτελούν εύκολες πόρτες «εισόδου» για εισβολείς.
- Απουσία πολιτικής ασφαλείας. Πολλά Πληροφορικά Συστήματα στο Internet έχουν σχεδιαστεί να παρέχουν ελεύθερη πρόσβαση χωρίς να λαμβάνεται υπόψη μια πιθανή κατάχρηση των πόρων τους. Επίσης αρκετά επιτρέπουν την χρήση υπηρεσιών (π.χ anonymous ftp) που δεν είναι απαραίτητες και δεν περιορίζουν την πρόσβαση στους πόρους τους αφήνοντας έτσι τις πόρτες ανοιχτές στους εισβολείς.
- Η φύση του πρωτοκόλλου TCP/IP και των περισσότερων υπηρεσιών που υποστηρίζει, προσθέτουν νέες ευπάθειες και σημεία επιθέσεων. Το γεγονός ότι επιτρέπονται τα πακέτα των δεδομένων να περνούν από μια σειρά απρόβλεπτων ενδιάμεσων υπολογιστών και επιμέρους δικτύων μέχρι να φτάσουν στο τελικό τους προορισμό, δίνει τη δυνατότητα σε ένα τρίτο μέρος να παρέμβει με διάφορους τρόπους στην επικοινωνία δύο νόμιμων μερών.

Στην συνέχεια αξίζει να αναφερθούμε σε ορισμένα προβλήματα τα οποία απασχολούν κατά καιρούς τους διαχειριστές συστημάτων αλλά και τους χρήστες ενός TCP/IP δικτύου.

### 2.4.3.1 **Επιθέσεις Άρνησης Υπηρεσίας** (Denial of Service)

Οι επιθέσεις αυτού του είδους έχουν ως σκοπό την μείωση ή την εξάλειψη της ικανότητας ενός συστήματος να προσφέρει τις υπηρεσίες τους στους νόμιμους χρήστες. Χαρακτηριστικότερες είναι το TCP SYN Flooding επιθέσεις, οι επιθέσεις με το γνωστό πρόγραμμα και οι επιθέσεις με την χρήση του UDP. Συνήθως η δυσλειτουργία διατηρείται και για ένα αρκετά μεγάλο διάστημα μετά το πέρας της επίθεσης.

### 2.4.3.2 **Επιθέσεις Μεταμφίεσης** (Spoofing)

Κατά τις επιθέσεις αυτές ο επιτιθέμενος προσποιείται κάποιον άλλον, «μεταμφιέζεται» ώστε να αποκτήσει εξουσιοδοτημένη πρόσβαση στους πόρους του συστήματος. Οι χαρακτηριστικότερες επιθέσεις του είδους είναι το IP Spoofing, το DNS Spoofing και το ARP Spoofing.

***IP Spoofing***

Η επίθεση αυτή ουσιαστικά βασίζεται σε σχέσεις εμπιστοσύνης που υπάρχουν μεταξύ των δικτύων ή και των συστημάτων κάθε δικτύου στο internet. Γενικά ή επίθεση αυτή γίνεται από το root λογαριασμό του επιτιθέμενου host προς τον root λογαριασμό του host-θύματος.

Μια λύση θα ήταν η απενεργοποίηση των r εντολών, το σβήσιμο των αρχείων.rhosts και των περιεχομένων του αρχείου /etc/hosts.equiv. Η χρήση ενός καλά διαμορφωμένου δρομολογητή με δυνατότητες φιλτραρίσματος είναι επίσης απαραίτητη. Επιπλέον το IP Spoofing αποτρέπεται εάν όλα τα πακέτα που εισέρχονται ή εξέρχονται του δικτύου κρυπτογραφούνται ή και αυθεντικοποιούνται.

***DNS Spoofing***

Όταν το software σε έναν host χρειάζεται να μετατρέψει ένα domain όνομα σε διεύθυνση, στέλνει ένα «ερώτημα εύρεσης διεύθυνσης» σε DNS server. Όταν ένας Client συνδέεται με έναν host που διαθέτει ένα domain όνομα, ο client πρέπει να μετατρέψει το όνομα σε IP διεύθυνση. Ο client εμπιστεύεται αφενός το DNS σύστημα ώστε να επιστρέψει τη σωστή διεύθυνση, αφετέρου το σύστημα δρομολόγησης ώστε να παραδώσει τα δεδομένα στον προορισμό τους. Το ίδιο συμβαίνει και όταν ο host χρειάζεται να μετατρέψει μια IP διεύθυνση σε domain όνομα. Τότε λέμε ότι απευθύνει ένα «ερώτημα εύρεσης ονόματος» (reverse lookup query).

Ένας DNS server ενδέχεται να έχει παραβιαστεί από κάποιον cracker. Όταν γίνει αίτηση σύνδεσης με τον server μας, ο server στέλνει αίτηση στο DNS server ώστε να μάθει πιο domain name αντιστοιχεί στην αίτηση που ήλθε από μια δεδομένη IP address. Ο DNS server εάν είναι παραβιασμένος μπορεί να επιστρέψει το όνομα ενός 'έμπιστου'domain και κατ' επέκταση «έμπιστου host". Προκειμένου να ελαττωθεί ο

κίνδυνος ορισμένοι servers μπορούν να ρυθμιστούν ούτως ώστε κάνουν «έξτρα» έλεγχο για κάποιο client. Μετά δηλαδή από τον εντοπισμό (έπειτα από την αίτηση στο DNS server) του host, ο server μας στέλνει αίτηση εύρεσης της IP διεύθυνσης που αντιστοιχείς στο host όνομα. Εάν οι δύο διευθύνσεις η αρχική και η τελική, δεν συμφωνούν, η αίτηση σύνδεσης με τον server απορρίπτεται. Οι πίνακες που περιέχουν IP διευθύνσεις για συγκεκριμένα ονόματα hosts, βρίσκονται συνήθως σε διαφορετικά αρχεία και τα αρχεία αυτά βρίσκονται σε διαφορετικούς mane servers. Έτσι είναι σαφώς πιο δύσκολο για ένα cracker να ελέγχει και τους δύο DNS Servers.

***ARP Spoofing***

Το ARP (address Resolution Protocol) αποτελεί αναπόσπαστο κομμάτι του Ethernet στο επίπεδο πρόσβασης Δικτύου. Όταν ένα IP datagram είναι έτοιμο να παραδοθεί σε έναν host του Ethernet τοπικού δικτύου, host που έχει την ευθύνη να το παραδώσει, πρέπει να ξέρει τη hardware διεύθυνση προορισμού που αντιστοιχεί στην IP διεύθυνση του datagram που διαθέτει. Για μη τοπικές διευθύνσεις η hardware διεύθυνση που θα χρησιμοποιήσει είναι η διεύθυνση ενός από τους δρομολογητές στο τοπικό δίκτυο.

Προκειμένου να βρει τη hardware διεύθυνση, ο host στέλνει μια «αίτηση ARP" με προορισμό την hardware broadcast διεύθυνση. Τα πακέτα με αυτήν την διεύθυνση φθάνουν στα interfaces όλων των hosts του τοπικού δικτύου, προκαλώντας ένα interrupt στη CPU τους για περαιτέρω επεξεργασία. Λογικά μόνον ένας host με την αντίστοιχη IP διεύθυνση θα στείλει μια "απάντηση ARP" και οι υπόλοιποί hosts θα αγνοήσουν την προηγούμενη αίτηση.

Οι αντιστοιχίες μεταξύ hardware και IP διευθύνσεων στους υπολογιστές του τοπικού δικτύου αποθηκεύονται σε μια ARP cache για κάθε host. Όταν το IP datagram είναι έτοιμο να φύγει από έναν host, ο host συμβουλεύεται τον ARP πίνακα ώστε να βρει τη hardware διεύθυνση προορισμού. Εάν ο host βρει μια είσοδο (entry) για την IP διεύθυνση, τότε δε χρειάζεται να αποστείλει μια "αίτηση ARP". Οι είσοδοι στο ARP πίνακα εκπνέουν μετά από αρκετά λεπτά.

### 2.4.3.3 **Επιθέσεις Παρακολούθησης** (Sniffing)

Sniffing είναι η χρήση ενός interface δικτύου προκειμένου να ληφθούν δεδομένα τα οποία δεν προορίζονται για τον υπολογιστή στον οποίο υφίσταται το interface. Μια ποικιλία τύπων μηχανών έχουν αυτή τη δυνατότητα. Όπως για παράδειγμα μια γέφυρα σε ένα token ring δίκτυο, έχει δύο interfaces δικτύου και κανονικά λαμβάνει όλα τα δεδομένα που διέρχονται από το φυσικό μέσο στο ένα interface και μεταδίδει ορισμένα από αυτά τα πακέτα αλλά όχι όλα, στο άλλο interface. Μια άλλη συσκευή ενσωματώνει το sniffing στη λειτουργία της, είναι ένας "network analyzer". Ο analyzer βοηθάει το διαχειριστή ενός δικτύου στη διάγνωση μιας ποικιλίας προβλημάτων που μπορεί να μην είναι ορατά σε οποιονδήποτε host.

Οι συσκευές με δυνατότητες sniffing είναι χρήσιμες και απαραίτητες. Εντούτοις η ύπαρξη τους σημαίνει ότι και ένα «κακόβουλο» άτομο θα μπορούσε να τις χρησιμοποιήσει ώστε να συλλαμβάνει την κίνηση σε ένα δίκτυο. Υπάρχουν ειδικά sniffing προγράμματα ορισμένα από τα οποία είναι δωρεάν, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση:

- Passwords (συνθηματικών)
- Στοιχείων οικονομικών συναλλαγών
- Εμπιστευτικών δεδομένων
- Πληροφορίες πρωτοκόλλων χαμηλού επιπέδου

Υπάρχουν αρκετά προληπτικά μέτρα που μπορεί να λάβει ώστε να αποστρέψει μια επίθεση παρακολούθησης:

- Σωστή διαμόρφωση του δικτύου: κάθε τμήμα πρέπει να αποτελείται από μηχανές που εμπιστεύονται η μια την άλλη.
- Χρήση κρυπτογραφημένων passwords Τα passwords θα πρέπει να κρυπτογραφούνται, πριν χρησιμοποιηθούν για οποιονδήποτε λόγο.

### 2.4.3.4 **Πειρατεία Συνόδου** (Session Hijacking)

Έχοντας αποκτήσει root πρόσβαση σε ένα σύστημα, ένα cracker μπορεί να χρησιμοποιήσει κάποιο εργαλείο ώστε να μεταβάλλει το UNIX kernel. Αυτή η τροποποίηση επιτρέπει στο επιτιθέμενο να χειριστεί εξολοκλήρου ήδη υπάρχουσες συνδέσεις από οποιονδήποτε χρήστη στο σύστημα, κάνοντας ότι θα μπορούσε να κάνει και ο χρήστης. Με αυτόν τον τρόπο στο σύστημα αφού «αναλαμβάνει» τη σύνδεση του χρήστη μετά από την αυθεντικοποίηση του. Επίσης ο cracker μπορεί να αποκτήσει πρόσβαση σε απομακρυσμένα sites «αναλαμβάνοντας» τη σύνδεση αφού ο χρήστης αυθεντικοποιηθεί από απομακρυσμένο site.

### 2.4.3.5 **Επιθέσεις «σπασίματος» συνθηματικών** (password cracking)

Σήμερα υπάρχουν διαθέσιμα πολλά προγράμματα για «σπάσιμο» των passwords, διεξάγοντας επιθέσεις λεξικού, τα οποία συγκρίνουν το αρχείο των passwords ενός συστήματος με ένα λεξικό κρυπτογραφημένων passwords. Στόχος των επιθέσεων είναι κυρίως τα "αδύναμα" passwords [21],[22].

## 2.4.4 **Μηχανισμοί Ασφαλείας του πρωτοκόλλου TCP/IP και λύσεις**

Για να αντιμετωπιστούν τα προβλήματα του διαδικτύου, έχουν αναπτυχθεί από διαφόρους φορείς αρκετοί μηχανισμοί ασφαλείας που καλύπτουν διαφορές εφαρμογές. Εκμεταλλευόμενοι τα πρωτόκολλα επικοινωνίας από τα ανώτερα ιδεατά επίπεδα του TCP/IP μοντέλου, του επιπέδου διαδικτύου, μεταφοράς και εφαρμογής. Οι μηχανισμοί ασφαλείας λοιπόν, ομαδοποιήθηκαν όπως φαίνονται στο πίνακα που έπεται. Εμείς θα ασχοληθούμε κυρίως και τα επίπεδα διαδικτύου και μεταφοράς.

<table>
<tr><td>Επίπεδα</td><td colspan="5">Πρωτόκολλο</td><td colspan="3">Μηχανισμοί ασφαλείας στο διαδίκτυο</td></tr>
<tr><td rowspan="2">Επίπεδο Εφαρμογής</td><td rowspan="2">HTTP</td><td rowspan="2">SNMP</td><td rowspan="2">SMTP</td><td rowspan="2">TELNET</td><td rowspan="2">FTP</td><td>SET</td><td colspan="2">PGP</td></tr>
<tr><td>S-HTTP</td><td colspan="2">S/MIME</td></tr>
<tr><td>Επίπεδο μεταφοράς</td><td colspan="3">TCP</td><td colspan="2">UDP</td><td>SSL</td><td colspan="2">TLS</td></tr>
<tr><td rowspan="2">Επίπεδο διαδικτύου</td><td colspan="5" rowspan="2">IP</td><td colspan="3">IPSec</td></tr>
<tr><td>AH</td><td>ESP</td><td>IKE</td></tr>
</table>

Επίσης μια σημαντική τεχνολογία ασφαλείας του διαδικτύου είναι ένα σύστημα firewall. Ένα τέτοιο σύστημα προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο-εσωτερικό δίκτυο ενός οργανισμός (το οποίο θεωρείται έμπιστο) και στο εξωτερικό διαδίκτυο (το οποίο θεωρείται μη έμπιστο). Επιτρέπει τη προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά (συνθηματικά ή IP διευθύνσεις ή Domain Names). Ο κύριος στόχος του: να κρατήσει τις επικίνδυνες δραστηριότητες από το προστατευμένο δίκτυο.

Ένα firewall σε λειτουργία δεν είναι ένα συστατικό δικτύου αλλά αποτελεί την υλοποίηση μιας στρατηγικής για την προστασία των συνδεδεμένων πόρων στο διαδίκτυο ενός οργανισμού. Εξασφαλίζει ότι όλες οι επικοινωνίες από και προς το Internet είναι σύμφωνες με τη προκαθορισμένη πολιτική ασφαλείας του οργανισμού. Πρόκειται για ένα σημαντικό πλεονέκτημα. Όμως τα σπουδαία πλεονεκτήματα είναι τα επιμέρους :

- Προστατεύει από ευπαθείς υπηρεσίες δικτύων (protecting from vulnerable services). Είναι γνωστό ότι τα πρωτόκολλα επικοινωνίας του διαδικτύου παρουσιάζουν εγγενή προβλήματα ασφαλείας όπως είδαμε στο εδάφιο 2.4.3 (όπως το πρόβλημα του Spoofing), η εγκατάσταση ενός συστήματος firewall προσφέρει δυνατότητες φιλτραρίσματος που ελαχιστοποιούν τους κινδύνους. Ακόμη μπορεί και καλύπτει γνωστές ρωγμές ασφαλείας (όπως οι επιθέσεις αδυναμίες εξυπηρέτησης), έτσι κάποια σημεία για την ασφάλεια του δικτύου

πιο πιθανόν να εκμεταλλεύονται διάφοροι βάνδαλοι, έρχεται να προστατέψει το firewall.

- Αποτελεί μέσο καταγραφής και δημιουργίας στατιστικών στοιχείων για την χρήση και κατάχρηση του δικτύου (logging-alarming & statistics of network use/misuse).
- Επιβάλλει ελεγχόμενη προσπέλαση (Controlled Access) στους πόρους ενός εσωτερικού δικτύου .
- Προσφέρει διευρυμένη ιδιωτικότητα (Enhanced Privacy). Το firewall αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου. Γενικά υπάρχουν πάντοτε πληροφορίες που ενώ θεωρούνται αβλαβείς περιέχουν σημαντικά στοιχεία για κάποιο που θέλει να κάνει μια επίθεση. Επομένως μέσω του firewall,πολλοί οργανισμοί σταματούν υπηρεσίες όπως finger και η DNS (Domain Name Service). Η πρώτη δίνει πληροφορίες στου χρήστες πότε συνδέθηκαν, αν έχουνε διαβάσει το e-mail του. Η υπηρεσία DNS από την άλλη παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος όπως τα ονόματα των τόπων και IP διευθύνσεις του.
- Προσφέρουν ως μια επιπλέον λειτουργία και τις υπηρεσίες του ως πύλες κρυπτογράφησης (encrypting gateways). Δηλαδή έχουν ταυτόχρονα δυνατότητες κρυπτογράφησης στις επικοινωνίες μεταξύ των διακομιστών που προστατεύουν. Επίσης και εξωτερικά συστήματα μπορούν να «συνομιλήσουν» σε κρυπτογραφημένη μορφή. Ένας τέτοιος λογικός διαχωρισμός των δικτύων (firewall και τεχνικών κρυπτογράφησης δημιουργεί τα εικονικά ιδιωτικά δίκτυα (VPN-Virtual Private Networks).

Συνοπτικά ένα σύστημα firewall πρέπει να είναι ικανό να προσφέρει υπηρεσίες ασφαλείας ελέγχου προσπέλασης (access control), συνδυάζοντας μηχανισμούς αυθεντικοποίησης (authentication), εξουσιοδότησης (authorization), επίβλεψης (auditing) και όπου είναι δυνατόν και κρυπτογράφηση (encryption) [21].

### 2.4.4.1 Ασφάλεια από την πλευρά του εξυπηρετητή

Πρόκειται για μέτρα που προστατεύουν τον εξυπηρετητή του διαδικτύου και τη μηχανή που τρέχει πάνω σε αυτόν από παραβιάσεις, βανδαλισμούς χώρων και άρνηση από επιθέσεις υπηρεσιών. Ένα τέτοιο μέτρο είναι ο *έλεγχος πρόσβασης*.

Ο έλεγχος πρόσβασης απαρτίζεται από την *πιστοποίηση του χρήστη* και τη *εξουσιοδότηση του χρήστη*. Η πιστοποίηση του χρήστη είναι η διεργασία κατά την οποία αναγνωρίζεται το άτομο καθώς συνδέεται στο διαδίκτυο. Εφόσον ο χρηστής πιστοποιηθεί έχει δικαιώματα πρόσβασης. Παρακάτω θα δούμε μερικούς τύπους ελέγχου πρόσβασης:

- *Έλεγχος Πρόσβασης Βασισμένος σε IP Διεύθυνση*. Βασίζεται στο DNS όνομα και την διεύθυνση του browser. Οι browser που καλούν από εξουσιοδοτημένες διευθύνσεις επιτρέπονται να εισέλθουν. Στους άλλους αρνείται. Για να μειώσουμε τις επιθέσεις του spoofing DNS, μπορούμε να διαμορφώσουμε «παρανοϊκό έλεγχο του DNS. Όταν μια εισερχόμενη σύνδεση φτάνει ο εξυπηρετητής βγάζει έξω την IP διεύθυνση του browser από τις πληροφορίες επικεφαλίδας του TCP/IP και μετά κάνει δύο κλήσεις στο DNS σύστημα. Πρώτα ο εξυπηρετητής ζητά από το DNS να επιστρέψει το όνομα του κεντρικού υπολογιστή που έχει καταχωρηθεί για την IP διεύθυνση. Ύστερα ζητά από τον DNS σύστημα την IP διεύθυνση του κεντρικού υπολογιστή που μόλις έχει επιστραφεί. Για τεχνικούς λόγους είναι πιο εύκολο να παραπλανηθεί το κομμάτι του DNS που μεταφράζει τα ονόματα των κεντρικών υπολογιστών σε IP διευθύνσεις. Αν η IP διεύθυνση που έχει επιστραφεί από το DNS σύστημα στη δεύτερη αναζήτηση συμπίπτει με την αυθεντική IP διεύθυνση του browser, η πιθανότητα ο browser να είναι απατηλός είναι μικρή.
- Έλεγχος Πρόσβασης Βασισμένος στο όνομα χρήστη και στον κωδικό προσπέλασης. Κάθε χρήστης ανατίθεται σε ένα ID χρήστη και σε ένα κωδικό προσπέλασης. Για να χρησιμοποιηθεί ως ψηφιακή υπογραφή. Το πιστοποιητικό μπορεί να παρέχεται είτε από μια έμπιστη Τρίτη εταιρεία είτε από κάποιον οργανισμό.
- Έλεγχος Πρόσβασης Βασισμένος στα πιστοποιητικά. Παρόλο που οι κωδικοί προσπέλασης είναι ένας απλός και αποτελεσματικός τρόπος για να προσδιοριστούν οι χρήστες του διαδικτύου, η ασφάλεια τους είναι περιορισμένη από τα συνδυασμένα προβλήματα της επιλογής καλού κωδικού

προσπέλασης της υποκλοπής κωδικών προσπέλασης της υποκλοπής κωδικών προσπέλασης της υποκλοπής κωδικών προσπέλασης και την ευκολία με την οποία οι άνθρωποι τα μοιράζονται. Ένα σύστημα κωδικών προσπέλασης που δουλεύει καλά με ένα εξυπηρετητή του διαδικτύου και μερικούς εκατοντάδες χρήστες γίνεται μη διαχειρίσιμος απέναντι σε μια επιχείρηση δωδεκάδων εξυπηρετητών και χιλιάδων χρηστών. Για αυτό το λόγο οι SSL εξυπηρετητής μπορούν να πιστοποιήσουν τους browsers με βάση τα πιστοποιητικά των πελατών. Ο έλεγχος πρόσβασης βασίζεται μόνο στις πληροφορίες που περιέχονται μέσα στα χαρακτηριστικά του πιστοποιητικού. [23]

- Υπηρεσία Kerberos. Παρέχει κεντρικοποιημένο authentication εξυπηρετητή, η δουλεία είναι να πιστοποιεί την αυθεντικότητα των χρηστών προς τους εξυπηρετητές και των εξυπηρετητών προς του χρήστες.

### 2.4.4.2 Ασφάλεια από την πλευρά του χρήστη

Λύσεις ασφαλείας από την πλευρά του χρήστη για την υποστήριξη ηλεκτρονικών υπηρεσιών στο διαδίκτυο είναι :

- SSL (Secure Socket Layer) Στα εδάφια 2.15 και 2.4.3 αντίστοιχα, αναφέραμε ποιες υπηρεσίες παρέχει και ποια κριτήρια υλοποίησης. Σε αυτή τη ενότητα θα αναφέρουμε τον τρόπο λειτουργίας. Το SSL συνεπώς χρησιμοποιεί την RSA κρυπτογράφηση δημοσίου κλειδιού για να εξασφαλίσει την ασφαλή μετάδοση. Αυτού του είδους η κρυπτογράφηση ένα ζεύγος κλειδιών το δημόσιο για την κρυπτογράφηση και το ιδιωτικό για την αποκρυπτογράφηση. Ένα διαφορετικό κλειδί συνόδου (session key) χρησιμοποιείται σε κάθε πελάτη / εξυπηρετητή. Για την κρυπτογράφηση της συνόδου το SSL χρησιμοποιεί την συμμετρική κρυπτογραφία που είναι πιο γρήγορη.[22]
- Κρυπτογράφηση.

