ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

«Πολιτικές και Μοντέλα Ασφαλείας Πληροφοριακών Συστημάτων»

«Information Systems Security Models and Policies»

Μπούρα Βασιλική

Α.Ε.Μ: 1669

Επιβλέπων Καθηγητής: Δρ. Κωνσταντίνος Σ. Χειλάς

Σέρρες 2015

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ
ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΚΑΤΕΥΘΥΝΣΗ: ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Πτυχιακή Εργασία

«Πολιτικές και Μοντέλα Ασφαλείας Πληροφοριακών Συστημάτων»

«Information Systems Security Models and Policies»

Μπούρα Βασιλική

Α.Ε.Μ: 1669

Επιβλέπων Καθηγητής: Δρ. Κωνσταντίνος Σ. Χειλάς
(Αναπληρωτής Καθηγητής)

Σέρρες, Ιούλιος 2015

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα Αναπληρωτή Καθηγητή της εργασίας μου, Δρ. Κωνσταντίνο Σ. Χειλά, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτή την εργασία, για την πολύτιμη βοήθεια και καθοδήγησή του καθ' όλη τη διάρκειά της, και κυρίως για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα πολύ ενδιαφέρον αντικείμενο. Επίσης θέλω να εκφράσω την ευγνωμοσύνη μου στους γονείς μου για την διαρκή τους υποστήριξη, κατά την διάρκεια ολοκλήρωσης των σπουδών μου. Τέλος, θα ήθελα να ευχαριστήσω τον άντρα μου, για την επιμονή, την υπομονή και την κατανόηση του όλα αυτά τα χρόνια που είμαστε μαζί, προκειμένου να ολοκληρώσω τις σπουδές μου.

ΠΕΡΙΛΗΨΗ

Η χρήση των Πληροφοριακών Συστημάτων συνεχώς αυξάνεται. Πλέον οι περισσότεροι οργανισμοί βασίζονται στην λειτουργία τους. «Αχίλλειος πτέρνα» αυτών είναι η ασφάλεια τους. Στη παρούσα εργασία παρουσιάζονται τα βασικά θέματα που αφορούν τις Πολιτικές και τα Μοντέλα Ασφαλείας των Πληροφοριακών Συστημάτων. Αρχικά, θα συναντήσουμε μια μικρή εισαγωγή για να γνωρίσουμε το Πληροφοριακό Σύστημα. Έπειτα, θα δούμε τις βασικές έννοιες των Πληροφοριακών Συστημάτων. Στη συνέχεια αναπτύσσονται οι πολιτικές καθώς και μοντέλα ασφαλείας των Πληροφοριακών Συστημάτων, όπως επίσης και η προστασία των Πληροφοριακών Συστημάτων. Τελειώνοντας, θα δούμε τις τεχνικές ασφάλειας των Πληροφοριακών Συστημάτων.

ΚΑΤΑΛΟΓΟΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ ΚΑΙ ΠΙΝΑΚΩΝ

1. Εισαγωγή

Το πρόβλημα ης ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα πληροφοριακά συστήματα. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η ικανοποίηση των απαιτήσεων για την ασφάλεια των πληροφοριών (information security) είναι συνεπώς μια από τις βασικές προϋποθέσεις για την εισαγωγή και αξιοποίηση της τεχνολογίας της πληροφορικής.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας (ποιότητα, απόδοση, κ.α.) για την εξασφάλιση της εύρυθμης λειτουργίας ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα όπου πολύ συχνά το σύνολο των παρεχόμενων υπηρεσιών ενός οργανισμού στηρίζεται στην πληροφορική.

1.1. Τι είναι το Πληροφοριακό Σύστημα

Πληροφοριακό σύστημα ονομάζεται ένα σύνολο διαδικασιών, ανθρώπινου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, που προορίζονται για τη συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση πληροφοριών. Τα συστήματα αυτά μπορούν να περιλαμβάνουν λογισμικό, υλικό και τηλεπικοινωνιακό σκέλος.

Ένα Πληροφοριακό σύστημα αποτελείται από έξι στοιχεία:

1. άνθρωποι(το σύνολο των ανθρώπων που εργάζονται με το πληροφοριακό σύστημα σε διάφορους ρόλους όπως χρήστες ,διαχειριστές κ.τ.λ.)
2. διαδικασίες(το σύνολο των οδηγιών για τη χρήση και το συνδυασμό όλων των στοιχείων υποδομής ενός ΠΣ)
3. database(βάση δεδομένων)
4. software(λογισμικό)
5. hardware(υλικός εξοπλισμός)
6. network(δίκτυο)

Ένα Πληροφοριακό σύστημα βοηθάει στον έλεγχο, στο συντονισμό, στην ανάλυση προβλημάτων, στη λήψη αποφάσεων και στην ανάπτυξη νέων προϊόντων.

Κάθε πληροφοριακό σύστημα πρέπει να:

1. προσδιορίζει, αποδοτικά και αποτελεσματικά, τις ανθρώπινες ανάγκες αυτών που χρησιμοποιούν το πληροφοριακό σύστημα και
2. επεξεργάζεται όλες τις πληροφορίες με αποτέλεσμα την ικανοποίηση των αναγκών αυτών.

Αυτό γίνεται πραγματικότητα με:

1. την πιο αποτελεσματική ανάκτηση, αποθήκευση, επεξεργασία, παρουσίαση και διάδοση των πληροφοριών,
2. την παροχή των απαραίτητων μέσων και του κατάλληλου περιβάλλοντος μάθησης στους εμπλεκόμενους χρήστες ώστε να βελτιωθεί η αποτελεσματικότητα της διαδικασίας λήψης απόφασης
3. την υποστήριξη των διαδικασιών λειτουργίας, ελέγχου και στρατηγικού σχεδιασμού την επιχείρησης ή του οργανισμού.

Ένα πληροφοριακό σύστημα δημιουργείται, αναπτύσσεται, εξελίσσεται και αποσύρεται. Η ύπαρξή του αρχίζει από τη στιγμή που η επιχείρηση ή ο οργανισμός θα αποφασίσει τη δημιουργία του. Μετά έχουμε μια περίοδο στην οποία προσδιορίζονται οι βασικές απαιτήσεις των λειτουργιών του και σχεδιάζονται οι λειτουργίες που ικανοποιούν τις απαιτήσεις αυτές. Έπειτα αρχίζει μια μεγάλη χρονική περίοδος στην οποία πραγματοποιείται η ανάπτυξή του και η διαρκής εξέλιξή του ώστε να ικανοποιεί τις ανάγκες της επιχείρησης ή του οργανισμού στον οποίο ανήκει. Τέλος όταν η επιχείρηση ή ο οργανισμός αποφασίσει ότι είναι πια αναποτελεσματικό και μη αποδοτικό, το πληροφοριακό σύστημα αποσύρεται.

2. Βασικές Έννοιες

2.1. Τι είναι η Ασφάλεια των Πληροφοριακών Συστημάτων;

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του υπολογιστικού συστήματος.

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η ασφάλεια πληροφοριακών συστημάτων έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών ενός υπολογιστικού συστήματος καθώς και την λήψη μέτρων. Ποιο συγκεκριμένα η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με:

- Πρόληψη (prevention): Την λήψη δηλαδή μέτρων για να προληφθούν ‘φθορές’ των συστατικών ενός πληροφοριακού συστήματος.
- Ανίχνευση (detection): Την λήψη μέτρων για την ανίχνευση του πότε, πως και από ποιον προκλήθηκε φθορά σε ένα συστατικό ενός πληροφοριακού συστήματος.
- Αντίδραση (reaction): Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός πληροφοριακού συστήματος.

Παραδείγματα για κάθε ένα από τα παραπάνω σημεία είναι:

Α. Από την καθημερινή μας ζωή:

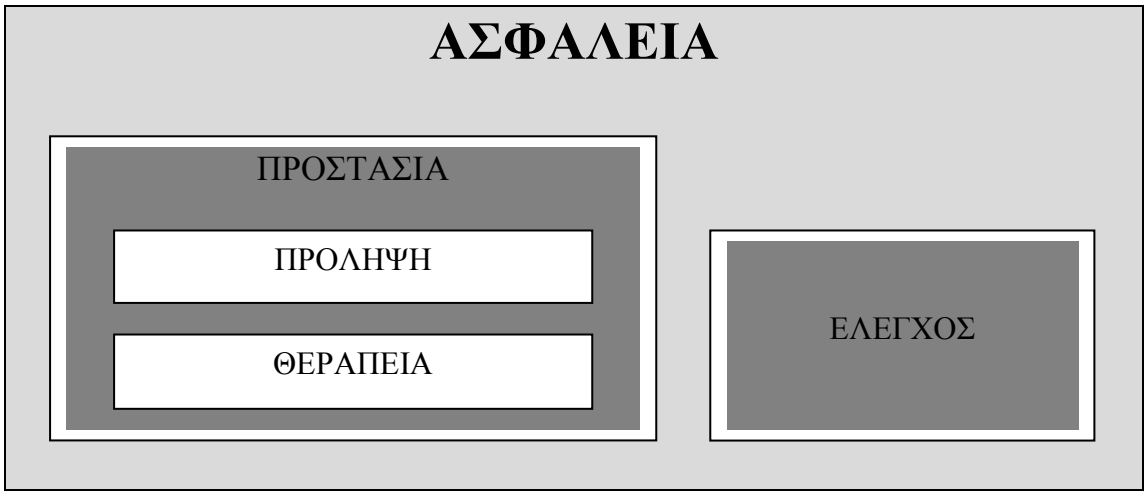
- Η τοποθέτηση κλειδαριών στις πόρτες ή κάγκελων στα παράθυρα (πρόληψη),
- Το σύστημα συναγερμού ή το κλειστό κύκλωμα τηλεόρασης (ανίχνευση),
- Η κλήση της αστυνομίας και η αντικατάσταση κλεμμένων αντικειμένων ή η ασφαλιστική κάλυψη (αντίδραση).

Β. Από το χώρο του ηλεκτρονικού εμπορίου:

- Η κρυπτογραφημένη διακίνηση δεδομένων παραγγελιών και πληρωμών (πρόληψη),

- Η καταγραφή μιας ξένης συναλλαγής στη λίστα της πιστωτικής κάρτας (ανίχνευση),
- Και τα πιθανά παράπονα, η ακύρωση συναλλαγής, η αλλαγή κάρτας, κλπ (αντίδραση).

Η ασφάλεια μπορεί ακόμη να θεωρηθεί ότι αποτελείται από δύο κύριες συνιστώσες, την προστασία και τον έλεγχο, από τις οποίες η προστασία αναλύεται στην πρόληψη και την θεραπεία. Αυτό αναπαρίσταται στο σχήμα της παρακάτω εικόνας:



Εικόνα 1. Η έννοια της ασφάλειας

Αξίζει να σημειώσουμε σε αυτό το σημείο, ότι δεν είναι εύκολο να δοθεί ένας μονοσήμαντος γενικός ορισμός της ασφάλειας πληροφοριακών συστημάτων. Κατά την μελέτη της ασφάλειας κάθε επιμέρους συστήματος τεχνολογιών πληροφορικής και επικοινωνιών (όπως για παράδειγμα, οι κινητές επικοινωνίες) πρέπει συχνά να δίνεται εξ αρχής ο κατάλληλος ορισμός. Επομένως, πρέπει να δίνεται ιδιαίτερη προσοχή, όταν για παράδειγμα, διαβάζουμε κάποιο σχετικό βιβλίο ή άρθρο, διαφορετικά υπάρχει κίνδυνος να δημιουργηθεί σύγχυση ανάμεσα σε αυτό που εμείς θεωρούμε ως ορισμό της ασφάλειας και τον ορισμό που εννοεί ο συγγραφέας.

2.2. Θεμελιώδεις έννοιες

Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των πληροφορικών συστημάτων (information system security) συνδέεται στενά με τρείς βασικές έννοιες:

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity), και
- Διαθεσιμότητα (Availability)

2.2.1. Εμπιστευτικότητα

Σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως σημαίνει ότι τα δεδομένα ενός υπολογιστικού συστήματος, καθώς και τα διακινούμενα μεταξύ των υπολογιστών δεδομένα, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.

Άλλες εκφάνσεις της εμπιστευτικότητας (Confidentiality) είναι:

- Η ιδιωτικότητα (privacy): προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα, και
- Η μυστικότητα (secrecy): προστασία των δεδομένων που ανήκουν σε έναν οργανισμό.

2.2.2. Ακεραιότητα

Η ακεραιότητα μπορεί να οριστεί γενικότερα ως η απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, συμπεριλαμβανομένης και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

Επομένως, σημαίνει ότι η μετατροπή, διαγραφή, και δημιουργία των δεδομένων ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέρη.

2.2.3. Διαθεσιμότητα

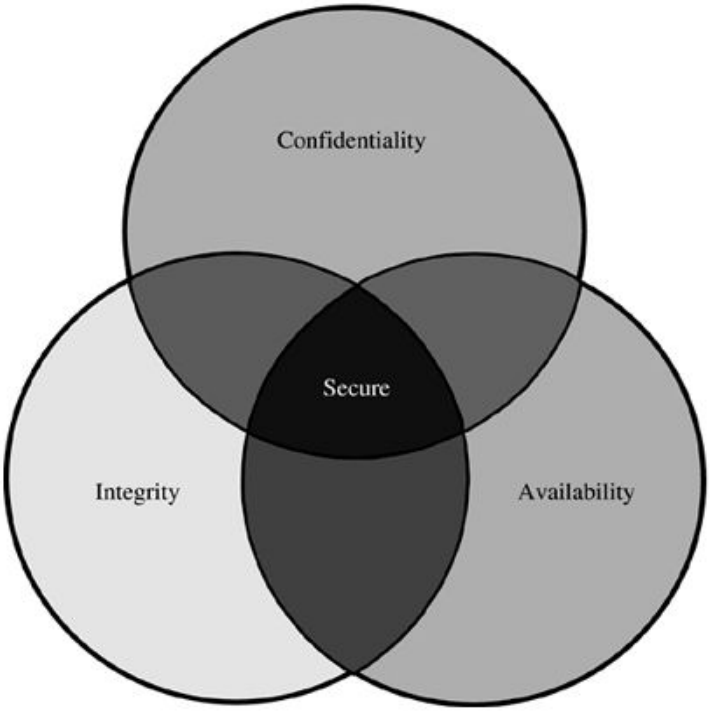
Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος (ΠΣ) όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των επικοινωνιακών μέσων δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του συστήματος.

Η διαθεσιμότητα καλύπτει περιοχές πέρα από το φυσικό σκοπό της ασφάλειας. Για παράδειγμα, ένα μεγάλο μέρος της τεχνολογίας που απαιτείται για τη διασφάλιση της διαθεσιμότητας προέρχεται από άλλες περιοχές, όπως fault – tolerant computing.

Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών (denial of service attacks). Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο (time - critical). Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη (που προκαλείται από κακόβουλα μέρη) παρά τυχαία απώλεια της διαθεσιμότητας. Ένα παράδειγμα επίθεσης άρνησης παροχής υπηρεσιών είναι οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν στην υποστήριξή της.

Στο παρακάτω σχήμα βλέπουμε και εικονικά τις τρεις θεμελιώδεις έννοιες.



Εικόνα 2. Οι βασικές αρχές που εξασφαλίζουν ότι το σύστημα είναι ασφαλές [Pfleeger, 1997].

2.3. Δευτερεύουσες Έννοιες

Εκτός από τις τρεις θεμελιώδεις έννοιες, υπάρχουν μερικές ακόμη δευτερεύουσες έννοιες της ασφάλειας ΠΣ, όπως:

- Εξουσιοδοτημένη χρήση (authorized use): μόνο εξουσιοδοτημένα άτομα μπορούν να χρησιμοποιούν το υπολογιστικό σύστημα ή τις περιφερειακές συσκευές του και μόνο σύμφωνα με ένα προκαθορισμένο τρόπο.
- Αυθεντικοποίηση μηνυμάτων (message authentication): η επιθυμία να γνωρίζουμε με βεβαιότητα κατά τη λήψη ενός μηνύματος (μέσω δικτύου) ότι το άτομο που το σύστημα αξιώνει ότι έστειλε το μήνυμα ότι πράγματι το έστειλε.
- Μη απάρνηση (non repudiation): η επιθυμία να γνωρίζουμε με βεβαιότητα κατά πόσον ένα άτομο παρέλαβε ένα μήνυμα που στάλθηκε, έτσι ώστε να μην μπορεί να απαρνηθεί την παραλαβή του.
- Απόδοση ευθυνών (accountability): στην πράξη δεν είναι εφικτό να προλαμβάνονται και να εμποδίζονται όλες οι ακατάλληλες ενέργειες, αφού ακόμη και εξουσιοδοτημένες ενέργειες μπορεί να προκαλέσουν προβλήματα ασφάλειας, ενώ ολοένα ανακαλύπτονται νέα ρήγματα στην

ασφάλεια των συστημάτων. Για την αντιμετώπιση πιθανών παραβάσεων της ασφάλειας, πρέπει οι χρήστες να είναι υπεύθυνοι (υπόλογοι) για τις πράξεις τους. Αυτό γίνεται με την ασφαλή αναγνώριση των χρηστών και τη διατήρηση εγγραφών ελέγχου (audit trails) για τα συμβάντα που αφορούν την ασφάλεια. Στην περίπτωση παράβασης της ασφάλειας του ΠΣ οι εγγραφές αυτές θα χρησιμοποιηθούν για την εξιχνίαση του προβλήματος και την ανακάλυψη του θύτη.

- Αξιοπιστία (reliability) και σιγουριά (safety): η ασφάλεια (security) σχετίζεται με την αξιοπιστία (reliability) και την σιγουριά (safety) καθώς έχει να κάνει με συστήματα που πρέπει να λειτουργούν κανονικά σε αντίξοες συνθήκες, π.χ. συστήματα πυρηνικών σταθμών και ελέγχου εναέριας κυκλοφορίας.

2.4. Παραβάσεις Ασφάλειας

Οι παραβάσεις ασφαλείας (security breaches) υπολογιστικών συστημάτων σχετίζονται με τις έννοιες των εκθέσεων, ευπαθειών, απειλών και χειρισμών, ως εξής:

- Η Έκθεση (Exposure) περιλαμβάνει αποκάλυψη των δεδομένων, μεταβολές των δεδομένων, άρνηση νόμιμης προσπέλασης για υπολογισμούς.
  Παραδείγματα εκθέσεων σε κίνδυνο είναι:

  - ✓ η μη εξουσιοδοτημένη αποκάλυψη δεδομένων
  - ✓ η μη εξουσιοδοτημένη τροποποίηση δεδομένων
  - ✓ η άρνηση θεμιτής προσπέλασης υπολογιστικών πόρων

- Η Ευπάθεια (Vulnerability) είναι μια αδυναμία στο σύστημα ασφάλειας που μπορεί να αξιοποιηθεί για την πρόκληση απωλειών ή ζημιών.
- Η Απειλή (Threat) για ένα υπολογιστικό σύστημα είναι μια κατάσταση όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών. Παραδείγματα απειλών είναι:

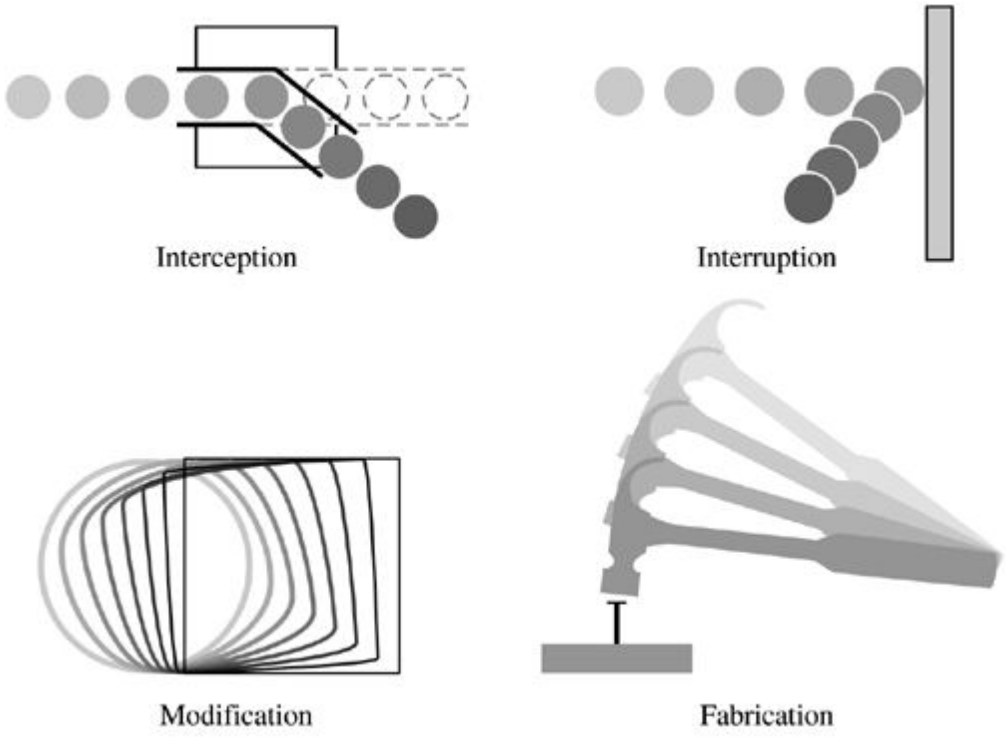
  - ✓ ανθρώπινες επιθέσεις,
  - ✓ φυσικές καταστροφές,
  - ✓ ακούσια ανθρώπινα λάθη,
  - ✓ εσωτερικές ατέλειες του εξοπλισμού ή του λογισμικού.

- Ο Χειρισμός ή Έλεγχος (Control) είναι ένα προστατευτικό μέτρο που μειώνει μια ευπάθεια του υπολογιστικού συστήματος.

Οι βασικές απειλές για την ασφάλεια ενός υπολογιστικού συστήματος είναι η διακοπή, η μεταβολή, η υποκλοπή, και η παραποίηση. Πιο αναλυτικά:

- Η Διακοπή (Interruption) συμβαίνει όταν ένα στοιχείο του συστήματος χάνεται ή γίνεται μη διαθέσιμο.
- Η Μεταβολή (Modification) συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος εκτός του ότι έχει καταφέρει να έχει προσπέλαση, παραποιεί (tampers) ένα στοιχείο.
- Η Υποκλοπή (Interception) συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος έχει καταφέρει να έχει προσπέλαση σε ένα στοιχείο.
- Η Παραποίηση (Fabrication) συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος παραποιεί αντικείμενα σε ένα υπολογιστικό σύστημα.

Στο παρακάτω σχήμα μπορούμε να διακρίνουμε και εικονικά τα όσα αναφέρθηκαν παραπάνω:



Εικόνα 3. Οι διάφορες απειλές στο χώρο της ασφάλειας [Pfleeger, 2002].

2.4.1. Κατηγορίες Απειλών

Σε σχέση με την προέλευσή τους, οι απειλές εντάσσονται στις τρεις ακόλουθες κατηγορίες:

- Φυσικές απειλές: Τέτοιου είδους καταστροφές (φωτιά, πλημμύρα κλπ.) δεν είναι πάντα δυνατόν να αποτραπούν. Όμως είναι σημαντικό η εκδήλωση παρόμοιων γεγονότων να διαπιστώνεται έγκαιρα, ώστε να ελαχιστοποιούνται οι πιθανότητες δραματικών ζημιών. Όπως επίσης σημαντικό είναι να αποφεύγονται ενέργειες που αυξάνουν την πιθανότητα εκδήλωσής τους (όπως για παράδειγμα, το κάπνισμα). Τέλος, η ετοιμότητα χρήσης εφεδρικού συστήματος, σε συνδυασμό με τη λήψη τακτικών εφεδρικών αρχείων (back - ups) για τα κρίσιμα δεδομένα, περιορίζει τις πιθανές δυσάρεστες συνέπειες.

- Ακούσιες απειλές: Προκαλούνται είτε από αστοχίες υλικού ή λογισμικού (HW/SW failures), είτε από άγνοια ή αδιαφορία του ανθρώπινου παράγοντα. Σημαντικός παράγοντας πρόκλησης τέτοιων απειλών είναι η έλλειψη σωστής εκπαίδευσης, είτε πρόκειται για απλούς χρήστες είτε για διαχειριστές των συστημάτων. Να σημειωθεί ότι το ποσοστό των προβλημάτων που δημιουργούνται από άγνοια στα πληροφοριακά συστήματα είναι πολύ μεγαλύτερο από εκείνο που οφείλεται σε κακή πρόθεση.

- Εκούσιες απειλές: Είναι αυτές που απασχολούν περισσότερο τη δημοσιότητα. Στην κατηγορία αυτή, οι κακόβουλοι χρήστες μπορεί να ανήκουν στο εσωτερικό του συστήματος (insiders), για παράδειγμα κάποιοι δυσαρεστημένοι υπάλληλοι. Είναι όμως πιθανό οι απειλές να προέρχονται από κάποιους επίδοξους εισβολείς που είναι εξωτερικοί χρήστες (outsiders). Στη περίπτωση αυτή η επιτυχία των επιθέσεων εξαρτάται κυρίως από τα μέσα που διαθέτουν δηλαδή το χρόνο, την υπολογιστική ισχύ, τις γνώσεις, τα άτομα, τα χρήματα, τις συσκευές και τα εξαρτήματα. Οι κακοήθεις χρήστες μπορεί να επιδιώκουν εκδίκηση, οικονομικό κέρδος, αναγνώριση ή λόγω ιδιοσυγκρασίας απλά τη δημιουργία προβληματικών καταστάσεων και τη διάπραξη βανδαλισμών.

2.5. Ευπάθειες

Κάθε Πληροφοριακό Σύστημα (ΠΣ) είναι ευπαθές σε πιθανές επιθέσεις. Οι πολιτικές και τα προϊόντα ασφάλειας μπορούν να μειώσουν την πιθανότητα του να καταστεί δυνατόν μια επίθεση να διαπεράσει τις άμυνες του συστήματος (ή τουλάχιστον απαιτούν από έναν φιλόδοξο εισβολέα να επενδύσει τόσο χρόνο και πόρους ώστε να μην αξίζει πλέον να συνεχίσει). Θα πρέπει να έχουμε σχετικά υπόψη μας ότι, στην πράξη για καμία σχεδόν

δραστηριότητα δεν υπάρχει αυτό που αποκαλούμε πλήρης ασφάλεια ή τελείως ασφαλές σύστημα.

Μια κατηγοριοποίηση των τυπικών σημείων ευπάθειας (vulnerability) σε ένα υπολογιστικό σύστημα θα μπορούσε να περιλαμβάνει τα εξής:

- Φυσικές Ευπάθειες (Physical)
- Εκ Φύσεως Ευπάθειες (Natural)
- Ευπάθειες Υλικού και Λογισμικού (Hardware and Software)
- Ευπάθειες Μέσων (Media)
- Ευπάθειες Εκπομπών (Emanation)
- Ευπάθειες Επικοινωνιών (Communications)
- Ανθρώπινες ευπάθειες (Human), κ.α.

2.5.1. Φυσικές Ευπάθειες

Αφορούν το 'φυσικό περιβάλλον' (για παράδειγμα τα κτίρια και τους χώρους των μηχανογραφικών κέντρων (computer rooms)). Μια πρώτη άμυνα ενάντια σε πιθανές εισβολές παρέχουν τα κλασσικά μέσα προστασίας, όπως ο έλεγχος της φυσικής προσπέλασης, (οι φύλακες, οι βιομετρικές συσκευές, οι αντικλεπτικοί συναγερμοί, κ.α.).

2.5.2. Εκ φύσεως Ευπάθειες

Οι υπολογιστές είναι ιδιαίτερα ευπαθείς σε φυσικές καταστροφές και περιβαλλοντικές απειλές, όπως οι πυρκαγιές, οι πλημμύρες, οι σεισμοί, οι κεραυνοί και οι διακοπές ρεύματος. Ακόμη επηρεάζονται αρνητικά από τη σκόνη, την υγρασία και τις ακραίες θερμοκρασιακές συνθήκες.

2.5.3. Ευπάθειες Υλικού και Λογισμικού

Πιθανές δυσλειτουργίες του υλικού και του λογισμικού μπορεί να προκαλέσουν την διακοπή παροχής των υπηρεσιών ενός ΠΣ είτε λόγω ενδογενών σφαλμάτων είτε λόγω εσφαλμένης εγκατάστασης των συστατικών μερών του.

2.5.4. Ευπάθειες Μέσων

Η κλοπή ή καταστροφή μαγνητικών μέσων και εκτυπωτικών καταστάσεων μπορεί να προκαλέσει την απώλεια ή διαρροή ευαίσθητων δεδομένων.

2.5.5. Ευπάθειες Εκπομπών

Όλες οι ηλεκτρονικές συσκευές εκπέμπουν ηλεκτρομαγνητική ακτινοβολία. Με κατάλληλο εξοπλισμό είναι πιθανή η υποκλοπή των εκπεμπόμενων σημάτων από συστήματα και δίκτυα υπολογιστών και η αποκωδικοποίησή τους με σκοπό την υφαρπαγή κρίσιμων πληροφοριών, ή την παρεμπόδιση της ομαλής λειτουργίας ενός πληροφοριακού συστήματος.

2.5.6. Ευπάθειες Επικοινωνιών

Η σύνδεση ενός υπολογιστή σε ένα ανοικτό δίκτυο (όπως το διαδίκτυο (Internet)) αυξάνει τον κίνδυνο διείσδυσης από τρίτα μη εξουσιοδοτημένα μέρη. Με αυτό τον τρόπο, μηνύματα μπορούν να υποκλαπούν, να αλλάξουν διαδρομή και να χαλκευτούν. Οι γραμμές σύνδεσης των υπολογιστών είναι τα συνηθέστερα σημεία που μπορούν να χρησιμοποιηθούν για υποκλοπή ή ακόμη και για καταστροφή.

2.5.7. Ανθρώπινες Ευπάθειες

Οι άνθρωποι που διαχειρίζονται και χρησιμοποιούν ένα υπολογιστικό σύστημα αποτελούν συνήθως την μεγαλύτερη πηγή ευπαθειών για αυτό. Συνήθως, η ασφάλεια ενός ΠΣ εξαρτάται κατά πρώτο λόγο από τους ανθρώπους που το χρησιμοποιούν νόμιμα. Η έλλειψη εκπαίδευσης, ο δόλος, η απροσεξία και η επιπολαιότητα στο χειρισμό ευαίσθητων στοιχείων, όπως για παράδειγμα τα συνθηματικά, καθώς και οι κακοπροαίρετοι ή παραπονεμένοι υπάλληλοι αποτελούν τις μεγαλύτερες απειλές (insiders) για την ασφάλεια ενός ΠΣ.

2.6. Μέτρα Προστασίας

Τα μέτρα προστασίας (controls) ή αντίμετρα (countermeasures) είναι όλες εκείνες οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός Πληροφοριακού Συστήματος (ΠΣ).

Οι διαφορετικοί τύποι αντίμετρων έχουν ως αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας πληροφοριακών στις ακόλουθες συνιστώσες:

- Φυσική ασφάλεια συστήματος (physical security): Αναφέρεται στην προστασία ολόκληρου του σχετικού εξοπλισμού του υπολογιστή από φυσικές καταστροφές, όπως κλοπή, βανδαλισμοί, πλημμύρες, φωτιά κλπ.

- Ασφάλεια Υπολογιστικού Συστήματος (computer security): Αναφέρεται στην προστασία εκείνων των πληροφοριών του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (προγράμματα εφαρμογών, αρχεία δεδομένων, κ.α.). Επικεντρώνεται κυρίως στις συγκεκριμένες υπηρεσίες των λειτουργικών συστημάτων που καθορίζουν το ποιος και το πώς θα δικαιούται να προσπελάσει τα δεδομένα και τις εφαρμογές που φιλοξενεί το υπολογιστικό σύστημα.

- Ασφάλεια Βάσεων Δεδομένων (database security): Αναφέρεται στην ικανότητα του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, στην οποία διευκρινίζεται ποιοι εξουσιοδοτούνται να δουν ή / και να τροποποιήσουν τα προστατευμένα δεδομένα.

- Ασφάλεια Δικτύων Επικοινωνιών (network security): Αναφέρεται στην προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω των τηλεφωνικών, δορυφορικών ή άλλων δικτύων, όπως είναι τα τοπικά δίκτυα και το Internet.

2.6.1. Κατηγορίες Μέτρων Προστασίας

Γενικά, υπάρχουν τέσσερις βασικοί τρόποι άμυνας οι οποίοι μπορεί να βοηθήσουν ώστε να υπάρξει επαρκής ασφάλεια σε ένα πληροφοριακό σύστημα (ΠΣ):

- Μέτρα προσπέλασης συστήματος: Εξασφαλίζουν ότι οι μη εξουσιοδοτημένοι χρήστες δεν εισάγονται (log in) στο σύστημα.

- Μέτρα προσπέλασης δεδομένων: Ελέγχουν ποιος μπορεί να έχει πρόσβαση σε ποια δεδομένα και με ποιο σκοπό. Οι εφαρμογές βάσεων δεδομένων τυπικά απαιτούν έναν υψηλό βαθμό λεπτομέρειας (granularity) του ελέγχου προσπέλασης.

- Διαχείριση συστήματος και ασφάλειας: Εκτέλεση των off – line διαδικασιών που διαμορφώνουν ή επιβάλλουν ένα ασφαλές σύστημα, ορίζοντας ξεκάθαρα τις υπευθυνότητες του διαχειριστή συστήματος, εκπαιδεύοντας τους χρήστες κατάλληλα και ελέγχοντας ότι οι διαδικασίες ασφάλειας τηρούνται από τους χρήστες.

- Σχεδιασμός συστήματος: Αξιοποίηση βασικών χαρακτηριστικών και δυνατοτήτων ασφάλειας του υλικού και του λογισμικού.

2.6.2. Τύποι Μέτρων Προστασίας

Οι κύριοι τύποι μέτρων (controls) για την πρόληψη της εκμετάλλευσης των ευπαθειών ενός πληροφοριακού συστήματος είναι:

- Κρυπτογράφηση (encryption):
  Μετασχηματίζοντας τα δεδομένα ώστε να είναι ακατάληπτα από τον εξωτερικό παρατηρητή, η αξία των υποκλοπών και η πιθανότητα για τροποποιήσεις σχεδόν εκμηδενίζεται.

- Μέτρα Λογισμικού (software controls):
  Τα προγράμματα πρέπει να είναι αρκετά ασφαλή και αξιόπιστα ώστε να αποτρέπουν εξωτερικές επιθέσεις. Τα μέτρα προγραμμάτων περιλαμβάνουν:
  - Μέτρα ανάπτυξης (development controls): Πρόκειται για τα πρότυπα (standards) σύμφωνα με τα οποία σχεδιάζονται, κωδικοποιούνται, ελέγχονται και συντηρούνται τα προγράμματα.

  - Μέτρα λειτουργικού συστήματος (operating system controls): Πρόκειται για περιορισμούς που επιβάλλονται από το λειτουργικό σύστημα με σκοπό την προστασία κάθε χρήστη από τους υπόλοιπους χρήστες.

  - Μέτρα μέσα στα προγράμματα (internal program controls): Πρόκειται για μέτρα που επιβάλλουν περιορισμούς ασφάλειας, όπως για παράδειγμα οι περιορισμοί προσπέλασης σε ένα σύστημα διαχείρισης βάσης δεδομένων (ΣΔΒΔ).

- Μέτρα Υλικού (hardware controls):
  Έχουν εφευρεθεί αρκετές συσκευές για να βοηθούν στην ασφάλεια υπολογιστών. Αυτές ποικίλλουν από την υλοποίηση της κρυπτογράφησης με υλικό μέχρι τις συσκευές για επιβεβαίωση της ταυτότητας των χρηστών.

- Φυσικά Μέτρα Υλικού (physical controls):
  Τα φυσικά μέτρα είναι από τα πιο εύκολα, πιο αποτελεσματικά και λιγότερο δαπανηρά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων και των συστημάτων βάσεων δεδομένων (για παράδειγμα, κλειδαριές στις πόρτες, φύλακες, αντίγραφα ασφάλειας, κ.α.).

- Πολιτικές Ασφάλειας (security policies):
  Μερικά άλλα μέτρα αποτελούν αντικείμενο πολιτικής, όπως για παράδειγμα ο έλεγχος προσπέλασης. Παρά τα προβλήματα διαχείρισης σε μεγάλους και εξελισσόμενους οργανισμούς, οι πολιτικές ελέγχου προσπέλασης πρέπει να προσαρμόζονται στις επιμέρους συνθήκες και απαιτήσεις ασφάλειας του κάθε πληροφοριακού συστήματος.

2.6.3. Αποτελεσματικότητα των μέτρων προστασίας

Η αποτελεσματικότητα των μέτρων προστασίας ή αντίμετρων εξαρτάται από το πόσο σωστά χρησιμοποιούνται. Ορισμένοι βασικοί παράγοντες που επηρεάζουν την αποτελεσματικότητα των αντίμετρων είναι:

- Η επίγνωση του μεγέθους του προβλήματος:
  Τα άτομα που εφαρμόζουν τα μέτρα, ή ακόμη περισσότερο αυτά που είναι υπεύθυνα για την διαμόρφωσή τους, πρέπει να έχουν πειστεί για την ανάγκη για ασφάλεια και για το επίπεδο της ασφάλειας που προβλέπεται σε κάθε περίπτωση.

- Οι περιοδικές αναθεωρήσεις:
  Η αμφισβήτηση της αποτελεσματικότητας ενός μέτρου πρέπει να είναι συνεχής. Το περιβάλλον λειτουργίας ενός πληροφοριακού συστήματος (ΠΣ) είναι δυναμικό αφού συνεχώς οι συνθήκες, οι απειλές και οι ανάγκες εξελίσσονται. Είναι πολύ λογικό λοιπόν τα περισσότερα μέτρα προστασίας να παύουν να είναι αποδοτικά αν δεν γίνουν οι κατάλληλες προσαρμογές και αντικαταστάσεις.

- Η αλληλοεπικάλυψη μέτρων:
  Στις περισσότερες περιπτώσεις η ορθή αντιμετώπιση μιας ευπάθειας απαιτεί την εφαρμογή διαφορετικών μεταξύ τους αντίμετρων. Ένας συνδυασμός φυσικών, δικτυακών – επικοινωνιακών και υπολογιστικών μέτρων προστασίας ελαχιστοποιεί τις υπαρκτές απειλές, ενώ συχνά η συνολική αξιοπιστία του συστήματος προστασίας στηρίζεται στις δυνατότητες αλληλοσυμπλήρωσης αλληλοεπικάλυψης των μέτρων αυτών. Αυτό φυσικά δεν σημαίνει ότι το κάθε μέτρο μεμονωμένα δεν είναι ανθεκτικό και ισχυρό. Άλλωστε, σύμφωνα με την «αρχή του ασθενέστερου σημείου» (weakest point philosophy), οι ειδικοί στην ασφάλεια πληροφοριακών συστημάτων πρέπει να συνυπολογίζουν όλα τα υπάρχοντα ρήγματα ασφάλειας, διότι οχυρώνοντας μόνον κάποια από αυτά απλώς κάνουν τις υπόλοιπες ευπάθειες πιο ελκυστικές για όσους κακοήθεις σκοπεύουν να εκδηλώσουν επιθέσεις. Συχνά λέγεται σχετικά ότι η ασφάλεια έχει παρόμοια συμπεριφορά με μια αλυσίδα: η ισχύς της είναι τόση όση και η ισχύς του ασθενέστερου κρίκου της.