### 2.4.4.3 Άλλες λύσεις ασφαλείας

Μια άλλη σημαντική λύση ασφαλείας είναι η υλοποίηση του Εικονικού ιδιωτικού δικτύου (Virtual Private Network, VPN). Το VPN καλύπτει το πρόβλημα της κρυπτογράφησης των δεδομένων. Επίσης το Quality of Service, τη χαμηλή διαθεσιμότητα, η αξιοπιστία του δικτύου, η χρήση τρόπων διευθυνσιοδότησης.

Για να υλοποιήσουμε ένα VPN χρησιμοποιούμε το IPsec σε μέθοδο σήραγγας και ενεργοποιώντας τις υπηρεσίες κρυπτογράφησης και αυθεντικοποίησης. Το IPsec δίνει τη δυνατότητα να δημιουργήσουμε μια σύνδεση μεταξύ δύο ασφαλών πυλών, η μια στο ένα δίκτυο και η άλλη στο άλλο, και μέσω αυτών των ασφαλών πυλών να διοχετεύουμε όλη την κίνηση από το ένα δίκτυο προς το άλλο. Έτσι τα δεδομένα διακινούνται κρυπτογραφημένα και χωρίς να εμφανίζεται στο δημόσιο δίκτυο η εσωτερική δομή των δύο υπό-δικτύων.

*Το δικτυακά συστήματα ανίχνευσης εισβολέων* (Network Intrusion Detection System-NIDS) είναι μια τεχνολογία που μπορεί να χρησιμοποιηθεί για να μειώσει τον κίνδυνο που συνδέεται με την επέκταση της περιμέτρου ασφάλειας. Το NIDS πραγματοποιεί δύο αρχικές λειτουργίες στα σχέδια VPN. Κατά αρχάς, NIDS μπορεί να χρησιμοποιηθεί για να αναλύσει την κυκλοφορία που έρχεται από, ή προς, τη συσκευή VPN πριν από την κρυπτογράφηση. Ένα NIDS θα ανιχνεύσει τις επιθέσεις που προέρχονται μέσω του VPN από τις μακρινές περιοχές ή τους μακρινούς χρήστες. Επειδή ξέρουμε την προέλευση αυτής της δικτυακής κίνησης, και οι πιθανότητες ότι είναι χαμηλές, οποιαδήποτε επίθεση μπορεί να αντιμετωπίσει μια ισχυρή απάντηση από το NIDS. Ένα NIDS είναι κρίσιμο στα περισσότερα περιβάλλοντα VPN. Αυτή η οργάνωση αυξάνει την εμπιστοσύνη σε NIDS στη σύλληψη και τη στάση οι περισσότερες από τις επιθέσεις από τις μακρινούς περιοχές ή τους χρήστες. Επίσης NIDS μπορεί να χρησιμοποιηθεί μετά από την κρυπτογράφηση που επικυρώνει ότι μόνο η κρυπτογραφημένη κυκλοφορία στέλνεται και παραλαμβάνεται από VPN τις συσκευές. Με το συντονισμό ενός NIDS στο συναγερμό σε οποιοδήποτε πακέτο μη-vpn, μπορούν να επικυρωθούν μόνο τα κρυπτογραφημένα πακέτα ρέουν πέρα από το δίκτυο. Αυτή η οργάνωση προστατεύει από οποιοδήποτε λανθασμένη διαμόρφωση δικτύου των συσκευών VPN που θα μπορούσαν ακούσια να επιτρέψουν τη κυκλοφορία μέσω της συσκευής. Αυτή η λειτουργία απαιτείται λεπτομερέστερα στο μεγάλο σχέδιο δικτύων VPN.

## 2.5 Χαρακτηριστικά Φορητών Συσκευών

Πρόκειται για συσκευές εισαγωγής μηνύματος κείμενου , PDAs, και έξυπνα τηλέφωνα. Η χρήση αυτών των συσκευών εισάγει τους νέους κινδύνους ασφάλειας για το υπάρχον δίκτυο μιας αντιπροσωπείας. Επιπλέον, δεδομένου ότι αυτές οι συσκευές ορίζουν τις διευθύνσεις IP τους, οι συσκευές οι ίδιες μπορούν να γίνουν οι στόχοι των επιθέσεων. Οι διαφορές μεταξύ των φορητών συσκευών και των desktop υπολογιστών που έχουν επιπτώσεις στην ασφάλεια της αντιπροσωπείας συνοψίζονται παρακάτω :

- Το μικρό μέγεθος, το σχετικά χαμηλό κόστος, και η κινητικότητα των φορητών συσκευών τις καθιστούν πιθανότερες να κλαπούν, να τοποθετηθούν σε λάθος μέρος, ή να χαθούν.
- Οι φυσικοί έλεγχοι ασφάλειας που προστατεύουν τους desktop υπολογιστές δεν προσφέρουν την ίδια προστασία για τις φορητές συσκευές. Δεν ψάχνουν φυσικά τους ανθρώπους κατόχους των φορητών συσκευών.
- Οι συσκευές οι ίδιες έχουν περιορίσει την ισχύ, τη μνήμη, και τις περιφερειακές μονάδες υπολογισμού που καθιστούν τα υπάρχοντα αντίμετρα ασφάλειας για desktop μη πρακτικά για τις φορητές συσκευές.
- Τα μέλη μιας οργάνωσης αγοράζουν συχνά και χρησιμοποιούν τις φορητές συσκευές χωρίς τη διαβούλευση ή την ειδοποίηση του διοικητή δικτύων της οργάνωσης. Οι ασύρματες φορητές συσκευές χρησιμοποιούνται συχνά και για τα προσωπικά και επιχειρησιακά στοιχεία.
- Πολλοί χρήστες έχουν περιορισμένη συνείδηση ή κατάρτιση ασφάλειας .
- Οι χρήστες φορητών συσκευών μπορούν να 'κατεβάσουν' διάφορα προγράμματα παραγωγικότητας, προγράμματα συνδετικότητας, παιχνίδια, και βοηθήματα -- συμπεριλαμβανομένων των προγραμμάτων δωρεάν λογισμικού και διανεμόμενων λογισμικών -- από τις untrusted πηγές.
- Υπάρχουν λίγες δυνατότητες ελέγχου ασφάλειας ή εργαλεία ασφάλειας διαθέσιμα για πολλές από αυτές τις συσκευές.
- Οι χρήστες προσυπογράφουν συχνά στους ασύρματους προμηθευτές υπηρεσίας Διαδικτύου τρίτων (WISP) και έχουν πρόσβαση στο Διαδίκτυο μέσω των ασύρματων modem. Οι χρήστες μπορούν να μεταφορτώσουν ή να φορτώσουν

τα στοιχεία σε άλλους υπολογιστές χωρίς τη συμμόρφωση με την πολιτική firewall της οργάνωσης.

### 2.5.1 Τα χαρακτηριστικά του ασυρμάτου πρωτοκόλλου εφαρμογής (GPRS-WAP)

Το WAP είναι ένα πρωτόκολλο που έχει βελτιστοποιηθεί για τις κινητές συσκευές. Μια αρχική έννοια που η προδιαγραφή WAP έχει υιοθετήσει είναι η έννοια της διάταξης σε στρώματα του πρωτοκόλλου. Η διάταξη σε στρώματα είναι η έννοια του χωρισμού ολόκληρης της διαδικασίας επικοινωνίας σε διακριτά κομμάτια. Κάθε ένα από αυτά τα κομμάτια χειρίζεται μια συγκεκριμένη λειτουργία.

Η προδιαγραφή WAP καθορίζει τα πρωτόκολλα στην εφαρμογή, την περίοδο επικοινωνίας, και τα στρώματα μεταφοράς. Το στρώμα εφαρμογής εξετάζει τις εφαρμογές που ο χρήστης υιοθετεί και το scripting (σενάριο) που αυξάνει τη λειτουργικότητα των εφαρμογών. Το στρώμα επικοινωνίας διαχειρίζεται τη σύνδεση για το χρήστη. Το στρώμα μεταφοράς λαμβάνει την επικοινωνία από έναν από διάφορους τύπους ασύρματων δικτύων, την εξασφαλίζει, και την παραδίδει με έναν σχηματοποιημένο τρόπο. Τα ανώτερα στρώματα του πρωτοκόλλου διαμορφώνονται σύμφωνα με το πρωτόκολλο HTTP 1.1, τις scripting γλώσσες, και τις γλώσσες σήμανσης.

Οι εξωτερικές εφαρμογές μπορούν να διασυνδεθούν με την στοίβα οπουδήποτε επάνω από το στρώμα μεταφοράς. Το ένα στρώμα αφιερώνεται στην ασφάλεια. Οι περισσότερες WAP -ικανές συσκευές είναι κυρίως τηλέφωνα εντούτοις και άλλοι τύποι συσκευών υποστηρίζουν επίσης WAP.

### 2.5.2 Οι απαιτήσεις και απειλές ασφαλείας

Όμως οι απαιτήσεις ασφάλειας για την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικότητα, και τη διαθεσιμότητα για τα φορητά περιβάλλοντα υπολογισμού συσκευών μπορούν να απειληθούν

- Η απώλεια εμπιστευτικότητας. Κατά τη διάρκεια επικοινωνίας των συσκευών μεταξύ τους κάποιος, ο οποίος είναι κοντά σε αυτές, θα μπορεί να υποκλέψει και παρακολουθήσει τα δεδομένα.
- Η απώλεια ακεραιότητας. Οι πληροφορίες που είναι καταχωρημένες, το λογισμικό και το υλικό που χρησιμοποιούνται από την φορητή συσκευή πρέπει να προστατευθούν από την αναρμόδια, απρόβλεπτη, ή ακούσια τροποποίηση.
- Η απώλεια διαθεσιμότητας. Ο σκοπός μιας επίθεσης DoS είναι να κατασταλούν τα υπολογιστικά ή τα στοιχεία συμπεριφοράς δικτύων μη διαθέσιμα ή να περιοριστεί σοβαρά η διαθεσιμότητα τους με την κατανάλωση των πόρων τους με ένα μεγάλο ποσό αιτημάτων υπηρεσίας. Οι φορητές συσκευές μπορούν επίσης να είναι οι στόχοι των επιθέσεων DoS μέσω άλλων μέσων. Τα τρωικά άλογα, τα σκουλήκια, οι ιοί, και άλλα επικίνδυνα προγράμματα μπορούν να έχουν επιπτώσεις στη διαθεσιμότητα ενός δικτύου. Πολλές φορητές συσκευές υποστηρίζουν ήδη τη χρήση FIREWALL και αντιικών προγραμμάτων για να προστατευθούν ενάντια σε ορισμένες επιθέσεις DoS και άλλους τύπους επιθέσεων.

### 2.5.3 Επιθέσεις κατά της ασφάλειας στα ασύρματα δίκτυα

Οι επιθέσεις στις ασύρματες τεχνολογίες θα αυξάνονται σε αριθμό και ποιότητα ανάλογα με την εξάπλωση της τεχνολογίας και διακρίνονται στις παρακάτω κατηγόριες:

- Επιθέσεις παράνομης χρήσης της ασύρματης επικοινωνίας. Οι επιθέσεις παράνομης χρήση είναι βασισμένες στη εγκατάσταση παράνομων συσκευών ή τη δημιουργία νέων ασύρματων δικτύων, διακρίνονται στις παρακάτω κατηγορίες επιθέσεων : 1) *Μη Εξουσιοδοτημένοι Πελάτες*. Ένας επιτιθέμενος προσπαθεί να συνδέσει έναν ασύρματο πελάτη πχ ένα PDA με ένα σημείο πρόσβασης χωρίς να έχει έγκριση. Τα σημεία πρόσβασης μπορούν να διαμορφωθούν κατάλληλα για να απαιτήσουν έναν κωδικό πρόσβασης, ένας εισβολέας μπορεί να συνδεθεί με το εσωτερικό δίκτυο απλά με τη ενεργοποίηση της επικοινωνίας με το σημείο πρόσβασης μέσω μιας ασύρματης

κάρτας. Επιπλέον μερικά σημεία πρόσβασης έχοντας κακή πολιτική ασφαλείας χρησιμοποιούν τον ίδιο κωδικό για όλες τις ασύρματες συνδέσεις. 2) *Μη εξουσιοδοτημένα σημεία πρόσβασης*. Ένας οργανισμός που διαθέτει ασύρματο δίκτυο μπορεί να μην γνωρίζει (παρανόμως) επιπλέον access points στο υπάρχον δίκτυο. Αυτή η έλλειψη γνώσης μπορεί να οδηγήσει στην προηγούμενη επίθεση. Επιβάλλεται λοιπόν από τους οργανισμούς να εφαρμόσουν μια πολιτική ασφαλείας για να εξασφαλίσουν αφενός τη ασφαλή ρύθμιση των σημείων πρόσβασης και αφετέρου το δίκτυο να ανιχνεύεται για την προστασία μη εξουσιοδοτημένων συσκευών.

- Επιθέσεις παρακολούθησης της κίνησης (Interception and Monitoring of Wireless Traffic). Στο ασύρματο δίκτυο όπως και στο ενσύρματο είναι δυνατό να καταγράψει και να ελεγχθεί η κυκλοφορία του σημείο πρόσβασης. Η καταγραφή γίνεται πιο εύκολα από το ενσύρματο μιας και δεν απαιτείται ενεργητική παρακολούθηση του δικτύου, αρκεί μόνο ένα λογισμικό καταγραφής της κίνησης το οποίο δεν γίνεται αντιληπτό.
- Επιθέσεις παρεμβολής παρασίτων (Jamming). Οι επιθέσεις παρεμβολής παρασίτων οδηγούν στην άρνηση υπηρεσιών και εφαρμόζονται εύκολα στα ασύρματα δίκτυα, όπου σε τέτοιες περιπτώσεις η νόμιμη κυκλοφορία δεν μπορεί να φθάσει στους πελάτες ή στο σημείο πρόσβασης εξαιτίας της παράνομης κυκλοφορίας που καταναλώνει τις συχνότητες. Ένας επιτιθέμενος με τον κατάλληλο εξοπλισμό και τα εργαλεία μπορεί εύκολα να πλημμυρίσει την συχνότητα των 2,4 GHz, αλλοιώνοντας το σήμα έως ότου πάψει να λειτουργεί το ασύρματο δίκτυο.
- Επιθέσεις εναντίων των Password στα Access Points (Brute Force Attacks Against Access Point Passwords). Τα περισσότερα σημεία πρόσβασης χρησιμοποιούν ένα ενιαίο κλειδί ή ένα κωδικό πρόσβασης που μοιράζονται με όλους τους συνδεδεμένους ασύρματους πελάτες τους. Οι επιθέσεις brute force προσπαθούν να ανακαλύψουν αυτό το κλειδί μεθοδικά εξετάζοντας κάθε πιθανό κωδικό πρόσβασης. Ο εισβολέας αποκτά πρόσβαση από το σημείο πρόσβασης μόλις ο κωδικός πρόσβασης αποκαλυφτεί.
- Έλλειψη καταλλήλων ρυθμίσεων (Misconfiquration). Αποτελούν οι περιπτώσεις όπου ή πώληση των AP γίνεται με τα εργαλεία να μην είναι ενεργοποιημένα εξορισμού. Τα μη σωστά ρυθμισμένα APs έθεταν σε σοβαρό

κίνδυνο το δίκτυο εκτός αν οι διαχειριστές αντιλαμβάνονταν τους κινδύνους ασφαλείας και διαμόρφωναν κατάλληλα κάθε μονάδα πριν από την εγκατάσταση.

### 2.5.4 Τρόποι προστασίας των φορητών συσκευών

Για να ελέγξουμε και να μειώσουμε τους κινδύνους ασφαλείας, χρειαζόμαστε να εφαρμόσουμε λειτουργικά και τεχνικά αντίμετρα διαχείρισης για να προστατεύσουμε τις φορητές συσκευές και τα δίκτυα. Χρησιμοποιούμε την πιστοποίηση ταυτότητας, κρυπτογράφηση, τεχνολογία PKI (Public Key Infrastructure) , firewalls, αντϊικό λογισμικό και άλλες μεθόδους οι οποίες συνεχώς αναπτύσσονται μαζί με την επέκταση χρήσης των φορητών συσκευών.

Όσον αφορά την τεχνολογία PKI, αυτή προσφέρει ένα ασύμμετρο αλγόριθμος κρυπτογράφησης και χρησιμοποιεί ψηφιακά πιστοποιητικά. Στον παρακάτω πίνακα συνοψίζονται οι τρόποι προστασίας των φορητών συσκευών.

| | ***Σύσταση Ασφαλείας*** | ***Ανάγκη ή απαίτηση Ασφαλείας*** |
|---|---|---|
| **1** | Ανάπτυξη συνοπτικής σύστασης πολιτικής ασφάλειας που θα εξετάζει τη χρήση όλων των φορητών συσκευών. | Μια πολιτική ασφάλειας είναι το θεμέλιο υποδομής στο οποίο άλλα αντίμετρα (λειτουργικά και τεχνικά), οργανώνονται ορθολογικά και εφαρμόζονται. Μια τεκμηριωμένη πολιτική ασφάλειας επιτρέπει σε μια οργάνωση να καθορίσει τις αποδεκτές εφαρμογές και χρήσεις για τις φορητές συσκευές. |
| **2** | Εξασφάλιση ότι οι χρήστες στο δίκτυο εκπαιδεύονται πλήρως στη συνειδητοποίηση ασφάλειας | Ένα πρόγραμμα συνειδητοποίησης ασφάλειας βοηθά τους χρήστες να καθιερώσουν καλές πρακτικές |

| | | |
|---|---|---|
| | υπολογιστών και τους κίνδυνους που σχετίζονται με τις φορητές συσκευές. | ασφάλειας εμποδίζοντας αμελείς ή κακόβουλες παρεισφρήσεις στο αυτοματοποιημένο πληροφοριακό σύστημα μιας οργάνωσης |
| **3** | Διεξαγωγή τυχαίων διαχειριστικών ελέγχων ασφάλειας για τον έλεγχο των συσκευών. | Η επιβολή πολιτικής ασφάλειας είναι ζωτικής σημασίας για την εξασφάλιση ότι μόνο εξουσιοδοτημένες φορητές ασύρματες συσκευές λειτουργούν σύμφωνα με την πολιτική ασφάλειας της οργάνωσης.<br>Οι τυχαίοι διαχειριστικοί έλεγχοι ασφάλειας παρέχουν μια ρεαλιστική όψη των περιβαλλόντων ασφάλειας. |
| **4** | Ελαχιστοποίηση του κίνδυνου απώλειας ή κλοπής μέσω της χρήσης των φυσικών κλειδαριών. | Όπως με οποιαδήποτε φορητή συσκευή, χρησιμοποιήστε φυσικές κλειδαριές για να ελαχιστοποιήσετε τον κίνδυνο απώλειας ή κλοπής. |
| **5** | Ονομάζουμε όλες τις φορητές συσκευές με τις πληροφορίες του ιδιοκτήτη και του οργανισμού | Όπως με οποιαδήποτε φορητή συσκευή, ονομάστε όλες τις φορητές συσκευές με τις κατάλληλες πληροφορίες ιδιοκτητών και οργανισμών |
| **6** | Εξασφαλίζουμε ότι οι χρήστες ξέρουν πού να αναφερθεί μια χαμένη ή κλεμμένη συσκευή. | Όπως με οποιαδήποτε φορητή συσκευή, μια ετικέτα πρέπει να είναι στη συσκευή που δείχνει πώς μπορεί να επιστραφεί στο νόμιμο ιδιοκτήτη. |
| **7** | Ενεργοποίηση ενός κωδικού πρόσβασης για κάθε φορητή συσκευή. | Απαιτώντας τις οδηγίες πιστοποίησης ταυτότητας χρηστών αποτρέψτε την αναρμόδια πρόσβαση συσκευών και την πιθανή κλοπή των στοιχείων. |
| **8** | Αποθήκευση backup στοιχείων σε κρυπτογραφημένη μορφή. | Σε περίπτωση που η εφεδρική αποθήκευση κλέβεται, οι πληροφορίες |

| | | |
|---|---|---|
| | | πρέπει να καταχωρηθούν κρυπτογραφημένες. |
| **9** | Πλήρως εξετάζουμε και επεκτείνουμε τα 'μπαλώματα' και αναβαθμίζουμε το λογισμικό τακτικά. | Οι πρόσφατα ανακαλυμμένες ευπάθειες ασφάλειας των προϊόντων των προμηθευτών πρέπει να επιδιορθωθούν για να αποτρέψουν τους κακόβουλους και αμελείς.<br>Τα «μπαλώματα» (patches) πρέπει επίσης να εξεταστούν πλήρως πριν από την εφαρμογή για να εξασφαλίσουν ότι εργάζονται. |
| **10** | Αποφύγουμε τη τοποθέτηση ευαίσθητων πληροφοριών σε μια φορητή συσκευή. Εάν είναι απαραίτητο να το κάνουμε, διαγράψουμε τα ευαίσθητα στοιχεία από τη φορητή συσκευή και τα αρχειοθετούμε στο PC όταν δεν χρειάζεται άλλο στη φορητή συσκευή. | Λόγω της φορητότητας των φορητών συσκευών και της μεγαλύτερης απειλής στην απώλεια και την κλοπή, οι ευαίσθητες πληροφορίες που καταχωρούνται στη συσκευή πρέπει να μεταφερθούν στο PC . |
| **11** | Κλείνουμε τις πύλες επικοινωνίας κατά τη διάρκεια των περιόδων αδράνειας. | Το κλείσιμο των αχρησιμοποίητων πυλών επικοινωνίας ελαχιστοποιεί τον κίνδυνο της κακόβουλης πρόσβασης. |
| **12** | Εγκατάσταση αντιικού λογισμικού σε όλες τις φορητές συσκευές. | Το αντιικό λογισμικό εξασφαλίζει ότι η φορητή συσκευή δεν εισάγει σκουλήκια και ιούς στο συνδεμένο δίκτυο. Επίσης, η φορητή συσκευή είναι προστατευμένη. |
| **13** | Εγκατάσταση firewall σε όλες τις δικτυωμένες φορητές συσκευές. | Η φορητή συσκευή είναι ένας πιθανός στόχος για τους κακόβουλους χρήστες. |
| **14** | Εγκατάσταση λογισμικού VPN | Όλη η ασύρματη επικοινωνία πρέπει να |

| | | |
|---|---|---|
| | σε όλες τις φορητές συσκευές που διαβιβάζουν τα στοιχεία ασύρματα. | χρησιμοποιήσει ένα ισχυρό σύστημα κρυπτογραφίας, να έχει τη ισχυρή διαχείριση κλειδιών, και να έχει ισχυρή πιστοποίηση ταυτότητας χρηστών. |
| **15** | Εξασφαλίζουμε ότι ένας χρήστης μπορεί να επικυρωθεί ασφαλώς όταν λειτουργεί τοπικά ή από απόσταση. | Πρέπει να απαιτηθεί από τους χρήστες να επικυρωθούν όταν πρόκειται να λειτουργήσουν τοπικά ή από απόσταση. |
| **16** | Χρησιμοποιούμε κρυπτογράφηση και προστασία κωδικού πρόσβασης για την προστασία των ευαίσθητων αρχείων και των εφαρμογών. | Τα ευαίσθητα αρχεία δεδομένων και εφαρμογής πρέπει να κρυπτογραφηθούν με τις κατάλληλες τεχνικές κρυπτογράφησης. |
| **17** | Εξασφαλίζουμε ότι τα εργαλεία αξιολόγησης ασφάλειας χρησιμοποιούνται στις φορητές συσκευές. | Οι φορητές συσκευές πρέπει να υποβληθούν στις αξιολογήσεις ασφάλειας για να προσδιορίσουν τις ευπάθειες ασφάλειας. |
| **18** | Κατά το απαλλαγή των φορητών συσκευών που δεν θα χρησιμοποιηθούν πλέον από τον οργανισμό, θα πρέπει να σβηστούν οι τιμές των παραμέτρων διαμόρφωσης για να αποτραπεί η κοινοποίηση των ευαίσθητων δεδομένων του δικτύου. | Οι ευαίσθητες ή ιδιόκτητες τιμές των παραμέτρων διαμόρφωσης πρέπει να καθαριστούν για να αποτρέψουν την αμελή κοινοποίηση των πληροφοριών σε κακόβουλους χρήστες. |