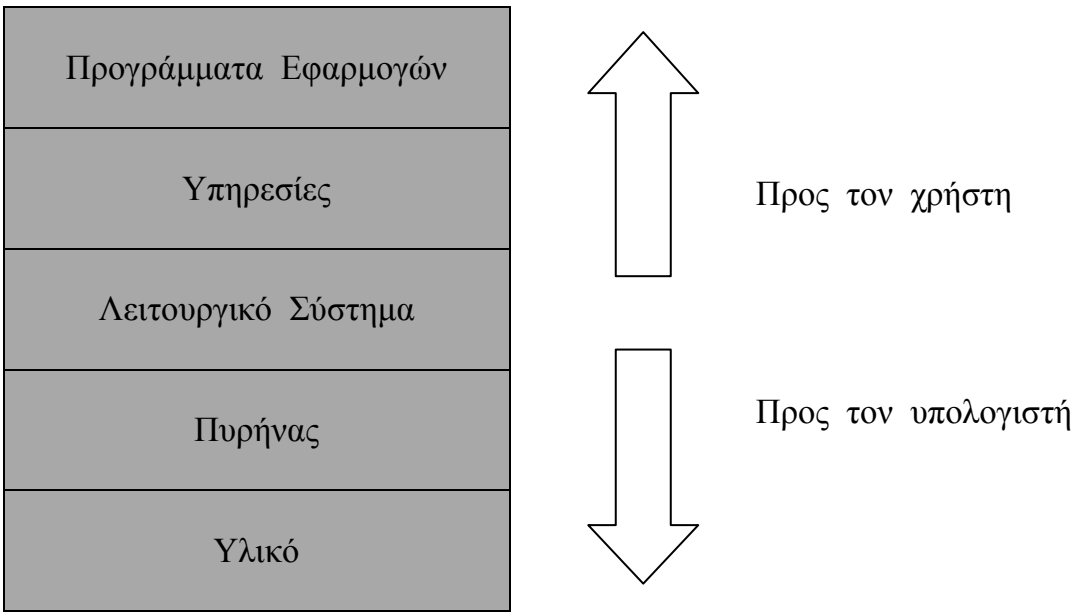
- Οι πιθανότητες χρησιμοποίησης:
  Σύμφωνα με την «αρχή της αποτελεσματικότητας» (principle of effectiveness), για να είναι αποτελεσματικά τα μέτρα πρέπει να χρησιμοποιούνται και να είναι επαρκή, κατάλληλα και εύκολα στη χρήση τους. Δηλαδή, υπονοείται εδώ ότι πρωταρχική προϋπόθεση για την απόδοση ενός μέτρου είναι το να βρίσκεται σε εφαρμογή την κρίσιμη στιγμή. Αυτό σημαίνει ότι η χρήση των αντίμετρων δεν πρέπει να επηρεάζει ως προς την κατανάλωση των πόρων του συστήματος (χρόνο, χώρο μνήμης, ανθρώπινη δραστηριότητα κλπ).

2.6.4. Τοποθέτηση των Μέτρων Προστασίας

Ένα τυπικό πληροφοριακό σύστημα (ΠΣ) μπορεί να μοντελοποιηθεί χρησιμοποιώντας πέντε διαφορετικά στρώματα (layers) συστατικών:

- Τα Προγράμματα Εφαρμογών, που είναι προσαρμοσμένα να ικανοποιούν τις απαιτήσεις των χρηστών.
- Τις Υπηρεσίες, που χρησιμοποιούνται από τα προγράμματα εφαρμογών, όπως για παράδειγμα αυτές που παρέχονται από ένα Σύστημα Διαχείρισης Βάσεων Δεδομένων (ΣΔΒΔ) ή ένα κατανεμημένο σύστημα αρχείων.
- Το Λειτουργικό Σύστημα, με βάση το οποίο παρέχονται οι υπηρεσίες και το οποίο παρέχει διαχείριση αρχείων, εκτυπωτών, κ.λ.π.
- Τον Πυρήνα (το κεντρικό τμήμα του λειτουργικού συστήματος), που κανονίζει την προσπέλαση της μνήμης και του επεξεργαστή.
- Το Υλικό, για παράδειγμα επεξεργαστές και μνήμη.

Με βάση τον παραπάνω διαχωρισμό, τα μέτρα προστασίας μπορούν να τοποθετηθούν σε ένα ή περισσότερα στρώματα, όπως δείχνεται στην εικόνα που ακολουθεί:



Εικόνα 4. Τοποθέτηση των μέτρων προστασίας

Οι μηχανισμοί των στρωμάτων που βρίσκονται πιο κοντά στο υλικό θεωρούνται περισσότερο γενικοί και προσανατολισμένοι στον υπολογιστή (computer-oriented), ενώ αυτοί που είναι κοντά στις εφαρμογές είναι περισσότερο προσανατολισμένοι στον χρήστη (user - oriented).

2.7. Απαιτήσεις Ασφάλειας Πληροφοριακών Συστημάτων (ΠΣ)

Ο βασικός σκοπός της ασφάλειας πληροφοριακών συστημάτων πρέπει να είναι η προστασία του υπολογιστικού συστήματος και οποιουδήποτε άλλου στοιχείου που σχετίζεται με αυτό (όπως για παράδειγμα ο Η/Υ αυτός καθαυτός, οι κτιριακές εγκαταστάσεις, οι θέσεις εργασίας, η καλωδίωση, τα μαγνητικά και οπτικά μέσα αποθήκευσης, κ.α.), με πρώτη προτεραιότητα για τις πληροφορίες που είναι αποθηκευμένες στο ΠΣ.

Αξίζει να σημειωθεί ότι η μη – εξουσιοδοτημένη ενέργεια δεν περιορίζεται μόνο σε μη – εξουσιοδοτημένα πρόσωπα, όπως οι επισκέπτες ενός νοσοκομείου. Ακόμη και εξουσιοδοτημένοι χρήστες, ή ακόμη χειρότερα, διαχειριστές συστήματος, πιθανόν να προσπαθήσουν να εκτελέσουν μη – εξουσιοδοτημένες ενέργειες. Αυτό αυξάνει την ανάγκη για μια τεχνολογία πληροφορικής που να είναι ικανή να παρέχει σε ένα άτομο αναμφισβήτητες αποδείξεις για το αν έκανε μια κάποια ενέργεια ή όχι (απόδοση ευθυνών).

2.8. Προβλήματα κατά την Εισαγωγή Ασφάλειας

Η εισαγωγή (προσθήκη μηχανισμών) ασφάλειας σε ένα ΠΣ είναι ένα δύσκολο και περίπλοκο έργο. Η δυσκολία οφείλεται κυρίως στο ότι:

- τα σύγχρονα πληροφοριακά συστήματα περιέχουν συχνά ένα τεράστιο σε όγκο και πολυπλοκότητα όγκο λογισμικού, και τα μεγάλα έργα λογισμικού έχει ιστορικά αποδειχθεί ότι είναι σχεδόν αδύνατο να υλοποιηθούν χωρίς λάθη.
- η ασφάλεια συνήθως δεν περιλαμβάνεται στο αρχικά σχεδιασμένο ή υλοποιημένο σύστημα αλλά προστίθεται κατόπιν.
- η ασφάλεια κοστίζει, συνήθως αρκετά.
- πολύ συχνά το πρόβλημα έγκειται στους ανθρώπους που χρησιμοποιούν το σύστημα και όχι στην τεχνολογία που χρησιμοποιείται.

2.9. Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας

Είναι γεγονός ότι, παρά την προφανή της χρησιμότητα, η λήψη των απαραίτητων μέτρων ασφάλειας δημιουργεί πολλές φορές κάποια πρόσθετη επιβάρυνση στην απόδοση και το κόστος λειτουργίας του πληροφοριακού συστήματος του οργανισμού. Θα πρέπει ακόμη να αποδεχτούμε το κόστος της ασφάλειας και ως κόστος χρόνου και ως κόστος χρήματος. Συνεπώς, μπορεί να θεωρηθεί ότι η ασφάλεια βρίσκεται σε σχέση αντιστρόφως ανάλογη με την αποδοτικότητα του πληροφοριακού συστήματος του οργανισμού. Αυτό όμως

δεν είναι σωστό γιατί η ασφάλεια είναι κόστος αναγκαίο για την ομαλή και εύρυθμη λειτουργία του.

Το συγκεκριμένο κόστος για την ασφάλεια των πληροφοριακών συστημάτων ενός οργανισμού εξαρτάται και προκύπτει από την εκάστοτε ακολουθούμενη πολιτική ασφάλειας. Απαιτείται συνεπώς μια πολιτική ασφάλειας η οποία θα πρέπει να εξισορροπεί το κόστος εισαγωγής ασφάλειας από την μία πλευρά και το κόστος ζημιών από πιθανολογούμενο κίνδυνο από την άλλη. Επίσης, θα πρέπει να δημιουργούνται τέτοιες συνθήκες ασφάλειας ώστε να μη παρεμποδίζεται η ευελιξία και η ανάπτυξη του οργανισμού.

Η αναγκαία πολιτική ασφάλειας καθορίζεται από μία δυναμική εκτίμηση του κόστους των μέτρων ασφάλειας σε σχέση με τις συνέπειες που θα έχει για τον οργανισμό οποιαδήποτε πρόκληση δυσλειτουργίας. Ο βασικός αυτός κανόνας ισχύει για όλους τους τομείς και όλα τα επίπεδα ασφάλειας. Έτσι, σε κάθε περίπτωση όπου απαιτείται η λήψη κάποιου μέτρου ασφάλειας, πρέπει να εξετάζεται η πιθανότητα να συμβεί κάποιο γεγονός / πρόβλημα ασφάλειας (possibility of event), σε σχέση με τις συνέπειες που αυτό θα δημιουργήσει (impact). Εάν η τιμή των δύο αυτών παραμέτρων είναι υψηλή, τότε πρέπει απαραίτητα να ληφθούν μέτρα, ανεξάρτητα από το κόστος πρόληψης.

Τέλος, πρέπει να σημειωθεί ότι η ασφάλεια χαρακτηρίζεται από την φύση της ως δυναμική παράμετρος και όχι στατική, καθώς η τεχνολογία, ο ανταγωνισμός, η πολυπλοκότητα των πληροφοριακών συστημάτων και η ολοένα βελτιούμενη επιτηδειότητα των ‘επιτιθέμενων’, απαιτούν τη λήψη νέων και συνεχώς αυστηρότερων μέτρων ασφάλειας. Συνεπώς, η ακολουθούμενη πολιτική ασφαλείας θα πρέπει να επανεξετάζεται τακτικά και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

3. Πολιτικές και Μοντέλα Ασφάλειας Πληροφοριακών Συστημάτων (ΠΣ)

3.1. Ασφαλές ή Έμπιστο σύστημα;

Υπάρχει διαφορά στο χαρακτηριστικό ενός ΠΣ ως ασφαλούς και ως έμπιστου. Οι ειδικοί της ασφάλειας προτιμούν συνήθως να αναφέρονται σε έμπιστα παρά σε ασφαλή συστήματα. Με τον όρο 'έμπιστα' υπονοούν ότι αυτά ικανοποιούν τις επιδιωκόμενες απαιτήσεις ασφάλειας και έχουν αρκετά υψηλή και βεβαιωμένη ποιότητα. Ο παρακάτω πίνακας παραθέτει μια χρήσιμη αντιπαραβολή των κυριότερων ιδιοτήτων των δύο όρων:

ΑΣΦΑΛΕΣ	ΕΜΠΙΣΤΟ
Είναι ή δεν είναι ασφαλές;	Υπάρχουν διάφορες βαθμίδες εμπιστοσύνης
Ισχυρισμός	Πεποίθηση
Βεβαιώνεται στη βάση χαρακτηριστικών ασφάλειας του προϊόντος	Κρίνεται στη βάση γεγονότων και αναλύσεων
Απόλυτο: χωρίς επιφυλάξεις για το πώς, που, πότε και από ποιόν χρησιμοποιείται	Σχετικό: θεωρείται στο πλαίσιο της χρήσης
Σκοπός	Χαρακτηριστικό

Πίνακας 1. Αντιπαραβολή ιδιοτήτων ασφαλούς και έμπιστου ΠΣ.

3.2. Πολιτικές και Μηχανισμοί Ασφάλειας

Για να μπορούμε να γνωρίζουμε κατά πόσον ένα υπολογιστικό σύστημα παρέχει την αναμενόμενη ασφάλεια, πρέπει να μπορούμε να διατυπώσουμε το τι είναι αυτή η ασφάλεια. Οι απαιτήσεις ασφάλειας ενός υπολογιστικού συστήματος προσδιορίζονται διαμέσου μιας πολιτικής ασφάλειας.

Η πολιτική ασφάλειας (security policy) ενός υπολογιστικού συστήματος είναι ένα σύνολο από αρχές (principles) και οδηγίες υψηλού επιπέδου (high level guidelines) που αφορούν τη σχεδίαση και διαχείριση συστημάτων ασφάλειας.

Μια πολιτική ασφάλειας εκφράζεται με *κανόνες (rules)* που ρυθμίζουν πως ελέγχονται τα συμμετέχοντα μέρη και πως λαμβάνονται οι αποφάσεις για

προσπέλαση. Συνήθως επιβάλλονται από διάφορους μηχανισμούς ασφάλειας, οι οποίοι μπορούν να καταταγούν στις παρακάτω κατηγορίες:

- ✓ *αναγνώριση (identification),*
- ✓ *αυθεντικοποίηση (authentication),*
- ✓ *εξουσιοδότηση (authorization),*
- ✓ *έλεγχο προσπέλασης (access control),*
- ✓ *ακεραιότητα (integrity),*
- ✓ *συνέπεια (consistency),*
- ✓ *επίβλεψη (auditing).*

Οι μηχανισμοί ασφάλειας (security mechanisms) είναι χαμηλού επιπέδου λειτουργίες λογισμικού και υλικού που μπορούν να διαμορφώνονται κατάλληλα για την υλοποίηση μιας πολιτικής ασφάλειας.

Το λεξιλόγιο TCSEC ορίζει μια πολιτική ασφάλειας ως 'το σύνολο νόμων, κανόνων και πρακτικών που ρυθμίζουν πως ένας οργανισμός διαχειρίζεται, προστατεύει και κατανέμει ευαίσθητες πληροφορίες'. Ομοίως, το λεξιλόγιο ITSEC ορίζει τον όρο πολιτική ασφάλειας ως 'το σύνολο νόμων, κανόνων και πρακτικών που ρυθμίζουν πως τα στοιχεία διαχειρίζονται, προστατεύονται και κατανέμονται μέσα σε έναν οργανισμό χρηστών'.

Μια πολιτική ασφάλειας ορίζεται τυπικά στη βάση των όρων υποκείμενα και αντικείμενα. Ένα *υποκείμενο* είναι κάτι ενεργό στο σύστημα, όπως για παράδειγμα οι χρήστες (users), οι διεργασίες (processes) και τα προγράμματα (programs). *Αντικείμενο* είναι κάτι στο οποίο ενεργεί το υποκείμενο. Παραδείγματα αντικειμένων είναι τα αρχεία (files), οι κατάλογοι (directories), οι συσκευές (devices), οι υποδοχές (sockets) και τα παράθυρα (windows).

3.3. Μοντέλα Ασφάλειας

Οι μηχανισμοί που είναι απαραίτητοι για την επιβολή μιας πολιτικής ασφάλειας συμμορφώνονται με ένα συγκεκριμένο μοντέλο ασφάλειας. Ένα μοντέλο ασφάλειας εκφράζει με ακρίβεια και χωρίς συγχύσεις τις απαιτήσεις ασφάλειας ενός συστήματος.

Μέχρι σήμερα έχουν αναπτυχθεί αρκετά μοντέλα ασφάλειας. Εκείνα που προορίζονται για ιδιαίτερα ασφαλή συστήματα έχουν εκφρασθεί με μαθηματικό τρόπο και συχνά χρησιμοποιούν την θεωρία συνόλων για να περιγράψουν τους κανόνες πρόσβασης στο σύστημα.

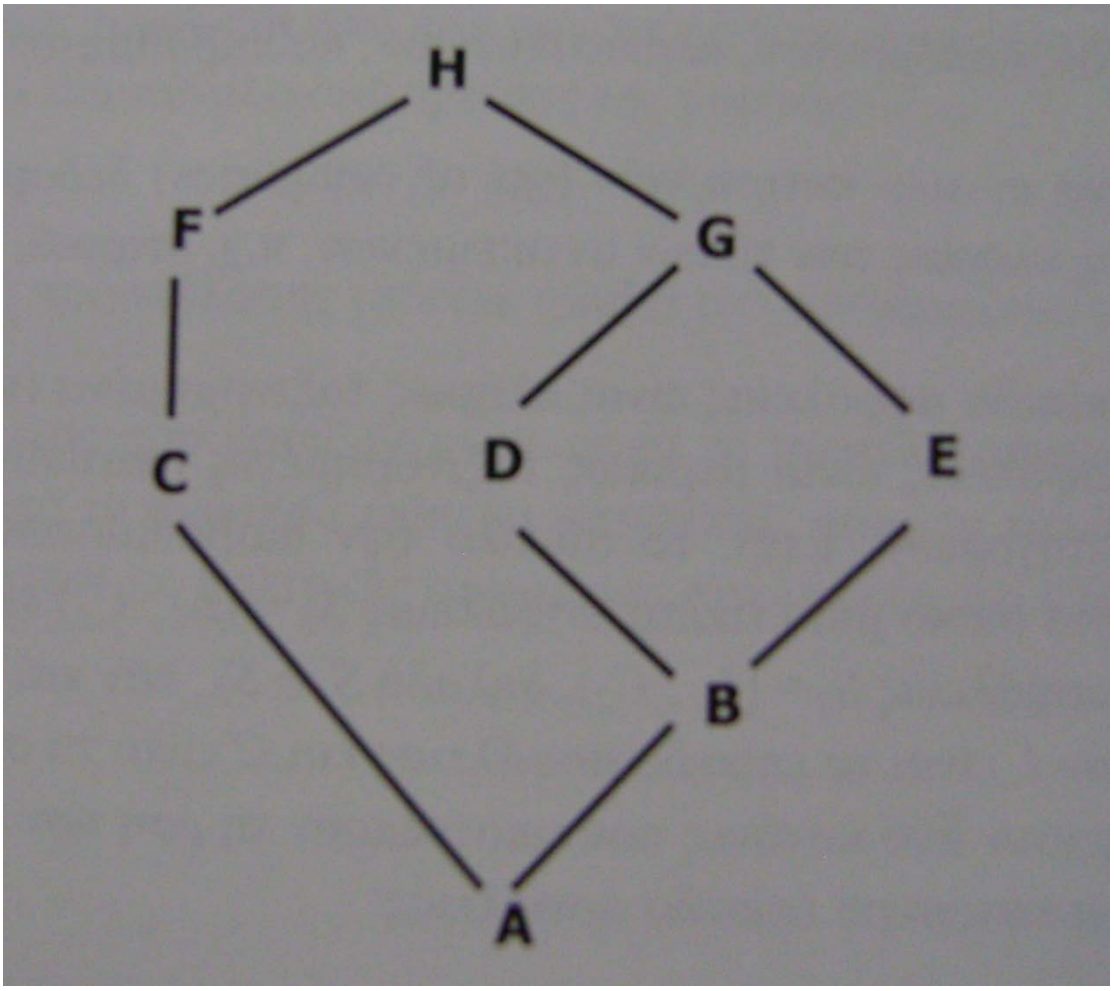
3.3.1. Το Δικτυωτό Μοντέλο

Σε εφαρμογές όπου υπάρχει διαβάθμιση της ευαισθησίας των πληροφοριών, έχει υιοθετηθεί ένα γενικό μοντέλο το οποίο πρώτοι περιέγραψαν με μαθηματικό φορμαλισμό οι Bell La Padula και Denning. Το γενικότερο μοντέλο ονομάζεται *δικτυωτό μοντέλο ασφάλειας* (lattice model).

Τα στοιχεία ενός δικτυωτού είναι μερικώς ταξινομημένα (partially ordered) σύμφωνα με την σχέση επικράτησης (dominance) $\alpha \leq b$, η οποία είναι:

- μεταβατική: αν $\alpha \leq b$ και $b \leq c$ τότε $\alpha \leq c$ και
- αντισυμμετρική: αν $\alpha \leq b$ και $b \leq \alpha$ τότε $\alpha = b$.

Σε ένα δικτυωτό δεν χρειάζεται να είναι συγκρίσιμα μεταξύ τους όλα τα στοιχεία. Αυτό σημαίνει ότι μπορεί να υπάρχουν δύο στοιχεία α και b για τα οποία δεν έχει ορισθεί η σχέση $\alpha \leq b$ ούτε η σχέση $b \leq \alpha$. όμως, ακόμη και τότε υπάρχει ένα στοιχείο άνω ορίου u τέτοιο ώστε $\alpha \leq u$ και $b \leq u$. Ακόμη, σε ένα δικτυωτό, κάθε ζεύγος στοιχείων διαθέτει ένα κάτω όριο, δηλαδή ένα τέτοιο στοιχείο l ώστε $l \leq \alpha$ και $l \leq b$.



Εικόνα 5. Παράδειγμα Δικτυωτού Μοντέλου

Για παράδειγμα, στο δικτυωτό του σχήματος 8, το στοιχείο H υπερισχύει (dominates) όλων των υπολοίπων στοιχείων. Το G υπερισχύει των D, E, B και A, ενώ τα D και E υπερισχύουν των B και A. Όμως τα C και B δεν μπορούν να συγκριθούν (είναι μεταξύ τους ασύγκριτα).

3.3.2. Το Μοντέλο Εμπιστευτικότητας Bell – La Padula

Το μοντέλο Bell – La Padula παρέχει μια φορμαλιστική περιγραφή των επιτρεπόμενων διαδρομών ροής των πληροφοριών σε ένα ασφαλές σύστημα.

Στο μοντέλο αυτό κάθε σύστημα θεωρείται ότι περιέχει ένα σύνολο υποκειμένων *S* και ένα σύνολο αντικειμένων *O*. Σε κάθε υποκείμενο (subject) και αντικείμενο (object) εκχωρείται μια *ετικέτα ασφάλειας* (security label). Η ετικέτα ενός αντικειμένου *o* καλείται *διαβάθμιση* (classification). Η ετικέτα ενός υποκειμένου *s* καλείται *εκκαθάριση* (clearance). Η διαβάθμιση εκφράζει την ευαισθησία (sensitivity) των μαρκαρισμένων δεδομένων, ενώ η εκκαθάριση ενός υποκειμένου εκφράζει την φερεγγυότητα (trustworthiness) του στο να μην φανερώσει ευαίσθητες πληροφορίες σε τρίτους.

Μια ετικέτα ασφάλειας αποτελείται από δύο μέρη:

- ένα επίπεδο (level), ορισμένο στο πλαίσιο μιας ιεραρχικής λίστας επιπέδων ευαισθησίας ή κλάσεων προσπέλασης, για παράδειγμα: «άκρως απόρρητο», «απόρρητο», «εμπιστευτικό», «αδιαβάθμητο».
- ένα σύνολο κατηγοριών (set of categories) δεδομένων που αναπαριστούν τις κλάσεις των τύπων αντικειμένων, π.χ. ιατρικά, λογιστικά, κ.ά.

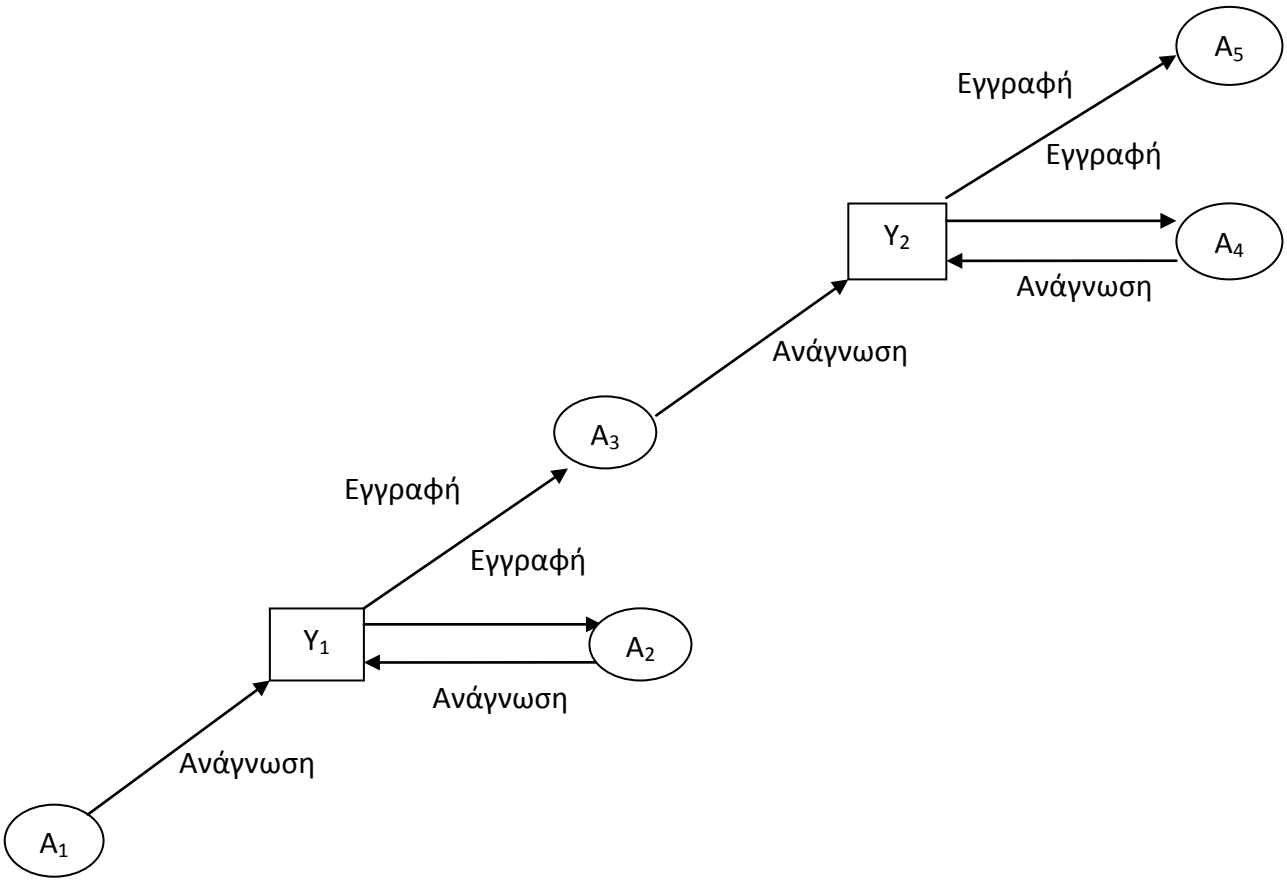
Τα επίπεδα ασφάλειας είναι πλήρως ταξινομημένα (totally ordered), ενώ οι ετικέτες ασφάλειας είναι μερικώς ταξινομημένες (partially ordered) λόγω των συνόλων κατηγοριών. Έτσι, το σύνολο των διαβαθμίσεων αποτελεί ένα δικτυωτό (lattice) στο οποίο μια ετικέτα ασφάλειας $S_1 = (L_1, C_1)$ επικρατεί (dominates) μιας ετικέτας ασφάλειας $S_2 = (L_2, C_2)$, δηλαδή $S_1 \geq S_2$, εάν και μόνον εάν $L_1 \geq L_2$ και $C_1 \supseteq C_2$, όπου L είναι το επίπεδο ασφάλειας και C είναι το σύνολο κατηγοριών.

Υπάρχουν δυο κανόνες που αποτρέπουν τη ροή των πληροφοριών από ανώτερα προς τα κατώτερα επίπεδα ασφάλειας:

1) η *απλή ιδιότητα* (simple security property) ή *προστασία από διάβασμα – προς – τα – πάνω*, που προστατεύει τις πληροφορίες του συστήματος από μη εξουσιοδοτημένη ανάγνωση:
    - ένα υποκείμενο *α* επιτρέπεται να διαβάσει ένα αντικείμενο β εάν και μόνον εάν $S_\alpha \geq S_\beta$.

2) η *ιδιότητα αστερίσκου* (*-property) ή *προστασία από εγγραφή – προς – τα – κάτω*, που προστατεύει τις πληροφορίες του συστήματος από μη εξουσιοδοτημένη εγγραφή ή μετατροπή:
    - ένα υποκείμενο *α* επιτρέπεται να εγγράψει ένα αντικείμενο β εάν και μόνον εάν $S_\alpha \geq S_\beta$.

Η σημασία της ιδιότητας αστερίσκου είναι ότι το άτομο που αποκτά πληροφορίες ενός επιπέδου μπορεί να περάσει αυτές τις πληροφορίες μόνο στα άτομα με επίπεδα που δεν είναι χαμηλότερα από το επίπεδο των πληροφοριών. Αυτό γίνεται για την αποφυγή της εγγραφής – προς – τα – κάτω (write - down), που συμβαίνει όταν ένα υποκείμενο με πρόσβαση σε υψηλού επιπέδου δεδομένα μεταφέρει αυτά τα δεδομένα γράφοντάς τα σε χαμηλότερο επίπεδο. Αποτέλεσμα της εφαρμογής των δυο ιδιοτήτων που αναφέρθηκαν παραπάνω, είναι η δημιουργία ασφαλών ροών πληροφοριών μεταξύ των υποκειμένων, όπως αναπαρίστανται στην εικόνα 6 που ακολουθεί.



Εικόνα 6. Ασφαλής Ροή Πληροφοριών

Τα πεδία ορισμού των αδειών προσπέλασης των υποκειμένων καθορίζονται από τα επίπεδα ασφάλειας αλλά και από τον *πίνακα ελέγχου πρόσβασης* (access control matrix) που είναι ένα σύνολο από τριάδες της μορφής:

$$\{ S, O, AM \}$$

όπου AM είναι ο τρόπος προσπέλασης (access mode) του αντικειμένου (*O*) από το υποκείμενο (*S*).

Οι πολιτικές ασφάλειας που βασίζονται σε αυτό το μοντέλο αποτρέπουν την ροή των πληροφοριών από τα ανώτερα επίπεδα ασφάλειας προς τα κατώτερα. Αυτές οι πολιτικές αναφέρονται ως πολιτικές ασφάλειας πολλαπλών επιπέδων (multi – level – security - MLS).

Μια σημαντική αδυναμία του μοντέλου BLP είναι ότι επιτρέπει την ύπαρξη *συγκαλυμμένων καναλιών* (covert channels). Συγκαλυμμένο κανάλι είναι μια ροή πληροφοριών που δεν ελέγχεται από τους μηχανισμούς ασφάλειας του συστήματος. Στο BLP μοντέλο μπορούν να χρησιμοποιηθούν οι μηχανισμοί ασφάλειας για το στήσιμο ενός συγκαλυμμένου καναλιού, καθώς είναι δυνατή η ροή πληροφοριών υψηλού επιπέδου ασφάλειας σε χαμηλότερα επίπεδα ως εξής:

- ένα χαμηλού – επιπέδου υποκείμενο *S* δημιουργεί ένα αντικείμενο *O* στο επίπεδό του,
- ο ανώτερου – επιπέδου συνεργός του *P* είτε αναβαθμίζει το επίπεδο ασφάλειας του *O* σε υψηλό είτε το αφήνει το ίδιο.
- αργότερα, το χαμηλού – επιπέδου υποκείμενο *S* δοκιμάζει να διαβάσει το αντικείμενο *O*. Ενδεχόμενη επιτυχία ή αποτυχία της αίτησής του φανερώνει την ενέργεια του υψηλού – επιπέδου υποκειμένου. Με αυτό τον τρόπο ένα κομματάκι πληροφορίας έχει διαρρεύσει από πάνω προς τα κάτω, καθώς το να ειπωθεί σε ένα υποκείμενο ότι μια συγκεκριμένη λειτουργία δεν επιτρέπεται συνιστά διαρροή πληροφορίας.

Μια αποδοτική λύση στο πρόβλημα δίνει η *χρήση πολλαπλών αντιγράφων* (polyinstantiation), όπου ένα αντικείμενο μπορεί να έχει διαφορετικές τιμές σε διαφορετικά επίπεδα ασφάλειας με σκοπό την αποφυγή τέτοιου είδους προβλημάτων.

3.3.3. Το Μοντέλο Ακεραιότητας Biba

Το μοντέλο Bell – La Padula παρέχει μόνο προστασία της μυστικότητας των δεδομένων. Όμως, επειδή η ακεραιότητα είναι επίσης σημαντική σε πολλές περιπτώσεις, προτάθηκε το μοντέλο Biba για την προστασία από ακατάλληλη μεταβολή των δεδομένων.

Το μοντέλο Biba είναι δίδυμο του μοντέλου Bell – La Padula για τον τομέα της προστασίας της ακεραιότητας. Το μοντέλο Biba ορίζει επίπεδα ακεραιότητας, τα οποία είναι ανάλογα με τα επίπεδα ευαισθησίας του μοντέλου Bell – La Padula. Τα υποκείμενα και τα αντικείμενα ταξινομούνται με ένα αντίστοιχο σχήμα ταξινόμησης για την ακεραιότητα. Οι αντίστοιχες ετικέτες ακεραιότητας I_α και $_{I\beta}$, ικανοποιούν τους εξής κανόνες:

1. *απλή ιδιότητα ακεραιότητας* (simple integrity property) ή *προστασία από εγγραφή προς τα πάνω*:
    - ένα υποκείμενο α επιτρέπεται να μεταβάλει (να έχει πρόσβαση εγγραφής σε) ένα αντικείμενο β εάν και μόνον εάν $I_\alpha \geq I_\beta$.
2. *ιδιότητα αστερίσκου για την ακεραιότητα* (integrity *-property):
    - αν ένα υποκείμενο α έχει πρόσβαση ανάγνωσης σε ένα αντικείμενο β με επίπεδο ακεραιότητας I_β, τότε το υποκείμενο α επιτρέπεται να έχει πρόσβαση εγγραφής σε ένα άλλο αντικείμενο γ εάν και μόνον εάν $I_\gamma \leq I_\alpha$.

Οι κανόνες αυτοί καλύπτουν την περίπτωση αναξιόπιστων πληροφοριών. Για παράδειγμα, αν υποτεθεί ότι κάποιος είναι γνωστός ως αναξιόπιστος, τότε στην περίπτωση που δημιουργήσει ή μεταβάλλει ένα έγγραφο, οι υπόλοιποι θα πρέπει να μην εμπιστεύονται την αλήθεια των όσων αποτυπώνονται σε αυτό το έγγραφο. Έτσι, αν ένα αναξιόπιστο υποκείμενο έχει δικαίωμα εγγραφής σε ένα αντικείμενο, τότε μειώνεται η ακεραιότητα αυτού του αντικειμένου, όπως ακριβώς οι άνθρωποι γενικώς δείχνουν σκεπτικοί για μια είδηση που βασίζεται σε αναπόδεικτα στοιχεία. Η χαμηλού επιπέδου ακεραιότητα ενός αντικειμένου συνεπάγεται και χαμηλή ακεραιότητα για κάθε άλλο αντικείμενο που βασίζεται σε αυτό.

3.3.4. Το Μοντέλο Lampson

Ο Lampson [Lampson, 1974] εισήγαγε την έννοια της πλέον διαδεδομένης δομής ελέγχου προσπέλασης: του πίνακα ελέγχου προσπέλασης (access control matrix). Ο πίνακας ελέγχου προσπέλασης αποτελείται από μία γραμμή για κάθε υποκείμενο και μια στήλη για κάθε υποκείμενο ή αντικείμενο. Τα δικαιώματα ενός υποκειμένου για να προσπελάσει ένα άλλο υποκείμενο ή αντικείμενο παριστάνονται από τα περιεχόμενα του αντίστοιχου κελιού του πίνακα. Για κάθε αντικείμενο, υπάρχει πάντα ένα υποκείμενο που έχει ορισθεί ως ο ιδιοκτήτης του (owner). Ο ιδιοκτήτης έχει το δικαίωμα προσπέλασης των αντικειμένων του αλλά μπορεί να μεταφέρει το δικαίωμα αυτό και σε άλλα υποκείμενα.

Τα δικαιώματα προσπέλασης αναπαρίστανται με τη μορφή των ιδιοτήτων προσπέλασης (access attributes) σε ένα κελί του πίνακα ελέγχου προσπέλασης $A_{i,j}$. Ο συμβολισμός $A_{i,j}$ ορίζει το δικαίωμα προσπέλασης που έχει ένα

υποκείμενο *i* σε ένα αντικείμενο *j*. Τυπικές ιδιότητες προσπέλασης είναι τα "read" και "write". Δίπλα σε κάθε ιδιότητα προσπέλασης υπάρχει μια σημαία-αντιγραφής (copy flag), με βάση την οποία γίνεται η μεταβίβαση των ιδιοτήτων προσπέλασης.

Στον παρακάτω πίνακα ελέγχου προσπέλασης το υποκείμενο User1 είναι ο ιδιοκτήτης (owner) του αντικειμένου File1 και για αυτό έχει στη διάθεσή του τα δικαιώματα προσπέλασης Read και Write. Επιπλέον, το υποκείμενο User2 για το ίδιο αντικείμενο (File1) διαθέτει το δικαίωμα προσπέλασης Read. Σύμφωνα με τον παραπάνω συμβολισμό, το συγκεκριμένο δικαίωμα προσπέλασης εκφράζεται ως: $A_{User1,\ File1}$ = <Read>.

	File1
User1	Owner / Read / Write
User2	Read

Πίνακας 2. Πίνακας Ελέγχου Προσπέλασης

Το κύριο χαρακτηριστικό του μοντέλου του Lampson είναι η ιδιοκτησία (Ownership). Για κάθε αντικείμενο, υπάρχει πάντα ένα υποκείμενο που έχει ορισθεί ως ο ιδιοκτήτης του (owner).

Παρόλο που υπάρχει η δυνατότητα για μερική μεταβίβαση των προνομίων (privileges) του ιδιοκτήτη σε άλλο χρήστη, δεν υπάρχουν καθορισμένες λειτουργίες με τις οποίες μπορεί να γίνει αυτή η μεταβίβαση, ούτε μια διαχειριστική πολιτική που να ελέγχει και να περιορίζει την διαδικασία της μεταβίβασης. Ωστόσο, ο Lampson όρισε τρεις κανόνες προστασίας (protection rules), καθώς και τη χρήση της λεγόμενης «σημαίας αντιγραφής» (copy flag). Οι κανόνες για την υποστήριξη των μεταβολών στον πίνακα προσπέλασης (access matrix), περιγράφουν το πως ένας ιδιοκτήτης Δ1 ενός αντικειμένου ψ, μπορεί να διαγράψει, να αντιγράψει και να προσθέσει νέες ιδιότητες προσπέλασης (access attributes) σε ένα κελί του πίνακα προσπέλασης Αχψ. Τυπικές ιδιότητες προσπέλασης είναι τα "read" και "write". Δίπλα σε κάθε ιδιότητα προσπέλασης υπάρχει μια σημαία αντιγραφής (copy flag), η οποία συμβολίζεται με ένα αστερίσκο (*) σε κάθε αντίστοιχη ιδιότητα προσπέλασης, με βάση την οποία γίνεται η μεταβίβαση των ιδιοτήτων προσπέλασης, όπως περιγράφεται πιο κάτω.

Οι τρεις κανόνες προστασίας είναι οι εξής [Lampson, 1974]:

- ο Δ_1 μπορεί να διαγράψει ιδιότητες προσπέλασης από το $A_{\Delta 2,\psi}$, εάν διαθέτει δικαίωμα προσπέλασης στο Δ_2.
- ο Δ_1 μπορεί να αντιγράψει στο $A_{\Delta 2,\psi}$ ιδιότητες προσπέλασης που έχει για το ψ, όπου ψ έχει σημαία-αντιγραφής (copy flag), και να διαλέξει αν

οι αντιγραμμένα ιδιότητες προσπέλασης θα έχουν σημαία-αντιγραφής (copy flag).

- ο Δ_1 μπορεί να εισάγει ιδιότητες προσπέλασης στο $A_{\Delta 2,\psi,}$ με ή χωρίς την σημαία - αντιγραφής, εάν είναι ιδιοκτήτης του ψ.

3.3.5. Το Μοντέλο 'Graham – Denning'

Ο Lampson και οι Graham και Denning εισήγαγαν την έννοια του φορμαλιστικού συστήματος κανόνων προστασίας (formal system of protection rules).

Οι Graham και Denning έφτιαξαν ένα μοντέλο με ιδιότητες γενικής προστασίας, το οποίο λειτουργεί πάνω:

- σε ένα σύνολο υποκειμένων *S*,
- ένα σύνολο αντικειμένων *O*,
- ένα σύνολο δικαιωμάτων προσπέλασης *R* και
- έναν πίνακα ελέγχου προσπέλασης *A*.

Ο πίνακας έχει μια γραμμή για κάθε υποκείμενο και μια στήλη για κάθε υποκείμενο και κάθε αντικείμενο. Τα δικαιώματα ενός υποκειμένου σε άλλο υποκείμενο ή αντικείμενο παριστάνονται από τα περιεχόμενα του αντίστοιχου στοιχείου του πίνακα. Για κάθε αντικείμενο, το υποκείμενο που ορίσθηκε ως ¨ιδιοκτήτης¨ έχει ειδικά δικαιώματα. Για κάθε υποκείμενο το υποκείμενο που έχει ορισθεί ως ο ¨ελεγκτής¨ του έχει και αυτό ειδικά δικαιώματα.