### 2.5.5 Ασφάλεια WAP

Η Ασφάλεια είναι προαιρετική στο ασύρματο πρωτόκολλο WAP. Στην προδιαγραφή WAP, η ασφάλεια παρέχεται μέσω του ασύρματου στρώματος ασφάλειας μεταφορών (WTLS), το οποίο λειτουργεί άμεσα πάνω από το στρώμα μεταφορών του

πρωτοκόλλου. Οι στόχοι της προδιαγραφής WTLS είναι να παρασχεθεί η πιστοποίηση ταυτότητας, η ιδιωτικότητα, και η ακεραιότητα στοιχείων μέσω της χρήσης των πιστοποιητικών και της κρυπτογράφησης. Είναι βασισμένο στην προδιαγραφή 1,0 IETF ασφάλειας στρώματος μεταφοράς (TLS), (ο διάδοχος για να εξασφαλίσει το στρώμα υποδοχών [SSL]). Το WTLS εξετάζει συγκεκριμένα το περιορισμένο δυναμικό μονάδας αποθήκευσης/μνήμης, το χαμηλό εύρος ζώνης συχνοτήτων, τις χαμηλές δυνατότητες επεξεργασίας, και την απρόβλεπτη λανθάνουσα κατάσταση. Το WTLS παρέχει την end-to-end ασφάλεια μεταξύ των σημείων τέλους πρωτοκόλλου. Στην περίπτωση WAP, τα σημεία τέλους πρωτοκόλλου είναι η κινητή συσκευή και η πύλη WAP. Εάν τα σημεία τέλους πρωτοκόλλου μπορούν να εμπιστευθούν, κατόπιν η σύνδεση μπορεί να εξασφαλιστεί. Το WTLS θέτει τις παραμέτρους ασφάλειας κατά τη διάρκεια μιας διαδικασίας χειραψιών με έναν κεντρικό υπολογιστή. Κατά τη διάρκεια αυτής της χειραψίας ο χρήστης και ο κεντρικός υπολογιστής συμφωνούν σχετικά με τις απαιτήσεις για την πιστοποίηση ταυτότητας και την κρυπτογράφηση, επιλέγεται η μέθοδος κρυπτογράφησης που θα χρησιμοποιηθεί, τα πιστοποιητικά που ο χρήστης θα αποδεχθεί, και οποιεσδήποτε άλλες μη προκαθορισμένες παράμετροι.

Αυτήν την περίοδο, οι τρεις τρόποι ασφάλειας στο WTLS είναι :

- κλάση 1 : Ανώνυμη πιστοποίηση ταυτότητας
- κλάση 2 : Server authentication (πιστοποίησης ταυτότητας κεντρικών υπολογιστών)
- κλάση 3 : πιστοποίησης ταυτότητας διπλής κατεύθυνσης (χρήστης και κεντρικός υπολογιστής)

Το αίτημα για την ασφάλεια έρχεται στο χρήστη με το μήνυμα "Γεια σου", ο οποίος αρχίζει τη χειραψία. Ο κεντρικός υπολογιστής αποκρίνεται από την αποστολή του πιστοποιητικού του.

Εάν ο κεντρικός υπολογιστής επικυρωθεί από το χρήστη, μπορεί έπειτα να απαιτήσει την πιστοποίηση ταυτότητας από το χρήστη (κλάση 3). Όταν αυτό το αίτημα γίνεται, ο χρήστης αποκρίνεται με το πιστοποιητικό του (εάν έχει ένα), ή με ένα κενό πιστοποιητικό (εάν δεν έχει ), ή ένα alert μήνυμα που τελειώνει τη χειραψία. Το κύριο μυστικό, που θα χρησιμοποιηθεί για να κρυπτογραφήσει όλη την κυκλοφορία ,

ανταλλάσσεται με τη χρησιμοποίηση του (RSA), ή τους ελλειπτικούς αλγορίθμους καμπυλών Diffie-Hellman.

Η ακεραιότητα και η ιδιωτικότητα των στοιχείων επιβάλλεται χρησιμοποιώντας τους κώδικες κρυπτογράφησης και πιστοποίησης ταυτότητας μηνυμάτων (MAC). Και οι δύο παράμετροι συζήτιουνται κατά τη διάρκεια της διαδικασίας χειραψιών. Το WAP στηρίζεται στους υπάρχοντες αλγορίθμους κρυπτογράφησης όπως DES, 3DES, RC5, και IDEA. [24]

## 2.6 Αρχιτεκτονικές location-based

Το κινητό Διαδίκτυο επιτρέπει μια ευρεία σειρά νέων εφαρμογών που λαμβάνουν δυναμικά τις πληροφορίες που είναι σχετικές με την τρέχουσα θέση τους. Αυτός ο τύπος εφαρμογής ωφελείται πολύ από τους γενικούς μηχανισμούς που είναι υπεύθυνοι για τη ένωση μεταξύ των πόρων δικτύων και της φυσικής απόστασης . Υπάρχει *ένα μοντέλο για την συσχέτιση της θέσης πεδία με τις υπηρεσίες, μια αρχιτεκτονική για να υποστηρίξει την ανακάλυψη των location-based υπηρεσιών στο διαδίκτυο, και μια πρωτότυπη υποδομή στην οποία διάφορες υπηρεσίες και εφαρμογές έχουν αναπτυχθεί για την επικύρωση της αρχιτεκτονικής.*

Η λειτουργική δομή της AROUND αρχιτεκτονικής περιλαμβάνει τη *AROUND υπηρεσία*, η διαδικασία *contextualisation*, και η *υπηρεσία Ονομασίας* Η *AROUND υπηρεσία* είναι κατανεμημένη υποδομή location-based υπηρεσιών που οργανώνεται από τα πλαίσια θέσης και διαχειρίζεται από AROUND Servers.

*Το Contextualisation* είναι η διαδικασία καθορισμού της θέσης πλαισίου που ταιριάζει καλύτερα στην τρέχουσα θέση της κινητής συσκευής. Αυτή η διαδικασία μπορεί να βασιστεί στις πληροφορίες που αποκτώνται από τους πολλαπλούς τύπους πηγών και αντιμετωπίζει το ζήτημα της συσχέτισης της φυσικής θέσης μιας συσκευής με ένα πλαίσιο θέσης. Το πλαίσιο ή τα πλαίσια θέσης που είναι αποτέλεσμα των μηχανισμών contextualisation αποκαλούνται *πλαίσια βάσης*. Η *υπηρεσία ονομασίας*

επιλύει τα ονόματα των πλαισίων γενικής θέσης σε αναφορές σε συγκεκριμένο AROUND server στους οποίους μπορούν να προσπελαστούν [5].

Υφίσταται μια εφαρμογή για την ασφαλή ανακάλυψη υπηρεσιών-Service Discovery Service (SDS). Οι πάροχοι υπηρεσιών χρησιμοποιούν το SDS για να διαφημίσουν τις σύνθετες περιγραφές από τις διαθέσιμες ή ήδη εκτελέσιμες υπηρεσίες, ενώ πελάτες χρησιμοποιούν το SDS για να συνθέσουν τις ερωτήσεις για τον εντοπισμό αυτών των υπηρεσιών.. Η ασφάλεια του απαιτεί οι επικοινωνίες να κρυπτογραφούνται και να επικυρώνονται. Οι εφαρμογές SDS μπορούν να δεχτούν επιθέσεις man-in-the-middle. Για να αποτραπούν τέτοιες επιθέσεις, απαιτείται η μυστικότητα και η ακεραιότητα των δεδομένων να διατηρούνται μέσω της κρυπτογράφησης όλων των πληροφοριών που στέλνονται μεταξύ συστημάτων (δηλ., μεταξύ των πελατών και των κεντρικών υπολογιστών SDS και μεταξύ των υπηρεσιών και των κεντρικών υπολογιστών SDS). Το SDS χρησιμοποιεί κρυπτογραφικές μεθόδους που παρέχουνε ισχυρή αυθεντικοποίηση.

Για την κρυπτογράφηση χρησιμοποιείται ένα υβριδικό σύστημα κλειδιών δημόσιο/συμμετρικό Η λύση είναι να χρησιμοποιήσουμε ένα υβριδικό δημόσιο/συμμετρικό κλειδί σύστημα που επιτρέπει στις υπηρεσίες να διαβιβάσουν ένα πακέτο που τις περιγράφει με ασφάλεια επιτρέποντας τους SDS servers να αποκρυπτογραφούν το περιεχόμενο χρησιμοποιώντας ένα συμμετρικό κλειδί. [15].

| ID | Ciphered Secret | Payload |
|---|---|---|
| Sender Name | $\{Sender, Destination, Expire, S_K, Sign(C_P)\}_{E_K}$ | $\{Data, Time, MAC\}_{S_K}$ |

***Σχήμα 4:*** *Secure One-Way Broadcast Packet format: SK { shared client-server secret ke Sign(CP ) { signature of the ciphered secret using the client public key, EK { server publ key, and MAC { message authentication code.*

## 2.7 Αρχιτεκτονικές VPN

### 2.7.1 Συγκρίνοντας MPLS VPN με IPSec VPNs και με την συνδυαστική τους προσέγγιση

Δύο συνδυαστικές αρχιτεκτονικές (*Multiprotocol Label Switching*-MPLS based και *IP Security*-IPsec based), επιτρέπουν στους παρόχους υπηρεσιών να επεκτείνουν το VPN τους πάνω σε ένα ασφαλές δίκτυο με εξ'αποστάσεως πρόσβαση.

Η τεχνολογία MPLS επεκτείνει τις ικανότητες της IP να επιτραπούν οι πολύ μεγάλης κλίμακας εφαρμογές VPNs, οι οποίες βοηθάνε τους φορείς παροχής υπηρεσιών να παραδώσουν ιδιαίτερα εξελικτικές, διαφοροποιημένες, end-to-end IP-based υπηρεσίες.

Μερικά σημαντικά χαρακτηριστικά αυτής της τεχνολογίας είναι τα εξής :

- *Ασφάλεια* : MPLS: παρέχει το χωρισμό κυκλοφορίας μεταξύ VPNs με τη χρησιμοποίηση των μοναδικών ξεχωριστών διαδρομών. Επιτρέπει σε VPNs να δημιουργηθεί μέσω του πυρήνα παρέχοντας την ασφάλεια μέσω της απομόνωσης στοιχείων.
- *Εφαρμοσμένη μηχανική κυκλοφορίας*: με την ανάπτυξη της εφαρμοσμένης μηχανικής κυκλοφορίας στον πυρήνα, οι μηχανικοί δικτύων φορέων παροχής υπηρεσιών μπορούν να εφαρμόσουν τις πολιτικές για να βοηθήσουν να εξασφαλίσουν βέλτιστη διανομή κυκλοφορίας και να βελτιώσουν τη γενική χρησιμοποίηση δικτύων.

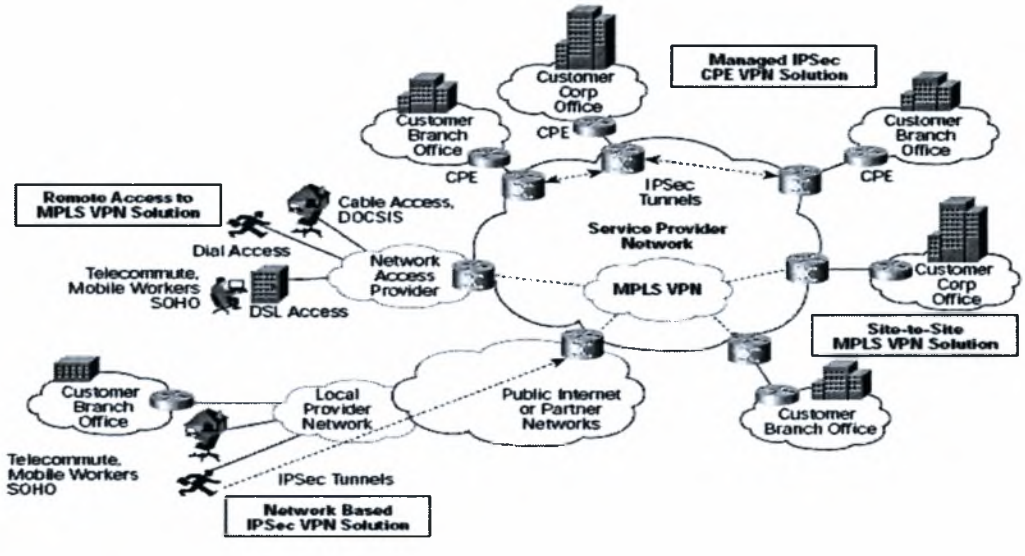
Η τεχνολογία IPsec-βασισμένο VPN παρέχει οποιοδήποτε συνδυασμό των ακόλουθων υπηρεσιών ασφάλειας δικτύων:

- Εμπιστευτικότητα στοιχείων: κρυπτογραφεί τα πακέτα πριν από τη μετάδοση.
- Ακεραιότητα στοιχείων: επικυρώνει τα πακέτα για να βοηθήσει να εξασφαλίσει ότι το στοιχείο δεν έχουν αλλάξει κατά τη διάρκεια της μετάδοσης.
- Επικύρωση προέλευσης στοιχείων: επικυρώνει την πηγή λαμβανόμενων πακέτων, από κοινού με την ακεραιότητα στοιχείων υπηρεσία.

Μερικά σημαντικά χαρακτηριστικά αυτής της τεχνολογίας είναι τα εξής :

- *Ασφάλεια*: εξασφαλίζει ιδιωτικότητα στοιχείων με μια εύκαμπτη ακολουθία της κρυπτογράφησης και των ανοίγοντας μηχανισμών που προστατεύουν τα πακέτα καθώς ταξιδεύουν πέρα από το δίκτυο. Οι χρήστες επικυρώνονται με τα ψηφιακά πιστοποιητικά ή με κλειδιά.
- *Ευκολία της επέκτασης* : μπορεί να επεκταθεί μέσω οποιοδήποτε υπάρχον δίκτυο IP με ελάχιστη ή καμία αλλαγή στην υπάρχουσα υποδομή δικτύων IP.

Μια λύση αρχιτεκτονικής VPN που χρησιμοποιούν MPLS και IPSec μεμονωμένα και σε συνδυασμό είναι η ακόλουθη:




***Σχήμα 5:*** *VPN Architecture Solutions*

Σε ότι αφορά το VPN site-to-site MPLS, επιτρέπει στους φορείς παροχής υπηρεσιών να προσφέρουν τα ασφαλή στοιχεία, τη φωνή, και τις τηλεοπτικές επικοινωνίες μεταξύ των εταιρικών θέσεων, με τις εγγυήσεις QoS. Αυτή η λύση μπορεί να είναι είτε έναν πυρήνα MPLS είτε να είναι πυρήνα IP του φορέα παροχής υπηρεσιών.

Η εξ' αποστάσεως πρόσβαση (Remote Access to MPLS VPN Solution) επιτρέπει στους φορείς παροχής υπηρεσιών για να προσφέρουν τις διοικούμενες υπηρεσίες VPN στους μακρινούς χρήστες. του συνδρομητή.

Η Managed IPSec CPE VPN Solution είναι μια δοκιμασμένη αρχιτεκτονική που οι φορείς παροχής υπηρεσιών μπορούν να επεκτείνουν γρήγορα για να συνδέσουν τα μακρινά γραφεία πελατών με τα επιχειρηματικά δίκτυα. Η σύνδεση γίνεται μέσω μιας σήραγγας IPSec, είτε μέσω του Διαδικτύου είτε η υποδομή δικτύων IP του φορέα παροχής υπηρεσιών [19].

### 2.7.2 **Ασφαλή εικονικά δίκτυα σε βάθος** (SAFE VPN IPSec Virtual Private Networks in Depth)

Ανάλογα με το εύρος της επιχείρησης και τις απαιτήσεις μας, έχουμε να αντιπαραβάλουμε πέντε σχέδια υλοποίηση δικτύου VPN : 1) Remote-user VPN designs, 2) Small-network VPN design, 3) Medium-network VPN design, 4) Large-network VPN design (with extranet connectivity), 5) Distributed large-network VPN design.

Ο χαρακτηρισμός SAFE αντιπροσωπεύει μια μελέτη των συστημάτων στις πτυχές ασφαλείας που εμφανίζει κάθε σχέδιο VPN. Οι πτυχές αυτές είναι που αναφέρονται παρακάτω.

- Υψηλή διαθεσιμότητα
- Κλιμακοσιμότητα
- Απόδοση
- Ταυτότητα
- Network Address Translation (NAT)
- Ασφάλεια
- Δρομολόγηση

Υπάρχουνε δύο τύποι VPN. 1) remote-access VPNs και 2) site-to-site VPNs. Η χρήση του PDA χρησιμοποιεί τον τύπο remote-access VPN. Το site-to-site VPN αναφέρεται στις εφαρμογές στις οποίες το δίκτυο μιας θέσης συνδέεται με το δίκτυο μιας άλλης θέσης μέσω των συσκευών VPN. Στο τύπο remote-access VPNs se ότι αφορά τον έλεγχο ταυτότητας και πρόσβασης στο IPsec γίνεται και με την αυθεντικοποίηση του χρήστη και με αυθεντικοποίηση της συσκευής. Για τη αυθεντικοποίηση συσκευών χρησιμοποιούνται ψηφιακά πιστοποιητικά για να παρέχουν την ταυτότητα μιας συσκευής. Ο μακρινός χρήστης επικυρώνεται αρχικά από *access control lists* (ACLs) η οποία καθορίζεται από την πολιτική βάση δεδομένων ασφαλείας. Για την αυθεντικοποίηση χρησιμοποιούνται οι *one-time passwords* (OTPs) μέσω *extended authentication* (XAUTH) και στη συνέχεια λαμβάνει μια εικονική διεύθυνση IP που χρησιμοποιείται για την VPN-προορισμένη κυκλοφορία. Αφότου οι επικυρώσεις συσκευών και χρηστών είναι πλήρεις, ο έλεγχος πρόσβασης IPSec εμφανίζεται.

Το IPSec παρέχει τα πολυάριθμα χαρακτηριστικά γνωρίσματα ασφάλειας : **1)** Κρυπτογράφηση στοιχείων. Εδώ κάνουμε χρήση του αλγορίθμου *Triple Data Encryption Standard* (3DES). Όταν ο 3DES χρησιμοποιείται για επικοινωνία τόσο ο αποστολέας, όσο και ο δέκτης πρέπει να ξέρουν το ίδιο μυστικό κλειδί, το οποίο χρησιμοποιείται για να κρυπτογραφήσει και να αποκρυπτογραφήσει το μήνυμα ( για παράδειγμα κάποια αρχεία). **2)** Αυθεντικοποίηση και πιστοποιητικό συσκευών , **3)** Ακεραιότητα στοιχείων. Εδώ στοιχείων έχουμε 2 τύπους : 128-bit *Message Digest 5* (MD5) ή 160-bit του αλγορίθμου *secure hash algorithm* (SHA). Ο MD5 είναι ένας αλγόριθμος σύνοψης μηνυμάτων ( message digest ). Το μήνυμα «γεμίζεται» στο τέλος με bits ώστε το να εξασφαλισθεί ότι το μέγεθος του σε bits είναι διαιρέσιμο με το 512. Μια 64-bit αναπαράσταση του αρχικού μήκους του μηνύματος προστίθεται με το μηνύματος. Ο SHA αλγόριθμος παίρνει ένα μήνυμα μικρότερο $2^{64}$ bits σε μέγεθος και παράγει ένα συνοπτικό μήνυμα των 160 bit. Ο αλγόριθμος είναι λίγος αργός από τον MD5 αλλά το μεγαλύτερο συνοπτικό μήνυμα τον κάνει πιο ασφαλέστερο σε brute-force επιθέσεις. **4)** Κρύψιμο διευθύνσεων **5)** Συσχέτιση ασφαλείας-*Security-association* (SA).

Μια επιπλέον παράμετρος ασφαλείας στα δίκτυα VPN είναι τα *Δικτυακά συστήματα ανίχνευσης εισβολέων- Network intrusion detection system* (NIDS). Αυτά τα συστήματα ανιχνεύουν επιθέσεις που προέρχονται μέσω του VPN από τις μακρινές περιοχές ή από τους μακρινούς χρήστες [20].

### 2.7.3 IPsec vs SSL

Ήδη έχουμε αναφερθεί και παραπάνω στα χαρακτηριστικά που διέπουν αυτές τις τεχνολογίες. Ουσιαστικά αυτές οι τεχνολογίες εξυπηρετούν όπως ασφαλείς "σήραγγες" που προστατεύουν την κυκλοφορία στοιχείων. Είναι σημαντικό να αναφερθούμε στα ποια είναι τα συγκριτικά κριτήρια ανάμεσα στο IPsec και στο SSL. Ακολουθεί ο ανάλογος πίνακας: [18]

| **Κριτήρια υλοποίησης** | **IPSec VPN** | **SSL VPN** |
|---|---|---|
| **Αυθεντικοποίηση και πρόσβαση ελέγχου** | Χρησιμοποιεί ανταλλαγή κλειδιών-Internet Key Exchange (IKE) για αυθεντικοποίηση είτε μέσω ψηφιακών πιστοποιητικών ή αυθεντικοποίηση δυο-βημάτων. Η Αυθεντικοποίηση χωρίς πιστοποιητικά είναι πιο ευπαθή | Οι SSL WEB Servers χρησιμοποιεί ψηφιακά πιστοποιητικά για αυθεντικοποίηση. Η Αυθεντικοποίηση χωρίς πιστοποιητικά είναι πιο Ασφαλής. |
| **Πρόσβαση Ελέγχου** | Ενιαία πρόσβαση, χορηγείται σε ομάδες χρηστών σε όλο το εύρος των υποδικτύων και των servers. | Έλεγχος πρόσβασης/ανά χρήστη, ανά εφαρμογή. Σαν αποτέλεσμα μπορεί να καθοριστεί πρόσβαση με βάση τα ports συγκεκριμένα URL's ή εφαρμογές. |
| **Τοποθεσία πρόσβασης στην** | Η πληροφορία είναι προσβάσιμη από συγκεκριμένες | Η πληροφορία είναι προσβάσιμη από |

| | | |
|---|---|---|
| **πληροφορία** | ομάδες χρηστών Η/Υ | οπουδήποτε ακόμη και περίπτερα Internet. Ωστόσο η πληροφορία μπορεί να περιοριστεί (με βάση τον έλεγχο πρόσβασης). |
| **Άμυνα έναντι των επιθέσεων** | Υποστηρίζει αλγορίθμους κρυπτογράφησης δέσμης (block encryption) 3DES, Αποτρέπει επιθέσεις man-in-the-middle μέσω ελέγχου πακέτων. Χρησιμοποιεί UDP ροές πακέτων και αποτρέπει επιθέσεις άρνησης παροχής υπηρεσιών/ Dos | Υποστηρίζει αλγορίθμους κρυπτογράφησης δέσμης (block encryption) 3DES. Υποστηρίζει RC4 και μέσω μηχανισμών TCP,TLS αποτρέπει την διακοπή ροής πακέτων. |
| **Ασφάλεια πελάτη** | Η κατάσταση συνόδου ανιχνεύει αν είναι ασφαλές κανάλι έχει κλείσει. Επίσης χρησιμοποιούνται IPsec πρωτόκολλα. | Παρέχει την δυνατότητα ασφαλούς αποσύνδεσης από το WEB, σβήνοντας όλα τα "ίχνη" του χρήστη. Χρήση συγκεκριμένων applets για διασφάλιση ανοιχτών port. |
| **Ευκολία πρόσβασης εφαρμογής** | Πρόσβαση σε όλες τις Web εφαρμογές, VoiIP κτλ. | Πρόσβαση στις περισσότερες Web εφαρμογές. |
| **Απαιτούμενο λογισμικό** | Λογισμικό IPSec Client | Standand Web browser |
| **Κλιμακοσιμότητα** | Υψηλά κλιμακώσιμο μέχρι από 10.000 χρήστες / πελάτες | Υψηλή κλιμακωσιμότητα |
| **Κάλυψη συνολικής ασφάλειας** | Επεκτείνει την ασφάλεια σε remote-level και χρησιμοποιεί τεχνολογία firewall | Περιορισμένα μέτρα ασφαλείας κατάλληλο για μη σημαντικές πληροφορίες |

| | | |
|---|---|---|
| **Σενάριο Χρήσης** | Ασφαλίζει εμπορικές και site-to-site πρόσβαση | Εξωτερική Web πρόσβαση πελατών. |

## 2.8 Μια προσανατολισμένη προσέγγιση στο ηλεκτρονικό εμπόριο-Ανάλυση διαδικασίας (Process Design)

Η εφαρμογή μιας ιδέας ηλεκτρονικού εμπορίου απαιτεί τα σχέδια των διαδικασιών του ηλεκτρονικού εμπορίου που ελαχιστοποιούν τις δαπάνες για τους επιχειρησιακούς χειριστές, συγχρόνως διατηρώντας την κατ' εκτίμηση αποδοτικότητα. Στόχος είναι να ταιριάσουμε τις επιχειρησιακές διαδικασίες με τις καταναλωτικές ανάγκες των χειριστών.

Υποστηρίζοντας την άποψη αξίας-value viewpoint μπορούμε να περιγράψουμε δυο ιδέες του ηλεκτρονικού εμπορίου:

- Ιεραρχία αξίας-Value Hierarchy. Αυτή η ιδέα προσδιορίζει την κορυφαία καταναλωτική ανάγκη και διαθέτει αυτό για να αρχίσει το αντικείμενο της οικονομικής αξίας που παράγονται από τους επιχειρησιακούς χειριστές.
- Γραφική παράσταση ανταλλαγής αξίας-value Exchange Graph. Αυτή η ιδέα προσδιορίζει τις δραστηριότητες μέσα στις οποίες δημιουργούνται τα αντικείμενα ή ανταλλάσσονται από τους επιχειρησιακούς χειριστές.

Υποστηρίζοντας την άποψη επιχειρησιακής διαδικασίας περιγράφουμε τις επιχειρησιακές διαδικασίες και τους επιχειρησιακούς . Δηλαδή :

- Ιεραρχία επιχειρησιακής διαδικασίας-Business process hierarchy. Περιγράφουμε τις συναλλαγές μεταξύ των επιχειρήσεων με τα αντικείμενα αξίας.
- Ιεραρχία στόχου-task hierarchy.. Αποσυνθέτει κάθε διαδικασία τους στόχους που εκτελούνται στους επιχειρησιακούς χειριστές [17].

# Κεφάλαιο 3

# Εφαρμόζοντας τα μοντέλα (ανάλυση διαδικασιών) για την ανάπτυξη μιας νέας ηλεκτρονικής υπηρεσίας

## 3.1 Επισκόπηση αξίας (Value viewpoint)

Για την ανάπτυξη μιας νέας ηλεκτρονικής υπηρεσίας θα χρησιμοποιήσουμε τις διαδικασίες του οργανισμού ΕΛ.Γ.Α. Ο ΕΛΓΑ λοιπόν είναι ένας γεωργικός ασφαλιστικός οργανισμός που καλύπτει και επιστρέφει γεωργικές ζημίες. Αυτό που πρέπει να έχει ξεχωριστή σημασία είναι πως πρέπει *να **αναπτυχθεί ένα σύστημα ώστε να στοχεύει στην αυτοματοποίηση και στη διαδικασία εκτίμησης ζημίας***, μέσα σε ένα σύντομο χρονικό διάστημα. Είναι σημαντικό, στην συνεχεία να μελετηθούν τα θέματα ασύρματης ασφάλειας που εμφανίζονται σε μια διαδικασία e-business. Στις διαδικασίες του ΕΛΓΑ εμπλέκονται πέντε φορείς, που ο καθένας τους έχουν να παρουσιάσουν κάποια βήματα. Πιο αναλυτικά έχουμε :

- ***Περιφερειακό Υποκατάστημα***

  Βήμα 1: το τοπικό υποκατάστημα (δήμος-διαμέρισμα που έγινε η ζημία) βγάζει την αναγγελία της ζημίας.

  Βήμα 2: μέσα σε 12 ημέρες, οι πληγέντες αγρότες πρέπει να υποβάλλουν τις δηλώσεις αποζημίωσης. Αν περάσει η χρονική περίοδος τότε η αίτηση θεωρείται εκπρόθεσμη δεν γίνεται δεκτή από τον ανταποκριτή.

  Βήμα 3: ενημερώνει του εκτιμητές για νέες πληροφορίες.

  Βήμα 4: Αίτηση επανεκτίμησης *(επόμενη ημέρα της τοιχοκόλλησης της σχετικής πρόσκλησης)* .

- ***Παραγωγός-κτηνοτρόφος-Αγρότης***

  Βήμα 1: Περιμένει την αναγγελία ζημιάς από τοπικό υποκατάστημα.

  Βήμα 2: Επιλογή της Ασφαλιστικής κάλυψης ( του ΕΛΓΑ )

  1) Φυτική Παραγωγή 2) Ζωική Παραγωγή.

  Βήμα 3: Συμπλήρωση της αίτησης ( ονοματεπώνυμο, αριθμός της αστυνομικής ταυτότητας, ΑΜΦ, διεύθυνση κατοικίας, τοποθεσία του αγροτεμαχίου που ζημιώθηκε, το είδος και η ποικιλία της καλλιέργειας και κάθε άλλο στοιχείο που κρίνεται αναγκαίο από την Υπηρεσία).

  Βήμα 4: Δικαίωμα επανεκτίμησης, ανάλογα με το πόρισμα της αίτησης

  Βήμα 5: Αίτηση αποζημίωσης on line.

- ***Ανταποκριτής του ΕΛΓΑ***

  Βήμα 1: Μέσα σε 2 μέρες από τότε που έγινε η ζημιά από κάποιο ασφαλισμένο αίτιο, είναι υποχρεωμένος να αναγγείλει στην αρμόδια υπηρεσία του ΕΛ.Γ.Α (τοπικό υποκατάστημα), τη χρονολογία, το είδος και τις εκτάσεις που ζημιώθηκαν.

  Βήμα 2: παραλάβει τη δήλωση ζημιάς, την καταχωρίζει στο ειδικό πρωτόκολλο του ΕΛ.Γ.Α. και παραδίδει στον αγρότη αντίγραφο, στο οποίο αναγράφεται ο αριθμός πρωτοκόλλου, τα τέλη εκτίμησης που καταβλήθηκαν και η χρονολογία παραλαβής της δήλωσης.

  Βήμα 3: Ενημερώνει τον εκτιμητή (επόπτης) για την ύπαρξη ζημιάς στον συγκεκριμένο δήμο ή διαμέρισμα.

  Βήμα 4: μετά τη 12ήμερη προθεσμία υποβολής των δηλώσεων ζημιάς ο ανταποκριτής ταξινομεί κατά απόλυτη αλφαβητική σειρά, αριθμεί τις « Δηλώσεις Ζημιάς » οι οποίες υποβλήθηκαν και συμπληρώνει σε έξη ( 6 ) αντίγραφα το έντυπο « Συνοπτικό Σημείωμα Ζημιάς » . Η ταξινόμηση και αρίθμηση των δηλώσεων ζημιάς και η συμπλήρωση του εντύπου « Συνοπτικό Σημείωμα Ζημιάς » γίνεται ξεχωριστά για κάθε αναγγελία ζημιάς και για κάθε δημοτικό ή κοινοτικό διαμέρισμα και Κοινότητα .

  Βήμα 5: Ενημερώνει τον αγρότη για έγκριση ή απόρριψης μια της αίτησης

  Βήμα 6: παραλαμβάνει τις αιτήσεις επανεκτίμησης.

  Βήμα 7: ελέγχει εάν είναι πλήρεις και κυρίως αν σ' αυτές προσδιορίζονται με ακρίβεια τα πορίσματα εκτίμησης για τα οποία υποβάλλεται η αίτηση.

επανεκτίμησης και εισπράττονται τα τέλη επανεκτίμησης, τα οποία είναι διπλάσια των τελών εκτίμησης.

Βήμα 8 : παραδίδουν στους εκτιμητές-επόπτες τις απαιτήσεις επανεκτίμησης και το αποδεικτικό κατάθεσης των τελών επανεκτίμησης .

Βήμα 9: Εφοδιάζει έγκαιρα τους δήμους και διαμερίσματα με τα αναγκαία έγγραφα.

Βήμα 10 : Ενημερώνει το αγρότη για το πόρισμα της επανεκτίμησης.

- ***Εκτιμητής-Επόπτης***

  Βήμα 1: Επιλέγει έναν άνθρωπο από τον δήμο (γεωπόνο) για να του υποδείξει τα κτήματα που υπέστησαν ζημίες.

  Βήμα 2: Αυτοψία στο φυσικό χώρο ( αν χρειάζεται τραβάει φωτογραφίες).

  Βήμα 3: Η αυτοψία γίνεται με την κοινοποίηση (συμπλήρωση) του πίνακα.

  Βήμα 4 : Επικοινωνία (μέσου κινητού τηλεφώνου ή ηλεκτρονικών συσκευών για πληροφορίες).

  Βήμα 5: Εφόσον ολοκληρωθεί η αυτοψία βγάζει 3 αντίγραφα με το πόρισμα της αυτοψίας (δήμος/διαμέρισμα-υποκατάστημα και στη διοίκηση κεντρικού οργανισμού για εκκαθάριση.

  Βήμα 6: για όσες φορές το κρίνει σκόπιμο μπορεί να προβαίνει σε προεκτίμηση της ζημιάς πριν από την οριστική εκτίμηση, καθώς και στην παρακολούθηση της καλλιέργειας που ζημιώθηκε.

  Βήμα 7 : παραλαμβάνουν τις αιτήσεις επανεκτίμησης.

  Βήμα 8 : Αυτοψία με την κοινοποίηση των πινάκων.

- ***ΟΡΓΑΝΙΣΜΟΣ ΕΛΓΑ***

  Βήμα 1 : Πρόσβαση σε Νομικές υπηρεσίες.

  Βήμα 2: (κοινοποίηση ) λαμβάνει το αντίγραφο της αυτοψίας από τον περιφερειακό υποκατάστημα.

  Βήμα 4:(εκκαθάριση) ενημερώνει το περιφερειακό υποκατάστημα για την έγκριση του αιτήματος.

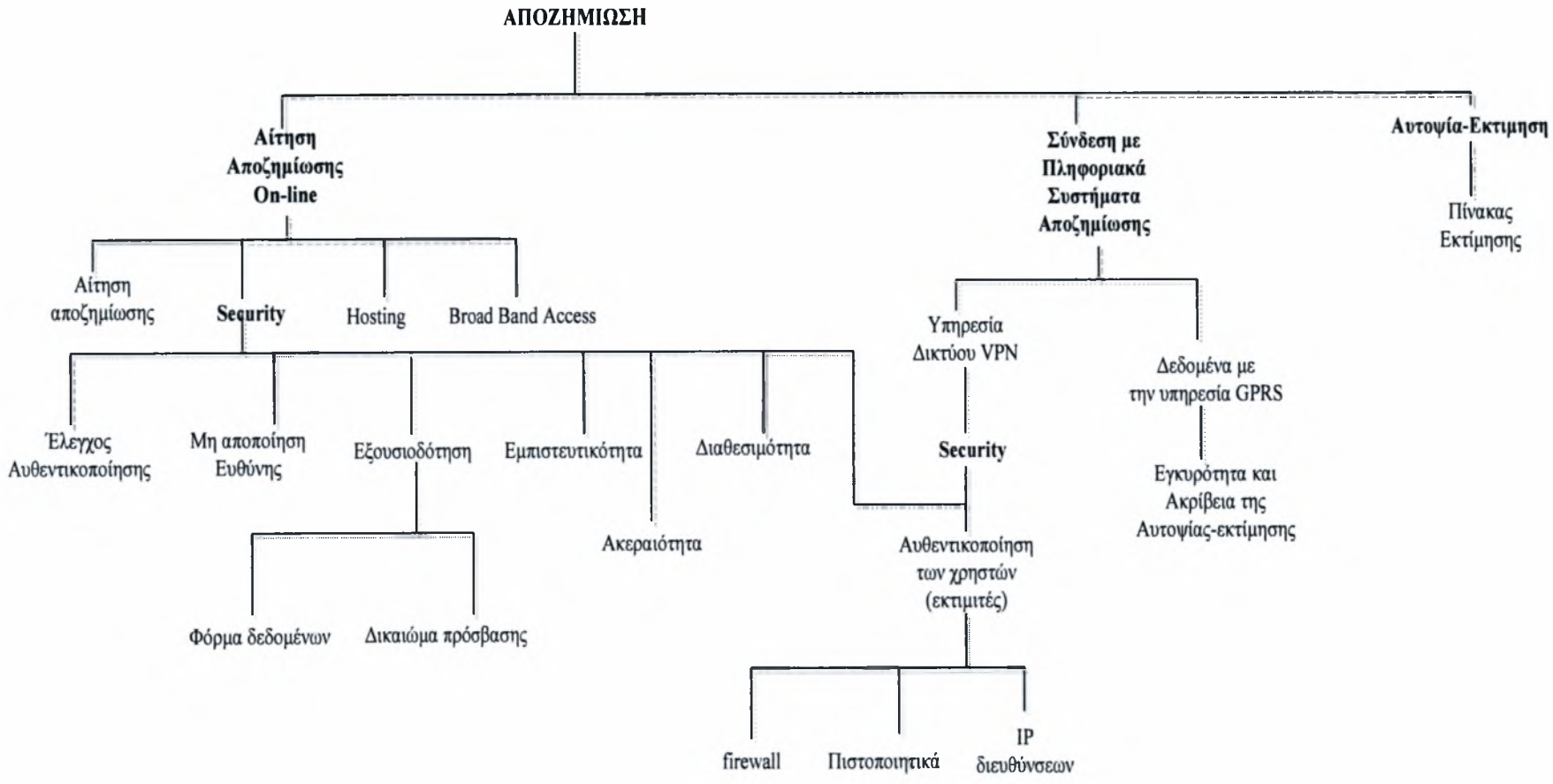
  Βήμα 5: η αποζημίωση γίνεται μέσω ταχυδρομικής επιταγής ή μέσω της Αγροτικής τράπεζας.

Στα παρακάτω διαγράμματα θα μας βοηθούν να μοντελοποιήσουμε την υπηρεσία μας και να παρουσιάσουμε την αξία του συστήματος μας. Το εργαλείο που χρησιμοποιήσαμε είναι το Microsoft Office Visio 2003.

### 3.1.1 **Ιεραρχία Αξίας** (Value Hierarchy)

Γενικά μια *Ιεραρχία Αξίας* (Value Hierarchy) είναι μια κυκλική κατευθυνόμενη γραφική παράσταση της οποίας η ρίζα αντιπροσωπεύει μια ανάγκη. Τα παιδία ενός κόμβου αντιπροσωπεύουν τα αντικείμενα αξίας (Value Objects) που χρησιμοποιούνται για να ικανοποιήσουν αυτήν την ανάγκη. Ένα *αντικείμενο αξίας* μπορεί να είναι ένα αγαθό ή υπηρεσία της οικονομικής αξίας σε κάποιο χειριστή (actor). Επί της ουσίας σε αυτή τη γραφική παράσταση έχουμε να κάνουμε με «κινητά αντικείμενα» όπου κάθε *αντικείμενο αξίας* (value objects) **ανταλλάσσεται** και ενώ ένας ***χειριστής*** (actor) ***ανταλλάσει***.

Στο *σχήμα 6* παρουσιάζεται η ιεραρχία αξίας (Value Hierarchy) που λέει για να ικανοποιηθεί η ανάγκη (ΑΠΟΖΗΜΙΩΣΗ), χρειαζόμαστε να κάνουμε μια αίτηση αποζημίωσης On-line, να υπάρχει σύνδεση με τα πληροφοριακά συστήματα αποζημίωσης και να υπάρξει Αυτοψία-Εκτίμηση. Στην On-line αίτηση αποζημίωσης για να γίνει πρέπει να υπάρχει μια αίτηση αποζημίωσης, μια Hosting υπηρεσία που αποθηκεύει την αίτηση, μια ευρυζωνική (Broadband Access) σύνδεση στο Internet και πρέπει να πάρουμε τις παραμέτρους ασφαλείας που είναι δυνατό να παρέχονται από τον φορέα. Στα πληροφοριακά συστήματα αποζημίωσης, παρέχουμε υπηρεσία δικτύου VPN με παραμέτρους Ασφαλείας και υπηρεσία GPRS. Στην αυτοψία-εκτίμηση παρέχεται κάποιος πίνακας εκτίμησης.



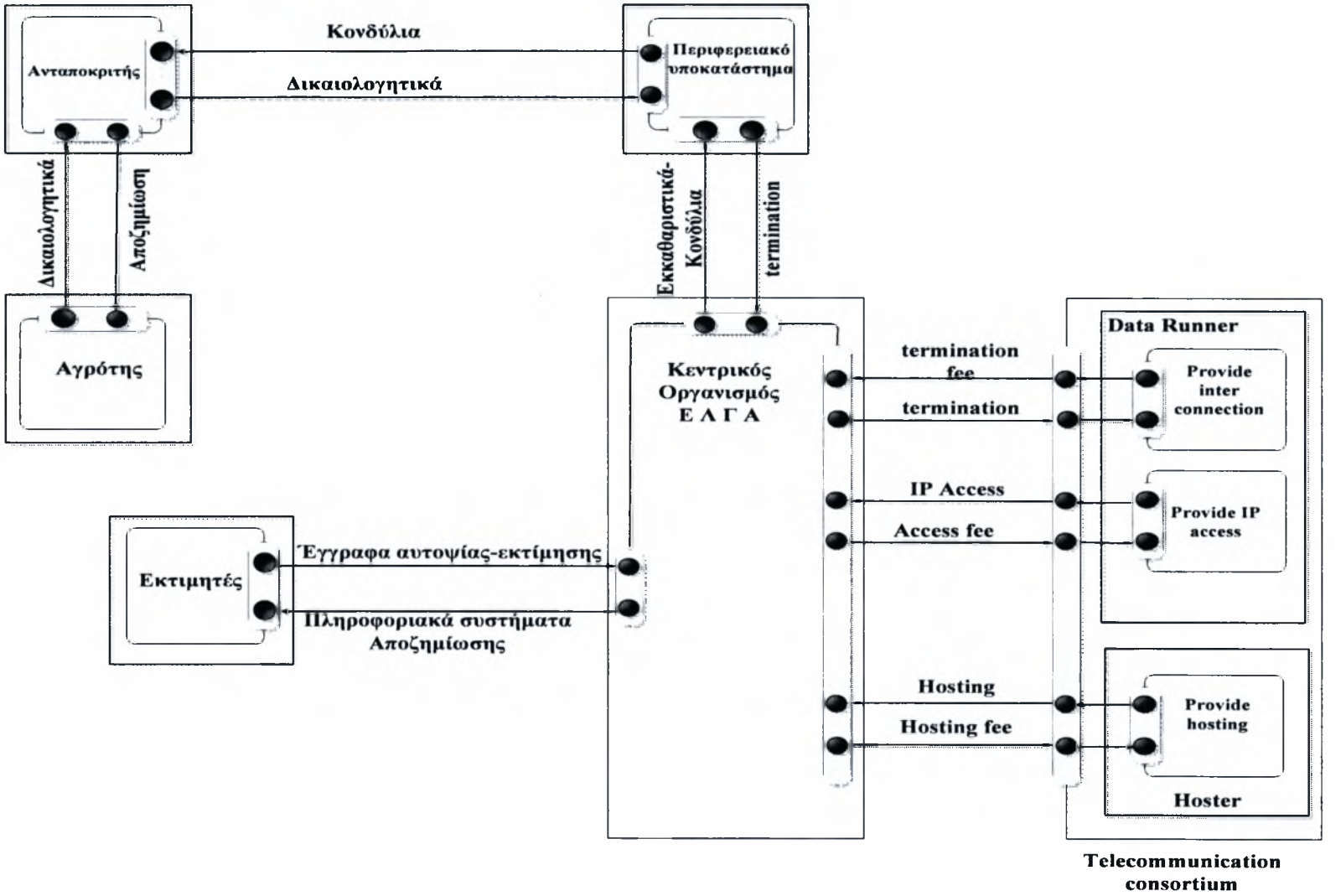

***Σχήμα 6:*** *Value Hierarchy*

### 3.1.2 Γράφημα συναλλαγών αξίας (Value Exchange Graph)

Ένα *γράφημα συναλλαγών ανταλλαγής αξίας* (Value Exchange Graph) παρουσιάζει ποιοι είναι οι εμπλεκόμενοι φορείς που συμμετάσχουν την δημιουργία και τα κινητά αντικείμενα (Value Objects) που εμφανίστηκαν στην ιεραρχία αξίας (Value Hierarchy).