Στο μοντέλο Graham – Denning υπάρχουν οκτώ στοιχειώδη δικαιώματα προστασίας. Τα δικαιώματα αυτά διατυπώνονται ως εντολές που εκδίδονται από υποκείμενα και εφαρμόζονται σε άλλα υποκείμενα ή αντικείμενα:

- *Δημιουργία και διαγραφή αντικειμένου*: επιτρέπει στο υποκείμενο να εισάγει ένα νέο ή να διαγράψει ένα αντικείμενο του συστήματος.
- *Δημιουργία και διαγραφή υποκειμένου*: επιτρέπει στο υποκείμενο να εισάγει ένα νέο ή να διαγράψει ένα υποκείμενο του συστήματος.
- *Ανάγνωση δικαιώματος προσπέλασης*: επιτρέπει σε ένα υποκείμενο να προσδιορίζει τα τρέχοντα δικαιώματα προσπέλασης ενός υποκειμένου σε ένα αντικείμενο.
- *Παραχώρηση δικαιώματος προσπέλασης*: επιτρέπει στον ιδιοκτήτη ενός αντικειμένου να μεταβιβάζει οποιαδήποτε δικαιώματα προσπέλασης για ένα αντικείμενο σε άλλο υποκείμενο.
- *Διαγραφή δικαιώματος προσπέλασης*: επιτρέπει σε ένα υποκείμενο να διαγράψει ένα δικαίωμα προσπέλασης ενός άλλου υποκειμένου για ένα αντικείμενο, εφόσον το υποκείμενο που διαγράφει είτε είναι ο ιδιοκτήτης του αντικειμένου είτε ελέγχει το υποκείμενο από το οποίο πρέπει να διαγράφει η προσπέλαση.
- *Μεταφορά δικαιώματος προσπέλασης*: επιτρέπει σε ένα υποκείμενο να μεταφέρει κάποιο από τα δικαιώματά του για ένα αντικείμενο σε ένα

άλλο υποκείμενο. Κάθε δικαίωμα μπορεί να είναι ή να μην είναι μεταφέρσιμο. Αν ένα υποκείμενο παραλάβει ένα μεταφέρσιμο δικαίωμα, το υποκείμενο μπορεί μετά να μεταφέρει αυτό το δικαίωμα (είτε είναι μεταφέρσιμο είτε όχι) σε άλλα υποκείμενα. Αν ένα υποκείμενο παραλάβει ένα μη – μεταφέρσιμο δικαίωμα, μπορεί να χρησιμοποιήσει το δικαίωμα αλλά δεν μπορεί να μεταφέρει το δικαίωμα σε άλλα υποκείμενα.

Οι κανόνες αυτοί παρέχουν τις αναγκαίες ιδιότητες για την μοντελοποίηση των μηχανισμών ελέγχου προσπέλασης σε ένα σύστημα προστασίας, για παράδειγμα με τη μορφή μιας *ελεγκτικής διάταξης αναφοράς* (reference monitor).

3.3.6. Το Μοντέλο 'Harrison – Ruzzo – Ullman'

Το μοντέλο Harrison – Ruzzo – Ullman (HRU) αποτελεί μια παραλλαγή του μοντέλου Graham – Denning και παρέχει τη δυνατότητα για τον ορισμό συστημάτων εξουσιοδότησης με μεταβλητά δικαιώματα προσπέλασης και λειτουργίες δημιουργίας και διαγραφής υποκειμένων και αντικειμένων. Για την περιγραφή του μοντέλου HRU χρειαζόμαστε:

- ένα σύνολο υποκειμένων *S*,
- ένα σύνολο αντικειμένων *O*,
- ένα σύνολο δικαιωμάτων προσπέλασης *R*,
- έναν πίνακα προσπέλασης $M = (M_{so})_s \in S, _o \in O$, όπου κάθε M_{so} είναι το υποσύνολο του *R* που προσδιορίζει τα δικαιώματα προσπέλασης του υποκειμένου *S* στο αντικείμενο *O*.

Υπάρχουν έξι πρωτογενείς λειτουργίες για τον χειρισμό των συνόλων υποκειμένων και αντικειμένων, καθώς και του πίνακα προσπέλασης:

- ✓ enter *r* into M_{so}
- ✓ delete *r* from M_{so}
- ✓ create subject *s*
- ✓ delete subject *s*
- ✓ create object *o*
- ✓ delete subject *o*

Οι εντολές του μοντέλου HRU είναι της μορφής:

command c (x_1, ….., x_k),
if r_1 in M_{S101} and
if r_2 in M_{S202} and
….

if r_m in M_{SmOm} and
then
$operation_1$

operation$_2$
….
operation$_n$
and

όπου οι δείκτες s_1, …., s_m και o_1, …., o_m είναι υποκείμενα και αντικείμενα που εμφανίζονται στην λίστα παραμέτρων (x1, …., xk). Οι συνθήκες (if) ελέγχουν κατά πόσον υπάρχουν τα επιμέρους δικαιώματα προσπέλασης.
Αν ικανοποιούνται όλες οι συνθήκες (που μπορεί και να μην υπάρχουν καθόλου) τότε εκτελούνται οι βασικές λειτουργίες (operations).

Κάθε εντολή περιέχει τουλάχιστον μια λειτουργία. Για παράδειγμα, η εντολή:

command *create_file (s,f)*
create *f*
enter o into $M_{s,f}$
enter r into $M_{s,f}$
enter w into $M_{s,f}$
end

χρησιμοποιείται από το υποκείμενο *s* για την δημιουργία ενός νέου αρχείου *f* έτσι ώστε το *s* να είναι ο κάτοχος του αρχείου (δικαίωμα προσπέλασης o) και να έχει άδεια ανάγνωσης και εγγραφής στο αρχείο (δικαίωμα προσπέλασης r και w). Ο κάτοχος *s* του αρχείου *f* παραχωρεί πρόσβαση ανάγνωσης σε ένα άλλο υποκείμενο *p* με την εντολή:

command *grant _ read (s,p,f),*
if o in $M_{s,f}$
then enter r in $M_{p,f}$
end

Το αποτέλεσμα της εκτέλεσης κάθε μιας εντολής καταγράφεται ως μεταβολή του πίνακα προσπέλασης.

3.3.7. Το Μοντέλο RBAC

Στο μοντέλο RBAC [Ferraiolo and Kuhn, 1995], [Sandhu, Coyne et al., 1996], [Sandhu, 1998], [Ferraiolo, Kuhn, et al., 2003] έχει αποδοθεί αξιόλογη προσοχή ως η πολλά υποσχόμενη προσέγγιση για επέκταση των παραδοσιακών κατά-απαίτηση (MAC) και κατά-διάκριση (DAC) έλεγχων προσπέλασης. Σύμφωνα με το [Sandhu, Coyne et al., 1996], ένα ενδιαφέρον χαρακτηριστικό του RBAC είναι ότι από μόνο του είναι ουδέτερο πολιτικής

(policy neutral). Επιτρέπει να παραχωρείται σε χρήστες ο προσδιορισμός των εξουσιοδοτήσεων σε αντικείμενα, όπως στον κατά-διάκριση έλεγχο προσπέλασης, ενώ επιπλέον μπορεί να επιβάλλει περιορισμούς, είτε άμεσα είτε μέσω των ιεραρχιών των ρόλων, στη χρήση τέτοιων εξουσιοδοτήσεων με σκοπό τον έλεγχο ροής πληροφοριών, όπως στον κατά-απαίτηση έλεγχο προσπέλασης. Ο έλεγχος προσπέλασης που τελικά επιβάλλεται σε ένα σύστημα, είναι το αποτέλεσμα της κατάλληλης διαμόρφωσης και των αλληλεπιδράσεων διαφόρων συστατικών (μηχανισμών) του RBAC. Ένα άλλο ενδιαφέρον πλεονέκτημα του RBAC είναι η δυνατότητα μετατροπής της πολιτικής ασφάλειας προκειμένου να συμμορφώνεται στις ανάγκες ενός οργανισμού καθώς αυτές αλλάζουν συνεχώς.

Οι άδειες (permissions) στα μοντέλα RBAC αποτελούν εγκρίσεις για επιμέρους τρόπους προσπέλασης αντικειμένων στο σύστημα. Οι όροι εξουσιοδότηση, άδεια, δικαίωμα προσπέλασης και προνόμιο (authorization, permission, access right and privilege) χρησιμοποιούνται στη βιβλιογραφία με την ίδια έννοια. Οι άδειες είναι πάντοτε θετικές (positive) και παρέχουν στον κάτοχο την δυνατότητα να εκτελεί μια πράξη στο σύστημα [Sandhu, Coyne et al., 1996].

Το μοντέλο RBAC παρέχει έναν τρόπο ονοματολογίας και ορισμού σχέσεων μεταξύ ατόμων (individuals) και δικαιωμάτων (rights) κάνοντας χρήση εννοιών όπως οι ρόλοι και οι ιεραρχίες ρόλων, η ενεργοποίηση ρόλου και οι περιορισμοί στην ιδιότητα μέλους ρόλου [Ferraiolo και Kuhn, 1992]. Τα πρώτα βήματα ορισμού του βασισμένου σε ρόλους ελέγχου προσπέλασης πραγματοποιήθηκαν από τους [Ferraiolo, Cugini et al., 1995], [Sandhu, Coyne et al., 1996] και [Nyanchama and Osborn, 1994]. Ένα περιεκτικό πλαίσιο ορισμού για το μοντέλο RBAC, μαζί με τον αντίστοιχο φορμαλισμό, ορίσθηκε στην εργασία [Sandhu, Coyne et al., 1996] και επεκτείνεται στις εργασίες [Sandhu, 1998b], [Sandhu, Bhamidipati et al., 1999], [Ahn και Sandhu, 2000] και [Osborn, Sandhu et al., 2000].

Το 2001 προτάθηκε ένα ολοκληρωμένο πρότυπο για το μοντέλο RBAC [Ferraiolo, Sandhu et al., 2001] που περιλαμβάνει τα ακόλουθα μέρη:

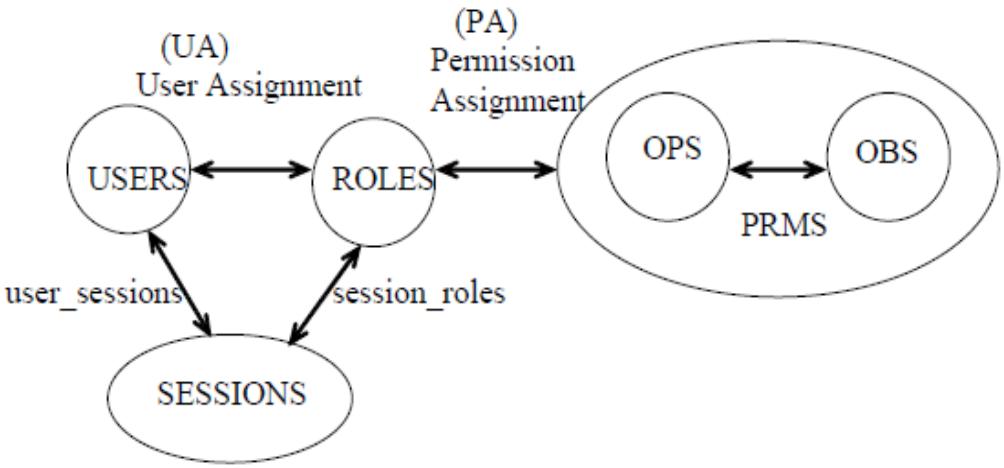
- Βασικό RBAC (Core RBAC)
- Ιεραρχικό RBAC (Hierarchical RBAC)
- RBAC με Περιορισμούς (Constrained RBAC)
  - σχέσεις στατικού διαχωρισμού καθηκόντων (Static separation of duty relations).
  - σχέσεις δυναμικού διαχωρισμού καθηκόντων (Dynamic separation of duty relations).

3.3.7.1. Το Βασικό RBAC

Το Βασικό RBAC (Core RBAC) ενσωματώνει τα βασικά χαρακτηριστικά ενός μοντέλου ελέγχου προσπέλασης βασισμένου σε ρόλους. Η βασική ιδέα του RBAC είναι ότι άδειες εκχωρούνται σε ρόλους και κατόπιν εκχωρούνται ρόλοι σε χρήστες, με αποτέλεσμα οι χρήστες να αποκτούν άδειες μέσω των εκχωρημένων σε αυτούς ρόλων.

Το βασικό RBAC περιλαμβάνει τις πολλαπλές σχέσεις χρήστη-ρόλου (user-role) και άδειας-ρόλου (permission-role). Κατά συνέπεια στον ίδιο χρήστη μπορούν να εκχωρηθούν πολλοί ρόλοι, ενώ ένας ρόλος μπορεί να έχει εκχωρηθεί σε πολλούς χρήστες. Ομοίως, σε ότι αφορά τις εκχωρήσεις αδειών σε ρόλους. Ακόμη, στο βασικό RBAC κάθε χρήστης στα πλαίσια μιας συνόδου (session) μπορεί να ενεργοποιήσει πολλούς ρόλους μαζί.

Τα συστατικά και οι σχέσεις του Βασικού RBAC φαίνονται στο παρακάτω σχήμα:



Εικόνα 7. Το Βασικό RBAC μοντέλο

Το βασικό RBAC αποτελείται από τρία συστατικά (Εικόνα 7):

- χρήστες (Users)
- άδειες (Permissions)
- ρόλοι (Roles)

Ένας χρήστης είναι ένα άτομο που χρησιμοποιεί το πληροφοριακό σύστημα. Ένας ρόλος αντιστοιχεί σε μια εργασιακή διαδικασία (job function) μέσα στα πλαίσια ενός οργανισμού, μαζί με κάποια σχετική σημασιολογία που αφορά

την υπευθυνότητα και την αρμοδιότητα που έχει αποδοθεί στα μέλη του (χρήστες).

Η άδεια είναι μια έγκριση ενός συγκεκριμένου τρόπου πρόσβασης σε έναν τύπο αντικειμένου. Στην πραγματικότητα είναι ένα ζεύγος που αποτελείται από ένα τύπο αντικειμένου (object - OBS) και έναν τρόπο πρόσβασης / λειτουργίας (operation - OPS) στο αντικείμενο αυτό.

Στο βασικό RBAC υπάρχουν ακόμα και οι εξής σχέσεις:

- User-assignment (UA): πολλά-προς-πολλά σχέση εκχώρησης των χρηστών σε ρόλους.
- Permission-assignment (PA): πολλά-προς-πολλά σχέση εκχώρησης των αδειών σε ρόλους.

Μια ακόμη βασική έννοια του βασικού RBAC είναι οι σύνοδοι (SESSIONS). Κάθε σύνοδος θεωρείται ότι παρέχει μια αντιστοιχία μεταξύ ενός χρήστη και του υποσυνόλου ενεργοποιημένων ρόλων από αυτούς που του έχουν αρχικά εκχωρηθεί. Το σύνολο των αδειών που είναι διαθέσιμες στον χρήστη προκύπτει από όλες τις άδειες που έχουν εκχωρηθεί στους ρόλους που είναι ενεργοποιημένοι κατά την διάρκεια της συνόδου του χρήστη.

Ακολουθεί η φορμαλιστική περιγραφή του βασικού (core) RBAC [Ferraiolo, Sandhu et al., 2001]:

- *USERS, ROLES, OPS,* και *OBS*: χρήστες, ρόλοι, λειτουργίες και αντικείμενα, αντίστοιχα.

- $UA \subseteq USERS \times ROLES$: πολλά-προς-πολλά σχέση εκχώρησης των χρηστών σε ρόλους.

- assigned_users: $(r{:}ROLES) \rightarrow 2^{USERS}$: αντιστοιχία ενός ρόλου r σε ένα σύνολο από χρήστες.

- $assigned\_users(r) = \{u \in USERS \mid (u, r) \in UA\}$

- $PRMS = 2^{(OPS \times OBS)}$: το σύνολο των αδειών.

- $Op(p{:}\ PRMS) \rightarrow \{op \subseteq OPS\}$: αντιστοιχία μιας άδειας σε μια λειτουργία.

- $Ob(p{:}\ PRMS) \rightarrow \{ob \subseteq OBS\}$: αντιστοιχία μιας άδειας σε ένα αντικείμενο.

- $PA \subseteq PRMS \times ROLES$: πολλά - προς - πολλά σχέση εκχώρησης των αδειών σε ρόλους.

- *assigned_permissions*(*r*: *ROLES*) → 2^{PRMS}: αντιστοιχία ενός ρόλου r σε ένα σύνολο από άδειες.

- assigned_permissions(r) = {p∈PRMS | (p, r) ∈ PA}

- *SESSIONS*: το σύνολο των συνόδων.

- *user_sessions* (*u*: *USERS*) → $2^{SESSIONS}$: αντιστοιχία ενός χρήστη *u* σε ένα σύνολο από συνόδους.

- *session_roles* (*s*: *SESSIONS*) → 2^{ROLES}: αντιστοιχία μιας συνόδου *s* σε ένα σύνολο από ρόλους.

- session_roles (si) ⊆ {r∈ ROLES | (session_users (si), r) ∈ UA}

- *avail_session_perms*(*s*:*SESSIONS*) → 2^{PRMS}: οι άδειες που είναι διαθέσιμες σε ένα
  χρήστη κατά την διάρκεια μια συνόδου = $\bigcup_{r \in session\_roles(s)} assigned\_permissions(r)$

3.3.7.2. Το Ιεραρχικό RBAC

Το Ιεραρχικό RBAC (Hierarchical RBAC), πέρα από τα συστατικά του Βασικού RBAC, υποστηρίζει τις ιεραρχίες ρόλων. Οι ιεραρχίες ρόλων στο RBAC αποτελούν φυσικά μέσα δόμησης ρόλων προκειμένου να αντικατοπτρίσουν τους σχηματισμούς αρμοδιότητας και υπευθυνότητας ενός οργανισμού. Οι πλέον ισχυροί (ανώτεροι) ρόλοι (senior roles) τοποθετούνται προς την κορυφή και οι λιγότερο ισχυροί (κατώτεροι) ρόλοι (junior roles) προς τη βάση των διαγραμμάτων απεικόνισης των ιεραρχιών [Sandhu, Coyne et al., 1996], [Sandhu, 1998].

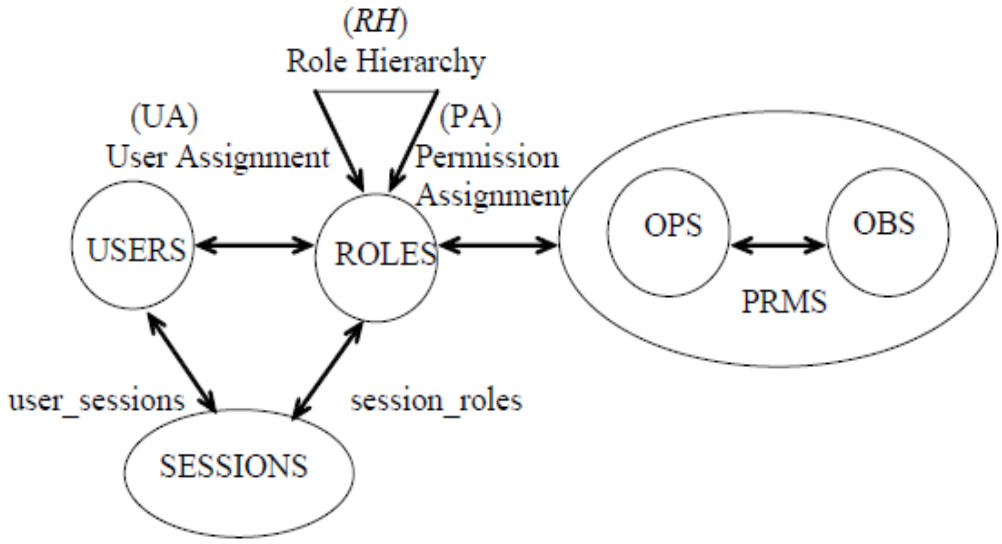
Από μαθηματικής απόψεως, μια ιεραρχία είναι μια μερική διάταξη ρόλων που καθορίζει μια σχέση ανωτερότητας (seniority) μεταξύ τους, κατά την οποία οι ανώτεροι (πρεσβύτεροι) ρόλοι στην ιεραρχία αποκτούν τις άδειες των κατωτέρων (νεοτερών) τους, ενώ οι χρήστες των ανωτέρων ρόλων αποκτούν την ιδιότητα μέλους των κατώτερων.

Στο Ιεραρχικό RBAC αναγνωρίζονται δύο τύποι ιεραρχιών των ρόλων:

- Γενικό Ιεραρχικό RBAC (General Hierarchical RBAC) : Υπάρχει μια αυθαίρετη μερική διάταξη των ρόλων που χρησιμοποιείται ως ιεραρχία ρόλων, ώστε να περιλαμβάνεται η έννοια της πολλαπλής κληρονομικότητας των αδειών μεταξύ των ρόλων.

- Περιορισμένο Ιεραρχικό RBAC (Limited Hierarchical RBAC) : Επιβάλλονται περιορισμοί στην ιεραρχία των ρόλων. Συνηθέστερα, οι ιεραρχίες ρόλων περιορίζονται σε απλές δομές, όπως τα ανεστραμμένα δέντρα.

Το Ιεραρχικό RBAC, δηλαδή το μοντέλο που περιλαμβάνει τις ιεραρχίες των ρόλων (role hierarchies - RH), παρουσιάζεται στο παρακάτω σχήμα (Εικόνα 8):

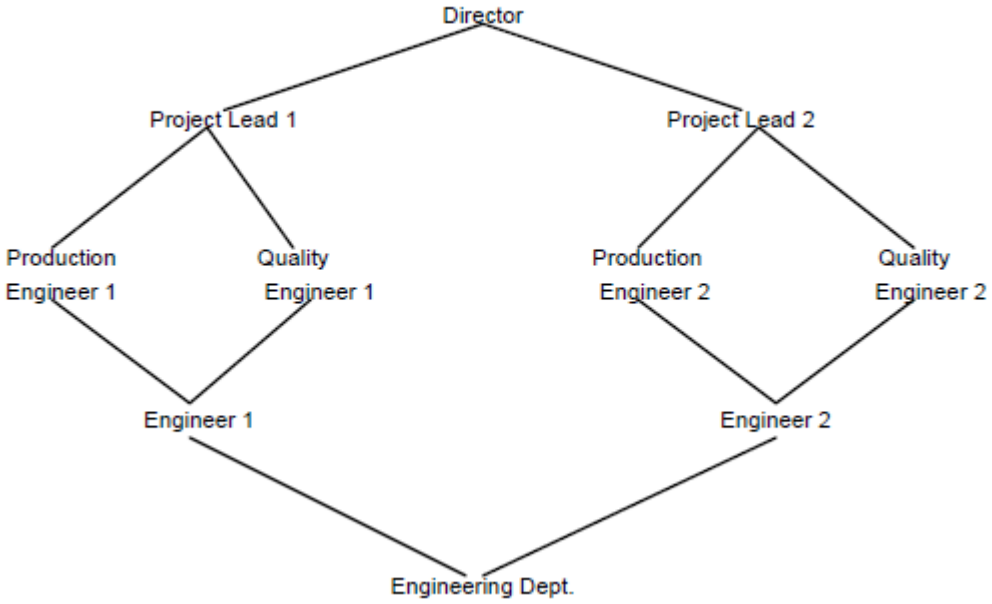


Εικόνα 8. Το ιεραρχικό RBAC μοντέλο

Η ιεραρχία των ρόλων ορίζει μια σχέση κληρονομικότητας μεταξύ των ρόλων. Η κληρονομικότητα των αδειών / προνομίων έχει διατυπωθεί ως εξής [Nyanchama and Osborn, 1999]:

- Ο ρόλος r1 κληρονομεί προνόμια από το ρόλο r2 εάν όλα τα προνόμια του ρόλου r2 είναι και προνόμια του ρόλου r1

Όπως φαίνεται στο παρακάτω παράδειγμα (Εικόνα 9), όταν λέμε ότι ο ρόλος «Project Lead 1» κληρονομεί προνόμια από τον ρόλο «Engineer 1», σημαίνει ότι τις άδειες του ρόλου «Engineer 1» περιλαμβάνονται στο σύνολο των αδειών του «Project Lead 1».



Εικόνα 9. Παράδειγμα ιεραρχίας ρόλων [Ferraiolo, Sandhu et al., 2001]

Στη συνέχεια ορίζεται φορμαλιστικά το Ιεραρχικό RBAC.

3.3.7.2.1. Γενικό ιεραρχικό RBAC

RH $\subseteq$ ROLES $\times$ ROLES, είναι μια σχέση μερικής διάταξης των ρόλων (ROLES) που ονομάζεται σχέση κληρονομικότητας. Η σχέση κληρονομικότητας συμβολίζεται ως $\geq$. Για δύο ρόλους r1 και r2 υπάρχει μια σχέση κληρονομικότητας $r1 \geq r2$ αν όλες οι άδειες του ρόλου r2 είναι και άδειες του r1 και όλοι οι εξουσιοδοτημένοι χρήστες στο ρόλο r1 είναι εξουσιοδοτημένοι και στο ρόλο r2, δηλαδή:

$r1 \geq r2 \Rightarrow$ authorized_permissions (r2) $\subseteq$ authorized_permissions (r1) $\wedge$ authorized_users (r1) $\subseteq$authorized_users (r2)

- authorized_users(r: ROLES) $\rightarrow 2^{USERS}$, είναι η αντιστοιχία του ρόλου r σε ένα σύνολο από χρήστες με την χρήση της ιεραρχίας των ρόλων:
  - authorized_users(r) = {u$\in$USERS | r' $\geq$ r, (u, r') $\in$ UA}

- authorized_permissions(r: ROLES) $\rightarrow 2^{PRMS}$ είναι η αντιστοιχία του ρόλου r σε ένα σύνολο από άδειες με την χρήση της ιεραρχίας των ρόλων:
  - authorized_permissions(r) = {p$\in$PRMS | r' $\geq$ r, (p, r') $\in$ PA}

3.3.7.2.2. Περιορισμένο ιεραρχικό RBAC

Στο περιορισμένο ιεραρχικό RBAC υπάρχει η έννοια του άμεσου απόγονου (immediate descendent). Θα λέμε ότι ο ρόλος r_1 είναι άμεσος απόγονος του ρόλου r_2, εάν $r_1 \geq r_2$ και δεν υπάρχει άλλος ρόλος μεταξύ των ρόλων r_1 και r_2. Με άλλα λόγια, δεν υπάρχει ρόλος r_3 μέσα στην ιεραρχία για τον οποίο να ισχύει $r_1 \geq r_3 \geq r_2$, με $r_1 \neq r_2$ και $r_2 \neq r_3$. Συμβολικά όταν ο ρόλος r_1 είναι άμεσος απόγονος του ρόλου r_2 θα απεικονίζεται ως $r_1 >> r_2$. Η φορμαλιστική περιγραφή του Περιορισμένου Ιεραρχικού RBAC [Ferraiolo, Sandhu et al., 2001] αποδίδεται ως εξής:

Για κάθε ρόλο r, r_1, $r_2 \in$ ROLES, θα πρέπει να ισχύει, $r \geq r_1 \wedge r \geq r_2 \Rightarrow r_1 = r_2$

3.3.7.3. RBAC με Περιορισμούς

Το μοντέλο RBAC με Περιορισμούς (Constrained RBAC) περιλαμβάνει τα συστατικά του Βασικού RBAC, καθώς και τις σχέσεις διαχωρισμού των καθηκόντων. Πιο συγκεκριμένα, στο RBAC με Περιορισμούς διακρίνουμε δύο περιπτώσεις:

- χρήση σχέσεων στατικού διαχωρισμού καθηκόντων και
- χρήση σχέσεων δυναμικού διαχωρισμού καθηκόντων.

3.3.7.3.1. Σχέσεις στατικού διαχωρισμού καθηκόντων

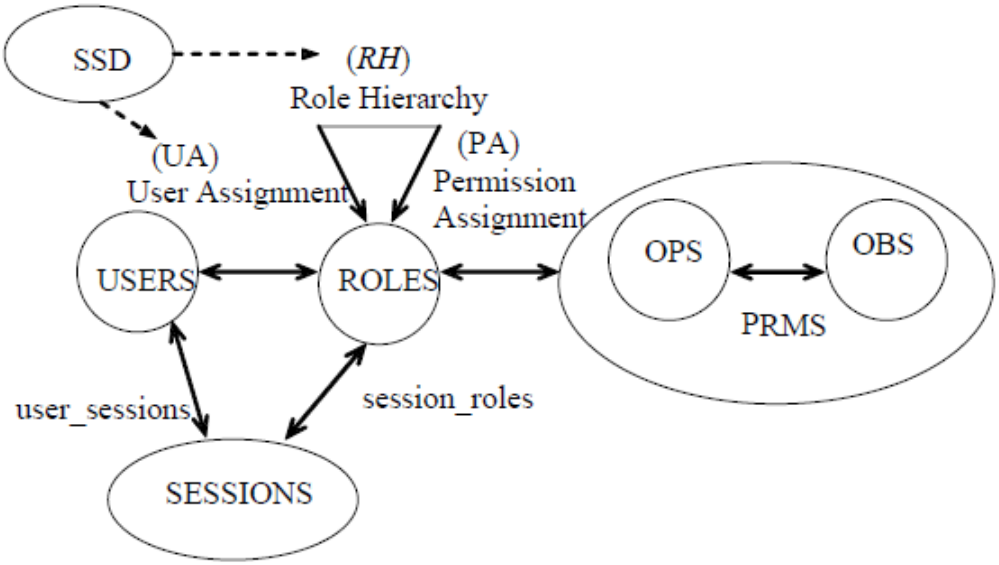
Οι σχέσεις στατικού διαχωρισμού των καθηκόντων (Static Separation of Duty relations - SSD) χρησιμοποιούνται για να επιβάλουν πολιτικές αντιμετώπισης της σύγκρουσης συμφερόντων (conflict of interest). Η σύγκρουση συμφερόντων για ένα βασισμένο – σε - ρόλους σύστημα μπορεί να προκύψει όταν ένας χρήστης έχει πρόσβαση σε άδειες που είναι εκχωρημένες σε συγκρουόμενους ρόλους. Αυτό μπορεί να αποφευχθεί με την χρήση του στατικού διαχωρισμού των καθηκόντων, δηλαδή μέσω της επιβολής περιορισμών στην εκχώρηση των χρηστών σε ρόλους.

Λόγω της ύπαρξης των μοντέλων RBAC, με και χωρίς ιεραρχίες ρόλων, ο στατικός διαχωρισμός των καθηκόντων παρουσιάζεται ξεχωριστά και για τις δύο περιπτώσεις:

- Στατικός διαχωρισμός καθηκόντων χωρίς ιεραρχίες: Οι περιορισμοί των σχέσεων SSD εφαρμόζονται στις εκχωρήσεις των χρηστών σε ρόλους. Η συμμετοχή ενός χρήστη σε έναν ρόλο μπορεί να του απαγορεύσει την συμμετοχή του σε έναν ή περισσότερους άλλους ρόλους, ανάλογα με τους περιορισμούς που επιβάλλονται από το SSD.

- Στατικός διαχωρισμός καθηκόντων με ιεραρχίες: Αυτός ο τύπος σχέσης SSD λειτουργεί με τον ίδιο τρόπο όπως το βασικό SSD εκτός από το ότι κατά την επιβολή των περιορισμών SSD εξετάζονται άμεσα και οι κληρονομημένοι ρόλοι (λόγω της ύπαρξης της ιεραρχίας).

Στο παρακάτω σχήμα (Εικόνα 10) απεικονίζεται το μοντέλο RBAC που περιλαμβάνει τις ιεραρχίες των ρόλων (role hierarchies (RH)) αλλά και τις σχέσεις SSD:



Εικόνα 10. Το μοντέλο RBAC με ιεραρχίες ρόλων και στατικό διαχωρισμό των καθηκόντων.

Φορμαλιστικά, ο στατικός διαχωρισμός καθηκόντων (SSD) ορίζεται ως εξής [Ferraiolo, Sandhu et al., 2001]:

- Στατικός διαχωρισμός καθηκόντων χωρίς ιεραρχίες:

  - SSD ⊆ (2^{ROLES} × N) είναι σύνολο από ζευγάρια (rs, n), όπου κάθε rs είναι ένα σύνολο από ρόλους και n είναι ένα φυσικός αριθμός ≥2, με την ιδιότητα ότι σε κανέναν χρήστη δεν εκχωρούνται n ή και περισσότεροι ρόλοι από το σύνολο rs για κάθε $(rs, n) \in SSD$:

$$\forall (rs,n) \in SSD, \forall s \subseteq rs : |s| \geq n \Rightarrow \bigcap_{r \in s} assigned\_users(r) = \varnothing$$

- Στατικός διαχωρισμός καθηκόντων με την παρουσία μιας ιεραρχίας :

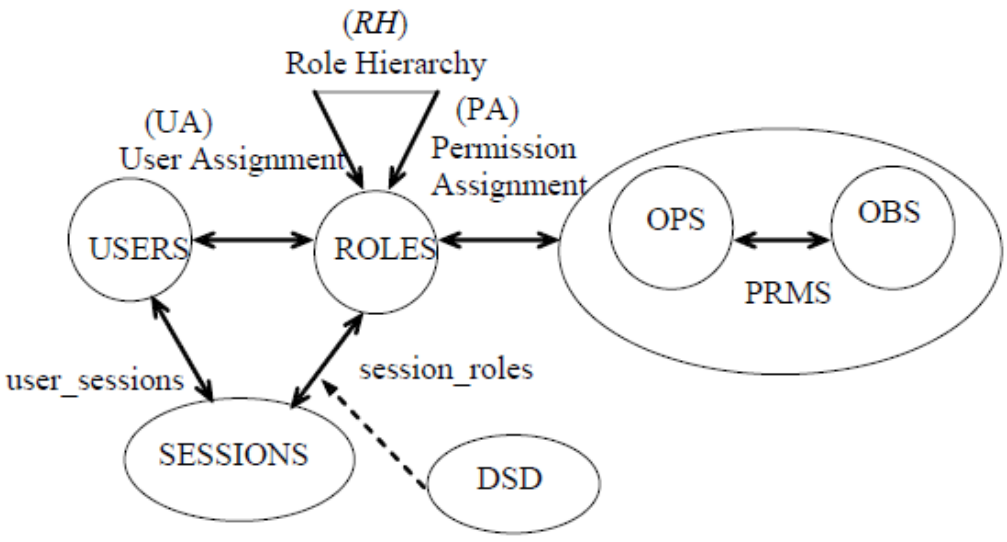
- Με την παρουσία μιας ιεραρχίας ο στατικός διαχωρισμός καθηκόντων ορίζεται στη βάση χρηστών που είναι εξουσιοδοτημένοι (authorized) παρά εκχωρημένοι (assigned) σε ρόλους, σύμφωνα με το φορμαλιστικό ορισμό του Ιεραρχικού RBAC :

$$\forall (rs, n) \in SSD, \forall s \subseteq rs : |s| \geq n \Rightarrow \bigcap_{res} authorized\_users\ (r) = \varnothing$$

3.3.7.3.2. Σχέσεις δυναμικού διαχωρισμού καθηκόντων

Οι σχέσεις δυναμικού διαχωρισμού καθηκόντων (Dynamic Separation of duty relations - DSD), όπως και οι σχέσεις SSD, περιορίζουν τις άδειες που είναι διαθέσιμες σε έναν χρήστη. Εντούτοις, οι DSD σχέσεις διαφέρουν από τις σχέσεις SSD σε ότι αφορά την χρονική περίοδο κατά την οποία επιβάλλονται αυτοί οι περιορισμοί. Οι απαιτήσεις DSD περιορίζουν τη διαθεσιμότητα των αδειών, με την τοποθέτηση περιορισμών στους ρόλους που μπορούν να ενεργοποιηθούν κατά την διάρκεια των συνόδων ενός χρήστη.

Το μοντέλο RBAC που περιλαμβάνει τις σχέσεις DSD παρουσιάζεται στο σχήμα της Εικόνας 11 :



Εικόνα 11. Το μοντέλο RBAC με ιεραρχίες ρόλων και δυναμικό διαχωρισμό των καθηκόντων.

Ο φορμαλιστικός ορισμός των σχέσεων δυναμικού διαχωρισμού των καθηκόντων παρατίθεται στη συνέχεια [Ferraiolo, Sandhu et al., 2001]:

$DSD \subseteq (2^{ROLES} \times \mathrm{N})$: ένα dsd είναι μια συλλογή από ζευγάρια (rs, n) που βρίσκονται σε δυναμικό διαχωρισμό καθηκόντων, όπου κάθε rs είναι ένα σύνολο ρόλων και n είναι ένας φυσικός αριθμός ≥ 2, με την ιδιότητα ότι κανένα υποκείμενο (χρήστης) δεν μπορεί να ενεργοποιήσει n ή περισσότερους ρόλους από το σύνολο rs για κάθε dsd ∈DSD. Φορμαλιστικά:

$$\forall rs \in 2^{ROLES}, n \in \mathrm{N}, (rs, n) \in DSD \Rightarrow n \geq 2 \wedge |rs| \geq n, \text{ και } \forall s \in SESSIONS, \forall rs \in 2^{ROLES},$$
$$\forall role\_subset \in 2^{ROLES}, \forall n \in \mathrm{N}, (rs, n) \in DSD, role\_subset \subseteq rs, role\_subset \subseteq$$
$$session\_roles(s) \Rightarrow |role\_subset| \leq n.$$

3.3.8. Μοντέλα 'Ροής – Πληροφοριών'

Είδαμε ότι στο μοντέλο Bell – La Padula (BLP) οι πληροφορίες μπορούν να ρέουν από ένα υψηλό επίπεδο ασφάλειας σε ένα χαμηλό επίπεδο μέσω ενός συγκαλυμμένου καναλιού (covert channel). Τα μοντέλα Ροής – Πληροφοριών (Information - Flow) εξετάζουν οποιοδήποτε είδος ροής πληροφοριών (όχι μόνο την άμεση πληροφοριακή ροή μέσω ενεργειών προσπέλασης που μοντελοποιούνται στο BLP).

Μια πληροφοριακή ροή προκαλείται από ένα αντικείμενο *x* σε ένα αντικείμενο *y* όταν μπορούμε να μάθουμε περισσότερα για το *x* παρατηρώντας το *y*. Αν ήδη γνωρίζουμε το *x* τότε δεν μπορεί να υπάρξει πληροφοριακή ροή από το *x*.

Μπορούμε να διαχωρίσουμε μεταξύ:

- *σαφούς πληροφοριακής ροής*: η παρατήρηση του *y* μετά την εκχώρηση y :=x μας λέει για την τιμή του *x*.
- Υπονοούμενης πληροφοριακής ροής: η παρατήρηση του *y* μετά την εξαρτώμενη εντολή if x = 0 then y := 1, πιθανώς να μας λέει κάτι για την τιμή του *x* αν δεν είχε εκτελεσθεί η εκχώρηση y :=1. Για παράδειγμα, αν *y* = 2, τότε ξέρουμε ότι x ≠ 0.

Τα συστατικά του μοντέλου ροής – πληροφοριών αποτελούνται από:

- ένα δικτυωτό (lattice) από ετικέτες ασφάλειας,
- ένα σύνολο αντικειμένων με ετικέτες,
- μια πολιτική ασφάλειας, όπου η ροή πληροφοριών από ένα αντικείμενο με ετικέτα c_1 σε ένα αντικείμενο με ετικέτα c_2 επιτρέπεται μόνον αν $c_1 \leq c_2$. Κάθε ροή πληροφοριών που παραβαίνει αυτόν τον κανόνα είναι παράνομη.

Σύμφωνα με αυτό το μοντέλο, ένα σύστημα ονομάζεται *ασφαλές* (secure) αν δεν υπάρχει παράνομη πληροφοριακή ροή. Το πλεονέκτημα του μοντέλου είναι ότι καλύπτει όλα τα είδη πληροφοριακών ροών. Το μειονέκτημά του είναι ότι με αυτό γίνεται πιο δύσκολος ο σχεδιασμός ασφαλών συστημάτων.

3.3.9. Μοντέλα 'Αποτροπής – Παρεμβολών'

Τα μοντέλα Αποτροπής – Παρεμβολών (Non - Interference) αποτελούν παραλλαγή των μοντέλων ροής πληροφοριών. Παρέχουν έναν διαφορετικό φορμαλισμό για την περιγραφή του τι γνωρίζει ένα υποκείμενο για την κατάσταση του συστήματος. Ένα υποκείμενο s_1 δεν παρεμβάλλεται με ένα υποκείμενο s_2 αν οι ενέργειες του s_1 δεν έχουν κάποια επίδραση στην άποψη του s_2 για το σύστημα.

3.4. Πολιτικές Ασφάλειας Υψηλού Επιπέδου

Οι πολιτικές ασφάλειας υψηλού επιπέδου (high level security policies - HLSP) είναι διαχωριστικές οδηγίες που υποδεικνύουν πως πρέπει να λειτουργεί ένας οργανισμός. Πρόκειται για εντολές υψηλού επιπέδου που αποσκοπούν στην παροχή καθοδήγησης στο τμήμα του προσωπικού που πρέπει να παίρνει τωρινές και μελλοντικές διαχειριστικές αποφάσεις. Μερικές φορές οι πολιτικές ασφάλειας υψηλού επιπέδου θεωρούνται ως το ισοδύναμο των γενικευμένων απαιτήσεων.