Θα εξηγήσουμε τώρα πιο λεπτομερειακά την γραφική παράσταση αξίας. Καταρχήν κάθε εμπλεκόμενος φορέας (Actor) θεωρείται μια οντότητα, που αντιπροσωπεύονται από ορθογώνια. Για να ικανοποιηθεί μια ανάγκη ή να ανταλλαχθούν αντικείμενα αξίας με άλλους actors πρέπει να εκτελεστεί μια δραστηριότητα αξίας. Μια *δραστηριότητα αξίας* είναι μια λειτουργία που μπορεί να εκτελεστεί με έναν οικονομικά κερδοφόρο τρόπο από τουλάχιστον ένα actor, απεικονίζεται από ένα στρογγυλευμένο ορθογώνιο. Μια σημαντική απόφαση σχεδίου που αναπαρίσταται από ένα γράφημα συναλλαγής αξιών είναι το κατά πόσο μπορεί ένα αντικείμενο αξίας να αποκτηθεί από άλλους actors μέσω συναλλαγής αξιών ή να παραχθεί μέσω δραστηριότητας αξιών κάποιου άλλου actor. Μια ανταλλαγή αξίας που απεικονίζεται από ένα βέλος στο σχήμα, δείχνει ότι οι actors είναι πρόθυμοι να ανταλλάξουν αντικείμενα αξίας μεταξύ τους. Υποθέτουμε πως οι actors είναι λογικές οντότητες που προσφέρουν ένα αντικείμενο αξίας ένα αποκτήσουν ένα άλλο αντικείμενο αξίας. Δηλαδή έχουμε μια αμοιβαιότητα, η οποία εκφράζεται μέσα από διεπαφές (Interface) και value port.

Λόγω αυτών και στο *σχήμα 7* υπάρχουν αρκετοί actors που απεικονίζονται με ορθογώνια. Σαφώς και υπάρχει αμοιβαιότητα ( μέσω διεπαφών και value port ) και εκτελείται η δραστηριότητα αξίας (ανταλλαγή αντικειμένων). Για παράδειγμα από τον actor "Κεντρικός Οργανισμός ΕΛΓΑ" έρχεται μια διεπαφή termination (χρηματικές δοσοληψίες) από τον actor "Περιφερειακό υποκατάστημα" και πηγαίνει πάλι σε αυτόν μια διεπαφή με εκκαθαριστικά κονδύλια . Τα ίδια συμβαίνουν και με τους υπόλοιπους actors.




***Σχήμα 7:*** *Value Exchange Graph*

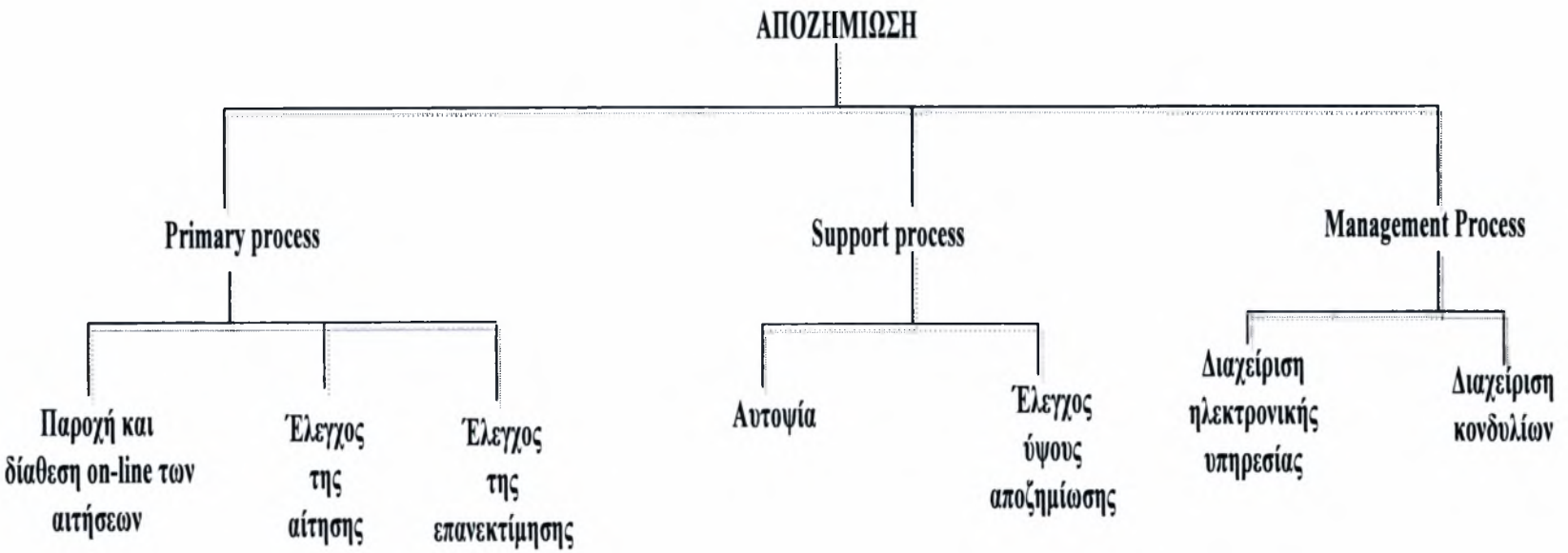
## 3.2 **Επισκόπηση διαδικασίας** (Process Viewpoint)

### 3.2.1 **Ιεραρχία επιχειρηματικών διαδικασιών** (Business process hierarchy )

Σε αυτό το διάγραμμα για να προσδιορίσουμε τις απαραίτητες διαδικασίες χρησιμοποιούμε τους ακόλουθους τύπους διαδικασιών :

- Αρχικές διαδικασίες (Primary Process): συμβάλλουν άμεσα προς την ικανοποίηση των αναγκών.
- Διαδικασίες υποστήριξης (Support Process): επιτρέπουν την εκτέλεση των αρχικών διαδικασιών και παρέχουν ένα κατάλληλο εργασιακό περιβάλλον.
- Διαδικασίες διαχείρισης (Management Process): κατευθύνουν και ελέγχουν τις αρχικές διαδικασίες και τις διαδικασίες υποστήριξης.

Στο *σχήμα 8* παρουσιάζει τις διαδικασίες που απαιτούνται για να ικανοποιηθεί η ανάγκη της αποζημίωσης . Η αρχική διαδικασία αποτελείται από την παροχή και διάθεση on-line των αιτήσεων, από τον έλεγχο της αίτησης και τον έλεγχο της επανεκτίμησης. Οι διαδικασίες υποστήριξης συμβάλλουν έμμεσα προς ικανοποίηση της ανάγκης. Εδώ προσδιορίζουμε δύο διαδικασίες, την Αυτοψία και τον Έλεγχο ύψους αποζημίωσης. Τέλος οι διαδικασίες διαχείρισης ελέγχουν οι άλλες διαδικασίες (αρχικές και υποστήριξης). Μια σημαντική διαδικασία διαχείρισης είναι η ηλεκτρονικής υπηρεσίας και μια άλλη διαδικασία είναι η διαχείριση κονδυλίων.




***Σχήμα 8:*** *Business process hierarchy*

### 3.2.2 **Ιεραρχία Στόχων** (Task Hierarchy)

Η Ιεραρχία Στόχων (Task Hierarchy) παρέχει μια ικανοποιητική λεπτομέρεια για τη περιγραφή μιας ιδέας ηλεκτρονικού εμπορίου. Όλοι οι στόχοι (διαδικασίες) που απαιτούνται για κάθε actor, εκπληρώνουν την ανάγκη. Επίσης κάθε διαδικασία ορίζεται η δραστηριότητα αξίας. Επομένως θα έχουμε :

- **Αγρότης**
  1. Περιμένει την αναγγελία της ζημίας.
  1. Δικαίωμα επανεκτίμησης.
  2. Βοηθάει τον εκτιμητή να περάσουν μέσω PDA τα στοιχεία που χρειάζονται (αν βέβαια οι αιτήσεις γίνονται μέσω του εκτιμητή).
  3. Επικοινωνία με τον ανταποκριτή για την πρόσθεση αποζημίωσης.

- **Ανταποκριτής**
  1. Αναγγελία στην αρμόδια υπηρεσία για την ύπαρξη ζημίας.

- **Περιφερειακό Υποκατάστημα**
  1. Αναγγελία της ζημιάς(αιτήσεις).
  2. Αναγγελία της επανεκτίμησης.
  3. Ενημερώνει τους εκτιμητές για ύπαρξη ζημίας.
  4. Συμπληρώνει τις αιτήσεις

- **Εκτιμητής**
  1. Ενημερώνεται από το περιφερειακό υποκατάστημα για τι ύπαρξη ζημιών.
  2. Αυτοψία στο φυσικό χώρο με την χρήση των PDA.
  3. Κοινοποίηση των πινάκων.
  4. Μεταφορά των δεδομένων και κοινοποίηση της αυτοψίας στο κεντρικό οργανισμό
  5. Προβαίνει σε προεκτίμηση.

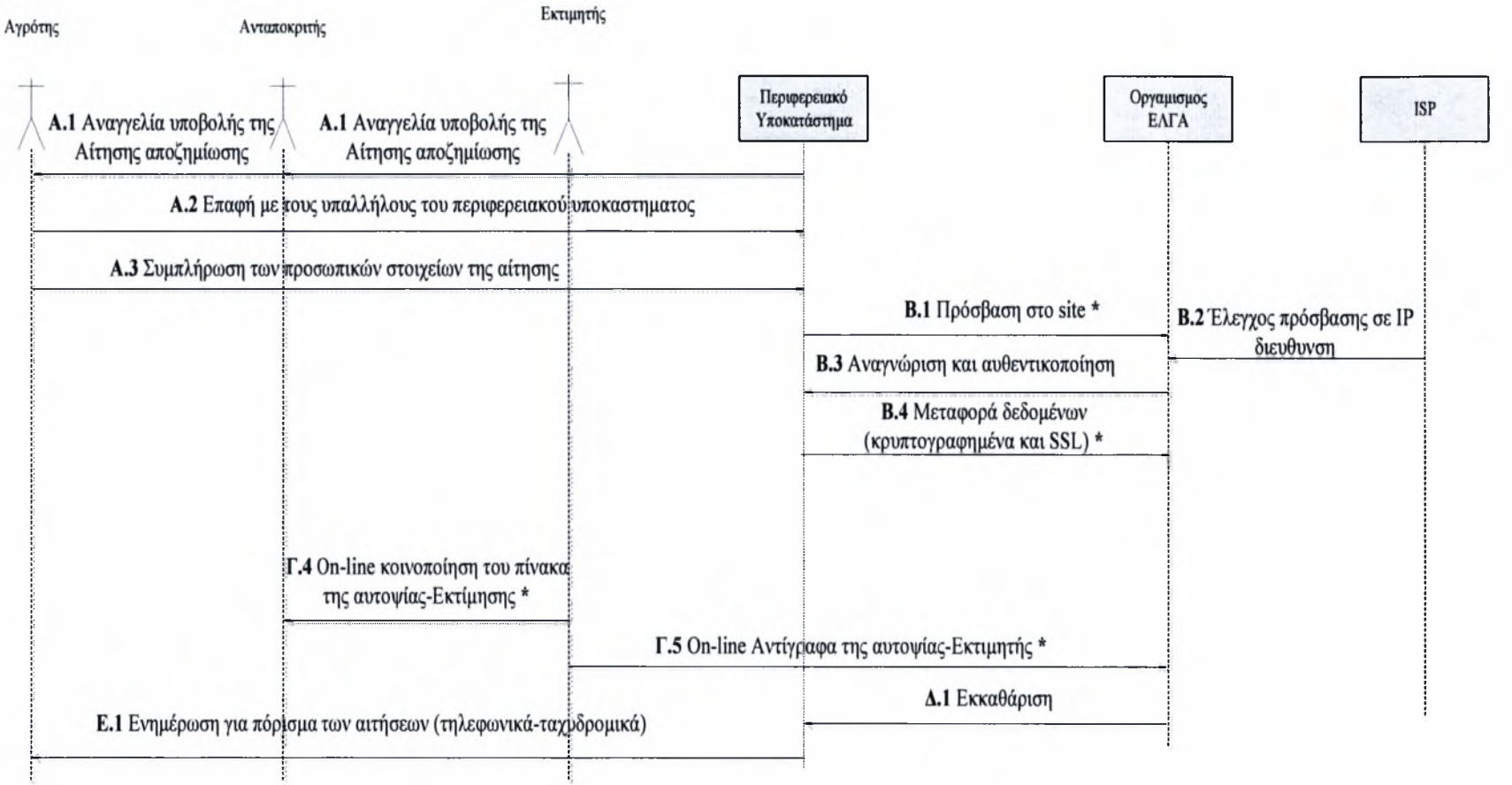
- **Οργανισμός ΕΛΓΑ**
  1. Συλλογή δεδομένων και πληροφοριών από τον Server.
  2. Παροχή πληροφοριών μέσω του PDA ή του διαδικτύου.
  3. Διαδικασία κοινοποίησης και εκκαθάρισης.
  4. Ενημερώνει ηλεκτρονικά το αγρότη για την έγκριση ή μη των αιτήσεων.

### 3.2.3 **Ροή διαδικασίας** (Interleaved Process Flow 1)

Σε αυτό το διάγραμμα (*σχήμα 9*) αναλύουμε τη διαδικασία υποβολής της αίτησης αποζημίωσης στο περιφερειακό υποκατάστημα και την τελική έγκριση του οργανισμό του ΕΛΓΑ μέσου του ηλεκτρονικού συστήματος.

Λεκτική περιγραφή:

Το Περιφερειακό Υποκατάστημα αναγγείλει την υποβολή αίτησης αποζημίωσης στον Ανταποκριτή και ο Ανταποκριτής αναγγείλει την υποβολή αίτησης αποζημίωσης στον αγρότη (**Α.1**). Στην συνέχεια ο Αγρότης έρχεται σε επαφή με τους υπαλλήλους του περιφερειακού υποκαταστήματος και συμπληρώσει την αίτηση προσωπικών στοιχείων της αίτησης ( **Α.2**, **Α.3**). Ύστερα ακολουθούνται οι διαδικασίες του Περιφερειακού Υποκαταστήματος προς το Οργανισμό του ΕΛΓΑ, δηλαδή πρόσβαση στο site του ΕΛΓΑ (υπάρχει έλεγχος πρόσβασης σε IP διεύθυνση), αναγνώριση και αυθεντικοποίηση και μεταφορά δεδομένων (**Β.1***, **Β.2**, **Β.3 Β.4***). Ακολούθως έχουμε την διαδικασία της εκτίμησης της ζημίας από τον Εκτιμητή ,την οποία θα αναλύσουμε στο παρακάτω διάγραμμα του *Interleaved Process Flow 2*. Μετέπειτα Οργανισμός του ΕΛΓΑ κοινοποιεί στο περιφερειακό υποκατάστημα την Εκκαθάριση (**Δ.1**) και το περιφερειακό υποκατάστημα ενημερώνει τον Αγρότη για τον πόρισμα των αιτήσεων. Οι διαδικασίες που φέρουν κάποιο αστερίσκο, αναπαριστούνε κάποια καταστάσεις και παραμέτρους, που θα αναλύσουμε και περαιτέρω.




***Σχήμα 9:*** *Interleaved Process Flow 1*

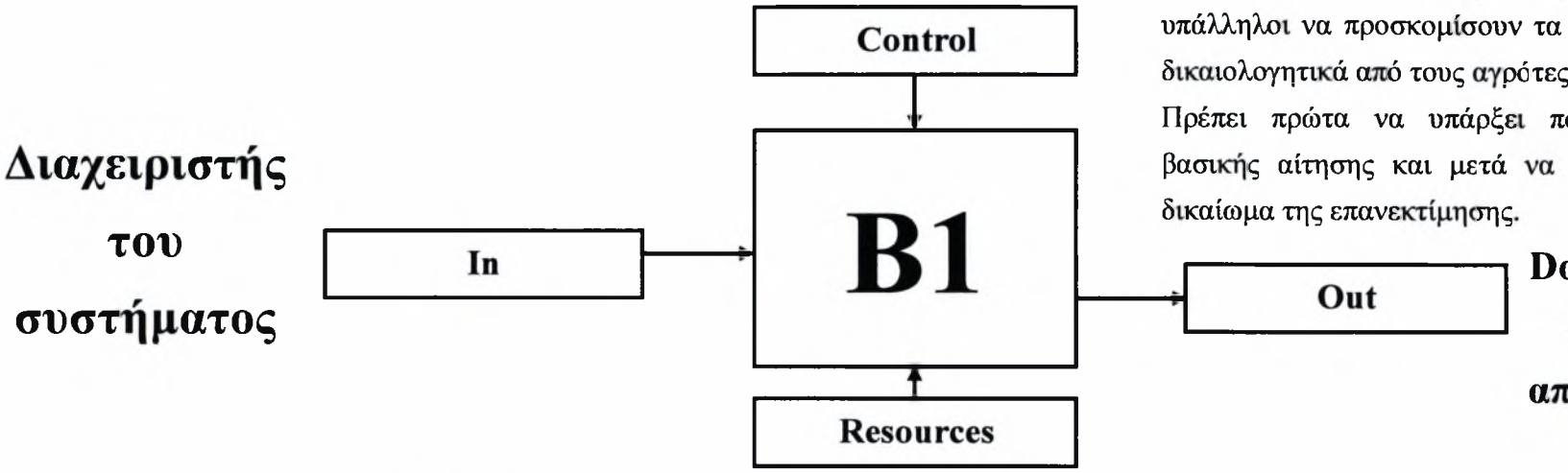
### 3.2.4 **Βήμα διαδικασίας 1** (Process Step 1-Πρόσβαση στο Site)

Το **B1** είναι ένα βήμα της διαδικασίας πρόσβασης *στο site*. Κάθε τέτοιο βήμα αποτελείται από εισόδους (In), Ελέγχους (Control), Πόρους (Resources), Εξόδους (Out) και από παράμετροι, καταστάσεις και Value Object. Για να εκτελεστεί ο έλεγχος αναγκαία συνθήκη είναι να έχει γίνει εκ των προτέρων μια άλλη διαδικασίας. Επίσης κάθε έξοδος είναι και είσοδος σε επόμενα βήματα. (όπως για παράδειγμα στο βήμα B1 η έξοδος είναι «Εκτιμητές», οι εκτιμητές είναι είσοδοι στο βήμα Γ1). Οι παράμετροι είναι κάτι που επεξεργαζόμαστε.

Έτσι στο *σχήμα 10* θα έχουμε :

Ως είσοδο (In) έχουμε τον διαχειριστή του συστήματος ( υπάλληλος ). Στον Έλεγχο (Control) έχουμε τις αναγκαίες συνθήκες: 1) πρέπει οι υπάλληλοι να προσκομίσουν τα απαραίτητα δικαιολογητικά από τους αγρότες και 2) να υπάρξει πόρισμα της βασικής αίτησης και μετά να ασκηθεί το δικαίωμα της επανεκτίμησης. Στους πόρους θα έχουμε σύνδεση στο web, Πληροφορίες, υποδομές ασφαλείας, servers, κεντρικό υποκατάστημα, Υπάλληλοι του περιφερειακού υποκαταστήματος. Επιπλέον χρειαζόμαστε και τρεις παραμέτρους με τις αντίστοιχες καταστάσεις.

Για να έχουμε πρόσβαση στο site πρέπει οι υπάλληλοι να προσκομίσουν τα απαραίτητα δικαιολογητικά από τους αγρότες
Πρέπει πρώτα να υπάρξει πόρισμα της βασικής αίτησης και μετά να ασκηθεί το δικαίωμα της επανεκτίμησης.