Οι πολιτικές ασφάλειας υψηλού επιπέδου είναι τα πρωταρχικά δομικά στοιχεία για κάθε προσπάθεια εφαρμογής ασφάλειας πληροφοριών. Προκειμένου να είναι αποτελεσματικός, ένας τεχνικός ασφάλειας πληροφοριών (που μπορεί να είναι είτε ένας επαγγελματίας πληροφορικής είτε ένας διαχειριστής) πρέπει να ακολουθεί μια πολιτική που να παρέχει υποστήριξη και προς την διεύθυνση και προς τη διαχείριση. Οι πολιτικές ασφάλειας υψηλού επιπέδου περιλαμβάνουν γενικές εντολές για σκοπούς, αντικείμενα, σχέδια, υπευθυνότητες, ήθη και γενικές διαδικασίες.

Οι πολιτικές ασφάλειας υψηλού επιπέδου χρησιμοποιούνται ως αναφορά για μια ευρεία ποικιλία ενεργειών ασφάλειας και απόρρητου πληροφοριών οι οποίες περιλαμβάνουν:

- τον προσδιορισμό των δικαιωμάτων ελέγχου προσπέλασης,
- την εκτέλεση αναλύσεων κινδύνων (risk analyses),
- την καθοδήγηση ερευνών για κινδύνους ασφάλειας, κ.α.

Η πολιτική ασφάλειας υψηλού επιπέδου είναι υποχρεωτική για όλα τα μέλη του προσωπικού ενός οργανισμού. Παρόλα αυτά πρέπει να επανεξετάζεται

περιοδικά από την διαχείριση του οργανισμού για να εντοπίζονται τα σημεία αναθεώρησής της.
Μια πολιτική ασφάλειας υψηλού επιπέδου αναφέρεται πρωταρχικά σε δυο βασικούς συντελεστές:

- τα δρώντα υποκείμενα (acting subjects), για παράδειγμα ασθενείς, γιατροί παθολόγοι, ειδικοί ιατρικής πληροφορικής, διαχειριστές, νοσοκομειακές αρχές, ασφαλιστικές εταιρείες, κ.λ.π.
- τα αντικείμενα δεδομένα που πρέπει να προστατευθούν, για παράδειγμα ιατρικές εγγραφές, δεδομένα επικοινωνίας, κ.λ.π.

σύμφωνα με την εννοιολογική προσέγγιση (conceptual approach) για πολιτικές ασφάλειας υψηλού επιπέδου, η ασφάλεια και η μυστικότητα πληροφοριακών συστημάτων μπορεί εννοιολογικά να θεωρηθεί στα εξής τέσσερα ξεχωριστά επίπεδα:

- *Γενικές αρχές (generic principles)*: Οι γενικές αρχές κυβερνούν την ασφάλεια και μυστικότητα των δεδομένων και των πληροφοριακών συστημάτων που επεξεργάζονται αυτά τα δεδομένα. Αυτές οι γενικές αρχές είναι κοινωνικά και πολιτιστικά εξαρτημένες.
- *Αρχές (principles)*: Οι αρχές προκύπτουν όταν οι γενικές αρχές εξετάζονται στα πλαίσια ενός συγκεκριμένου διαχειριστικού περιβάλλοντος.
- *Οδηγίες (guidelines)*: Οι οδηγίες είναι συγκεκριμένα λειτουργικά βήματα που θα πρέπει να ακολουθούνται από τα μέλη του προσωπικού με σκοπό την ικανοποίηση μιας συγκεκριμένης αρχής. Οι οδηγίες προκύπτουν όταν οι αρχές εξετάζονται στα πλαίσια ενός συγκεκριμένου τεχνολογικού περιβάλλοντος.
- *Κανόνες (measures)*: Οι κανόνες προκύπτουν όταν οι οδηγίες εξετάζονται μέσα σε ένα συγκεκριμένο περιβάλλον εγκατάστασης.

Μια πολιτική ασφάλειας υψηλού επιπέδου αφορά τα δυο μεσαία επίπεδα και επομένως αποτελείται από ένα σύνολο αρχών, κάθε μια από τις οποίες αναλύεται σε ένα σύνολο οδηγιών. Η πολιτική ασφάλειας υψηλού επιπέδου ορίζει με αυτόν τον τρόπο την γενική προσέγγιση που ένας οργανισμός θα πρέπει να έχει προς την κατεύθυνση της υλοποίησης ασφάλειας. Με άλλα λόγια, καθορίζει τι θα πρέπει να γίνει προκειμένου να έχουμε αποτελεσματική υλοποίηση ασφάλειας, χωρίς να παρέχει τεχνικές λεπτομέρειες για το πώς θα γίνει αυτό. Αυτές οι λεπτομέρειες μπορούν να βρεθούν στις επιμέρους πολιτικές ασφάλειας που θα αναπτυχθούν. Επιπλέον, η πολιτική ασφάλειας υψηλού επιπέδου παρέχει σε αυτή τη φάση ένα σύνολο υποχρεωτικών συνθηκών (mandatory conditions) για να διασφαλίζεται μια ικανοποιητική ασφάλεια των πληροφοριών που επεξεργάζονται από το πληροφοριακό σύστημα.

Τέλος, ένας από τους πλέον υπεύθυνους στόχους σε έναν οργανισμό είναι η λειτουργική ποιότητα και φήμη και κατ' επέκταση η εμπιστοσύνη και η αποδοχή των χρηστών. Αυτοί οι στόχοι μπορούν να επιτευχθούν εφόσον η πολιτική ασφάλειας του πληροφοριακού συστήματος αντικατοπτρίζει τις προσωπικές απαιτήσεις ασφάλειας όλων των ατόμων που επηρεάζονται. Ως εκ τούτου η πολιτική ασφάλειας που θα ορισθεί δεν μπορεί να είναι ανεξάρτητη από το τεχνικό σύστημα που χρησιμοποιείται, αφού είναι φανερό ότι δεν εμπιστεύονται όλα τα επηρεαζόμενα άτομα το τεχνικό σύστημα με τον ίδιο τρόπο και στο ίδιο μέτρο. Ακόμη κι αν το εμπιστεύονται το ίδιο, η εμπιστοσύνη τους αφορά διαφορετικά και επιτηρούμενα συστατικά (υλικό ή λογισμικό) ενός μεγάλου διαδικτυωμένου και κατανεμημένου πληροφοριακού συστήματος. Έτσι, η πολιτική ασφάλειας πρέπει να υιοθετηθεί μια κατά το δυνατόν αποκεντρωμένη άποψη για το ποια υποκείμενα (subjects) ή ομάδες τους (groups) πρέπει να έχουν δικαίωμα προσπέλασης στα αντικείμενα (objects) του πληροφοριακού συστήματος.

4. Προστασία Πληροφοριακών Συστημάτων

4.1. Αναγκαιότητα Προστασίας των Πληροφοριακών Συστημάτων

Τα πληροφοριακά συστήματα σχετίζονται άμεσα με τρία βασικά στοιχεία τα οποία απαιτούν ξεχωριστό τρόπο αντιμετώπισης:

1. Σχετίζονται διπλά με τον άνθρωπο αφού δημιουργούνται από αυτόν και λειτουργούν με τη βοήθειά του έτσι ώστε να υπηρετήσουν πάλι αυτόν. Ο άνθρωπος όμως είναι ένα σύστημα του οποίου η συμπεριφορά δύσκολα μπορεί να προβλεφθεί.

2. Σχετίζονται με την πληροφορία, ένα αγαθό με πάρα πολύ μεγάλη ζήτηση και αξία. Η πληροφορία όμως έχει μια σημαντική διαφορά έναντι των άλλων σημαντικών αγαθών (π.χ. της ύλης και της ενέργειας). Ενώ τα τελευταία μπορούν να αποτελούν αντικείμενο αποκλειστικών δικαιωμάτων υπέρ κάποιου δικαιούχου, η πληροφορία για να είναι χρήσιμη θα πρέπει να διαδίδεται και να κυκλοφορεί όσο το δυνατόν ευρύτερα. Παράλληλα όμως, υπάρχει και το θέμα της προστασίας των ευαίσθητων πληροφοριών, καθώς και το δικαίωμα του πολίτη να αποφασίζει μόνος του σχετικά με την αποκάλυψη και τη χρήση των προσωπικών του στοιχείων.

3. Στηρίζονται στην πληροφορική, μία τεχνολογία που χαρακτηρίζεται από το μεγάλο ρυθμό εξέλιξής της. Επιπλέον, με την πληροφορική οι διαδικασίες επεξεργασίας πληροφοριών παρουσιάζουν μεγάλα περιθώρια προστιθέμενης αξίας. Τέλος, το όλο πληροφοριακό σύστημα έχει ένα κύκλο ζωής μόλις 3-5 ετών, είναι ζωτικής σημασίας για μια επιχείρηση και αποτελεί σημαντική οικονομική επένδυση.

Από τα παραπάνω γίνεται φανερό ότι τα πληροφοριακά συστήματα θα πρέπει να προστατεύονται από τις κάθε μορφής απειλές, χωρίς όμως η προστασία αυτή να παρεμποδίζει υπέρμετρα τη ροή των πληροφοριών.

4.2. Μοντέλα Ασφάλειας Πληροφοριακών Συστημάτων

Κατά καιρούς έχουν προταθεί διάφορα μοντέλα ασφάλειας ενός πληροφοριακού συστήματος. Τα μοντέλα αυτά χρησιμοποιούνται στη συνέχεια ως βάση για τη δημιουργία των μηχανισμών και των μέτρων προστασίας. Παρακάτω θα δούμε τα πιο γνωστά από τα μοντέλα αυτά.

4.2.1. Μοντέλο του Κιβωτισμού

Είναι ίσως το περισσότερο διαδεδομένο μοντέλο ασφάλειας. Σύμφωνα με το μοντέλο, μια σειρά από ομόκεντρους κύκλους (ή ορθογώνια) εμφανίζονται να προστατεύουν τα δεδομένα, τα οποία θεωρούνται ως ο πυρήνας του πληροφοριακού συστήματος. Το μοντέλο αυτό είναι επίσης γνωστό σαν ¨onion skin model¨ και λόγω της εμφωλευμένης μορφής προστασίας που παρέχει, έχει οδηγήσει πολλούς στο να ισχυρισθούν ότι τέλεια προστασία του συστήματος μπορεί να επιτευχθεί μετά από καλή εφαρμογή των μέτρων και των μηχανισμών που αντιστοιχούν σε ένα μόνο κύκλο (ή ορθογώνιο). Οι κύκλοι αντιστοιχούν συνήθως, εξεταζόμενοι από μέσα προς τα έξω, με:

- ✓ τα δεδομένα,
- ✓ τον ηλεκτρονικό υπολογιστή,
- ✓ το υπολογιστικό κέντρο,
- ✓ την επιχείρηση,
- ✓ το υπάρχον νομικό πλαίσιο και
- ✓ το κοινωνικό πλαίσιο

Το μοντέλο αρχικά προτάθηκε από τον James Martin, στη συνέχεια όμως υιοθετήθηκε και χρησιμοποιήθηκε με παραλλαγές και από άλλους συγγραφείς. Τα μοντέλα που οι τελευταίοι έχουν προτείνει διαφέρουν κυρίως στον αριθμό των ομόκεντρων κύκλων (ορθογωνίων), στα ονόματα που φέρουν οι κύκλοι αυτοί, στο περιεχόμενο κάθε κύκλου και στη σειρά που οι κύκλοι έχουν γύρω από τον πυρήνα.

Η σειρά των κύκλων (ορθογωνίων) και το περιεχόμενό τους παίζει σημαντικό ρόλο στο μοντέλο του κιβωτισμού, αφού στην πράξη εισάγει την έννοια της δομής. Σύμφωνα με τη δομή αυτή οι δραστηριότητες, τα μέτρα και οι μηχανισμοί προφύλαξης εντάσσονται μέσα στο εσωτερικό κάποιου κύκλου, όπως ένα κιβώτιο μέσα σε κάποιο άλλο. Η διάταξη των κύκλων εξαρτάται από την οπτική γωνία εξέτασης και τα σημεία στα οποία δίνει έμφαση ο σχεδιαστής των μηχανισμών ασφάλειας.

4.2.2. Μοντέλο του Καταλόγου

Μια άλλη κατηγορία μοντέλων είναι αυτά που στηρίζονται σε κάποιο κατάλογο (checklist) από παράγοντες ή θέματα που θεωρούνται σημαντικά, χωρίς εδώ να παίζει ρόλο η διάταξη ή η σχέση μεταξύ των παραγόντων. Υπάρχουν δυο προσεγγίσεις (παραλλαγές) του μοντέλου αυτού, ανάλογα με τα θέματα που περιλαμβάνουν οι κατάλογοι, ως εξής:

1) Κατάλογοι που στηρίζονται στις ενέργειες που πρέπει να γίνουν (action based checklist) ώστε το σύστημα να θεωρείται ασφαλές, και

2) Κατάλογοι που στηρίζονται σε ανάλυση των απειλών (threat based checklist) και των σημείων ελέγχου.

4.2.3. Μοντέλο του Πίνακα

Το πλεονέκτημα που έχει το μοντέλο του πίνακα (matrix) είναι ότι επιτρέπει την απεικόνιση διαφορετικών θεμάτων ταυτόχρονα. Για παράδειγμα, το μοντέλο που χρησιμοποίησε ο John Mc Cumber στηρίζεται σε ένα πίνακα τριών διαστάσεων:

1) Στην πρώτη διάσταση αντιπροσωπεύονται τα κρίσιμα πληροφοριακά χαρακτηριστικά (critical information characteristics) για να θεωρείται ένα σύστημα ασφαλές, δηλαδή:
   - η εμπιστευτικότητα,
   - η ακεραιότητα, και
   - η διαθεσιμότητα.

2) Στην δεύτερη διάσταση απεικονίζονται οι τρεις καταστάσεις (information states) στις οποίες βρίσκεται η πληροφορία μέσα στο σύστημα, δηλαδή:
   - η μεταβίβαση (transmission),
   - η αποθήκευση (storage), και
   - η επεξεργασία (processing).

3) Η τρίτη διάσταση σχετίζεται με τα μέτρα προφύλαξης (security measures). Τα μέτρα αυτά ταξινομούνται σε τρεις μεγάλες κατηγορίες, οι οποίες και απεικονίζονται πάνω στη διάσταση αυτή. Οι κατηγορίες είναι:
   - η τεχνολογία,
   - η πολιτική (τρόποι πρακτικής), και
   - η εκπαίδευση (εξάσκηση, ενημερότητα) του προσωπικού.

4.2.4. Μοντέλο του Φίλτρου

Από έναν συνδυασμό των μοντέλων καταλόγου και πίνακα προκύπτει το μοντέλο του φίλτρου (filter model). Έχει προταθεί από τον A. Smith και συνοψίζει στη μορφή ενός πίνακα τα αποτελέσματα που έχουν οι διάφορες ενέργειες προφύλαξης για την παροχή προστασίας από κάθε είδους απειλές.

Το μοντέλο ξεκινάει με την ταξινόμηση της ανάλυσης των ενεργειών σε κατηγορίες (π.χ. λειτουργικό περιβάλλον, έλεγχοι πρόσβασης, προσωπικό, κ.λ.π.) και ακολουθεί με μια όμοια ταξινόμηση των απειλών (όπως βανδαλισμοί, κλοπή, απάτη, απειλές από το φυσικό περιβάλλον, κ.α.). Τέλος, σε έναν πίνακα δυο διαστάσεων απεικονίζονται οι σχέσεις μεταξύ της ομάδας

των ενεργειών (πρώτη διάσταση) και της ομάδας των απειλών (δεύτερη διάσταση).

Κάθε στοιχείο του πίνακα έχει μια από τις τιμές μηδέν, υψηλό, χαμηλό, που δείχνουν κατά πόσο συγκεκριμένες ενέργειες θα έχουν αποτέλεσμα σε συγκεκριμένη κατηγορία απειλών. Για παράδειγμα, οι έλεγχοι πρόσβασης παρέχουν μηδενική προστασία για απειλές από το φυσικό περιβάλλον, όπως φωτιά, πλημμύρα, διακοπή ρεύματος, κ.λ.π., αλλά υψηλή προστασία από απάτη, κλοπή, ή βανδαλισμό.

4.2.5. Μοντέλο των Επάλληλων Στρωμάτων

Τα τελευταία χρόνια υπήρξαν προσπάθειες σύμφωνα με τις οποίες τα θέματα της ασφάλειας μπορούν να αντιμετωπισθούν σε διαφορετικά, επάλληλα επίπεδα ή στρώματα, κατά το πρότυπο στρωματοποίησης OSI που χρησιμοποιείται για την επικοινωνία των ανοικτών συστημάτων. Κάθε ένα από τα επίπεδα αυτά ορίζεται να έχει συγκεκριμένους στόχους και οριοθετείται από συγκεκριμένους περιορισμούς.

Στην προσέγγιση που ακολουθεί ο Stewart Kowalski στο Security by Consensus μοντέλο του, υπάρχουν τρία μέρη:

a) Μία διαστρωμάτωση από πέντε επίπεδα (layers).
b) Μία συλλογή από κοινωνικούς και τεχνικούς μηχανισμούς.
c) Μία τεχνική ονοματοδοσίας (labeling technique).

Τα πέντε επάλληλα επίπεδα είναι:

1. Το κοινωνικό – ηθικό (ethical - cultural), που σχετίζεται με κώδικες ηθικής, δεοντολογίας και κοινωνικής πρακτικής.
2. Το νομικό (legal), το οποίο περιλαμβάνει το νομοθετικό πλαίσιο που διέπει την ασφάλεια του πληροφοριακού συστήματος.
3. Το επίπεδο διαχείρισης (administrative - managerial) το οποίο περιλαμβάνει τις απαιτήσεις για τις διαδικασίες (procedures) ασφάλειας και προστασίας. Στο επίπεδο αυτό αντιστοιχούν τα διάφορα Green Books, Yellow Books, Orange Books κ.λ.π., που έχουν εκδοθεί στις διάφορες χώρες.
4. Το λειτουργικό επίπεδο (operational layer) το οποίο περιέχει συγκεκριμένες οδηγίες πρακτικής εφαρμογής των μέτρων (cook book approach).
5. Το τεχνικό (technical) επίπεδο. Είναι το χαμηλότερο επίπεδο και περιλαμβάνει τα τεχνικά θέματα που σχετίζονται με την αποθήκευση, επεξεργασία και επικοινωνία. Τα 7 επίπεδα (layers) του μοντέλου OSI περιέχονται σε αυτό το επίπεδο.

Οι κοινωνικοτεχνικοί μηχανισμοί ελέγχου είναι μία αλυσίδα από ελέγχους η οποία διαδοχικά συνδέει όλα τα επίπεδα. Σε κάθε επίπεδο ορίζεται η συντακτική δομή (syntax) και η σημασιολογία του (semantics). Στη συνέχεια η σημασιολογία του ενός επιπέδου γίνεται προσπάθεια να συνδεθεί με τη συντακτική δομή του επομένου επιπέδου. Έτσι, για παράδειγμα, οι κώδικες ηθικής δεοντολογίας μπορούν να χρησιμοποιηθούν για να ερμηνευθεί το γράμμα του νόμου (στο νομικό επίπεδο). Όμοια, κάποιες συγκεκριμένες απαιτήσεις στις διαδικασίες ασφάλειας του επιπέδου διαχείρισης, έχουν νόημα εξαιτίας της ερμηνείας που δίνουμε σε ένα νόμο.

Τέλος, ο Stewart Kowalski κάνει μια προσπάθεια να τυποποιήσει τα ονόματα που παίρνουν τα χαρακτηριστικά, σε σχέση με την ασφάλεια κάθε στοιχείου του πληροφοριακού συστήματος. Έτσι, για παράδειγμα, για τα δεδομένα έχουμε τα γνωστά χαρακτηριστικά εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Σε κάθε ένα από τα χαρακτηριστικά αυτά θα αντιστοιχούν στοιχεία από τα πέντε στρώματα (π.χ. κώδικες ηθικής δεοντολογίας, άρθρα νόμων, συγκεκριμένες απαιτήσεις για διαδικασίες κ.λ.π.).

4.2.6. Αξιολόγηση των μοντέλων

Το μοντέλο του κιβωτισμού έχει το πλεονέκτημα ότι στα διάφορα περιβλήματα μπορούμε να δώσουμε διάφορα ονόματα (φυσική ασφάλεια, λογική ασφάλεια, κ.λ.π.), οπότε έχουμε ένα μοντέλο με ευρεία εφαρμογή. Όμως έχει δύο σημαντικά μειονεκτήματα:

1. Πιστή τήρηση των μέτρων προφύλαξης σε ένα επίπεδο δίνει την εντύπωση ότι μπορεί να δώσει απόλυτη ασφάλεια σε ολόκληρο το σύστημα.
2. Είναι ένα στατικό μοντέλο, αφού δεν προβλέπει κάτι, ούτε στηρίζεται στις υπάρχουσες σχέσεις αλληλεξάρτησης μεταξύ των στοιχείων του συστήματος.