Σύνδεση στο Web, Πληροφορίες, Υποδομές ασφαλείας, Servers, Κεντρικός υποκατάστημα, Υπάλληλοι του περιφερειακού

| Παράμετροι | Καταστάσεις | Value Object |
|---|---|---|
| 1. Έλεγχος IP Access | 1. Σύγκριση IP Access, επιτυχία ή αποτυχία πρόσβασης. | 1. Πιστοποιητικά / IP Access |
| 2. Κρυπτογραφία | 2. Μέσου του πρωτόκολλου SSL κρυπτογραφείτε ο κωδικός και το username. | |
| 3. Αυθεντικοποίηση του χρήστη | 3. Έλεγχος των στοιχείων | |

***Σχήμα 10:*** *Process Step 1 (Βήμα διαδικασίας B1-πρόσβαση στο site)*

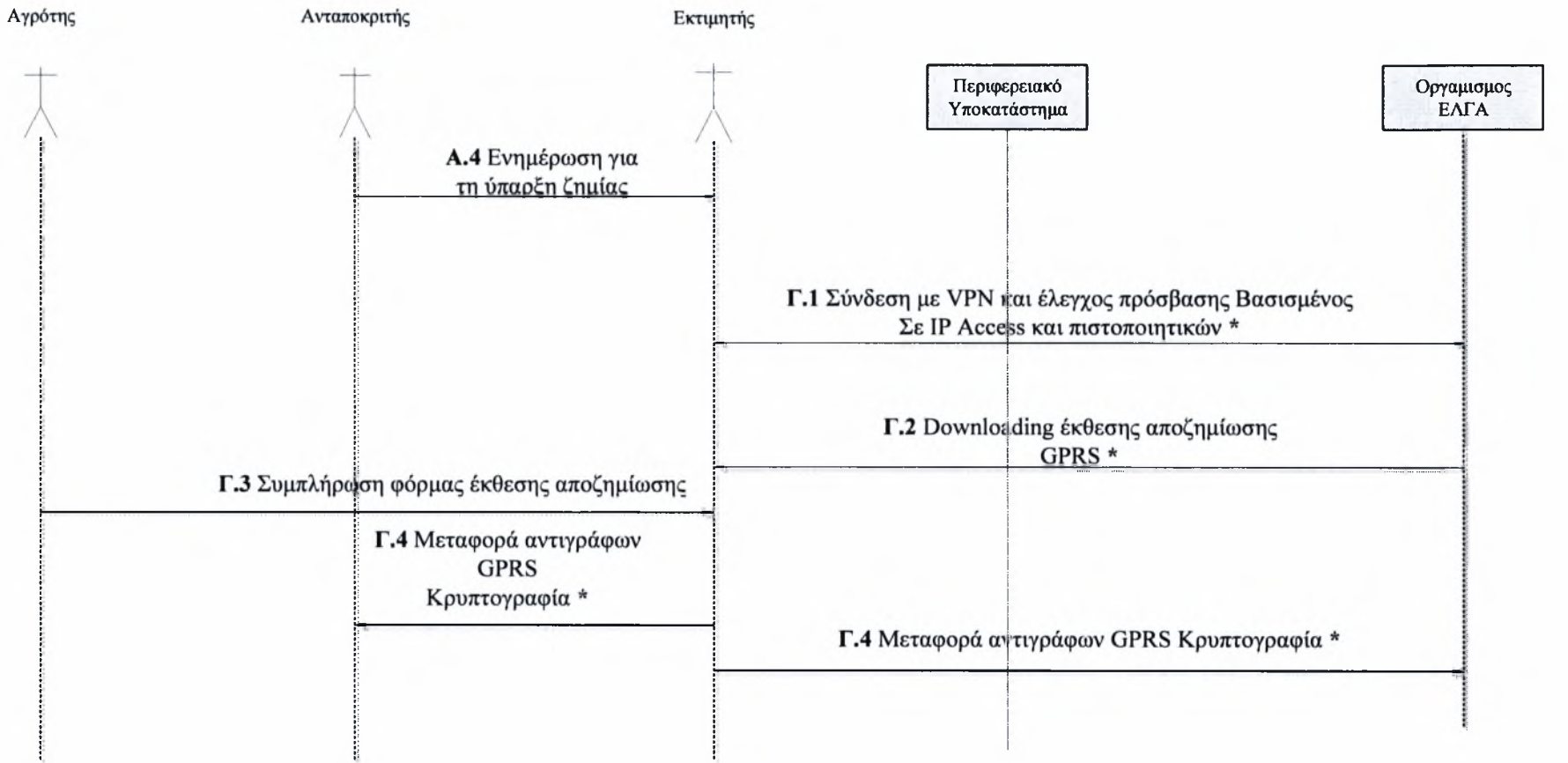
### 3.2.5 **Ροή διαδικασίας** (Interleaved Process Flow 2-Εκτίμηση της ζημίας-έγγραφο αποζημίωσης)

Σε αυτό το διάγραμμα (*σχήμα 11*) αναλύουμε τη διαδικασία εκτίμηση της ζημίας από τον από εκτιμητή. Αυτή η διαδικασία είναι μια ενδιάμεση κατάσταση από το *Interleaved Process Flow 1.*

Λεκτική περιγραφή:

ο Εκτιμητής ενημερώνεται από το Ανταποκριτή για την ύπαρξη ζημίας (**Α.4**). Ο οργανισμός του ΕΛΓΑ παρέχει στο Εκτιμητή πληροφοριακά συστήματα, ο οποίος συνδέεται και ελέγχεται με την IP διεύθυνση και με τα πιστοποιητικά (**Γ.1***). Στην συνέχεια εκτελούμε οι διαδικασίες της Downloading της έκθεσης αποζημίωσης και μετέπειτα έχουμε την μεταφορά αντιγράφων από τον εκτιμητή προς τον ανταποκριτή και στον οργανισμό του ΕΛΓΑ αντίστοιχα. (**Γ.3**, **Γ.4***).

Οι διαδικασίες που φέρουν κάποιο αστερίσκο, αναπαριστούνε κάποια καταστάσεις και παραμέτρους, που θα αναλύσουμε και περαιτέρω.




***Σχήμα 11:*** *Interleaved Process Flow 2*

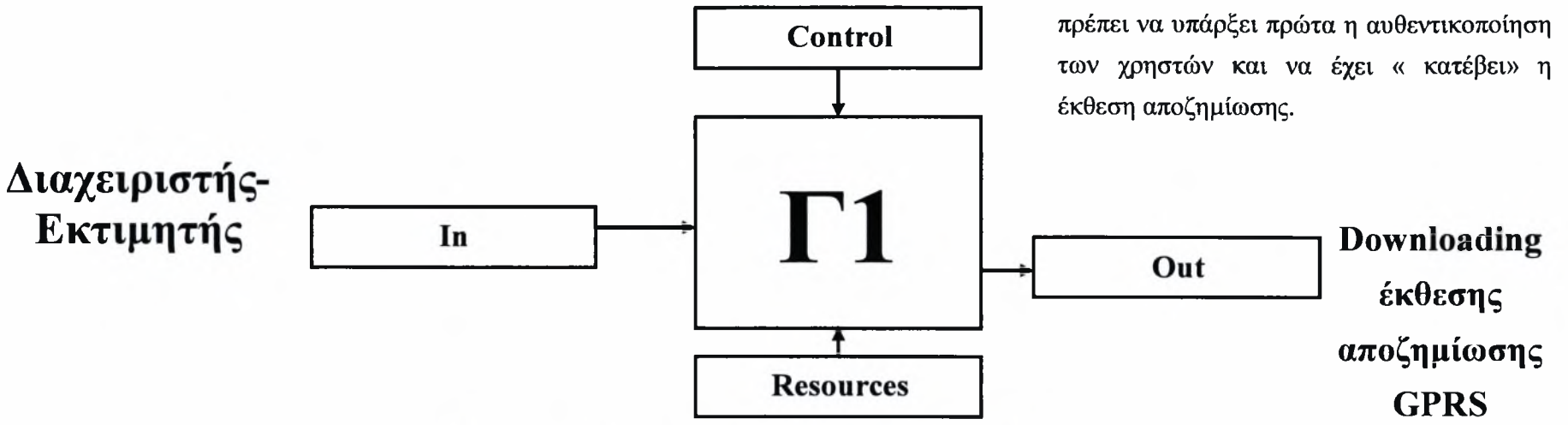
### 3.2.6 **Βήμα διαδικασίας 2** (Process Step 2- Σύνδεση με VPN και έλεγχος πρόσβασης βασισμένος σε IP access και πιστοποιητικών)

Το **Γ1** είναι ένα βήμα της διαδικασίας Σύνδεση *με VPN και έλεγχος πρόσβασης βασισμένος σε IP access και πιστοποιητικών*. Και αυτό το βήμα αποτελείται από εισόδους (In), Ελέγχους (Control), Πόρους (Resources), Εξόδους (Out) και από παράμετροι, καταστάσεις και Value Object. Για να εκτελεστεί ο έλεγχος αναγκαία συνθήκη είναι να έχει γίνει εκ των προτέρων μια άλλη διαδικασίας. Επίσης κάθε έξοδος είναι και είσοδος σε επόμενα βήματα. (όπως για παράδειγμα στο βήμα Β1 η έξοδος είναι «Εκτιμητές», οι εκτιμητές είναι είσοδοι στο βήμα Γ1). Οι παράμετροι είναι κάτι που επεξεργαζόμαστε.

Έτσι στο *σχήμα 12* θα έχουμε :

Ως είσοδο (In) έχουμε το *Downloading έκθεσης αποζημίωσης GPRS*. Στον Έλεγχο (Control) έχουμε τις αναγκαίες συνθήκες: 1) Για να ξεκινήσει το « κατέβασμα» της έκθεσης αποζημίωσης πρέπει να πρώτα να υπάρξει η αυθεντικοποίηση των χρηστών. Στους πόρους θα έχουμε Servers, Βάση δεδομένων, Σύνδεση στο Web, πληροφορίες, PDA.Επιπλέον χρειαζόμαστε και δύο παραμέτρους με τις αντίστοιχες καταστάσεις.

Για να ξεκινήσει η διαδικασία της αυτοψίας πρέπει να υπάρξει πρώτα η αυθεντικοποίηση των χρηστών και να έχει « κατέβει» η έκθεση αποζημίωσης.




Σύνδεση στο Web, Πληροφορίες, Υποδομές ασφαλείας, Servers, Κεντρικός υποκατάστημα, Εκτιμητές

| Παράμετροι | Καταστάσεις | Value Object |
|---|---|---|
| 1. Αυθεντικοποίηση της IP Access. | 1. Σύγκριση IP access. Ο VPN server δίνει στους VPN client μία IP διεύθυνση χρησιμοποιώντας το πρωτόκολλο( **DHCP** ) και ανάλογα γίνεται επιτυχία ή αποτυχία σύνδεσης. | 1. IP Access |
| 2. Πιστοποίηση του χρήστη | 2. Αριθμοί PIN. Έλεγχος υπάρξεις πιστοποιητικών, επιβεβαίωση των στοιχείων, Σύνδεση ή απόρριψη στο δίκτυο VPN | 2. Πιστοποιητικά |

| Παράμετροι | Καταστάσεις | Value Object |
|---|---|---|
| 3. Πιστοποίηση δεδομένων | 3. Τα δεδομένα δεν πρέπει να τροποποιούνται κατά την διαδρομή μέσα στην σύνδεση VPN και κάποιο κρυπτογραφικό πεδίο. | |
| 4. Κρυπτογράφηση Δεδομένων | 4. Απαιτείται να γνωρίζουν και ο παραλήπτης και ο αποστολέας το κοινό κλειδί αποκρυπτογράφησης. | |

***Σχήμα 12:*** *Process Step 2 (Βήμα διαδικασίας Γ1-Σύνδεση με VPN και έλεγχος πρόσβασης βασισμένος σε IP Access και πιστοποιητικών)*

### 3.2.7 **Βήμα διαδικασίας 3** (Process Step 3-Downloading έκθεσης αποζημίωσης GPRS)

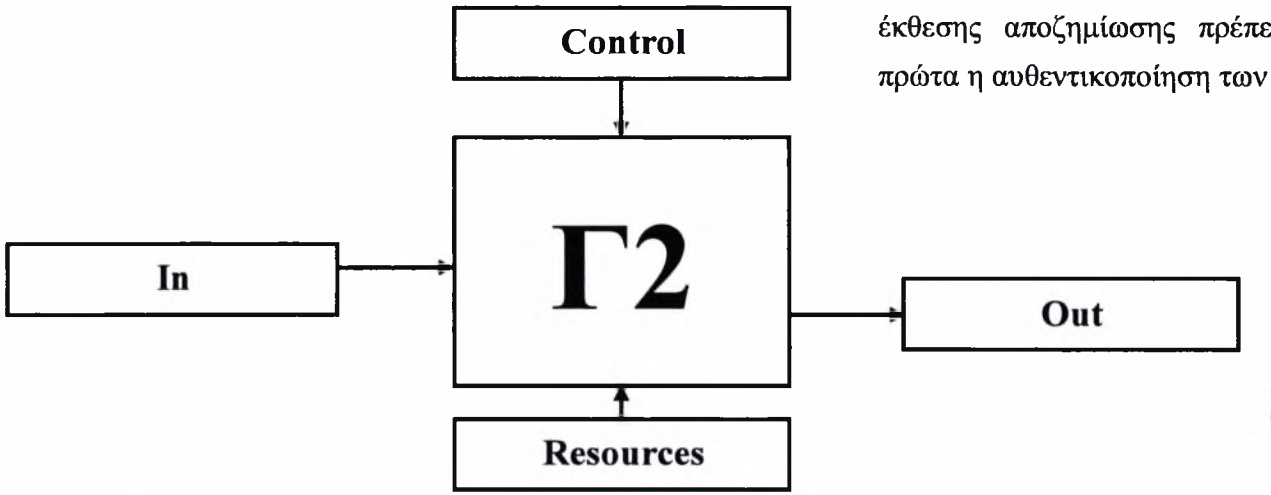
Το **Γ2** είναι ένα βήμα της διαδικασίας Downloading *έκθεσης αποζημίωσης GPRS.* Κάθε τέτοιο βήμα αποτελείται από εισόδους (In), Ελέγχους (Control), Πόρους (Resources), Εξόδους (Out) και από παράμετροι, καταστάσεις και Value Object. Για να εκτελεστεί ο έλεγχος αναγκαία συνθήκη είναι να έχει γίνει εκ των προτέρων μια άλλη διαδικασίας. Επίσης κάθε έξοδος είναι και είσοδος σε επόμενα βήματα. (όπως για παράδειγμα στο βήμα Β1 η έξοδος είναι «Εκτιμητές», οι εκτιμητές είναι είσοδοι στο βήμα Γ1). Οι παράμετροι είναι κάτι που επεξεργαζόμαστε.

Έτσι στο σχήμα 13 θα έχουμε :

Ως είσοδο (In) τον διαχειριστή του συστήματος ( υπάλληλος ). Στον Έλεγχο (Control) έχουμε τις αναγκαίες συνθήκες: 1) πρέπει οι υπάλληλοι να προσκομίσουν τα απαραίτητα δικαιολογητικά από τους αγρότες και 2) να υπάρξει πόρισμα της βασικής αίτησης και μετά να ασκηθεί το δικαίωμα της επανεκτίμησης. Στους πόρους θα έχουμε σύνδεση στο web, Πληροφορίες, υποδομές ασφαλείας, server, κεντρικό υποκατάστημα, Υπάλληλοι του περιφερειακού υποκαταστήματος. Επιπλέον χρειαζόμαστε και τρεις παραμέτρους με τις αντίστοιχες καταστάσεις.

Για να ξεκινήσει το «κατέβασμα» της έκθεσης αποζημίωσης πρέπει να υπάρξει πρώτα η αυθεντικοποίηση των χρηστών.

**Downloading έκθεσης αποζημίωσης GPRS**




**Αυτοψία+ αποζημίωση (σε χρηματικό ποσό)**

Servers, Βάση δεδομένων, Σύνδεση στο Web, Πληροφορίες, PDA

| **Παράμετροι** | **Καταστάσεις** | **Value Object** |
|---|---|---|
| 1. Έκθεσης αποζημίωσης | 1. Η έκθεση είναι κενή και πρέπει να κατέβει. Συμπλήρωση και αποστολή | 1. Έκθεση αποζημίωσης |
| 2. Υποδομές ασφαλείας | 2. Κρυπτογράφηση- αποκρυπτογράφηση | |

***Σχήμα 13:*** *Process Step3 (Βήμα διαδικασίας Γ2-downloading έκθεσης αποζημίωσης GPRS)*

# Κεφάλαιο 4

# Ανάλυση των θεμάτων Ασφαλείας και προτεινόμενες λύσεις

## 4.1 Επισκόπηση Κεφαλαίου

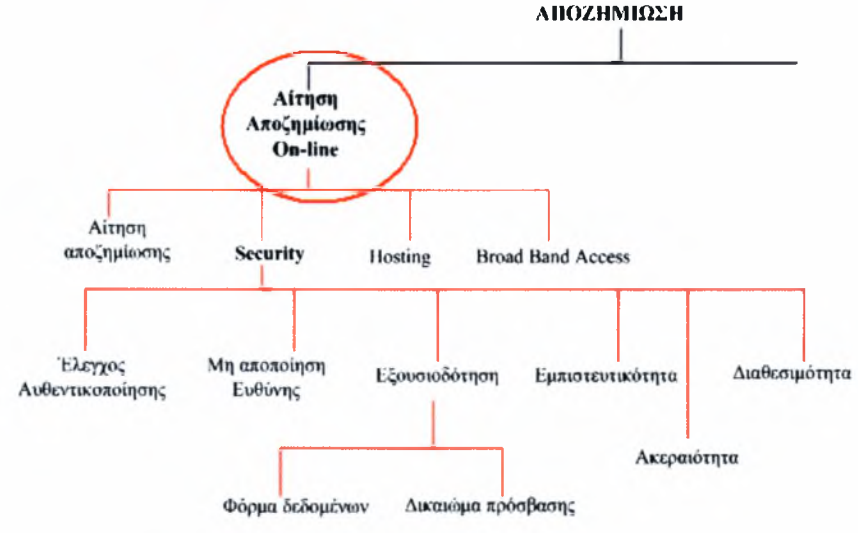
Εφόσον έχει ολοκληρωθεί η ανάπτυξη μια ηλεκτρονικής υπηρεσίας, σε αυτό το κεφαλαίο θα επιχειρηθεί να γίνει μια λεπτομερέστατη ανάλυση των προβλημάτων και των λύσεων που συσχετίζονται με τη προαναφερθείσα διαδικασία e-business. Παρατηρώντας λοιπόν τα διαγράμματα της ηλεκτρονικής υπηρεσίας, εύκολα γίνεται αντιληπτό, πως τα προβλήματα και λύσεις εγκλείονται σε δύο ενότητες. Αφενός στα ενσύρματα δίκτυα και αφετέρου στα ασύρματα δίκτυα .

## 4.2 Ηλεκτρονική υπηρεσία: Ενσύρματα Δίκτυα, Προβλήματα και Μηχανισμοί ασφαλείας

Στα ενσύρματα δίκτυα βρίσκουμε τις εφαρμογές του διαδικτύου (Internet). Τα προβλήματα και οι λύσεις τους θα πρέπει να συσχετιστούνε με τα διαγράμματα της ηλεκτρονικής υπηρεσίας. Δηλαδή *με τη Ιεραρχία Αξίας, με το Γράφημα Συναλλαγών Αξίας, την Ιεραρχία Επιχειρηματικών Διαδικασιών, με την Ιεραρχία Στόχων, με τις Ροές Διαδικασιών, καθώς επίσης και τα βήματα τους.* Τα *σχήματα* από *14* μέχρι *18* δείχνουμε σε ποια σημεία εστιάζονται τα όποια προβλήματα και που μπορούμε να προτείνουμε λύσεις.

### 4.2.1 Ιεραρχία Αξίας : ανάλυση θεμάτων ασφαλείας και προβλήματα

Πριν ξεκινήσει η καταγραφή των θεμάτων ασφαλείας και των λύσεων, στο *σχήμα 14* που ακολουθεί σημειώνεται τι είδους εφαρμογή θέλουμε να υλοποιήσουμε στο Διαδίκτυο (Internet). Συγκεκριμένα έχουμε να συμπληρώσουμε της αίτηση αποζημίωσης on-line.




***Σχήμα 14:*** *Value Hierarchy και τα σημείο εστίασης των προβλημάτων και λύσεων*

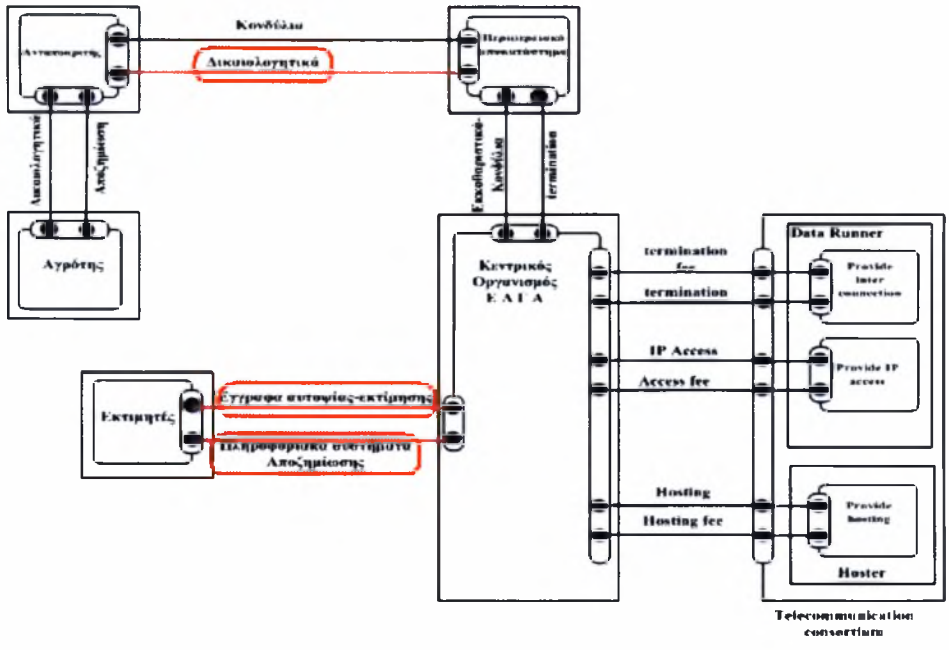
Συνεπώς θα ασχοληθούμε κυρίως με τα επίπεδα διαδικτύου και μεταφοράς. Κατά την μεταφορά της αίτησης, ορατοί είναι οι κίνδυνοι : η *έλλειψη εμπιστευτικότητας* και η *μη εξουσιοδοτημένη τροποποίηση των πληροφοριών*. Στην μεν έλλειψη εμπιστευτικότητας τα δεδομένα είναι χωρισμένα σε πακέτα που μπορούν εύκολα να κλαπούν και να αποκαλυφθεί το περιεχόμενο. Στη δε μη εξουσιοδοτημένη τροποποίηση των πληροφοριών, οι πληροφορίες μπορούν να τροποποιηθούν, κατά την μεταφορά του με τέτοιο τρόπο που ο παραλήπτης δεν μπορεί να αντιληφθεί τις διενεργηθείσες μεταβολές. Τα προβλήματα που είναι πιθανά να υπάρχουν στην Ιεραρχία Αξίας (Value Hierarcy) είναι: 1) *Εύκολη παρακολούθηση και ανίχνευση*. Εδώ όλες οι πληροφορίες που κινούνται με την μορφή πακέτων tcp/ip, μπορούν να

παρακολουθήσουν εύκολα χρησιμοποιώντας ευρέως διαθέσιμο software (π.χ sniffer). Αυτό είναι πάρα πολύ σημαντικό πρόβλημα μιας και η πλειοψηφία των πληροφοριών που ανταλλάσσονται είναι μη κρυπτογραφημένες, 2) *η Άρνηση Εξυπηρέτησης (Denial of Service).* Αυτός ο κίνδυνος έχει σαν αποτέλεσμα την μη διάθεση υπηρεσιών σε νόμιμους χρήστες, 3) *Επιθέσεις Παρακολούθησης( Sniffing).* Στο εδάφιο 2.4.2.3.3 υπάρχει μια λεπτομερή ανάλυση αυτού του προβλήματος

Εφόσον μιλήσαμε για προβλήματα που μπορούν να συμβούνε στην Ιεραρχία Αξίας (Value Hierarchy), είναι επίσης σημαντικό να γίνει αναφορά και στις *λύσεις*. Σε επίπεδο διαδικτύου χρησιμοποιούμε την *τεχνολογία IPsec*. Τα σημαντικότερα χαρακτηριστικά της συγκεκριμένης τεχνολογίας είναι η εμπιστευτικότητα και η ακεραιότητα. Δηλαδή τα πακέτα δεν αλλοιώνονται κατά την μεταφορά. Επιπρόσθετα η τεχνολογία υποστηρίζει αλγορίθμους κρυπτογράφησης δέσμης (block encryption) 3DES, Αποτρέπει επιθέσεις man-in-the-middle μέσω ελέγχου πακέτων και μεταχειρίζεται UDP ροές πακέτων και αποτρέπει επιθέσεις άρνησης παροχής υπηρεσιών/ Dos. Τέλος για να αποτρέψουμε τις επιθέσεις παρακολούθησης, συνιστάτε η χρήση κρυπτογραφημένων passwords Τα passwords θα πρέπει να κρυπτογραφούνται, πριν χρησιμοποιηθούν για οποιονδήποτε λόγο.

### 4.2.2 Γράφημα συναλλαγών αξίας : ανάλυση θεμάτων ασφαλείας και προβλήματα

Στο *σχήμα 15* που ακολουθεί σημειώνεται τι είδους εφαρμογή θέλουμε να υλοποιήσουμε στο Διαδίκτυο (Internet). Και πάλι στο γράφημα συναλλαγών αξίας (Value Exchange Graph) έχουμε μεταφορά δεδομένων από το διαδίκτυο. Επομένως για προβλήματα και λύσεις ισχύουνε ότι και στη Ιεραρχία Αξίας.



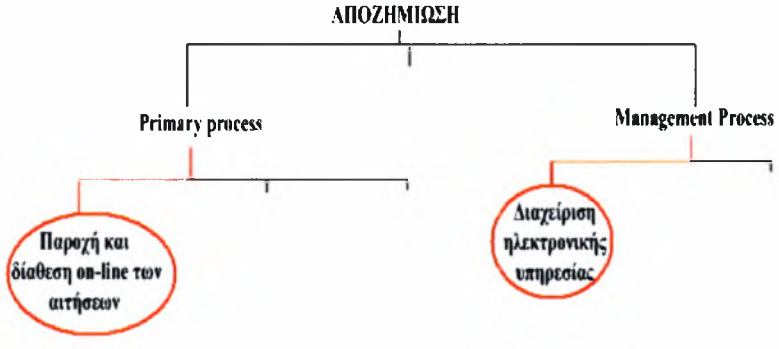

***Σχήμα 15:*** *Value Exchange Graph και τα σημεία εστίασης των προβλημάτων και λύσεων*

Τα "κινητά αντικείμενα", περιστρέφονται γύρω από τον Κεντρικό Οργανισμό του ΕΛΓΑ. Έτσι και το περιφερειακό υποκατάστημα, οι οποιαδήποτε "συναλλαγές" με το Κεντρικό οργανισμό ΕΛΓΑ γίνονται με το διαδίκτυο. Αρχικά γίνεται έλεγχος IP access, σαφώς και έχουμε την κατάσταση της επιτυχίας ή αποτυχίας πρόσβασης. Για την κρυπτογράφηση των στοιχείων χρησιμοποιείται ο μηχανισμός SSL. Ο ανταποκριτής συλλέγει τα δικαιολογητικά από τον αγρότη και τα στέλνει στο Περιφερειακό υποκατάστημα. Αντίστοιχα το Περιφερειακό υποκατάστημα στέλνει στον Ανταποκριτή οικονομικά στοιχεία (κονδύλια).

Σημαντική παρατήρηση είναι πως σε αυτό το διάγραμμα οι εκτιμητές που είναι και εκείνοι, κινητά αντικείμενα, τους παρέχονται πληροφοριακά συστήματα αποζημίωσης (PDA). Για την συγκεκριμένη εφαρμογή θα την αναλυθεί κάπου παρακάτω (εδάφιο 4.3.2)

### 4.2.3 Ιεραρχία Επιχειρηματικών διαδικασιών: ανάλυση θεμάτων ασφαλείας και προβλήματα

Στο ακολούθως *σχήμα 16* σημειώνεται τι είδους εφαρμογές θέλουμε να υλοποιήσουμε στο Διαδίκτυο (Internet).




***Σχήμα 16:*** *Business Process Hierarchy και τα σημεία εστίασης των προβλημάτων και λύσεων*

Αξίζει να υπομνησθεί πως στις αρχικές διαδικασίες είναι εκείνες που συμβάλλουν άμεσα προς την ικανοποίηση των αναγκών μας, στην προκειμένη περίπτωση είναι η *Αποζημίωση*. Είναι ήδη γνωστό από τα προαναφερθείσα διαγράμματα, τις προβλήματα και λύσεις αντιμετωπίζουμε κατά την παροχή και διάθεση των αιτήσεων on-line. Αυτό που έχε μέγιστη σημασία να καταγράψουμε πλήρως, στην διαχείριση της ηλεκτρονικής υπηρεσίας, τι προβλήματα και τι λύσεις έχουμε να αντιπαραβάλλουμε σε αυτά .

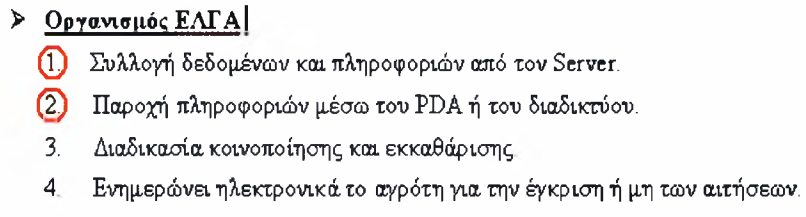
Σοβαρά υποψίν θα πρέπει να λάβουμε πως θα εξασφαλίσουμε τη ιδιωτικότητα του χρήση που διαχειρίζεται την εν λόγω ηλεκτρονική υπηρεσία. Τα προβλήματα που είναι εφικτό να παρουσιαστούν στην ανάπτυξη μιας ηλεκτρονικής υπηρεσίας οφείλονται εν πολύς στην απουσία καλής πολιτικής ασφαλείας. Τέτοιου είδους προβλήματα παρουσιάζονται εκτενέστερα στα εδάφια 2.4.2 ως και 2.4.3.5.

Πέρα όμως από τα προβλήματα μια ηλεκτρονική υπηρεσία θα πρέπει να εκπληρώνει στο έπακρο το θέμα της Ασφάλειας. Η Ασφάλεια ως εκ τούτου, θεμελιώνεται πάνω σε δύο κατευθυντήριους άξονες. Από την πλευρά του εξυπηρετητή και από την πλευρά του χρήστη. Από την πλευρά του Εξυπηρετητή μπορούμε να παρέχουμε : 1) *Έλεγχο Πρόσβασης Βασισμένο σε IP Διεύθυνση*, 2) *Έλεγχο Πρόσβασης Βασισμένο στο όνομα του χρήστη και στο κωδικό προσπέλασης*, 3) *Έλεγχο Πρόσβασης*

*Βασισμένο σε πιστοποιητικά.* Αυτοί οι έλεγχοι μπορούν να γίνουνε αφενός με τη τεχνολογία του firewall και αφετέρου με την υπηρεσία του Kerberos Από την πλευρά του χρήστη μπορούμε να παρέχουμε : 1) SSL 2) VPN (με την απαραίτητη υποστήριξη του IPsec) 3) Δικτυακά συστήματα ανίχνευσης εισβολέων. Λεπτομερειακά αυτές οι λύσεις ασφαλείας αναφέρονται στα εδάφια 2.4.4 ως και 2.4.4.3.

### 4.2.4 Ιεραρχία Στόχων : ανάλυση θεμάτων ασφαλείας και προβλήματα

Ξανά στο *σχήμα 17* δείχνουμε ποια είναι τα μέρη που συναντούμε την εφαρμογή του διαδικτύου και αντίστοιχα τα προβλήματα με τις λύσεις που εντοπίζονται.



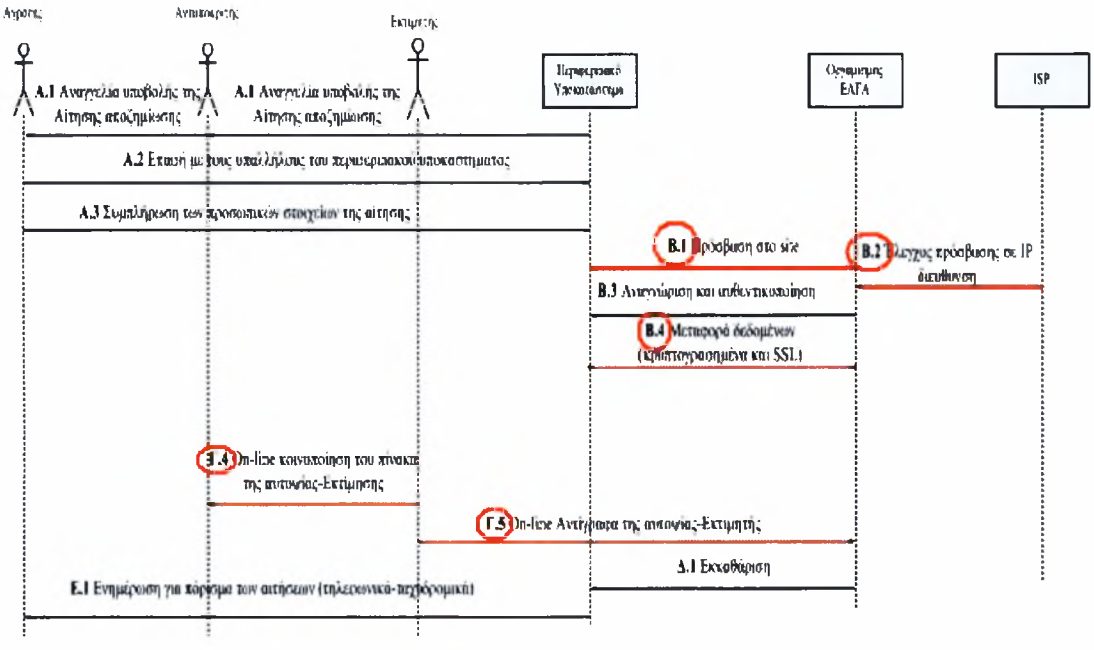

***Σχήμα 17:*** *Task Hierarchy και τα σημεία εστίασης των προβλημάτων και λύσεων*

Κατά τα γνωστά τα προβλήματα που εντοπίζουμε και εδώ 1) *Εύκολη παρακολούθηση και ανίχνευση.* 2) *η Άρνηση Εξυπηρέτησης (Denial of Service).* Αυτός ο κίνδυνος έχει σαν αποτέλεσμα την μη διάθεση υπηρεσιών σε νόμιμους χρήστες, 3) *Επιθέσεις Παρακολούθησης (Sniffing).* Προφανώς και οι λύσεις θα είναι IPsec και SSL.

### 4.2.5 Λοιπά διαγράμματα : ανάλυση θεμάτων ασφαλείας και προβλήματα

Οι ροές αλλά και τα βήματα διαδικασίας είναι υποδιαγράμματα της Ιεραρχίας επιχειρηματικών διαδικασιών (Business Process Hierarchy). Τα εντοπιζόμενα

προβλήματα (και οι λύσεις) επαναλαμβάνονται. Στο *σχήμα 18* έχουμε το διάγραμμα της Ροής Διαδικασίας που αφορά την εφαρμογή του διαδικτύου. Στα βήματα που φέρουν ένα κόκκινο κύκλο είναι τα σημεία που μπορούμε να εντοπίσουμε τα προβλήματα.




***Σχήμα 18:*** *Interleaved Process Flow 1 τα σημεία εστίασης των προβλημάτων και λύσεων*

Παραδείγματος χάρη, ας αναλύσουμε το *Βήμα διαδικασίας B1* (Process Step1[2]) θα έχουμε: η υπηρεσία του SSL εφαρμόζεται στα επίπεδα 4-7. Οι κίνδυνοι που μπορούν να γίνουν σε αυτά τα επίπεδα οφείλονται σε επιθέσεις. Τέτοιες επιθέσεις μπορεί είναι : 1) προσποίηση (spoofing) IP διεύθυνσης, 2) υποκλοπή δεδομένων 3) Άρνηση προσπέλασης. Καταρχήν κατά επικύρωση και την πρόσβαση ελέγχου χρησιμοποιούνται ψηφιακά πιστοποιητικά. Όσο για την κρυπτογράφηση του κωδικού και του username χρησιμοποιούνται οι κρυπτογραφικοί αλγόριθμοι 3DES και RC4.

[2] *Δείτε το διάγραμμα στη σελίδα 67*

## 4.3 Ηλεκτρονική υπηρεσία: Ασύρματα Δίκτυα, Προβλήματα και Μηχανισμοί ασφαλείας

Στα ασύρματα δίκτυα βρίσκουμε τις εφαρμογές του δικτύου υλοποίησης VPN με τα ασύρματα πρωτόκολλα εφαρμογής GPRS. Τα προβλήματα και οι λύσεις θα πρέπει να συσχετιστούνε με τα διαγράμματα της ηλεκτρονικής υπηρεσίας όπως έχει γίνει και στα ενσύρματα δίκτυα. Δηλαδή να συγκρίνουμε εν νέου με τα διαγράμματα της Ιεραρχία Αξίας, με το γράφημα συναλλαγών αξίας, την Ιεραρχία επιχειρηματικών διαδικασιών, με την ιεραρχία στόχων, με τις Ροές διαδικασιών και τα βήματα τους. Συνεπώς με το ίδιο τρόπο, *τα σχήματα από 19 μέχρι 23* δείχνουμε σε ποια σημεία εστιάζονται τα όποια προβλήματα και που μπορούμε να προτείνουμε λύσεις.

### 4.3.1 Ιεραρχία Αξίας : ανάλυση θεμάτων ασφαλείας και προβλήματα

Στο *σχήμα 19* που ακολουθεί εστιάζονται τα εντοπιζόμενα προβλήματα που έχουμε με την σύνδεση των πληροφοριακών συστημάτων. Στην προκειμένη περίπτωση στη ανάπτυξη της δικής μας ηλεκτρονικής υπηρεσίας με την σύνδεση των πληροφοριακών συστημάτων εννοούμε τις φορητές συσκευές PDA.

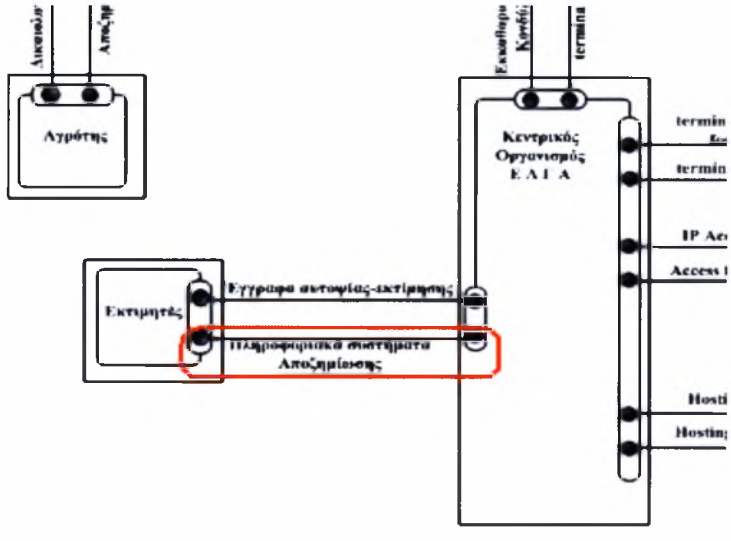

***Σχήμα 19:*** *Value Hierarchy τα σημεία εστίασης των προβλημάτων σε Πληροφοριακά Συστήματα Αποζημίωσης*

Δεδομένου ότι αυτές οι συσκευές ορίζουν τις διευθύνσεις IP τους, οι συσκευές οι ίδιες μπορούν να γίνουν οι στόχοι των επιθέσεων. Τέτοιες επιθέσεις έχουνε να κάνουν και με την αυθεντικοποίηση των χρηστών (εκτιμητών) Για την αυθεντικοποίηση απαιτείται κάποιος κωδικός πρόσβασης Αν το σύστημα δεν έχει μια καλή πολιτική ασφαλείας μπορεί ένας εισβολέας μπορεί να συνδεθεί με το εσωτερικό δίκτυο. Με άλλα λόγια μπορούμε να έχουμε *Επιθέσεις εναντίων των Password στα Access Points* Αναγκαίο είναι λοιπόν από τους οργανισμούς να εφαρμόσουνε μια πολιτική ασφαλείας για να εξασφαλίσουν αφενός τη ασφαλή ρύθμιση των σημείων πρόσβασης και αφετέρου το δίκτυο να ανιχνεύεται για την προστασία μη εξουσιοδοτημένων συσκευών. Ένα σημαντικό πρόβλημα είναι οι *Επιθέσεις παρεμβολής παρασίτων (Jamming).* Οι επιθέσεις παρεμβολής παρασίτων οδηγούν στην άρνηση υπηρεσιών και εφαρμόζονται εύκολα στα ασύρματα δίκτυα. Η συνέπεια του προβλήματος είναι η απώλεια της διαθεσιμότητας. Οι λύσεις σε αυτά τα προβλήματα είναι να δημιουργήσουμε ένα VPN χρησιμοποιώντας το IPSec σε μέθοδο σήραγγας και ενεργοποιώντας τις υπηρεσίες κρυπτογράφησης και αυθεντικοποίησης. Επιπρόσθετα πρέπει να υποστηρίζεται η χρήση FIREWALL και αντιικών προγραμμάτων για να προστατευθούν ενάντια σε ορισμένες επιθέσεις DoS. Στο εδάφιο 2.5.4 γίνεται αναφορά για του τρόπους προστασίας των φορητών συσκευών.

Κατά την σύνδεση με τα πληροφοριακά συστήματα έχουμε και την υπηρεσία του GPRS. Τα προβλήματα που μπορούμε να εντοπίσουμε εδώ είναι: *Επιθέσεις παρακολούθησης της κίνησης* Στο ασύρματο δίκτυο όπως και στο ενσύρματο είναι δυνατό να καταγράψει και να ελεγχθεί η κυκλοφορία του σημείο πρόσβασης. Η καταγραφή γίνεται πιο εύκολα από το ενσύρματο μιας και δεν απαιτείται ενεργητική παρακολούθηση του δικτύου, αρκεί μόνο ένα λογισμικό καταγραφής της κίνησης το οποίο δεν γίνεται αντιληπτό. Η λύσης ασφάλειας, παρέχεται μέσω του ασύρματου στρώματος ασφάλειας μεταφορών (WTLS), το οποίο λειτουργεί άμεσα πάνω από το στρώμα μεταφορών του πρωτοκόλλου. Οι στόχοι της προδιαγραφής WTLS είναι να παρασχεθεί η πιστοποίηση ταυτότητας, η ιδιωτικότητα, και η ακεραιότητα στοιχείων μέσω της χρήσης των πιστοποιητικών και της κρυπτογράφησης.

### 4.3.2 Γράφημα συναλλαγών αξίας : ανάλυση θεμάτων ασφαλείας και προβλήματα

Στο *σχήμα 20* που ακολουθεί εστιάζονται τα εντοπιζόμενα προβλήματα που έχουμε με την σύνδεση των πληροφοριακών συστημάτων.



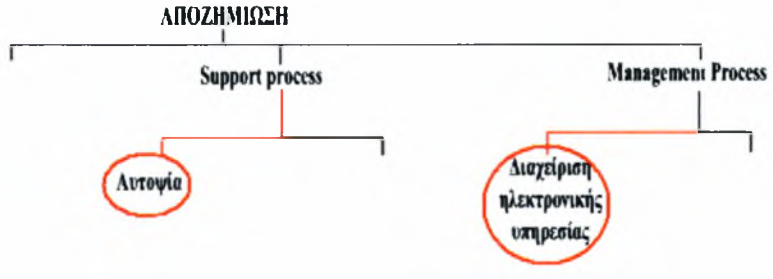

***Σχήμα 20:*** *Value Exchange Graph το σημεία εστίασης των προβλημάτων σε Πληροφοριακά Συστήματα Αποζημίωσης*

Εφόσον τα πληροφοριακά συστήματα αποζημίωσης (PDA) παρέχονται στο Εκτιμητή, έτσι και ο μηχανισμός IPsec κάνει πιο ΑΣΦΑΛΕΣ την επικοινωνία Εκτιμητή και του Οργανισμού του ΕΛΓΑ. Πιο συγκεκριμένα η μακρινή πρόσβαση VPNs απαραίτητη είναι η αυθεντικοποίηση των χρηστών και συσκευών. Η αυθεντικοποίηση συσκευών χρησιμοποιείται κάποιο βασικό κλειδί ή κάποιο ψηφιακό πιστοποιητικό για να παρέχει την ταυτότητα μιας συσκευής. Τα ψηφιακά πιστοποιητικά περιέχουν υπογεγραμμένες πληροφορίες για τη συσκευή που επικυρώνεται από την *Certificate-Authority* (CA). Ο μακρινός χρήστης επικυρώνεται αρχικά από *Access Control Lists* (ACLs) η οποία καθορίζεται από την πολιτική βάση δεδομένων ασφαλείας. Για την αυθεντικοποίηση χρησιμοποιούνται οι *One-Time Passwords* (OTPs) μέσω *Extended Authentication* (XAUTH) και στη συνέχεια λαμβάνει μια εικονική διεύθυνση IP που χρησιμοποιούνται

για την VPN-προορισμένη κυκλοφορία. Βεβαίως τα προβλήματα και λύσεις είναι ήδη γνωστά από το προηγούμενο διάγραμμα της Ιεραρχίας Αξίας.

### 4.3.3 Ιεραρχία Επιχειρηματικών διαδικασιών: ανάλυση θεμάτων ασφαλείας και προβλήματα

Στο επακολουθούμενο *σχήμα 21* εστιάζονται τα εντοπιζόμενα προβλήματα που έχουμε με την σύνδεση των πληροφοριακών συστημάτων.

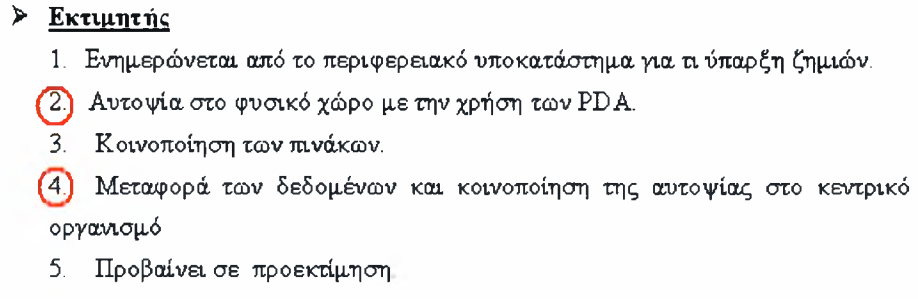



***Σχήμα 21:*** *Value Exchange Graph το σημεία εστίασης των προβλημάτων σε Πληροφοριακά Συστήματα Αποζημίωσης*

Να θυμίσουμε απλά πως οι διαδικασίες υποστήριξης (Support Process): επιτρέπουν την εκτέλεση των αρχικών διαδικασιών και παρέχουν ένα κατάλληλο εργασιακό περιβάλλον. Επίσης οι διαδικασίες διαχείρισης (Management Process): κατευθύνουν και ελέγχουν τις αρχικές διαδικασίες και τις διαδικασίες υποστήριξης. Στο καθορισμένο διάγραμμα σημειώνεται αφενός η «Αυτοψία» που προϋποθέτει να έχει γίνει η σύνδεση με τα Πληροφοριακά συστήματα και αφετέρου η «Διαχείριση ηλεκτρονικής υπηρεσίας», σε συνδυασμό με την εφαρμογή του Διαδικτύου, ολοκληρώνεται την η ανάπτυξη της ηλεκτρονικής υπηρεσίας. Λαμβάνοντας υπόψιν όσα έχουν υποθεί στη Ιεραρχία αξία και στο γράφημα συναλλαγών αξίας, ως προς τα προβλήματα και λύσεις, έχουμε φτάσει στο διάγραμμα των ιεραρχικών επιχειρηματικών διαδικασιών.

### 4.3.4 Ιεραρχία Στόχων : ανάλυση θεμάτων ασφαλείας και προβλήματα

Ξανά στο *σχήμα 22* δείχνουμε ποια είναι τα μέρη που συναντούμε τα προβλήματα με τις λύσεις που εντοπίζονται κατά την σύνδεση με τα VPN.

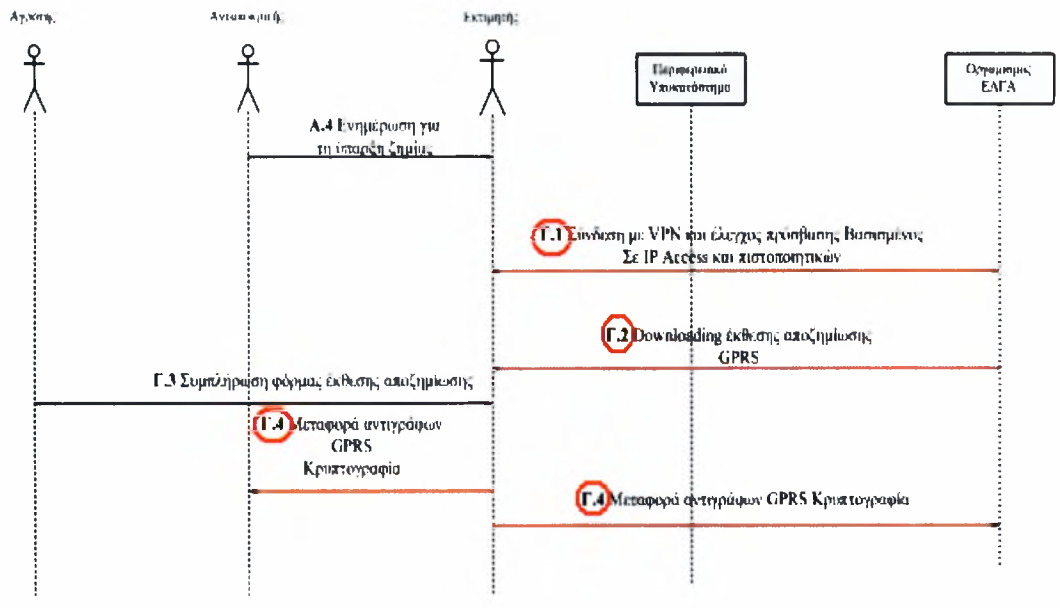



***Σχήμα 22:*** *Task Hierarchy το σημείο εστίασης των προβλημάτων σε Πληροφοριακά Συστήματα Αποζημίωσης*

Το IPsec VPN χρησιμοποιείται για να επικυρωθεί ο χρήστης του PDA (εκτιμητής). Κατά την μεταφορά των πακέτων (από τον οργανισμό ΕΛΓΑ προς τον εκτιμητή και αντίστροφα) χρησιμοποιούνται μηχανισμοί κρυπτογράφησης.

### 4.3.5 Λοιπά διαγράμματα : ανάλυση θεμάτων ασφαλείας και προβλήματα

Όπως και τα ενσύρματα δίκτυα, οι ροές αλλά και τα βήματα διαδικασίας είναι υποδιαγράμματα της Ιεραρχίας επιχειρηματικών διαδικασιών (Business Process Hierarchy). Τα εντοπιζόμενα προβλήματα (και οι λύσεις) επαναλαμβάνονται. Έτσι *σχήμα 23* έχουμε το διάγραμμα της Ροής Διαδικασίας που αφορά την παροχή πληροφοριακών συστημάτων. Στα βήματα που φέρουν ένα κόκκινο κύκλο είναι τα σημεία που μπορούμε να εντοπίσουμε τα προβλήματα

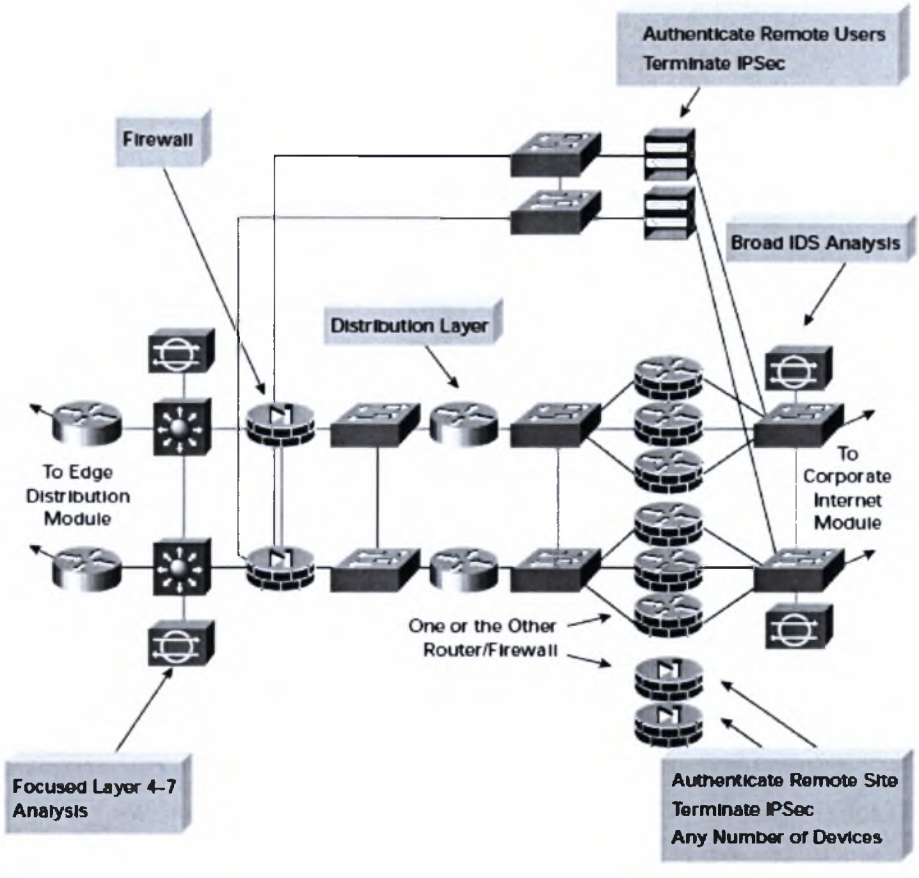



***Σχήμα 23 :*** *Interleaved Process Flow 2 το σημείο εστίασης των προβλημάτων σε Πληροφοριακά Συστήματα Αποζημίωσης*

Ας εξετάσουμε για παραδείγματος χάρη τα *Βήματα διαδικασιών Γ1και Γ2* (Process Step2,3[3]. Τα προβλήματα σε αυτά τα βήματα είναι τα εξής 1) *Επιθέσεις εναντίων των Password στα Access Points, 2) Επιθέσεις παρεμβολής παρασίτων* 3) *Επιθέσεις παρακολούθησης της κίνησης.*

Για να κάνουμε ένα ΑΣΦΑΛΕΣ VPN σε αυτά τα διαγράμματα, καινοτομούμε, αντιπαραβάλλοντας κάποια βιώσιμα σχέδια (όπως παρουσιάζονται στο paper : SAFE VPN IPSec Virtual Private Networks in Depth [21]). Ένα ασφαλές σχέδιο έχει να κάνει με το εύρος της επιχείρησης (μικρή, μεγάλη, κ.τ.λ) που θέλουμε να παρέχουμε μια ασφαλής υλοποίηση, πόσους χρήστες πρέπει να εξυπηρετήσουμε και ποιες είναι οι απαιτήσεις για να πετύχουμε ένα ΑΣΦΑΛΕΣ δίκτυο VPN. Όταν λέμε "απαιτήσεις" εννοούμε τη ασφαλή συνδετικότητα, τη αξιοπιστία, τη απόδοση, τη Αυθεντικοποίηση των χρηστών και των συσκευών στο VPN, ασφαλή διαχείριση και ασφάλεια επιθέσεων πριν και μετά το IPSec.. Θεωρώ ότι ένα ασφαλές σχέδιο για την συγκεκριμένο παράδειγμα του ΕΛΓΑ είναι το μοντέλο μεγάλου δικτύου VPN και remote Access. Στο *σχήμα 24* βλέπουμε ένα τέτοιο σχέδιο.

[3] *Δείτε το διαγράμματα στις σελίδες 71 και 74 αντίστοιχα*




***Σχήμα 24:*** *Detailed Model of Large Network VPN and Remote-Access : VPN*

Αυτό σχέδιο υποστηρίζει και βρίσκουμε δύο τύπους VPN. 1) remote-access VPNs , 2) site-to-site VPNs. Η χρήση του PDA χρησιμοποιεί τον τύπο remote-access VPN. Το site-to-site VPN αναφέρεται στις εφαρμογές στις οποίες το δίκτυο μιας θέσης συνδέεται με το δίκτυο μιας άλλης θέσης μέσω των συσκευών VPN.

Για τις συνδέσεις site-to-site VPN στις μακρινές θέσεις, τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για την ισχυρή αυθεντικοποίηση συσκευών. Επίσης λαμβάνοντας υπόψη το υψηλό επίπεδο πρόσβασης στο εταιρικό δίκτυο, αυτή το σχέδιο εκθέτει ένα υψηλό επίπεδο ασφάλειας. Το stateful λογισμικό επιτρέπει μόνο σε (Internet-key Exchangen ή IKE) και (Encapsulating security payload ή ESP) την κυκλοφορία για να ολοκληρώσει στη δημόσια διεπαφή των firewall VPN. Τέλος αυτό το σχέδιο μπορεί να υποστηρίξει από 100 με 250 μακρινούς χρήστες.

# Κεφάλαιο 5

# Συμπεράσματα και Μελλοντικές Επεκτάσεις

Η διατριβή αυτή στοχεύει σε δύο ενότητες. Η πρώτη ενότητα επικεντρώνεται στην ανάπτυξη και στην παροχή μιας ηλεκτρονικής υπηρεσίας, μέσω των τεχνολογιών των ενσύρματων και ασυρμάτων δικτύων. Εμείς παρουσιάζουμε ένα αντιπροσωπευτικό παράδειγμα εφαρμογής χρήσης μιας ηλεκτρονικής υπηρεσίας το οποίο μπορεί να αναδείξει κάποιες στρατηγικές επιλογές για άλλες σύγχρονες Επιχειρήσεις. Ως αποτέλεσμα έχουμε : αφενός να συνδέσουμε τις (επιχειρησιακές) διαδικασίες με τις ανάγκες των πολιτών και αφετέρου να αυτοματοποιηθεί η εκτίμηση της ζημίας, το συντομότερο χρονικό διάστημα. Η ανάπτυξη μιας τέτοιας ιδέας, προϋποθέτει να περιγράψουμε τα μοντέλα των διαδικασιών (του οργανισμού ΕΛΓΑ) για συστήματα e-business. Πιο αναλυτικά τα μοντέλα των διαδικασιών μπορούν να ομαδοποιηθούν σε δύο κατηγορίες. 1) Την **επισκόπηση αξίας** (Value Viewpoint) όπου περιγράφουμε την *Ιεραρχία Αξίας* (Value hierarchy) και το *Γράφημα Συναλλαγών Αξίας* (Value Exchange Graph). 2) Την **επισκόπηση διαδικασίας** (Process Viewpoint) όπου περιγράφουμε την *Ιεραρχία επιχειρηματικών διαδικασιών* (Business Process Hierarchy), την *Ιεραρχία Στόχων* (Task Hierarchy) καθώς με τις *Ροές διαδικασιών* με τα αντίστοιχα *βήματα διαδικασιών*. Στο πίνακα που έπεται, επιδεικνύονται οι περιγραφές των μοντέλων.

| **Μοντέλο διαδικασιών** | **Περιγραφή** |
|---|---|
| *Value Hierarchy* | Προσδιορίζει την κορυφαία καταναλωτική ανάγκη και διαθέτει αυτό για να αρχίσει το αντικείμενο της οικονομικής αξίας που παράγονται από τους επιχειρησιακούς χειριστές. |
| *Value Exchange Graph* | Προσδιορίζει τις δραστηριότητες μέσα στις οποίες δημιουργούνται τα αντικείμενα ή ανταλλάσσονται από τους επιχειρησιακούς χειριστές. |
| *Business Process Hierarchy* | Περιγράφουμε τις συναλλαγές μεταξύ των επιχειρήσεων με τα αντικείμενα αξίας. |

| | |
|---|---|
| *Task Hierarchy* | Αποσυνθέτει κάθε διαδικασία στους στόχους που εκτελούνται στους επιχειρησιακούς χειριστές |

Εν συντομία τα μοντέλα της η επισκόπηση αξίας, προσδιορίζουν τους χειριστές (actors), τις δραστηριότητες και τις ανταλλαγές που απαιτούνται για να ικανοποιηθεί η ανάγκη. Ομοίως τα μοντέλα της επισκόπησης διαδικασίας προσδιορίζουν στους στόχους που απαιτούνται για να εκτελεστούν οι δραστηριότητες και οι ανταλλαγές.

Αξίζει να σημειωθεί πως η «ανάγκη» της υπηρεσίας, που θέλουμε να ικανοποιήσουμε, συνεπάγεται με τη έννοια της *αποζημίωσης*. Επίσης ως χειριστές θεωρούμαι ότι είναι οι υπάλληλοι των περιφερειακών υποκαταστημάτων, αφού από τα στατιστικά προκύπτει πως το διαδίκτυο δεν είναι ευρέως αναπτυγμένο, ώστε να το χρησιμοποιούν όλοι οι πολίτες.

Η δεύτερη ενότητα παρουσιάζει μια λεπτομερέστατη ανάλυση των προβλημάτων ασφαλείας υπό το πρίσμα των μοντέλων διαδικασιών. Τα προβλήματα ασφαλείας εντοπίζονται και στα δύο περιβάλλοντα εφαρμογών (διαδικτύου και ασύρματης επικοινωνίας), τόσο κατά την επικύρωση των χρηστών σε αυτά, αλλά και τόσο κατά την μεταφορά των δεδομένων. Στις εφαρμογές του διαδικτύου, τα μοντέλα διαδικασιών της Ιεραρχίας αξίας, του γραφήματος συναλλαγών αξίας, της Ιεραρχίας επιχειρηματικών διαδικασιών και της Ιεραρχίας στόχων μπορεί να έχουμε τα εξής προβλήματα 1) Επιθέσεις παρακολούθησης (Sniffing) και ανιχνεύσεις, 2) Άρνηση εξυπηρέτησης (Denial of Service), 3)Επιθέσεις μεταμφίεσης (spoofing), 4) Επιθέσεις «σπασίματος» συνθηματικών, 5) Υποκλοπές δεδομένων. Η άλλη όψη των προβλημάτων είναι οι μηχανισμοί ασφαλείας που προτείνουμε. Έτσι λοιπόν έχουμε: 1)Μηχανισμοί IPsec και SSL. Το IPsec χαρακτηρίζεται από την εμπιστευτικότητα και ακεραιότητα (δεν έχουμε αλλοίωση των δεδομένων) και υπάρχουν αλγόριθμοι κρυπτογράφησης. Στο SSL έχουμε ξανά κρυπτογράφηση των στοιχείων. 2) Χρήση κρυπτογραφημένων passwords και στοιχείων, 3) Παροχή πιστοποιητικών, 4) Δικτυακά συστήματα ανιχνεύσεις εισβολέων. Αντίστοιχα στις εφαρμογές των ασύρματων, τα προβλήματα εντοπίζονται με τις κινητές συσκευές των πληροφοριακών συστημάτων (PDA). Μέσα από τα μοντέλα διαδικασιών της Ιεραρχίας αξίας, του γραφήματος συναλλαγών αξίας, της Ιεραρχία επιχειρηματικών διαδικασιών και της Ιεραρχίας Στόχων έχουμε 1) επιθέσεις ενάντια της αυθεντικοποίησης και κρυπτογράφησης, Στις

ροές και στα βήματα διαδικασιών έχουμε τις 2) Επιθέσεις εναντίων των passwords στα Access Points 3) Επιθέσεις παρεμβολής παρασίτων 4) Επιθέσεις παρακολούθησης της κίνησης. Ομοίως και σε αυτή τη εφαρμογή, η άλλη όψη των προβλημάτων είναι οι μηχανισμοί ασφαλείας που προτείνουμε. Έτσι λοιπόν έχουμε: 1) δίκτυα VPN με τη υποστήριξη του IPSec με τη μέθοδο σήραγγας και ενεργοποιώντας τις υπηρεσίες κρυπτογράφησης και αυθεντικοποίησης. Επίσης θα πρέπει να υποστηρίζεται η χρήση του *Firewall* και αντικών προγραμμάτων για να προστατευθούν ενάντια σε ορισμένες επιθέσεις DoS. 2) ψηφιακά πιστοποιητικά, μηχανισμούς κρυπτογράφησης, 3) Προτεινόμενα Ασφαλή σχέδια

Στην ήδη υπάρχουσα εργασία μια ενδιαφέρουσα μελλοντική επέκταση της διατριβής, είναι στα δίκτυα υλοποίησης VPN να προστεθεί η παράμετρος της φωνής. Οι παροχείς υπηρεσιών είναι πιθανό να παρέχουν έτσι πιο διαφοροποιημένες end-to-end IP-based υπηρεσίες. Και επειδή η φωνή είναι ευαίσθητο προσωπικό δεδομένο θα πρέπει να μελετηθούν, εκ νέου, τι είδους προβλήματα μπορεί να υπάρξουν, τι λύσεις και μηχανισμούς ασφαλείας είναι εφικτό να παρουσιαστούν. Επιπρόσθετα μπορεί μελετηθεί αν μπορούνε να υπάρξουν άλλου είδους προβλήματα και λύσεις στα ασύρματα πρωτόκολλα εφαρμογής του GPRS.

# Βιβλιογραφία


[1] Gaetano Borriello, Matthew Chalmers, Anthony LaMarca, Paddy Nixon, **Delivering Real-World Ubiquitous Location Systems,** *University of Washington, University of Glasgow, University of Strathclyde.*

[2] Bharat Rao, Louis Minakakis, **Assessing the Business Impact of Location Based Services** . In Proceedings of the 37th Hawaii International Conference on System Sciences – 2004.

[3] *Fawsy Bendeckl, Boris Kottingl, Martin Schaaf, Frank Maure, Matthew Valenti, Max Robert,* **Engineering of e-Business Applications & Infrastructure and Applications for the Mobile Internet.** Proceedings of the 10th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE .01).

[4] Iris A. Junglas, Christiane Spitzmóller, **A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services**. *University of Houston.* In Proceedings of the 38th Hawaii International Conference on System Sciences – 2005.

[5] Rui Jos´e, Adriano Moreira, Filipe Meneses, Geoff Coulson**, An Open Architecture for Developing Mobile Location-Based Applications over the Internet.** In Proceedings of the Sixth IEEE Symposium on Computers and Communications (ISCC'01).

[6] Beinat, Euro (2001), **Privacy and Location-based Services**, GeoInformatics, September.

[7] Charles Steinfield, **The Development of Location Based Services in Mobile Commerce.** Department of Telecommunication Michigan State University

[8] Marc Langheinrich, **Privacy by Design - Principles of Privacy-Aware Ubiquitous.** URL: www.inf.ethz.ch/~langhein/

[9] Sharad Chandra Agrawal Sandeep Agrawal, **Location Based Services.** Tata Consultancy Services. 2003

[10] **Location Based Services: considerations and Challenges.** URL: www.northstream.se

[11] Harvey. Applebe, **Mobile Location Based Services & Privacy**, Mapflow, 2003.

[12] Giovanni Camponovo and Yves Pigneur, **ANALYZING THE M-BUSINESS LANDSCAPE.** University of Lausanne. In the *Annals of telecommunications*, 2002

[13] Giovanni Camponovo and Yves Pigneur, ***BUSINESS MODEL ANALYSIS APPLIED TO MOBILE BUSINESS.*** University of Lausanne

[14] Diep Dao, Chris Rizos and Jinling Wang, **Location-Based Services: Technical and Business Issues.** The University of New South Wales, Sydney NSW 2052, Australia

[15] *Steven E. Czerwinski, Ben Y. Zhao, Todd D. Hodes, Anthony D. Joseph, and Randy H. Katz.* **An architecture for a secure service discovery service.** *University of California, Berkeley.* In *Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking - Mobicom 99*, pages 24–25, Seattle, Washington, USA, August, 15-20 1999.

[16] Agamemnon Kakanelis, **Security in Wireless Networks.** The Members of the MobiCom Consortium. 2001.

[17] Jaap Gordijn and Roel Wieringa, **A Value-Oriented Approach to E-Business Process Design.** *Universiteit*, De Boelelaan.

[18] Nils Odhner, **Face Off : IPSec vs. SSL VPNS.** 2003

[19] Cicso Systems **Comparing MPLS-Based VPNs, IPSec-Based VPNs, and a Combined Approach from Cisco Systems.** 1992-2004

[20] Cicso Systems **SAFE VPN IPSec Virtual Private Networks in Depth.** 1992-2004

[21] Χρήστος Ηλιούδης. **Ασφάλεια και διαχείριση Δικτύων** . 2003

[22] Γ. ΠΑΓΚΑΛΟΥ και Ι. ΜΑΥΡΙΔΗ «**ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ**» Σύγγραμμα 2002

[23] Lincoln D. Stein "Ασφαλεια Δικτύων WEB, Ένας βήμα προς βήμα οδηγός" 2000

[24] Αθανασίου Γεώργιος, Καρακωνσταντής Γεώργιος « Ασφάλεια Ασύρματων Δικτύων (Wireless Security)»

[25] ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ. Βρυξέλλες 2006