Τόσο το μοντέλο του καταλόγου όσο και αυτό του πίνακα δίνουν έμφαση στις πρακτικές πλευρές εφαρμογής των μέτρων ασφάλειας, χωρίς να φωτίζουν την σχέση των μέτρων και των συνθηκών απειλής. Το μειονέκτημα αυτό φαίνεται να αμβλύνεται στο μοντέλου του φίλτρου. Όμως, και τα τρία αυτά μοντέλα εξακολουθούν να εξετάζουν το σύστημα στατικά.

Το μοντέλο των επάλληλων στρωμάτων δέχεται ότι η ασφάλεια είναι πολυπαραγοντική και με αλληλεπιδράσεις και αντιμετωπίζει το θέμα με μία συστηματική διαδικασία, δηλαδή με καλά διατεταγμένα και ακριβώς ορισμένα βήματα μετάβασης από επίπεδο σε επίπεδο. Όμως είναι γνωστό ότι η συστηματική προσέγγιση, ειδικά στην ανάπτυξη πληροφοριακών συστημάτων δεν δίνει πάντα ικανοποιητικά αποτελέσματα. Η προσέγγιση αυτή θα πρέπει να συμπληρωθεί ώστε να αμβλυνθούν τα μειονεκτήματα που παρουσιάζει.

5. Τεχνικές Ασφάλειας Πληροφοριακών Συστημάτων

5.1. Κατηγορίες Μεθόδων και Τεχνικών Προστασίας

Οι μέθοδοι και τεχνικές προστασίας ασφάλειας των πληροφοριακών συστημάτων μπορούν να διακριθούν σε δυο βασικές κατηγορίες, ανάλογα με τις περιπτώσεις εφαρμογής τους:

1. σε περίπτωση έκτακτης ανάγκης,
2. κατά τις καθημερινές διεργασίες.

5.1.1. Σε περίπτωση έκτακτης ανάγκης

Με τον όρο *«έκτακτη ανάγκη»* εννοείται μια τέτοιας έκτασης καταστροφή στο σύστημα πληροφορικής που ουσιαστικά είναι αδύνατη η άμεση (ή έστω εντός λίγων ωρών, ή και μίας ή δύο ημερών) επαναλειτουργία του. Οι βασικές περιπτώσεις καταστάσεων έκτακτης ανάγκης είναι:

- περιπτώσεις δυσλειτουργίας,
- περιπτώσεις ολικής καταστροφής.

5.1.1.1. Περιπτώσεις δυσλειτουργίας

Οι πιο συνηθισμένες *περιπτώσεις δυσλειτουργίας* ενός συστήματος πληροφορικής οφείλονται σε:

- φυσικά αίτια, όπως οι διακοπές ηλεκτρικής ενέργειας, προσωρινές βλάβες από πυρκαγιά, πλημμύρα κ.λ.π.,
- απώλειες γραμμών επικοινωνίας,
- βλάβη από <<πτώση>> μέρους του εξοπλισμού ή και του κεντρικού Η/Υ, κ.λ.π.

Αυτές οι περιπτώσεις θα πρέπει να αντιμετωπίζονται με άμεση μετάπτωση στο εφεδρικό σύστημα (backup) που θα πρέπει να υπάρχει. Σε αντίθετη περίπτωση προκαλείται αναπόφευκτα κάποια καθυστέρηση στην ανάκτηση της κανονικής λειτουργίας του ΠΣ, μέχρι να γίνει η απαραίτητη αποκατάσταση των βλαβών και η επαναφορά της πλήρους λειτουργίας του εξοπλισμού. Περιπτώσεις μέτρων προληπτικής ασφάλειας εξετάζονται στη συνέχεια.

5.1.1.2. Περιπτώσεις ολικής καταστροφής

Στην περίπτωση *ολικής καταστροφής* είναι απαραίτητη η ύπαρξη τόσο μίας *Εφεδρικής Εγκατάστασης* (Disaster Recovery Facility), όσο και ενός λεπτομερειακού *Σχεδίου Αποκατάστασης Λειτουργίας* του οργανισμού (Contingency Action Plan). Η εφεδρική εγκατάσταση μπορεί να βρίσκεται σε άλλο χώρο ή κάποιο γραφείο εξυπηρέτησης ή παροχής υπηρεσιών πληροφορικής (Service Bureau), σε μια κινητή μονάδα παροχής υπολογιστικών υπηρεσιών Η/Υ ή και σε άλλη πόλη.

Το λεπτομερές *Σχέδιο Έκτακτης Ανάγκης* θα πρέπει απαραίτητα να συντάσσεται και να ελέγχεται σε πραγματικές συνθήκες, να δοκιμάζεται σε τακτά χρονικά διαστήματα και να αναθεωρείται όποτε αυτό είναι απαραίτητο, για παράδειγμα όταν συμβαίνουν σημαντικές αλλαγές σε λειτουργικά συστήματα κ.λ.π.

5.1.2. Κατά τις καθημερινές διεργασίες

Η μέριμνα της διοίκησης και οι προβλέψεις της πολιτικής ασφάλειας πρέπει ακόμα να επικεντρώνονται με το ίδιο, αν όχι και με μεγαλύτερο, βάρος και στην ασφάλεια κατά τη διάρκεια της καθημερινής λειτουργίας των πληροφοριακών συστημάτων.

Η συγκεκριμένη πολιτική ασφάλειας του οργανισμού θα πρέπει κατ' αρχήν να καλύπτει τα κτίρια, τις εγκαταστάσεις, τον μηχανογραφικό εξοπλισμό και το λογισμικό. Θα πρέπει παράλληλα να μεριμνά για θέματα όπως:

- ποιοι και πως αναπτύσσουν, συντηρούν τα διάφορα πληροφοριακά συστήματα
- ποιοι χρήστες έχουν πρόσβαση σε ποιες πληροφορίες και κάτω από ποιες προϋποθέσεις
- ποιοι έχουν πρόσβαση σε ευαίσθητους χώρους (π.χ. Κέντρο Η/Υ)
- πως διακινούνται οι εμπιστευτικές πληροφορίες εκτός δικτύων (π.χ. εκτυπώσεις, δισκέτες, ταινίες)
- πως και πόσες γενιές αντιγράφων φυλάσσονται, από ποια δεδομένα και πού, κ.λ.π.

Η συστηματική καταγραφή και παρακολούθηση όλων αυτών, αποτελεί μία βασικότατη, επίπονη και αρκετά εξειδικευμένη λειτουργία ελεγκτικού και εμπιστευτικού χαρακτήρα. Η εποπτεία και ο έλεγχος της τήρησης των προδιαγραφών, η τακτική επιθεώρηση ή αναθεώρηση τους, και η λήψη κάποιων νέων μέτρων, πρέπει να είναι μια συνεχής και μόνιμη απασχόληση των υπεύθυνων ασφαλείας που πρέπει να αποτελούν ξεχωριστή υπηρεσία στο Κέντρο Πληροφορικής με απευθείας αναφορά στην διοίκηση του οργανισμού.

Σε γενικές γραμμές οι καθημερινές εργασίες προστασίας του ΠΣ θα μπορούσαν να διακριθούν στις εξής βασικές κατηγορίες:

1. Φυσική Προστασία του Πληροφοριακού Συστήματος,
2. Λογική Προστασία του Πληροφοριακού Συστήματος,

Για κάθε κατηγορία επιβάλλεται η λήψη μέτρων προφύλαξης από φυσικά αίτια ή τυχαίες ενέργειες, καθώς και από σκόπιμες ενέργειες, όπως για παράδειγμα η βιομηχανική κατασκοπία, τα σαμποτάζ, κ.α. Στη συνέχεια παρουσιάζονται συνοπτικά, για κάθε προαναφερόμενη ενότητα οι συνιστώσες που πρέπει να προστατευθούν, οι κίνδυνοι και τα μέτρα που πρέπει να ληφθούν σε όλη την υλικοτεχνική υποδομή και τη χρήση ενός Πληροφοριακού Συστήματος με σκοπό την αποφυγή των αρνητικών συνεπειών.

5.1.2.1. Φυσική Προστασία

Περιλαμβάνει τα παρακάτω βασικά θέματα προστασίας:

- Προστασία των χώρων του Κέντρου Πληροφορικής και ιδιαίτερα του computer room (π.χ. ελεγχόμενη πρόσβαση).
- Προστασία του υλικού (hardware) από οποιαδήποτε απειλή, βλάβη ή ανθρώπινη απροσεξία.
- Προστασία των εφεδρικών αντιγράφων (backup) του λογισμικού συστήματος των προγραμμάτων εφαρμογών (βιβλιοθηκών, πακέτων) και των δεδομένων του οργανισμού.
- Εγκατάσταση συστημάτων προστασίας, όπως για παράδειγμα συστήματος αδιάλειπτης λειτουργίας (U.P.S), συστήματος πυρόσβεσης με αδρανές αέριο, κ.α.

Παραδείγματα πιθανών κινδύνων (security threats):

I. Βλάβη ή καταστροφή υλικού (hardware).
II. Απώλεια δεδομένων.
III. Αλλαγή δηλωμένων χαρακτηριστικών των περιφερειακών συσκευών.
IV. Λανθασμένα αποτελέσματα.
V. Λανθασμένες εκτυπώσεις.

Παραδείγματα βασικών μέτρων προστασίας (counter - measures):

I. Έλεγχος και απαγόρευση της μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητους χώρους, όπως τα computer room, τα τερματικά, οι βιβλιοθήκες ταινιών και δίσκων, κ.λ.π.

II. Δημιουργία πινάκων εξουσιοδότησης που απεικονίζουν το δικαίωμα πρόσβασης του κάθε χρήστη (κατηγορίας χρηστών) στους διάφορους πόρους του συστήματος (δίσκους, ταινίες, αρχεία ή πίνακες βάσεων δεδομένων, κ.λ.π.).
III. Στατιστική παρακολούθηση των παραβιάσεων της ασφάλειας του πληροφοριακού συστήματος.
IV. Προσεκτική επιλογή και σωστή διοικητική εποπτεία των εργαζομένων στο Κέντρο Πληροφορικής
V. Δημιουργία χώρων εργασίας που ικανοποιούν τις βασικές προϋποθέσεις ασφάλειας (προστασία από πιθανές φυσικές καταστροφές, συνθήκες κατάλληλου φωτισμού και κλιματισμού κ.λ.π.).
VI. Τήρηση ασφαλών δομικών προδιαγραφών με συστήματα πυρόσβεσης, πυρασφαλή δωμάτια ή χώρους φύλαξης αρχείων κ.λ.π.

5.1.2.2. Λογική Προστασία

Στην λογική προστασία περιλαμβάνονται:

1. η προφύλαξη (προστασία) του λογισμικού, και
2. η προφύλαξη των δεδομένων

5.1.2.2.1. Προφύλαξη του λογισμικού

Προστασία των Λειτουργικών Προγραμμάτων

Περιλαμβάνει τα παρακάτω βασικά θέματα προστασίας:

- Προστασία λειτουργίας της μνήμης και της κεντρικής μονάδας επεξεργασίας των υπολογιστών.
- Προστασία των αρχείων και βάσεων δεδομένων του λειτουργικού συστήματος.
- Προστασία των βιβλιοθηκών εγκατάστασης (γλώσσες προγραμματισμού, εκτελέσιμα προγράμματα, υπορουτίνες).
- Έλεγχος προσπέλασης.

Παραδείγματα πιθανών κινδύνων (security threats):

I. Αλλοίωση των παραμέτρων (configuration) του συστήματος
II. Λογική απώλεια δίσκων, βιβλιοθηκών, κ.λ.π.
III. Ενεργοποίηση κρυμμένων λογικών επιλογών
IV. Ετεροπροσωπία (Piggybacking)
V. Χρήση Παρακαμπτηρίων εργαλείων (Superzapping)

VI. Αρπαγή συνθηματικών (password grabbers) των εξουσιοδοτημένων χειριστών του συστήματος (system programmers, system administrators, DBA ‘s, κ.λ.π.).

Παραδείγματα βασικών μέτρων προστασίας (counter - measures):

I. Μηχανισμοί προστασίας μνήμης (π.χ. χρήση τεχνικών τεμαχισμού, σελιδοποίησης, κ.λ.π.)
II. Μηχανισμοί ελέγχου προσπέλασης (δημιουργία πίνακα ελέγχου προσπελάσεων)
III. Μηχανισμοί προστασίας αρχείων (π.χ. μηχανισμός ομαδοποίησης, μηχανισμός προσωρινής εξουσιοδότησης)
IV. Εφεδρικά αντίγραφα συστήματος (backup)
V. Συστήματα Αδιάλειπτου Λειτουργίας (U.P.S)
VI. Προγράμματα ανίχνευσης ιών (antivirus)
VII. Ημερολόγια κινήσεων (logs) όπου καταγράφονται όλες οι μεταβολές οι οποίες έχουν σχέση με την λειτουργία και την ασφάλεια του συστήματος.

Προστασία των Προγραμμάτων Εφαρμογών

Περιλαμβάνει τα παρακάτω θέματα προστασίας:

- Προστασία βιβλιοθηκών προγραμματισμού
- Έλεγχος διαδικασιών παραγωγής λογισμικού
- Έλεγχος προσπέλασης

Παραδείγματα πιθανών κινδύνων (security threats):

I. Δούρειοι Ίπποι (Trojan Horses)
II. <<Καρφωτές>> τροποποιήσεις (αφαίρεση του τροποποιημένου πηγαίου κώδικα μετά τη δημιουργία του εκτελέσιμου προγράμματος)
III. Τεχνική <<σαλαμιού>> στους αριθμητικούς υπολογισμούς σημαντικών εφαρμογών (π.χ. εκτοκισμός καταθέσεων, ποσοστά προμηθειών, κ.λ.π.)
IV. Λογικές βόμβες, δηλαδή κρυμμένες εντολές που ενεργοποιούνται όταν επαληθευτεί κάποια συνθήκη ή ημερομηνία.
V. Παράνομη τροποποίηση μορφοποίησης (format) αρχείων, περιεχόμενων πεδίων, κ.λ.π.
VI. Προσομοίωση και μεταβολή των λογισμικών
VII. Διακοπές προγραμμάτων
VIII. Στρογγυλοποιήσεις ποσών λογαριασμών (rounding down)

Παραδείγματα βασικών μέτρων προστασίας (counter - measures):

I. Κλειδιά (Password)
II. Πίνακες ελέγχου προσπέλασης
III. Έξυπνες κάρτες
IV. Τήρηση ενημερωμένης τεκμηρίωσης
V. Εφαρμογή ειδικών πακέτων λογισμικού ασφάλειας
VI. Μηχανισμοί ελέγχου αλλαγών σε κρίσιμα προγράμματα κατά τη διαδικασία ανάπτυξης και συντήρησης.

5.1.2.2.2. Προφύλαξη των δεδομένων

Περιλαμβάνει τα παρακάτω θέματα προστασίας:

- Προστασία των ¨ευαίσθητων¨ δεδομένων (χρήση κρυπτογραφίας)
- Προστασία των δεδομένων από τυχαίες ή ηθελημένες διαγραφές και αλλοιώσεις
- Προστασία της ροής των δεδομένων (για παράδειγμα με την ταξινόμησή τους σε επίπεδα ευαισθησίας, όπως: κοινό, εμπιστευτικό, μυστικό, απόρρητο)
- Προστασία των βάσεων δεδομένων

Παραδείγματα πιθανών κινδύνων (security threats):

I. Παράνομη αναζήτηση δεδομένων
II. Διαρροή πληροφοριών (data leakage)
III. Τροποποίηση δεδομένων πριν ή μετά την καταχώρηση
IV. Τυχαία καταστροφή δεδομένων
V. Τυχαία ή σκόπιμη βλάβη της βάσης δεδομένων, με αποτέλεσμα παράνομη τροποποίηση και διασύνδεση δεδομένων.

Παραδείγματα βασικών μέτρων προστασίας (counter - measures):

I. Διαδικασία επιβεβαίωσης της ταυτότητας (identification / authentication) και εξουσιοδότησης (authorization) του οποιουδήποτε χρήστη επηρεάζει δεδομένα
II. Χρήση συνθηματικού (password) και ταυτότητας χρήστη (user ID)
III. Υποχρεωτικοί έλεγχοι προσπέλασης (για παράδειγμα, με την ταξινόμηση των δεδομένων σε επίπεδα ευαισθησίας όπως: κοινό, εμπιστευτικό, μυστικό, απόρρητο)
IV. Χρήση κρυπτογραφίας κατά την προσπέλαση των βάσεων δεδομένων και κατά τη μετάδοση δεδομένων

V. Πίνακες εξουσιοδότησης για τις κατηγορίες δεδομένων που ο χρήστης μπορεί να διαβάσει ή να γράψει
VI. Τακτική λήψη εφεδρικών αντιγράφων (backup)
VII. Χρήση πακέτων λογισμικού ασφάλειας (security software packages).

Ένα θέμα το οποίο επίσης συσχετίζεται άμεσα με την προστασία των δεδομένων είναι οι εκτυπωμένες καταστάσεις στις οποίες εμφανίζονται τα δεδομένα του οργανισμού. Θα πρέπει να λαμβάνονται ιδιαίτερα μέτρα για την ασφαλή διακίνηση των εκτυπωμένων καταστάσεων ώστε να φθάνουν έγκαιρα στους εξουσιοδοτημένους υπαλλήλους. Ο μεγάλος αριθμός εκτυπωμένων καταστάσεων αποτελεί συνήθως πραγματικό πρόβλημα για το πληροφοριακό σύστημα (ΠΣ). Θα πρέπει να ακολουθείτε μια κατάλληλη πολιτική έτσι ώστε να ελέγχεται η χρησιμότητα, η συχνότητα εκτύπωσης και ο τρόπος διακίνησης των εκτυπωτικών καταστάσεων. Οι εμπιστευτικής μορφής καταστάσεις θα πρέπει κατά το δυνατό να τυπώνονται σε τοπικούς εκτυπωτές.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Μηχανές Αναζήτησης:
https://www.google.gr/

2. Μελετητής Google:
http://scholar.google.gr/

3.Βικιεπιστήμιο:
https://el.wikiversity.org/wiki/%CE%95%CE%B9%CF%83%CE%B1%CE%B3%CF%89%CE%B3%CE%AE_%CF%83%CF%84%CE%B1_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1

4. Φωλίνας Δ.(2006), «Ολοκληρωμένα πληροφοριακά συστήματα διαχείρισης επιχειρηματικών πόρων», Αθήνα, Εκδόσεις Ανίκουλα.

5. «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Γ. Πάγκαλου, Ι. Μαυρίδη, Εκδόσεις Ανίκουλα.

6. «Ασφάλεια πληροφοριακών συστημάτων», Σωκρ. Κάτσικας, Δημήτρης Γκρίτζαλης, επιμέλεια: Στέφανος Γκρίτζαλης, Εκδόσεις Νέων Τεχνολογιών, 2004.

7. ΕΠΥ – (1999) Ασφάλεια Πληροφοριών, Εκδόσεις Νέων Τεχνολογιών, Αθήνα. Κιουντούζης Β, Ασφάλεια Πληροφοριών, Αθήνα, 1998.

8. Bell D. and LaPadula L., (1973) Secure Computer Systems: Mathematical Foundations, Technical Report 2547, Volume I, MITRE Corporation.

9. Bell D. and LaPadula L., (1976) Secure Comuter Systems: Unified Exposition and Multics Interpretation, Technical Report ESD – TR – 75 – 306, MITRE Corporation.

10. Εθνικό Αρχείο Διδακτορικών Διατριβών:
http://phdtheses.ekt.gr/eadd/handle/10442/19890
Διδακτορική Διατριβή του Ανδρέα Κ. Μάττα, με θέμα: «ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΣΕ ΣΥΝΕΡΓΑΤΙΚΑ ΠΕΡΙΒΑΛΛΟΝΤΑ ΕΦΑΡΜΟΓΩΝ ΜΕ ΒΑΣΗ ΤΟ ΔΙΑΔΙΚΤΥΟ».

11. http://www.icte.uowm.gr/uploads/thesis/dipl_ergasia_am14.pdf
Διπλωματική Εργασία της Λέρα Μαρίας, με θέμα: «ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ».