ΚΕΦΑΛΑΙΟ 8

ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ

ΣΤΟΧΟΙ ΚΕΦΑΛΑΙΟΥ

Στο τέλος αυτού του κεφαλαίου
θα είστε ικανοί:

- *Να κατανοήσετε τι εννοούμε διαχείριση δικτύου και ποιες είναι οι πέντε περιοχές που καλύπτει η διαχείριση δικτύου.*
- *Να γνωρίζετε τα βασικότερα μοντέλα διαχείρισης.*
- *Να κατανοήσετε τη δομή της διαχειρίσιμης πληροφορίας.*
- *Να κατανοείτε τις έννοιες, που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων.*
- *Να κατανοείτε την ορολογία, που χρησιμοποιείται, για τα θέματα ασφάλειας των πληροφοριακών συστημάτων.*
- *Να γνωρίζετε και να κατανοείτε τις πλέον διαδεδομένες μεθόδους παραβίασης ασφάλειας στα πληροφοριακά συστήματα.*

Εισαγωγή

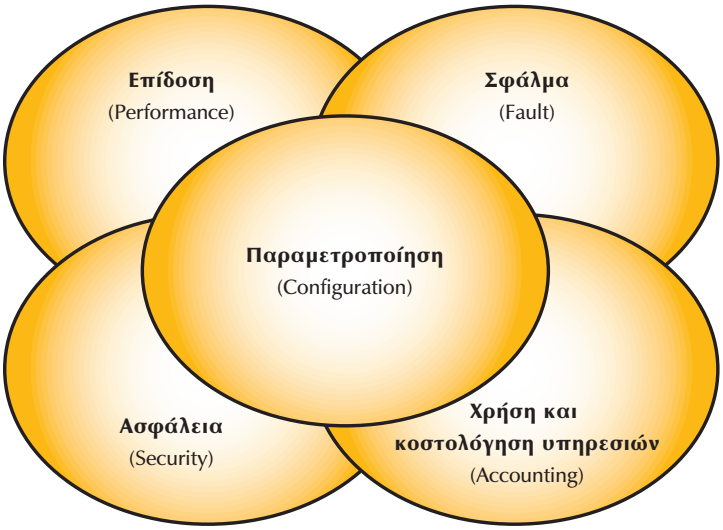
Η ανάγκη σήμερα για διαδικτύωση γίνεται ολοένα και πιο επιτακτική. Όλες σχεδόν οι επιχειρήσεις έχουν προχωρήσει στη εγκατάσταση τοπικών δικτύων. Αρκετές από αυτές έχουν προχωρήσει στη διασύνδεση απομακρυσμένων τοπικών δικτύων με τη βοήθεια γραμμών WAN. Οι δομές των δικτύων έχουν γίνει αρκετά πολύπλοκες. Ακόμα και τα εσωτερικά δίκτυα τείνουν να αποκτήσουν αυξημένη πολυπλοκότητα. Πολλές φορές η ύπαρξη συσκευών από διαφορετικούς κατασκευαστές αυξάνει την πολυπλοκότητα των δικτύων και ταυτόχρονα τη δυσκολία στη διαχείρισή τους.

Η ανάγκη για κεντρική διαχείριση μεγάλου, σύνθετου και πολλές φορές κατανεμημένου δικτύου είναι προφανής. Η ύπαρξη, όμως, ενιαίας και κεντρικής διαχείρισης σύνθετου δικτύου συναντά συχνά εμπόδια από την ύπαρξη συσκευών διαφορετικών κατασκευαστών, καθώς και από τον τρόπο, που ο κάθε κατασκευαστής υλοποιεί τους μηχανισμούς διαχείρισης. Για να ξεπεραστούν τα προβλήματα στον τρόπο διαχείρισης έχουν γίνει και συνεχίζονται να γίνονται προσπάθειες δημιουργίας προτύπων.

Μέρος του έργου διαχείρισης δικτύου αποτελεί και η ασφάλεια του. Η ασφάλειά του δικτύου είναι αρκετά σύνθετο θέμα, περικλείει πολλές παραμέτρους και είναι πολύ σημαντική η δυνατότητα εγκατάστασης μηχανισμών κεντρικής εποπτείας και διαχείρισης αυτών. Γίνονται επίσης προσπάθειες για τη δημιουργία κάποιων προτύπων. Στο κεφάλαιο αυτό θα αναφερθούμε σε θέματα που σχετίζονται με τη διαχείριση και την ασφάλεια δικτύου, δύο παράγοντες πολύ σημαντικοί για την εύρυθμη λειτουργία και αξιοπιστία του.

8.1 Διαχείριση Δικτύου

Ο **Διεθνής Οργανισμός προτυποποίησης (International Organization for Standardization, ISO)** έχει ορίσει το πλαίσιο εργασίας (framework) για το μοντέλο διαχείρισης δικτύων OSI. Με βάση το μοντέλο, έχουν ορισθεί πέντε περιοχές διαχείρισης: η **διαχείριση παραμέτρων του δικτύου (configuration management)**, η **διαχείριση επίδοσης του δικτύου (performance management)**, η **διαχείριση σφαλμάτων (fault management)**, η **διαχείριση του κόστους των υπηρεσιών (accountig management)** και τέλος, η **διαχείριση ασφάλειας (security management).**



Σχήμα 8-1 Μοντέλο OSI για Διαχείριση Δικτύων

Στη συνέχεια, θα αναφερθούμε με περισσότερες λεπτομέρειες στο έργο των πέντε διαφορετικών περιοχών διαχείρισης, που έχει ορίσει το πλαίσιο εργασίας του μοντέλου OSI.

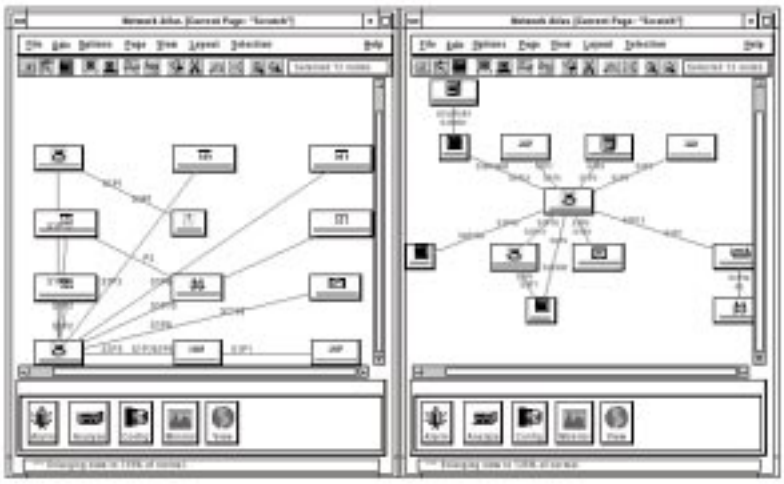
8.1.1 Διαχείριση παραμέτρων (Configuration Management)

Με τον όρο διαχείριση παραμέτρων, εννοούμε τη διαδικασία αλλαγής της τοπολογίας του δικτύου καθώς και τη ρύθμιση των παραμέτρων των συσκευών, που το αποτελούν, είτε σε επίπεδο υλικού είτε σε επίπεδο λογισμικού, προκειμένου να διασφαλίσουμε τη σωστή λειτουργία του δικτύου ανάλογα με τις εκάστοτε απαιτήσεις. Η αρχική εγκατάσταση του δικτύου καθώς και η ρύθμιση των παραμέτρων των συσκευών, που το αποτελούν, δεν συνιστούν με βάση τον επίσημο ορισμό του μοντέλου OSI μέρος της διαχείρισης δικτύου. Παρόλα αυτά, είναι πολύ συνηθισμένο να χρησιμοποιούμε τα ίδια εργαλεία (εφαρμογές, ειδικό λογισμικό) για την αρχική εγκατάσταση δικτύου όσο και για τη μετέπειτα παρακολούθηση και διαχείρισή του. Γι' αυτό συχνά και η αρχική διαμόρφωση δικτύου, θεωρείται από πολλούς μέρος της διαχείρισης του.

Ένα από τα σημαντικότερα έργα είναι και η τεκμηρίωση του δικτύου. Τεκμηρίωση τόσο των συσκευών που το αποτελούν με τις ρυθμίσεις που έχουν (π.χ πρωτόκολλα που χρησιμοποιούν, αριθμό ενεργών θυρών, φίλτρα που υπάρχουν κ.ο.κ.), όσο και της τοπολογίας του δικτύου και του τρόπου λειτουργίας.

Η τεκμηρίωση του δικτύου βοηθείται σημαντικά από την ύπαρξη λογισμικού, που ανακαλύπτει και καταγράφει σε **βάση δεδομένων καταλόγου υλικών (inventory database)** όλες τις συσκευές ενός δικτύου, καθώς και τον τρόπο δια-

σύνδεσή τους. Συνήθως, γίνεται καταγραφή όλων των ενεργών συσκευών που απαρτίζουν ένα δίκτυο όπως δρομολογητές, μεταγωγείς (switches), γέφυρες, επαναλήπτες (hubs), τα είδη των τοπικών δικτύων, όπως τμήματα ethernet, token ring κ.ο.κ, καθώς επίσης και οι τυχόν wan γραμμές, όπως ppp μισθωμένες ή επιλεγόμενες (ISDN), συνδέσεις X.25, Frame Relay κ.ο.κ. Αν το λογισμικό, που διαθέτουμε, χρησιμοποιείται και για διαχείριση συστημάτων, τότε γίνεται ανακάλυψη μέσω του δικτύου και των ηλεκτρονικών υπολογιστών, εκτυπωτών και γενικότερα κάθε συσκευής, που διασυνδέεται στο δίκτυο. Οι εφαρμογές, που διαχειρίζονται το δίκτυο, μπορούν να σχηματίσουν γραφικές απεικονίσεις των συσκευών του δικτύου και την μεταξύ τους συνδεσμολογία.



Σχήμα 8-2 Παράδειγμα Διαγράμματος Δικτύου
(από πρόγραμμα διαχείρισης δικτύου)

8.1.2 Διαχείριση επίδοσης του δικτύου (Performance Management)

Για τη διαχείριση της απόδοσης του δικτύου πρέπει, πρώτα, να ορίσουμε τι θέλουμε να μετράμε, να σχεδιάσουμε, τον τρόπο που θα γίνονται οι μετρήσεις και στη συνέχεια να υλοποιήσουμε τις μετρήσεις μας. Σε ένα δίκτυο είναι λογικό να μετρώνται σε τακτά χρονικά διαστήματα διάφορα χαρακτηριστικά, όπως:

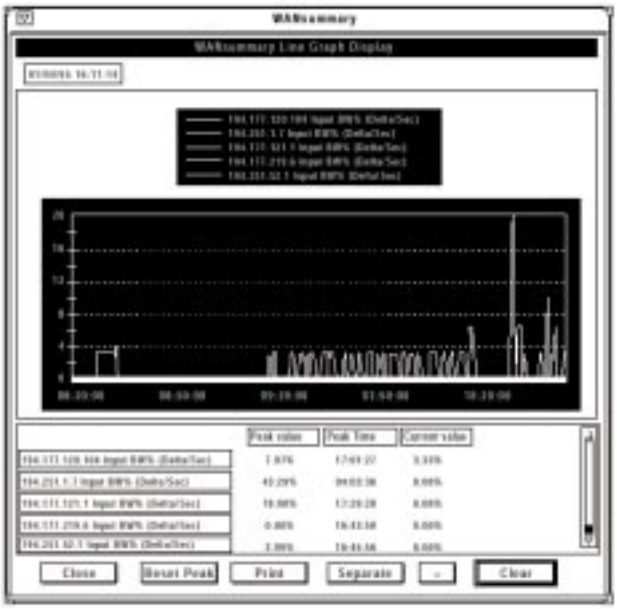
- το ποσοστό χρησιμοποίησης των WAN γραμμών ή των διαφόρων τμημάτων τοπικού δικτύου
- η ανάλυση του ποσοστού κίνησης ανά πρωτόκολλο π.χ. IP, IPX, Netbios κ.ο.κ
- το ποσοστό λαθών σε σχέση με όλη την κίνηση
- ο χρόνος καθυστέρησης διαφόρων σημείων του δικτύου
- ο χρόνος απόκρισης κάποιων συσκευών
- ο καθορισμός κατωφλίων σε μερικές μετρούμενες παραμέτρους. Όταν οι τιμές των παραμέτρων υπερβούν τις τιμές που έχουν ορισθεί ως κατώφλια τότε θα πρέπει να δημιουργούνται κάποιοι συναγερμοί (alarm).

Είναι δυνατόν να αποθηκευτούν οι μετρήσεις επίδοσης για μελλοντική επεξερ-

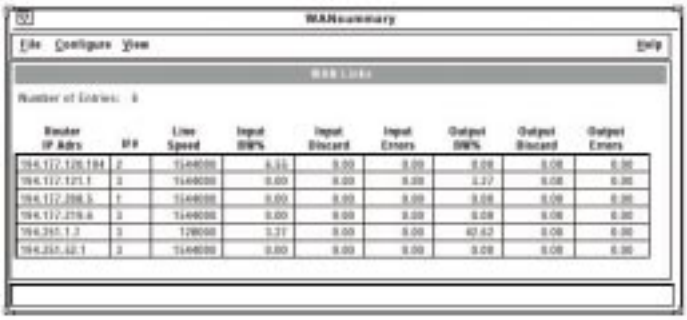
γασία. Οι διαχειριστές του δικτύου θα πρέπει να αναλύουν τις μετρήσεις και να μπορούν να εντοπίσουν σημεία συμφόρησης ή προβληματικής λειτουργίας του δικτύου. Με βάση τα συμπεράσματα από την ανάλυση των μετρήσεων είναι πιθανό να χρειαστεί να πραγματοποιηθεί η ανασχεδίαση μερικών σημείων του δικτύου. Όταν πραγματοποιούνται αλλαγές στο δίκτυο, με βάση τις μετρήσεις που θα ληφθούν, θα πρέπει να ελέγχεται στο κατά πόσο πέτυχαν το σκοπό, για τον οποίο έγιναν.

Συνήθως οι τιμές μπορούν να καταγραφούν σε πίνακες ή /και σε μορφή γραφημάτων.

(α)



(β)



Σχήμα 8-3 Παραδείγματα διαχείρισης απόδοσης δικτύου, με την βοήθεια προγράμματος διαχείρισης δικτύου.
(α) ποσοστό χρησιμοποίησης WAN σύνδεσης σε μορφή γραφήματος
(β) μετρήσεις WAN σύνδεσης σε πίνακα

8.1.3 Διαχείριση σφαλμάτων (Fault Management)

Το έργο της διαχείρισης σφαλμάτων είναι η αναγνώριση ύπαρξης προβλήματος / δυσλειτουργίας, ο εντοπισμός του σημείου, που υπάρχει το πρόβλημα, η επίλυση του προβλήματος ή η τεκμηρίωσή του και η προώθηση της περιγραφής του προβλήματος σε άλλη ομάδα. Συνήθως γίνεται και καταγραφή των προβλημάτων (τύπος λάθους, τοποθεσία, βαθμός κρισιμότητας κ.λ.π.) και τι λύση δόθηκε, για μελλοντική χρήση, όπως για παράδειγμα δημιουργία στατιστικών στοιχείων για κάποιες συσκευές. Μερικά προβλήματα είναι εύκολο να εντοπιστούν, όπως για παράδειγμα η μη λειτουργία συσκευής, η διακοπή σύνδεσης. Ο στόχος, όμως, της διαχείρισης δεν πρέπει να σταματά εκεί, αλλά να μπορεί να προβλέπει τη δημιουργία πιθανόν προβλημάτων πριν αυτά επηρεάσουν τους χρήστες του δικτύου. Το κομμάτι πρόβλεψης πιθανών προβλημάτων σχετίζεται άμεσα με τη διαχείριση επίδοσης του δικτύου.

Σχήμα 8-4 Οθόνη με καταγεγραμμένα alarm δικτύου (από πρόγραμμα διαχείρισης Δικτύου)

Τα προβλήματα έρχονται με τη μορφή συναγερμού (alarm) και συνήθως γίνεται καταγραφή σε αρχεία (logs) ή /και με μορφή αλλαγής της χρωματικής ένδειξης σε κάποιες γραφικές απεικονίσεις του δικτύου. Η λύση των προβλημάτων διαφέρει κάθε φορά και όπως είναι φυσικό εξαρτάται από το πρόβλημα. Μερικές φορές χρειάζεται η αποσύνδεση προβληματικών συσκευών από το δίκτυο, ή αντικατάσταση ελαττωματικού υλικού, ή ρύθμιση παραμέτρων στο λογισμικό των συσκευών.

8.1.4 Διαχείριση κόστους (Accounting Management)

Το έργο της διαχείρισης κόστους ενός δικτύου περιλαμβάνει την παρακολούθηση της χρήσης των πόρων του δικτύου, την ανάλυση των διαθέσιμων επιπέδων των πόρων του δικτύου για συγκεκριμένες ομάδες χρηστών, την αντιστοίχηση του κόστους της χρήσης, την καταγραφή της χρήσης των δικτυακών πόρων

από τις διάφορες ομάδες χρηστών και την εξασφάλιση ότι οι χρήστες δεν κάνουν χρήση υπηρεσιών, που δεν είναι συμφωνημένες.

8.1.5 Διαχείριση ασφάλειας (Security Management)

Η διαχείριση ασφάλειας περικλείει τον έλεγχο πρόσβασης σε συσκευές, δεδομένα και προγράμματα, απέναντι σε κάθε μη εξουσιοδοτημένη χρήση ηθελημένη ή μη, την επίβλεψη για προσπάθειες παραβίασης των κανόνων ασφάλειας και λήψη των απαραίτητων μέτρων προκειμένου να εξασφαλισθεί η ασφάλεια των πόρων του δικτύου. Η εξασφάλιση ασφάλειας σε πόρους του συστήματος αποτελεί πολύπλοκο και δύσκολο θέμα και αναλυτικότερη αναφορά σε μεθόδους επίτευξή της θα γίνει σε επόμενες παραγράφους.

Τα μέτρα ασφάλειας για κατανεμημένο πληροφορικό σύστημα δεν πρέπει σε καμία περίπτωση να είναι αποσπασματικά σε ένα τομέα, αλλά να περιλαμβάνουν όλους τους τομείς που συγκροτούν το πληροφορικό σύστημα. Θα μπορούσαμε να πούμε, ότι ο οργανισμός, που έχει εγκαταστήσει και χρησιμοποιεί πληροφορικό σύστημα, θα πρέπει να δεσμευτεί για την οργάνωση και τήρηση κανόνων ασφάλειας. Τα μέτρα ασφάλειας πρέπει να αφορούν:

- τη φυσική προστασία των πόρων του συστήματος από πρόσβαση μη εξουσιοδοτημένων ατόμων.
- την ασφάλεια των συστημάτων που συνδέονται σε δίκτυο. Το κομμάτι αυτό ανήκει επίσης στη διαχείριση ασφάλειας των συστημάτων (για παράδειγμα μηχανισμοί ασφάλειας σε επίπεδο λειτουργικού συστήματος)
- την ασφάλεια του δικτύου και την προστασία των δεδομένων, που μεταφέρονται με αυτό.

8.2 Πρότυπα διαχείρισης

Όπως έχουμε αναφέρει και στην αρχή του κεφαλαίου, γίνονται προσπάθειες για τη δημιουργία προτύπων, που θα αφορούν τις μεθόδους διαχείρισης των συστημάτων, που συμμετέχουν σε ολοκληρωμένο πληροφορικό σύστημα. Ο οργανισμός ISO περιγράφει με διάφορους κωδικούς έργων το μοντέλο διαχείρισης συστημάτων που ακολουθούν το μοντέλο OSI, γνωστό ως **Πρωτόκολο Πληροφοριών Κοινής Διαχείρισης (Common Management Information Protocol, CMIP)**. Επίσης, γνωστό πρότυπο διαχείρισης συστημάτων, που αναφέρεται κυρίως στην αρχιτεκτονική TCP/IP, είναι το **Απλό Πρωτόκολο Διαχείρισης Δικτύου (Simple Network Management Protocol, SNMP)**.

Υπάρχουν και άλλα μοντέλα διαχείρισης, αλλά τα παραπάνω είναι τα πλέον διαδεδομένα. Πολλοί κατασκευαστές αρχίζουν, πέρα από την ύπαρξη δικών τους μοντέλων, να βγάζουν προϊόντα συμβατά με ένα από τα παραπάνω μοντέλα. Εκτός από τα δύο μοντέλα, που προαναφέραμε, αρκετές εταιρείες είχαν αντιληφθεί την ανάγκη δημιουργίας ολοκληρωμένης διαχείρισης και ανέπτυξαν δικά

τους μοντέλα. Χαρακτηριστικό παράδειγμα είναι η εταιρία IBM, που έχει προτείνει την αρχιτεκτονική ONA. Το NetView ένα από τα πρώτα προϊόντα για διαχείριση δικτύου, που συμβαδίζει με την αρχιτεκτονική ONA. Στη συνέχεια, θα περιγράψουμε την αρχιτεκτονική των μοντέλων διαχείρισης CMIP και SNMP.

8.2.1 Πρότυπο CMIP

Ο διεθνής οργανισμός τυποποίησης ISO έχει δημιουργήσει την αρχιτεκτονική του πλαισίου εργασίας με τον κωδικό ISO 7498–4 για τη διαχείριση του μοντέλου OSI. Με βάση τον κωδικό ISO 10164–1 έως 15, περιγράφονται οι πέντε περιοχές ολοκληρωμένης διαχείρισης τις οποίες παρουσιάσαμε στην παράγραφο 8-1. Τις ξαναθυμίζουμε: η **διαχείριση παραμέτρων δικτύου (configuration management)**, **διαχείριση επίδοσης δικτύου (performance management)**, **διαχείριση σφαλμάτων (fault management)**, **διαχείριση κόστους υπηρεσιών (accountig management)** και τέλος **διαχείριση ασφάλειας (security management)**.

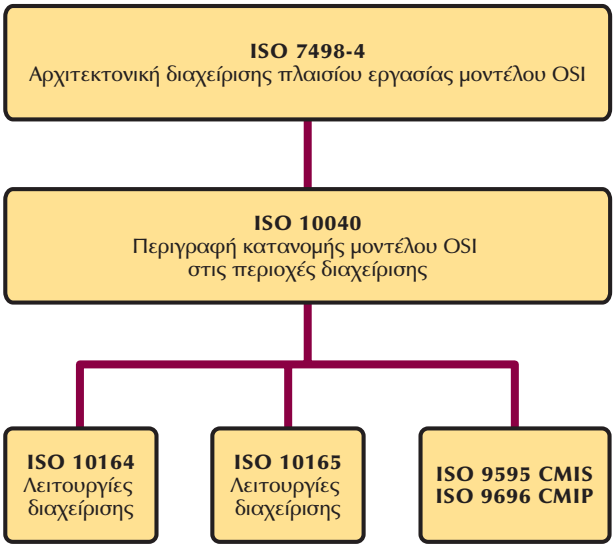
Το έργο με τον κωδικό ISO 100040, περιγράφει το τρόπο κατανομής των διαφόρων πληροφοριακών συστημάτων τύπου OSI , μεταξύ των διαφορετικών περιοχών διαχείρισης (managemnet domains). Η περιγραφή αυτή βασίζεται:

- στην ύπαρξη συστημάτων διαχείρισης (managers)
- στα συστήματα προς διαχείριση (managed systems), τα οποία για να παρέχουν στα συστήματα διαχείρησης την δυνατότητα διαχείρισής τους, έχουν εγκατεστημένο κάποιο ειδικό λογισμικό, γνωστό ως agent.

Επίσης ο οργανισμός ISO στο έργο με κωδικό ISO 10165–1 έως 4, **περιγράφει τη δομή της διαχειρίσιμης πληροφορίας σε δενδρική δομή, γνωστή ως Βάση πληροφοριών Διαχείρισης (mangement information base, MIB).** Στη δομή αυτή περιγράφονται τα αντικείμενα της διαχείρισης, καθώς και η πληροφορία, που πρέπει να χαρακτηρίζει το κάθε αντικείμενο.

Με τους κωδικούς ISO 9595 και 9596–1 και 2 προσδιορίζεται το **Πρωτόκολλο Πληροφοριών Κοινής Διαχείρισης (Common Management Information Protocol, CMIP**) και η υπηρεσία **Κοινών Πληροφοριών Διαχείρησης (Common Management Information Service, CMIS)** βάσει των οποίων γίνεται η ανταλλαγή πληροφοριών διαχείρισης. Οι εντολές, που μπορεί να στείλει ο σταθμός διαχείρισης προς το agent, είναι:

- m–get,για να διαβάσει τιμές από το MIB του λογισμικού agent του διαχειριζόμενου σταθμού.
- m–set, για να θέσει τιμές σε παραμέτρους του MIB του agent.
- m–action, για να ενεργοποιηθεί συγκεκριμένη ενέργεια στο agent.
- m–create, για να προστεθεί χαρακτηριστικό σε agent π.χ. το ανέβασμα κάποιου πρωτοκόλλου.
- m–delete. για να διαγραφεί χαρακτηριστικό από agent.

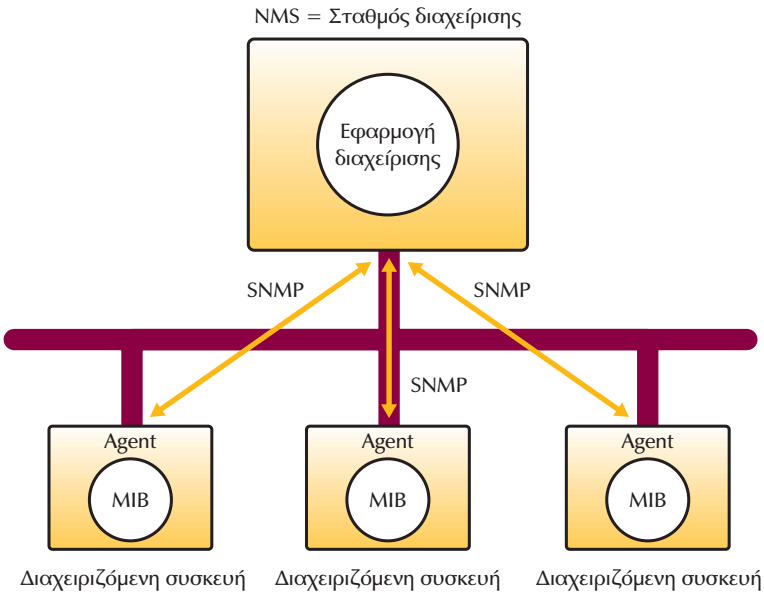


Σχήμα 8-5 Διάγραμμα των προτύπων Διαχείρισης

8.2.2 Πρότυπο διαχείρισης SNMP

Το πρωτόκολλο διαχείρισης SNMP είναι σήμερα το πλέον διαδεδομένο. Η εξέλιξη του είναι συνεχόμενη και παρουσιάζονται νέες πρότυπες εκδόσεις του πρωτοκόλλου. Η δομή του πρωτοκόλλου SNMP είναι απλή, αλλά τα χαρακτηριστικά που διαθέτει είναι αρκετά για να δώσουν λύσεις σε προβλήματα διαχείρισης σε ετερογενή δίκτυα. Το SNMP είναι πρωτόκολλο επιπέδου εφαρμογής και σχεδιάστηκε για την ανταλλαγή πληροφορίας διαχείρισης ανάμεσα σε συσκευές που συνδέονται σε δίκτυο. Στα δίκτυα που η διαχείριση γίνεται με χρήση του πρωτοκόλλου SNMP, υπάρχει η έννοια του **σταθμού διαχείρισης** (**management station**), η έννοια του λογισμικού agent, με το οποίο έχουν εφοδιαστεί οι σταθμοί εργασίας προς διαχείριση, που συνδέονται στο δίκτυο, καθώς και η έννοια του **MIB** (**management information base**), δηλαδή η καταγραφή της διαχειρίσιμης πληροφορίας σε ειδική δενδρική μορφή. Η γραφική αναπαράσταση του μοντέλο SNMP φαίνεται στο Σχήμα 8-6.

Η διαχειριζόμενη συσκευή μπορεί να είναι οτιδήποτε συνδέεται στο δίκτυο: υπολογιστές, εκτυπωτές, δικτυακές συσκευές, modems κ.λ.π. Επειδή αρκετές συσκευές μπορεί να μην έχουν μεγάλη δυνατότητα επεξεργασίας (για παράδειγμα λόγω χαμηλών επιδόσεων του επεξεργαστή που φέρουν), το λογισμικό διαχείρισης είναι έτσι σχεδιασμένο, ώστε να επιβαρύνει το ελάχιστο δυνατό τις επιδόσεις της συσκευής. Οι σταθμοί διαχείρισης όμως που τρέχουν και την εφαρμογή διαχείρισης, επιβαρύνονται με την επεξεργασία της πληροφορίας, που συλ-



Σχήμα 8-6 Μοντέλο Διαχείρισης SNMP

λέγουν από τους διάφορους agent και, συνήθως, είναι υπολογιστές μέσα σε δίκτυο, επιφορτισμένοι με αυτήν τη δραστηριότητα μόνο. Το λογισμικό παρέχει, συνήθως, τη δυνατότητα για γραφικές απεικονίσεις της κατάστασης του δικτύου, εξαγωγή στατιστικών στοιχείων και προβολή τους με διαφόρους τρόπους. Είναι δυνατή η παρουσία ενός ή και περισσοτέρων σταθμών διαχείρισης. Επίσης, είναι δυνατόν να γίνει διαχωρισμός αρμοδιοτήτων μεταξύ των σταθμών διαχείρισης και ο καθένας από αυτούς να ελέγχει συγκεκριμένο κομμάτι του δικτύου και οι σταθμοί εργασίας να ανταλλάσσουν μεταξύ τους πληροφορίες, που εμείς θεωρούμε κρίσιμες.

Για τη δομή του MIB και τις διάφορες τυποποιήσεις του θα έχουμε τη δυνατότητα να αναφερθούμε με λεπτομέρειες παρακάτω. Μπορούμε, όμως, να αναφέρουμε μερικά γενικά παραδείγματα πληροφοριών, που καταχωρούνται στο MIB, όπως:

- Ο αριθμός και η κατάσταση των θυρών συσκευής. Για παράδειγμα, ότι η συσκευή έχει τέσσερις θύρες από τις οποίες είναι σε κατάσταση λειτουργίας οι τρεις.
- Καταχωρήσεις διαφόρων λαθών που εμφανίστηκαν κατά την λειτουργία της συσκευής.
- Ο αριθμός των bytes ή / και πακέτων που πέρασαν από θύρα της συσκευής όση ώρα λειτουργούσε.

- Αριθμούς bytes / πακέτων για κάθε θύρα ανά πρωτόκολλο, π.χ IP.
- Πληροφορίες για τη θέση της συσκευής, το όνομα της, άτομα τα οποία μπορούμε να καλέσουμε σε περίπτωση που χρειαστούμε κάποια βοήθεια (π.χ να τεθεί προσωρινά εκτός λειτουργίας όταν βρίσκεται σε χώρο απομακρυσμένο από εμάς).

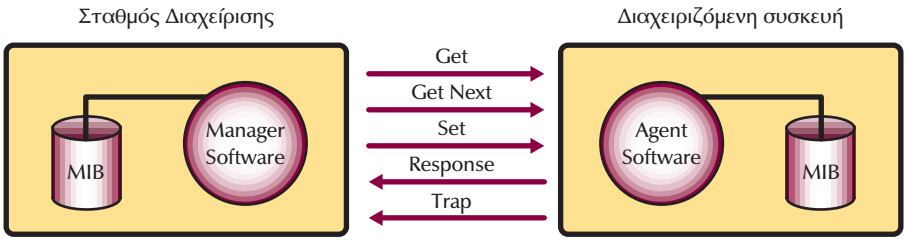
Τύποι εντολών στο πρωτόκολλο SNMP

Ο σταθμός διαχείρισης για να διαχειριστεί συσκευή, στέλνει μήνυμα προς το agent της συσκευής και αυτό με την σειρά του προβαίνει ανάλογα με τον τύπο του μηνύματος στην αντίστοιχη ενέργεια.

Το SNMP είναι πρωτόκολλο χωρίς επιβεβαίωση και κάνει χρήση του πρωτοκόλλου **UDP (User datagram Protocol)** για να επικοινωνήσει με τα agents των διαχειριζόμενων συσκευών.

Οι δυνατοί τύποι εντολών στο SNMP είναι:

Get
Get Next
Response
Set
Trap



Σχήμα 8-7 Εντολές που ανταλλάσσονται στο πρότυπο διαχείρισης SNMP

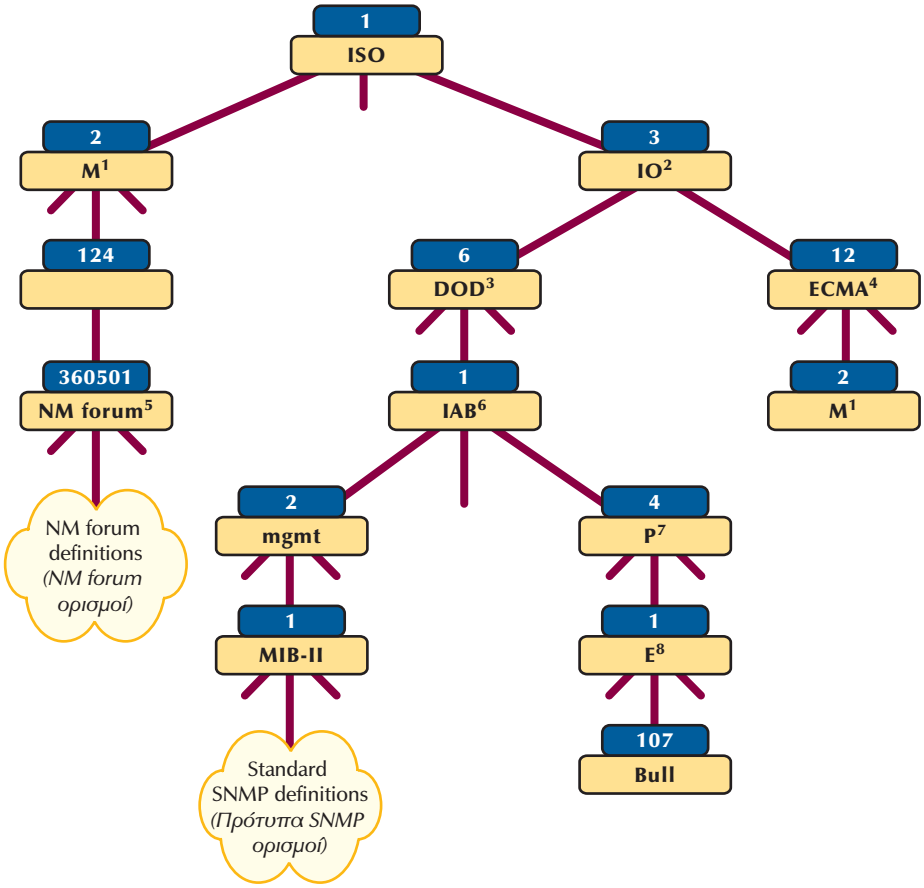
Από τις παραπάνω εντολές, άλλες στέλνονται από το σταθμό διαχείρισης και άλλες από το agent της διαχειριζόμενης συσκευής. Ο σταθμός διαχείρισης μπορεί να στείλει τις εντολές get, getnext και set. Με την εντολή get ο σταθμός μπορεί να διαβάσει την τιμή παραμέτρου του MIB, ενώ με την getnext διαβάζει την τιμή της επόμενης παραμέτρου. Με την εντολή set μπορεί να μεταβάλει την τιμή παραμέτρου στο MIB της διαχειριζόμενης συσκευής. Με τη σειρά του, το agent της διαχειριζόμενης συσκευής απαντά στις ερωτήσεις get και getnext του σταθμού

διαχείρισης με την εντολή response. Δηλαδή, με την εντολή response ο agent στέλνει την τιμή που ζητά η εντολή get ή getnext. Επίσης, το agent της διαχειριζόμενης συσκευής στέλνει με την εντολή trap σημαντικά συμβάντα, όπως alarm ή γεγονότα, που εμείς έχουμε ζητήσει από το agent να στέλνει, όταν συμβούν για άμεση ενημέρωση του σταθμού διαχείρισης. Τέλος, το agent μπορεί, αν ζητηθεί από την εντολή set να αλλάξει παραμέτρους στην συσκευή, όπως για παράδειγμα να απενεργοποιήσει ένα πρωτόκολλο ή μια θύρα. **Κάθε SNMP μήνυμα περικλείει το πεδίο community. Το πεδίο community λειτουργεί σαν είδος κωδικού (password).** Κάθε συσκευή που συνδέεται στο δίκτυο και την οποία πρόκειται να διαχειριστούμε με το πρωτόκολλο SNMP, ρυθμίζεται για το ποια ονόματα του πεδίου community θα θεωρεί ως σωστά. Συνήθως, υπάρχει community, που επιτρέπει μόνο την ανάγνωση (read) τιμών από το MIB και community, που επιτρέπει την ανάγνωση και εγγραφή (read / write) τιμών του MIB της διαχειριζόμενης συσκευής. Πιο συνηθισμένα community ονόματα είναι το public για ανάγνωση και το private για ανάγνωση / εγγραφή. Έτσι, εάν κάποιος σταθμός διαχείρισης επιχειρήσει να επικοινωνήσει μέσω agent με community διαφορετικά από αυτά που έχει δηλωμένα ο agent, η επικοινωνία δεν θα είναι εφικτή. Επιπλέον, μπορούμε να δηλώσουμε στο agent συγκεκριμένες IP διευθύνσεις τις οποίες θα αναγνωρίζει ως σταθμούς διαχείρισης καθώς και σε ποιες IP διευθύνσεις θα στέλνει τα traps. Με τον τρόπο αυτό εξασφαλίζουμε ότι το agent δεν θα βρεθεί υπό την διαχείριση κατά λάθος, ή ακόμα και εσκεμμένα, σταθμών που δεν είναι οι πραγματικοί σταθμοί διαχείρισης, επιτυγχάνοντας έτσι μεγαλύτερη ασφάλεια. Οι εκδόσεις 2 και 3 του πρωτοκόλλου SNMP έχουν ενσωματωμένα και άλλα χαρακτηριστικά ασφάλειας.

Βάση Πληροφοριών Διαχείρισης (Management Information Base, MIB)

Όπως έχουμε ήδη αναφέρει η διαχειρίσιμη πληροφορία αποθηκεύεται σε βάση δεδομένων γνωστή ως MIB. Η δομή του MIB έχει μορφή ανεστραμμένου δένδρου, όπου ξεκινώντας από τη ρίζα προχωρούμε προς τα φύλλα. Κάθε φύλλο αντιπροσωπεύει και ένα διαχειριζόμενο αντικείμενο. Σε κάθε φύλλο έχει δοθεί ένας αριθμός. Με τον τρόπο αυτό, η διαδρομή για ένα φύλλο, μπορεί να προσδιορισθεί από ακολουθία αριθμών OID (object identifier), ξεκινώντας από τον αριθμό της ρίζας και συνεχίζοντας με τους αριθμούς του κάθε φύλλου, που μεσολαβεί στη διαδρομή. Η ρίζα του δένδρου, που έχει την τιμή 1, είναι ο οργανισμός ISO. Τα επόμενα φύλλα που ακολουθούν, φαίνονται στο Σχήμα 8-8.

Για παράδειγμα, το φύλο MIB II μπορεί να προσδιορισθεί με την παρακάτω ακολουθία αριθμών: 1.3.6.1.2.1.



[1] Member *(Μέλος)*
[2] International organizations *(Διεθνείς οργανισμοί)*
[3] Department of Defense USA *(Υπουργείο Άμυνας ΗΠΑ)*
[4] European Computer Manufacturing Association *(Ένωση Ευρωπαίων Κατασκευαστών Υπολογιστών)*
[5] NM forum *(Δημόσια συζήτηση για διαχείριση δικτύων)*
[6] Internet Architecture Board *(Επιτροπή Αρχιτεκτονικής του Διαδικτύου)*
[7] Private *(Ιδιωτικές εταιρείες)*
[8] Enterprises *(Επιχειρήσεις)*

Σχήμα 8-8 Δένδρο καταχώρησης των διαφόρων οργανισμών και προτύπων

Όπως μπορούμε να δούμε στο Σχήμα 8-8 κάτω από τη διαδρομή 1.3.6.1.4.1 έχουν δοθεί συγκεκριμένοι αριθμοί για φύλλα, που αντιστοιχούν σε συγκεκριμένες εταιρείες. Για παράδειγμα στη διαδρομή 1.3.6.1.4.1.107 υπάρχει το αντικείμενο για την εταιρεία Bull. Μετά το συγκεκριμένο αντικείμενο, οι εταιρείες έχουν τη δυνατότητα να δημιουργήσουν τα δικά τους αντικείμενα και να δώσουν σε αυτά τους

αριθμούς, που επιθυμούν. Έτσι, οι εταιρείες έχουν τη δυνατότητα να εμπλουτίσουν τη διαχειριζόμενη πληροφορία συσκευής, πέρα από τα καθιερωμένα πρότυπα όπως για παράδειγμα το MIB II, με δικά τους MIB.

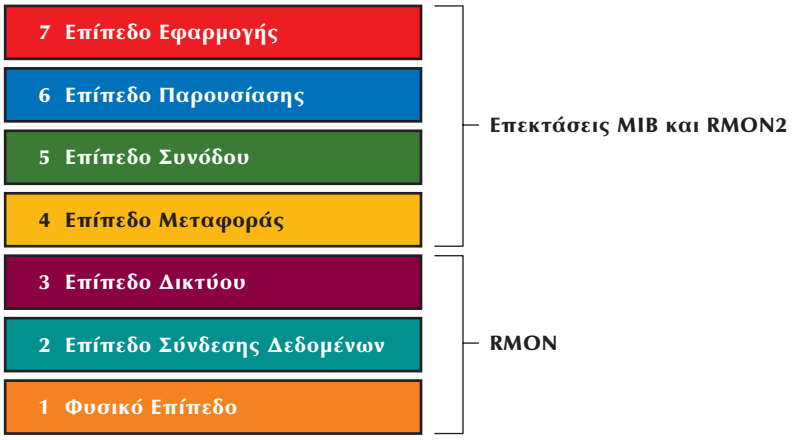
Υπάρχει σύσταση με το όνομα **Δομή Πληροφορίας Διαχείρισης (Structure of Management Information, SMI)** που προσδιορίζει το τρόπο δόμησης MIB. Το SMI και τους ακόλουθους τύπους δεδομένων μέσα στο MIB:

- Διευθύνσεις Δικτύων: Αναπαριστά τη διεύθυνση για κάποια οικογένεια πρωτοκόλλου.
- Μετρητές: Μη αρνητικοί ακέραιοι αριθμοί, που αυξάνουν μέχρι να φθάσουν τη μέγιστή τους τιμή, όπου και ξαναμηδενίζονται. Παράδειγμα μετρητή είναι ο αριθμός, που δείχνει τον αριθμό των bytes, που δέχθηκε πόρτα δικτυακής συσκευής.
- Μετρητές gauges: Μη αρνητικοί ακέραιοι αριθμοί, που αυξάνουν ή μειώνονται, αλλά κλειδώνουν σε μέγιστη τιμή. Παράδειγμα τέτοιου μετρητή, είναι για το μήκος της ουράς πακέτων εξόδου (σε πακέτα).
- Μετρητές χρόνου: Πραγματοποιούν μετρήσεις σε μονάδα χρόνου (π.χ σε sec), από τη στιγμή, που συνέβη ένα γεγονός. Για παράδειγμα ο χρόνος από τη στιγμή, που ξεκίνησε, η λειτουργία συσκευής.

Πρότυπα MIB II, RMON, RMON2

Όπως έχουμε ήδη αναφέρει, έχουν καταβληθεί και συνεχίζουν να καταβάλονται προσπάθειες για την καθιέρωση προτύπων για τη διαχείριση του δικτύου, όπως για παράδειγμα το MIB II (1.3.6.1.2.1). Στο MIB II κρατιέται η απαραίτητη πληροφορία για τις πλέον απαραίτητες ενέργειες διαχείρισης των συσκευών, που συνδέονται σε δίκτυο.

Εκτός από το MIB II , υπάρχουν και άλλα πρότυπα που παρέχουν περισσότερες δυνατότητες για την παρακολούθηση και διαχείριση των συσκευών, που συνδέονται σε δίκτυο. Το πρότυπο RMON είναι επέκταση του MIB II. Το RMON, αρχικά, όριζε εννέα ομάδες παραμέτρων για την επιτήρηση και διαχείριση τμήματος δικτύου Ethernet στο φυσικό επίπεδο και στο επίπεδο σύνδεσης δεδομένων του μοντέλου OSI. Στη συνέχεια, προστέθηκαν άλλες οχτώ ομάδες παραμέτρων, προκειμένου να είναι δυνατή η παρακολούθηση και η διαχείριση δικτύων τύπου Token Ring.

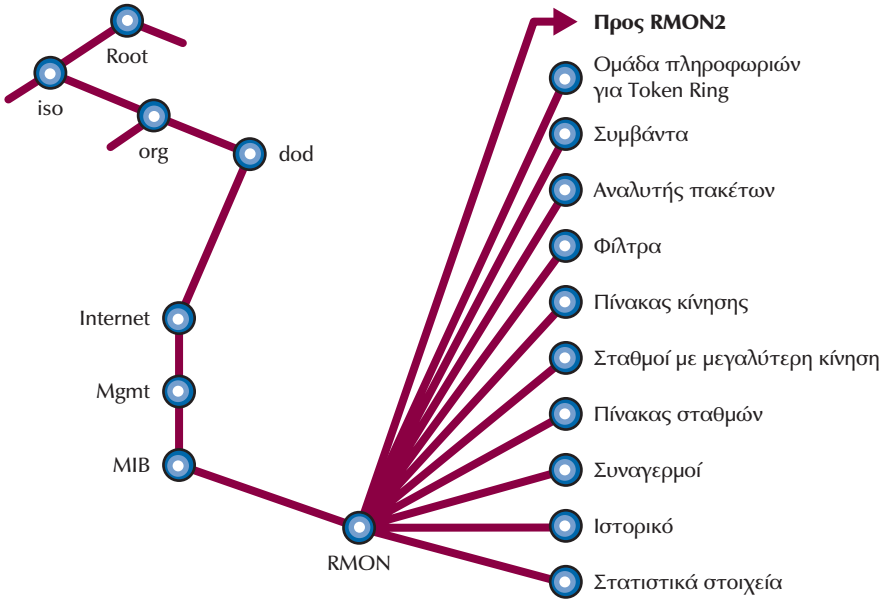


Σχήμα 8-9 Αντιστοιχία της διαχειριζόμενης πληροφορίας στα δένδρα RMON & RMON2, με τα επίπεδα του μοντέλου OSI

Καθώς η πολυπλοκότητα των δικτύων μεγαλώνει, έγινε φανερή η απαίτηση για δημιουργία προτύπου, που θα επιτρέπει τη συλλογή στοιχείων και για τα υπόλοιπα επίπεδα του μοντέλου OSI. Το RMON2 παρέχει πλέον τη δυνατότητα συλλογής στοιχείων και διαχείρισης των υπολοίπων επιπέδων του OSI μοντέλου. Ένα επίσης πρότυπο είναι υπό εξέλιξη το SMON και αφορά την δημιουργία ενός MIB για switches και καταγραφή πληροφοριών για τυχόν εικονικά δίκτυα (VLANs).

Στη συνέχεια θα αναφερθούμε στις ομάδες παραμέτρων RMON για δίκτυα τύπου Ethernet. Το RMON μπορεί να υποστηρίζεται από δικτυακή συσκευή που συνδέεται σε Ethernet δίκτυο. Οι ομάδες είναι:

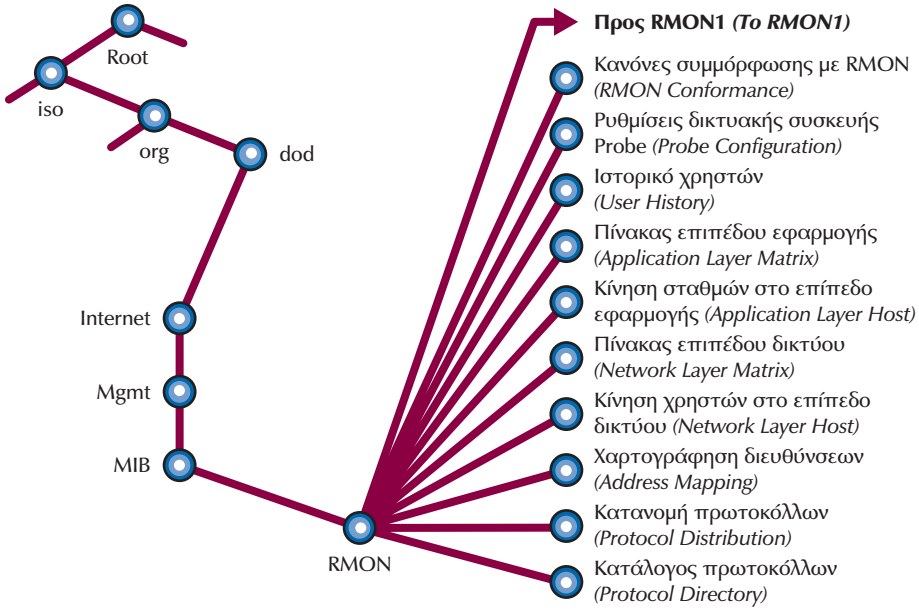
1. **Statistics**:παρέχει πληροφορίες, που απαιτούνται για την κατανόηση της επίδοσης τμήματος δικτύου. Τα στατιστικά περιλαμβάνουν μετρήσεις σε αληθινό χρόνο πακέτων, οκτάδων, πακέτα πολλαπλών εκπομπών, πακέτα, που απορρίφθηκαν, λάθη κ.ο.κ.
2. **History**: παρέχει ιστορικά δεδομένα για διάφορες παραμέτρους τμήματος δικτύου, που βοηθούν στην καλύτερη ανάλυση της συμπεριφοράς του.
3. **Host Table**: παρέχει πληροφορίες για την κίνηση, που δημιουργούν οι διάφοροι σταθμοί, που συνδέονται στο τμήμα του δικτύου, που μετράμε. Παρέχει τη δυνατότητα εντοπισμού της συσκευής, που δημιουργεί την περισσότερη κίνηση μέσα στο δίκτυο.
4. **HostTopN**:παρέχει στατιστικά στοιχεία ταξινομημένα με βάση τους σταθμούς που δημιουργούν την περισσότερη κίνηση στο δίκτυο.
5. **Traffic Matrix**:παρέχει στοιχεία για την κίνηση και τα λάθη για όλους τους δυνατούς συνδυασμούς ζευγαριών επικοινωνίας μεταξύ των σταθμών εργασίας μέσα στο δίκτυο.



Σχήμα 8-10 Οι ομάδες πληροφοριών του RMON

6. **Alarm**:αναφέρει αλλαγές στα χαρακτηριστικά λειτουργίας δικτύου. Συνήθως alarm δημιουργούνται από την ενεργοποίηση κατωφλίων για διάφορες παραμέτρους του MIB.
7. **Event**:καταγράφει συμβάντα στο δίκτυο. Και στην περίπτωση αυτή η καταγραφή γεγονότων προέρχεται, συνήθως, από την ενεργοποίηση κατωφλίων από το διαχειριστή του δικτύου.
8. **Filters**:παρέχει τη δυνατότητα ενεργοποίησης φίλτρων, που βασίζονται σε λογικούς κανόνες (π.χ. and, or, not). Όταν ικανοποιούνται οι κανόνες φίλτρου, μπορεί να ενεργοποιούνται μηχανισμοί όπως καταγραφής (log) συμβάντος, ή δημιουργίας alarm κ.λ.π.
9. **Packet Capture**: είναι η μόνη από τις ομάδες, που περιλαμβάνει και τα επτά επίπεδα του μοντέλου OSI. Με τη λειτουργία αυτή είναι δυνατή η αντιγραφή των πακέτων που κυκλοφορούν μέσα στο δίκτυο καθώς και η δυνατότητα ανάλυσή τους. Η ενεργοποίηση της αντιγραφής μπορεί να ελεγχθεί, επίσης, με βάση την ικανοποίηση κριτηρίων όπως ο τύπος του πρωτοκόλλου επικοινωνίας κ.ο.κ.

Στη συνέχεια θα αναφερθούμε στις ομάδες παραμέτρων RMON2 για δίκτυα τύπου Ethernet. Το RMON2 μπορεί να υποστηρίζεται από δικτυακή συσκευή, που συνδέεται σε Ethernet δίκτυο. Οι ομάδες παραμέτρων είναι:



Το πρότυπο RMON, το οποίο περιγράφτηκε στο σχήμα 8-10, αναφέρεται και σαν RMON1.

Σχήμα 8-11 Οι ομάδες πληροφοριών του RMON2

1. **Protocol Directory Group**: περιέχει σε κατάλογο όλα τα πρωτόκολλα, που μπορεί να καταλάβει η συσκευή, που υποστηρίζει το RMON2.
2. **Protocol Distribution**:κρατά στατιστικά στοιχεία για το ποσοστό της κίνησης, που δημιουργεί το κάθε πρωτόκολλο ανά τμήμα LAN ή ανά επίπεδο στο μοντέλο OSI.
3. **Address Mapping**:συσχετίζει τον αριθμό θύρας συσκευής με τη φυσική της διεύθυνση (MAC address) και τη διεύθυνση δικτύου (π.χ. IP address).
4. **Network Layer Host**:περιέχει στατιστικά στοιχεία για την κίνηση συγκεκριμένων σταθμών μέσα στο δίκτυο, βασισμένα στη διεύθυνση δικτύου που έχουν.
5. **Network Layer Matrix**: περιέχει στατιστικά στοιχεία για την κίνηση μεταξύ ζευγαριών επικοινωνίας από σταθμούς μέσα στο δίκτυο, βασισμένα στη διεύθυνση δικτύου, που έχουν.
6. **Network Layer TopN Matrix**:περιέχει στατιστικά στοιχεία του τρίτου επιπέδου του μοντέλου OSI, για τις πλέον ενεργές συνομιλίες μεταξύ των σταθμών μέσα στο δίκτυο.
7. **Application Layer Host**:περιέχει στατιστικά στοιχεία για την κίνηση ανά σταθμό στο δίκτυο σε επίπεδο εφαρμογής.

8. **Application Layer Matrix**:περιέχει στατιστικά στοιχεία για την κίνηση, που δημιουργούν στο δίκτυο, οι σταθμοί εργασίας στις μεταξύ τους συνομιλίες σε επίπεδο εφαρμογής.
9. **User History**:κρατά στατιστικά ιστορικά στοιχεία για μεταβλητές (32 bit ακέραιες μεταβλητές) που έχει ορίσει ο ίδιος ο χρήστης.
10. **Probe Configuration**:περιέχει τις καθιερωμένες ρυθμίσεις της συσκευής δικτύου, που κρατά το RMON2.
    Πρέπει να επισημάνουμε, ότι δεν έχουν εκδοθεί έως την ώρα που γράφεται το βιβλίο πρότυπα MIB για άλλου τύπου δίκτυα εκτός από τα δίκτυα τύπου Ethernet και Token Ring που, έχουμε αναφέρει. Για παράδειγμα δεν υπάρχουν πρότυπ MIB για δίκτυα τύπου FDDI, ATM. Στις περιπτώσεις αυτές ο κάθε κατασκευαστής έχει αναπτύξει τα δικά του MIB. Για να γίνει διαχείριση αυτών των δικτύων, θα πρέπει να έχουμε φορτώσει στο σταθμό διαχείρισης του δικτύου μας τις δομές των MIB των κατασκευαστών.

8.2.3 Προγράμματα Διαχείρισης

Στην αγορά κυκλοφορούν αρκετά προγράμματα διαχείρισης, που βασίζουν τον τρόπο λειτουργίας τους στα πρότυπα που προαναφέραμε. Χαρακτηριστικά αναφέρουμε μερικά: το Open View της HP, το Tivoli της IBM, το Unicenter TNG της C.A., το Open Master της Bull. Τα παραπάνω προγράμματα διαχείρισης έχουν συνήθως, την δυνατότητα να συνεργαστούν και με επιμέρους προγράμματα διαχείρισης, που παρέχουν οι κατασκευαστές δικτυακού εξοπλισμού (π.χ. το πρόγραμμα διαχείρισης Optivity της Nortel). Έτσι, είναι εφικτή η διαχείριση και των επιπρόσθετων χαρακτηριστικών, που προσδίδουν οι κατασκευαστές στα προϊόντα τους.

8.3 Ασφάλεια Δικτύων

Με την ανάπτυξη των δικτύων παρουσιάστηκε η ανάγκη προστασίας της πληροφορίας, που μεταδίδεται ή αποθηκεύεται. Στην ενότητα αυτή θα γίνει παρουσίαση προβλημάτων ασφάλειας δικτύων, υπηρεσιών ασφάλειας για την αντιμετώπιση τους, τεχνικών υλοποίησης των υπηρεσιών αυτών καθώς και των προϋποθέσεων ύπαρξης συστήματος ασφάλειας.

8.3.1 Ασφάλεια πληροφοριών

Η ασφάλεια των συστημάτων ασχολείται με την προστασία αντικειμένων που αξίζουν να προστατευθούν, τα αγαθά. Τα αγαθά με την σειρά τους έχει νόημα να προστατευθούν μόνο και μόνο επειδή έχουν κάποια αξία. Η αξία των αγαθών μπορεί να μειωθεί εάν υποστούν ζημιά. Από την στιγμή, που μπορεί να προκύψουν κίνδυνοι που θα μειώσουν την αξία των αγαθών πρέπει να ληφθούν μέτρα προστασίας για τα αγαθά, κάτι που συνεπάγεται και κάποιο κόστος (τόσο σε

χρήμα όσο και σε κόπο). Η μερική προστασία των αγαθών, είτε για λόγους υπερβολικού κόστους των μέτρων προστασίας, είτε για λόγους αδυναμίας ύπαρξης των κατάλληλων μηχανισμών, που μπορούν να εξασφαλίσουν την απόλυτη ασφάλεια, έχει ως συνέπεια τη δημιουργία επισφάλειας των αγαθών. Ο ιδιοκτήτης των αγαθών θα πρέπει να κρίνει, ποια είναι η πιο επωφελής ισορροπία ανάμεσα στο κόστος για τη λήψη μέτρων προστασίας και στην επισφάλεια των αγαθών με τις συνέπειες της. Ιδιοκτήτης μπορεί να είναι το πρόσωπο που κατέχει ή είναι υπεύθυνο για ολόκληρο ή για μέρος αγαθού. Σε πληροφοριακό σύστημα, σαν αγαθά μπορούν να θεωρηθούν οι πληροφορίες, που διακινούνται σε αυτό (ή τα δεδομένα) και οι υπολογιστικοί πόροι που χρησιμοποιούμε για να διαχειριστούμε τις πληροφορίες και τα δεδομένα. Ο ιδιοκτήτης διατηρεί το δικαίωμα να καθορίσει πως μπορεί να χρησιμοποιηθεί, να μεταβληθεί ή να διατεθεί το αγαθό. Εκτός, όμως, από τους ιδιοκτήτες, τα αγαθά είναι δυνατό να χρησιμοποιούνται και από τους χρήστες. Οι χρήστες μπορεί να είναι ή να μην είναι τα ίδια πρόσωπα με τους ιδιοκτήτες. Πρέπει να διευκρινίσουμε, ότι με τους όρους ιδιοκτήτες ή χρήστες, δεν αναφερόμαστε αποκλειστικά σε πρόσωπα αλλά και σε διεργασίες, που κάνουν χρήση μέρους ή ολόκληρου του πληροφοριακού συστήματος. Από τη στιγμή, που υπάρχει η έννοια της ιδιοκτησίας, πρέπει να εισάγουμε και την έννοια της εξουσιοδότησης. Ως εξουσιοδότηση μπορούμε να ορίσουμε την άδεια που παρέχει ο ιδιοκτήτης για συγκεκριμένο σκοπό, όπως για παράδειγμα, την άδεια για χρήση κάποιων υπολογιστικών πόρων ή την πρόσβαση σε συγκεκριμένο σύνολο δεδομένων βάσης δεδομένων. Έτσι, για την πρόσβαση σε κάποια μέσα ή πληροφορίες υπάρχει η έννοια του εξουσιοδοτημένου ή του μη εξουσιοδοτημένου.

Μεγάλο μέρος της ασφάλειας πληροφοριών ασχολείται με την εξασφάλιση της συνεχούς παροχής υπηρεσιών στους εξουσιοδοτημένους χρήστες και την προστασία τους από τους μη εξουσιοδοτημένους. Υπάρχουν τέσσερα ζητούμενα στα πλαίσια πολιτικής ασφάλειας, για να εξασφαλισθεί η χρήση των αγαθών από εξουσιοδοτημένους χρήστες:

- **Αυθεντικότητα (authentication)**: Η απόδειξη της ταυτότητας του χρήστη για παροχή πρόσβασης στα αγαθά συστήματος.
- **Ακεραιότητα (Integrity)**: Η διασφάλιση ότι τα δεδομένα έχουν υποστεί αλλαγές μόνο από εξουσιοδοτημένα άτομα.
- **Εμπιστευτικότητα (Confidentiality)**: Ο περιορισμός της πρόσβασης στα δεδομένα μόνο σε άτομα που επιτρέπεται να έχουν πρόσβαση σε αυτά.
- **Μη άρνηση ταυτότητας (Non repudiation)**: Η δυνατότητα απόδοσης πράξεων σε συγκεκριμένο χρήστη.

Από τα τέσσερα παραπάνω ζητούμενα μπορούμε να συνθέσουμε και την έννοια της **Εγκυρότητας (Validity)**: ως την απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας. Η εγκυρότητα είναι ο συνδυασμός της Ακεραιότητας και της Αυθεντικότητας**.**

Επίσης, θα πρέπει να διασφαλίσουμε στους εξουσιοδοτημένους χρήστες, που πιθανόν να κοστολογούνται για τη δυνατότητα πρόσβασης τους σε πληρο-

φορίες, ότι δεν συντρέχει περίπτωση άρνησης παροχής υπηρεσιών, για τις οποίες έχουν εξουσιοδότηση. Έτσι, μπορούμε να ορίσουμε και την **Διαθεσιμότητα Πληροφοριών (Information Availability)**: ως την αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης πληροφορίας σε εξουσιοδοτημένους χρήστες.

Με όσα έχουν αναφερθεί σε αυτήν την ενότητα μπορούμε να προχωρήσουμε στους παρακάτω ορισμούς της ασφάλειας και της ασφάλειας πληροφοριών:

- **Ασφάλεια (Security)**: Η προστασία της Διαθεσιμότητας, της Ακεραιότητας και της Εμπιστευτικότητας Πληροφοριών.
- **Ασφάλεια Πληροφοριών (Information Security)**: Ο συνδυασμός της Εμπιστευτικότητας, της Εγκυρότητας και της Διαθεσιμότητας Πληροφοριών.

Με βάση όσα προαναφέρθηκαν μπορούμε να ορίσουμε ως Παραβίαση (violation) ασφάλειας σε πληροφοριακό σύστημα, την παραβίαση ενός η περισσότερων ιδιοτήτων, όπως διαθεσιμότητα, εμπιστευτικότητα και εγκυρότητα**.**

Ένα πληροφοριακό σύστημα είναι εκτεθειμένο σε κινδύνους. Οι κίνδυνοι μπορούν να διαχωριστούν στις απειλές και στις αδυναμίες.

Με τον όρο απειλές αναφερόμαστε σε ενέργειες ή γεγονότα, που μπορούν να οδηγήσουν στην κατάρρευση κάποιου από τα χαρακτηριστικά ασφάλειας πληροφοριών (όπως αυτά ορίσθηκαν πιο πάνω). Οι απειλές μπορεί να προέρχονται είτε από φυσικά γεγονότα (π.χ. πυρκαγιά) είτε από ανθρώπινες ενέργειες, που μπορεί να είναι σκόπιμες ή τυχαίες. Ενώ με τον όρο αδυναμίες αναφερόμαστε στα σημεία του πληροφοριακού συστήματος, που αφήνουν περιθώρια για παραβιάσεις. Οι αδυναμίες μπορεί να οφείλονται σε ανεπαρκή γνώση για υποστήριξη του συστήματος από το ανθρώπινο δυναμικό, ή σε από κατασκευής δυσλειτουργίες του ίδιου του συστήματος (π.χ. ελαττώματα στο λογισμικό).

Στην προσπάθεια μας να δημιουργήσουμε πλαίσιο ασφάλειας για πληροφοριακό σύστημα, θα πρέπει πρώτα να εκτιμήσουμε και να συνυπολογίσουμε διάφορους παράγοντες, πριν προχωρήσουμε στη λήψη μέτρων ασφάλειας. Πρώτα από όλα, θα πρέπει να εντοπίσουμε ποια αγαθά πραγματικά χρήζουν ανάγκης προστασίας και να προσπαθήσουμε να βρούμε τους πιθανούς κινδύνους. Στη συνέχεια, θα πρέπει να προχωρήσουμε σε ένα πρώτο σχεδιασμό της αρχιτεκτονικής ασφάλειας και υπολογισμό του κόστους υλοποίησής της. Στο κόστος θα πρέπει να συμπεριλαμβάνεται το κόστος των υλικών που απαιτούνται για την υλοποίηση της λύσης, το κόστος του ανθρώπινου δυναμικού, που θα κληθεί να πραγματοποιήσει την εγκατάσταση, καθώς και το μόνιμο λειτουργικό κόστος για τη συντήρηση πλαισίου ασφάλειας στο πληροφοριακό σύστημα.

Σε περίπτωση που το κόστος για τα μέτρα προστασίας, που πρέπει να ληφθούν, ξεπερνούν τα προβλεπόμενα όρια, θα πρέπει να προβούμε σε νέες παραδοχές ή και συμβιβασμούς στο τι πραγματικά θα καλύπτει και σε ποιο βαθμό η πολιτική ασφάλειας, θα υλοποιηθεί. Με τον τρόπο αυτό αποδεχόμαστε την απομένουσα επικινδυνότητα και επισφάλεια μετά την εγκατάσταση των σχετικών μέτρων προστασίας.

Τώρα που αναφερθήκαμε γενικά σε θέματα ασφάλειας και έννοιες ασφάλειας

πληροφοριών, μπορούμε να προχωρήσουμε σε πιο τεχνική εξέταση των μεθόδων που συνήθως ακολουθούνται για την επίτευξη παραβιάσεων, αλλά και στα αντίμετρα, που κάποιος μπορεί να υλοποιήσει, για να προστατέψει το πληροφοριακό του σύστημα.

8.3.2 Επεξήγηση Ορολογίας

Πριν προχωρήσουμε στην παρουσίαση βασικών τεχνικών για την παραβίαση της ασφάλειας των δικτύων υπολογιστών καθώς και σε τεχνικές προστασίας αυτών, θα αναφερθούμε στην χρησιμοποιούμενη ορολογία. Μερικοί από τους όρους θα γίνουν πλήρως κατανοητοί, όταν θα ενταχθούν μέσα στα πλαίσια τεχνικής ασφάλειας, που θα αναφέρουμε στη συνέχεια. Οι ακόλουθοι όροι είναι από τους πιο βασικούς και ευρέως χρησιμοποιούμενους σε θέματα ασφάλειας πληροφοριακών συστημάτων:

- **Κρυπτογράφηση (Encryption)**: Η μέθοδος (συνήθως μαθηματικός αλγόριθμος, το αποτέλεσμα του οποίου μπορεί με αναστροφή να μας δώσει την είσοδο του αλγόριθμου) κωδικοποίησης της αρχικής πληροφορίας, έτσι ώστε να είναι αναγνώσιμη μόνο κατόπιν αποκωδικοποίησής της (αποκρυπτογράφησής της).
- **Αποκρυπτογράφηση (Decryption)**: Η μέθοδος (η ανάστροφη λειτουργία του αλγόριθμου κρυπτογράφησης) αποκωδικοποίησης για την ανάκτηση της αρχικής κωδικοποιημένης πληροφορίας.
- **Κλειδί (Key)**: Πέρα από την γνωστή εικόνα που όλοι μας έχουμε για το κλειδί, μπορούμε να θεωρήσουμε και ως κλειδί ένα ψηφιακό κωδικό (κάποιος αριθμός από bits), που χρησιμοποιείται από τους αλγόριθμους κρυπτογράφησης ή αποκρυπτογράφησης.
- **Δημόσιο Κλειδί (Public Key)**: Ψηφιακός κωδικός που χρησιμοποιείται για την κρυπτογράφηση / αποκρυπτογράφηση πληροφοριών καθώς και για τη πιστοποίηση ψηφιακών υπογραφών. Το δημόσιο κλειδί μοιράζεται σε όλους τους χρήστες ασφαλούς δικτύου και συνδυάζεται πάντα με ιδιωτικό κλειδί.
- **Ιδιωτικό Κλειδί (Private Key)**: Ψηφιακός κωδικός, για κρυπτογράφηση / αποκρυπτογράφηση και πιστοποίηση ψηφιακών υπογραφών, που ανήκει μόνο σε ένα χρήστη, είναι καθαρά προσωπικό και συνδυάζεται με δημόσιο κλειδί.
- **Μυστικό Κλειδί (Secret Key)**: Ψηφιακός κωδικός, που είναι γνωστός στα δύο μέρη, προκειμένου να επικοινωνήσουν με χρήση κρυπτογράφησης / αποκρυπτογράφησης.
- **Λειτουργία Κατατεμαχισμού (Hash Function)**: Μαθηματική συνάρτηση, το αποτέλεσμα της οποίας δεν μπορεί με αναστροφή να μας παράγει την αρχική είσοδο.
- **Σύνοψη Μηνύματος (Message Digest)**: Η τιμή, που δίνει η λειτουργία κατατεμαχισμού.
- **Ψηφιακή Υπογραφή (Digital Signature)**: Αριθμός από bits, προστιθέμενος στο τέλος μηνύματος για να εξασφαλίσει την αυθεντικότητα και ακεραιότητα του μηνύματος.

8.3.3 Μέθοδοι Παραβίασης

Σε δίκτυο υπολογιστών εμπιστευτική πληροφορία μπορεί να υπάρχει αποθηκευμένη σε μέσα αποθήκευσης (σκληροί δίσκοι, μνήμες κ.λ.π.), ή να κυκλοφορεί μέσου του δικτύου με τη μορφή πακέτων. Η ύπαρξη πληροφοριών σε αυτές τις δύο καταστάσεις μπορεί να απειληθεί με διαφόρους τρόπους από ενέργειες χρηστών τόσο του εσωτερικού δικτύου, όσο και από χρήστες του Διαδικτύου στην περίπτωση που έχουμε σύνδεση και με αυτό. Στη συνέχεια θα αναφερθούμε στους πλέον συνηθισμένους τρόπους επιθέσεων, που χρησιμοποιούνται για την παραβίαση της ασφάλειας δικτύου υπολογιστών:

- Επιθέσεις στους κωδικούς πρόσβασης (Password attacks)

Όπως είναι γνωστό, οι μυστικοί προσωπικοί κωδικοί (passwords) είναι η πλέον κοινή μέθοδος ελέγχου της πρόσβασης σε υπολογιστικά συστήματα. Υπάρχουν δύο είδη passwords:

– **Τα επαναχρησιμοποιούμενα passwords**, που μπορούν να χρησιμοποιούνται πολλές φορές για την πρόσβαση στο σύστημα.

– **Τα passwords μιας χρήσης**. Τα passwords αυτά αλλάζουν συνεχώς και μπορούν να χρησιμοποιηθούν μόνα μία φορά για πρόσβαση στο σύστημα.

Τα περισσότερα είδη λειτουργικών συστημάτων, όπως το Unix ή τα Windows, προσφέρονται με σύστημα πιστοποίησης χρηστών με τον πρώτο τύπο passwords.

Με την εξέλιξη της τεχνολογίας η προστασία με χρήση μόνο passwords, αποτελεί σύστημα ασθενούς προστασίας της πρόσβασης.

Για την παραβίαση κωδικών πρόσβασης πάρχουν προγράμματα, που σε μικρό χρονικό διάστημα μπορούν να δοκιμάσουν πολλούς συνδυασμούς χαρακτήρων και αριθμών. Άλλος τρόπος είναι η παρακολούθηση των πλήκτρων (key stroke monitoring), όταν κάποιος εισάγει τον κωδικό του και αυτό μπορεί να γίνει με διάφορους τρόπους, όπως η εκτέλεση προγράμματος, που παρακολουθεί τα πλήκτρα, που έχουν χρησιμοποιηθεί σε ένα πληκτρολόγιο και η αποθήκευση σε ένα αρχείο, ή ο δύσκολος τρόπος της παρακολούθησης της ακτινοβολίας της οθόνης.

Ένας άλλος τρόπος για την παραβίαση κωδικών πρόσβασης αναφέρεται σαν social engineering και επικεντρώνει στην παραπλάνηση χρηστών για την απόκτηση πληροφοριών. Για παράδειγμα, η περίπτωση, που κάποιος προσποιείται τον υπάλληλο γραφείου βοήθειας (help desk) και ζητά το password χρήστη, για να διορθώσει ανύπαρκτο πρόβλημα στο υπολογιστικό σύστημα. Στην κατηγορία αυτή υπάγεται και το λεγόμενο shoulder surfing, δηλαδή το γεγονός της τυχαίας παρακολούθησης της πληκτρολόγησης του password άλλου χρήστη.

Υπάρχει επίσης η δυνατότητα απόκτησης του password με τη χρήση φυσικής βίας. Οι περιπτώσεις φυσικής βίας μπορούν να ενταχθούν σε δύο κατηγορίες: στην εξωτερική και στην εσωτερική βία. Με την εξωτερική βία είναι προφανές, ότι ένας χρήστης, όταν θα κινδυνεύσει η σωματική του ακεραιότητα, μπορεί να αποκαλύψει το password, που χρησιμοποιεί. Με την εσωτερική βία αναφερόμα-

στε στην περίπτωση, όπου κάποιος αντιγράφει νόμιμα ή παράνομα κρυπτογραφημένα passwords και μετά εκτελεί πρόγραμμα crack, για να τα αποκρυπτογραφήσει. Το πρόγραμμα crack παίρνει λέξεις από λεξικό και τις κρυπτογραφεί με τον ίδιο αλγόριθμο, που χρησιμοποιεί το λειτουργικό σύστημα για την κρυπτογράφηση των password των χρηστών. Το πρόγραμμα συγκρίνει το αποτέλεσμα της κρυπτογράφησης με τα υποκλαπέντα passwords και όταν αυτά συμπέσουν, τότε έχουν βρεθεί τα πραγματικά passwords. Τα προγράμματα crack εδικά για συστήματα Unix είναι αρκετά διαδεδομένα και εξελιγμένα.

- **Παρακολούθηση Δικτύου (Network Monitoring ή Network Packet Sniffing)**

Όπως είναι γνωστό, η επικοινωνία των υπολογιστών μέσου δικτύου βασίζεται σε πρωτόκολλα και τα δεδομένα μεταφέρονται με τη μορφή πακέτων. Πολλές εφαρμογές μεταδίδουν τα πακέτα σε μορφή καθαρού κειμένου (clear text), δηλαδή χωρίς να προβούν από μόνες τους σε κάποιο είδος κωδικοποίησης ή κρυπτογράφησης. Από την στιγμή, που τα πακέτα μεταδίδονται χωρίς κωδικοποίηση, μπορούν να συλλεχθούν με κάποιους τρόπους, να συναρμολογηθούν και να παράγουν στο ακέραιο το σύνολο της πληροφορίας. Τα προγράμματα, που κάνουν ανίχνευση πακέτων (packet sniffing), χρησιμοποιούν την κάρτα δικτύου του υπολογιστή σε κατάσταση promiscuous mode. Στην κατάσταση promiscuous mode, η κάρτα δικτύου διαβάζει και αποθηκεύει όλα τα πακέτα, που κυκλοφορούν στο δίκτυο, που συνδέεται. Τα προγράμματα αυτά μπορούν να χρησιμοποιηθούν στην διάγνωση προβλημάτων από τους διαχειριστές δικτύων, αλλά ταυτόχρονα αποτελεί πολύ ισχυρό εργαλείο για τους επίδοξους εισβολείς. Εκτός του ότι μπορεί να συλλέξουν εμπιστευτική πληροφορία την ώρα, που διέρχεται μέσα από τις γραμμές του δικτύου, είναι πολύ πιθανό να αποκαλύψει και μεταδιδόμενα passwords (η αποκάλυψη των passwords με τον τρόπο αυτό είναι γνωστή και ως Man – In – The – Middle). Επομένως μπορεί η παρακολούθηση των πακέτων στο δίκτυο να χρησιμοποιηθεί και ως μέσο για την παραβίαση των passwords.

- **Μεταμφίεση (Masquerade)**

Επίθεση με μεταμφίεση παρατηρείται όταν ο επιτιθέμενος, που βρίσκεται σε άλλο δίκτυο από το δικό μας, προσποιείται ότι βρίσκεται στο δικό μας. Ειδικά στα πρωτόκολλα TCP/IP, η μέθοδος μεταμφίεσης είναι γνωστή και ως IP Spoofing, όπου ο επιτιθέμενος ανήκει σε άλλο δίκτυο και προσποιείται ότι η διεύθυνση του ανήκει στο δικό μας εύρος IP διευθύνσεων. Η μέθοδος αυτή χρησιμοποιείται κυρίως για να ξεγελάσει ο επιτιθέμενος το firewall που συνδέει το εσωτερικό μας δίκτυο με το διαδίκτυο ή γενικότερα με δίκτυο, που δεν θεωρείται έμπιστο (trusted). Συνήθως το IP Spoofing περιορίζεται στο να εισάγει δεδομένα ή εντολές σε υπάρχον πακέτο δεδομένων, κατά τη διάρκεια επικοινωνίας τύπου client / server ή σε δίκτυα σημείο προς σημείο.

Για να γίνει εφικτή η αμφίδρομη επικοινωνία, ο επιτιθέμενος θα πρέπει να αλλάξει τους πίνακες δρομολόγησης, που έδειχναν προς τη διεύθυνση, που έχει προσποιηθεί ότι βρίσκεται (spoofed IP address). Με τον τρόπο αυτό ο επιτιθέμενος θα μπορεί να λαμβάνει όλα τα πακέτα που προορίζονταν για τη spoofed IP

διεύθυνση. Στην περίπτωση αυτή, ο επιτιθέμενος μπορεί κλέψει passwords. Επίσης μπορεί προσποιούμενος, ότι είναι κάποιος από το δίκτυο μας, να στείλει προς τους συνεργάτες μας ή τους πελάτες μας e–mails.

- **Άρνηση Παροχής Υπηρεσίας (Denial of Service)**

Οι επιθέσεις άρνησης παροχής υπηρεσιών διαφοροποιούνται από τις άλλες, που έχουμε αναφέρει, στο ότι δεν προσπαθούν να πετύχουν πρόσβαση στο δίκτυό μας, ή να συλλέξουν πληροφορίες, που διακινούνται σε αυτό. Οι επιθέσεις αυτές εστιάζονται κυρίως στην εξάντληση των ορίων των πόρων του δικτύου, όπως για παράδειγμα τον αριθμό των πακέτων, που μπορεί να χειριστεί ταυτόχρονα ένας δρομολογητής, ή στις διεργασίες στις οποίες μπορεί να αντεπεξέλθει κεντρικός εξυπηρετητής στο δίκτυο μας (π.χ. web server, mail server). Παραδείγματα τέτοιων επιθέσεων παρατηρούνται πολλά τον τελευταίο καιρό, όπως αυτά που σημειώθηκαν στα site του Yahoo, CNN στις αρχές του 2000. Εάν από ένα εξυπηρετητή ζητηθεί να εξυπηρετήσει πολύ μεγαλύτερο όγκο εργασιών από ότι είναι σχεδιασμένος να εξυπηρετήσει μέσα σε συγκεκριμένο χρονικό διάστημα, τότε είναι λογικό, ότι θα καταρρεύσει. Στο παράδειγμα που προαναφέραμε τα sites δέχθηκαν μέσα σε τρεις ώρες απαίτηση για εξυπηρέτηση διεργασιών, που δέχονται μέσα σε ένα ολόκληρο χρόνο.

Οι επιθέσεις αυτού του είδους δεν χρειάζονται αυξημένες γνώσεις σε σχέση με τις άλλες είδους επιθέσεις, που προαναφέραμε. Βέβαια είναι αποτελεσματικότερες, εάν υπάρχει πληροφόρηση για την αρχιτεκτονική του δικτύου, που πρόκειται να δεχθεί επίθεση.

- **Επιθέσεις στο επίπεδο των Εφαρμογών (Application–Layer Attacks)**

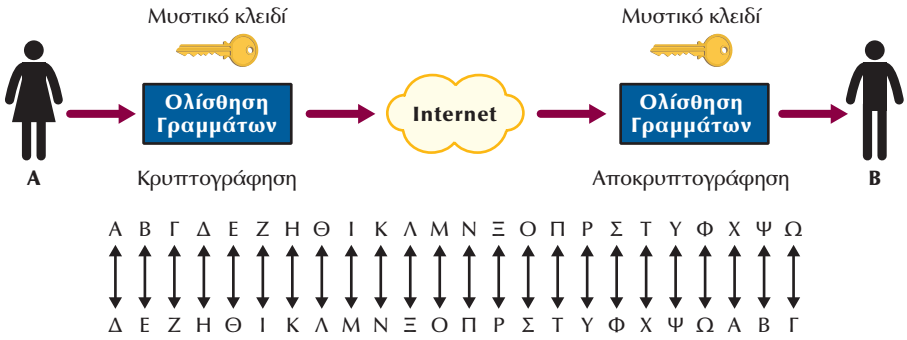
Όπως είναι γνωστό, πολλές φορές εφαρμογές, όπως HTTP, ActiveX, Telnet, Ftp, Telnet κ.λ.π., παρουσιάζουν αδυναμίες στον κώδικά τους (γνωστές και ως τρύπες, holes). Οι γνώστες αυτών των αδυναμιών μπορεί να τις εκμεταλλευθούν, προκειμένου να αποκτήσουν πρόσβαση στο σύστημα, με απώτερο σκοπό την δημιουργία σε αυτό προβλημάτων ή τη συλλογή πληροφοριών.

8.3.4 Τεχνικές ασφάλειας

Στη συνέχεια, θα παρουσιάσουμε κάποιες βασικές τεχνικές ασφάλειας των, πληροφοριών σε δίκτυο ηλεκτρονικών υπολογιστών. Πρέπει να σημειώσουμε ότι ο τομέας της ασφάλειας δεδομένων σε κατανεμημένο πληροφοριακό σύστημα είναι από τους πλέον εξελισσόμενους και υπάρχει συνεχής παρουσίαση νέων προϊόντων σε θέματα ασφάλειας από τις εταιρείες που δραστηριοποιούνται στον χώρο αυτό.

- **Συμμετρική Κρυπτογράφηση**

Η συμμετρική κρυπτογράφηση πολλές φορές αναφέρεται και ως κρυπτογράφηση συμμετρικού κλειδιού. Η μέθοδος αυτή χρησιμοποιείται κύρια για την εξασφάλιση της εμπιστευτικότητας των μεταδιδόμενων πληροφοριών πάνω από ένα κανάλι επικοινωνίας.



Σχήμα 8-12 Επικοινωνία με χρήση συμμετρικής κρυπτογράφησης

Στην περίπτωση που (σχήμα 8–12), δύο χρήστες ο Α και ο Β θέλουν να επικοινωνήσουν μεταξύ τους με ασφάλεια, θα πρέπει και οι δύο να συμφωνήσουν στη χρησιμοποίηση του ίδιου αλγόριθμου κρυπτογράφησης, καθώς επίσης και στη χρήση κοινού κλειδιού.

Πολύ απλοϊκός αλγόριθμος κρυπτογράφησης είναι ο Caesar Cipher, που, όπως φαίνεται στο σχήμα 8–12, αντικαθιστά το κάθε γράμμα του αλφαβήτου σε ένα μήνυμα με ένα άλλο γράμμα μερικές θέσεις πιο κάτω στο αλφάβητο. Ο αλγόριθμος ολισθαίνει τα γράμματα προς τα αριστερά, όταν κρυπτογραφεί κάποιο μήνυμα, ενώ προς τα δεξιά, όταν πρόκειται να αποκρυπτογραφήσει ήδη κρυπτογραφημένο μήνυμα. Στο σχήμα 8–12 ο συμφωνημένος αριθμός ολίσθησης στο αλφάβητο από τους χρήστες Α και Β είναι τρία γράμματα. Εύκολα καταλαβαίνουμε ότι, εάν κάποιος δει το κρυπτογραφημένο μήνυμα και γνωρίζει τον αλγόριθμο, θα μπορέσει σχετικά εύκολα να αποκρυπτογραφήσει το μήνυμα και αυτό γιατί ο αλγόριθμος, που προαναφέραμε, δεν είναι ιδιαίτερα σύνθετος.

Υπάρχουν προγράμματα, που προσπαθούν να αποκρυπτογραφήσουν μήνυμα, δοκιμάζοντας αρκετούς αλγόριθμους. Εάν ο αλγόριθμος είναι περίπλοκος, το σπάσιμό του ακόμα και με σύγχρονους υπολογιστές με μεγάλη υπολογιστική ισχύ, απαιτεί πολύ χρόνο, ακόμα και χρόνια, οπότε και η αποκάλυψη της πληροφορίας να μην έχει πλέον νόημα. Έχουν αναπτυχθεί πολλοί αλγόριθμοι κρυπτογράφησης, που στηρίζονται σε σύνθετη λογική και περίπλοκους μαθηματικούς συνδυασμούς. Πολλοί αλγόριθμοι μάλιστα, δεν είναι επαρκώς τεκμηριωμένοι, ενώ άλλοι δεν είναι καταχωρημένοι στη βιβλιογραφία, επειδή προστατεύονται ως κρατικά μυστικά. Είναι συνηθισμένο από χώρες, που έχουν αναπτύξει αλγόριθμους, να μην επιτρέπουν στις εταιρείες, που τους έχουν ενσωματώσει στη λειτουργία των προϊόντων τους, να εξάγουν στην πλήρη έκδοσή τους σε άλλες χώρες, χωρίς την έκδοση σχετικής άδειας.

Μερικοί από τους πλέον διαδεδομένους αλγόριθμους κρυπτογράφησης είναι το **Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard, DES**), ο **3DES (triple DES)** και ο **Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων**

(International Data Encryption Algorithm, IDEA). Οι αλγόριθμοι αυτοί δέχονται ως είσοδο μηνύματα των 64 bits. Εάν το μήνυμα έχει μεγαλύτερο μήκος, θα πρέπει να σπάσει σε τμήματα των 64 bits.

Όπως αναφέραμε η μέθοδος της συμμετρικής κρυπτογράφησης προσφέρει κυρίως εμπιστευτικότητα στην επικοινωνία. Μπορεί να χρησιμοποιηθεί και για την αυθεντικότητα και ακεραιότητα, αλλά όπως θα δούμε στη συνέχεια, υπάρχουν άλλες καλύτερες τεχνικές για τους σκοπού αυτούς. Πρόκληση αποτελεί η συχνή αλλαγή του χρησιμοποιούμενου κλειδιού καθώς, επίσης και η δημιουργία και η διανομή του κλειδιού με χρήση μη έμπιστου δικτύου, όπου ελλοχεύει ο κίνδυνος υποκλοπής του. Γίνονται πάντως προσπάθειες για την ανάπτυξη τεχνικών για διανομή του κλειδιού με χρήση μη έμπιστου δικτύου, με πιο γνωστό τον αλγόριθμο Diffie – Hellman.

- **Ασυμμετρική Κρυπτογράφηση**

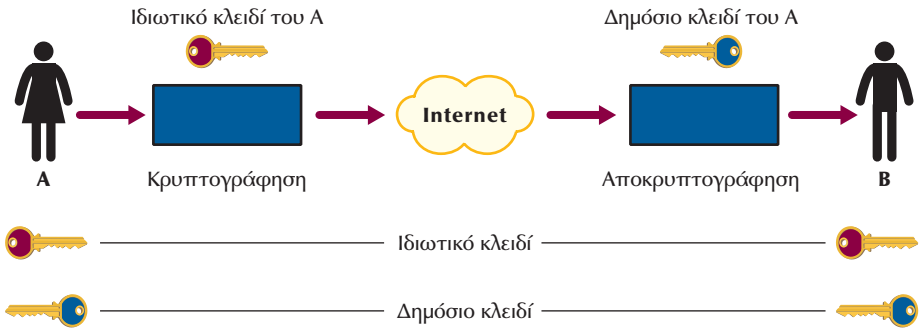
Η ασυμμετρική κρυπτογράφηση αναφέρεται, πολλές φορές, και ως κρυπτογράφηση δημοσίου κλειδιού. Ο μηχανισμός της βασίζεται στην χρήση δύο κλειδιών, ενός δημοσίου κλειδιού και ενός ιδιωτικού. Πρέπει να διευκρινίσουμε, ότι οι αλγόριθμοι ασυμμετρικής κρυπτογράφησης λειτουργούν με τη χρήση δύο διαφορετικών κλειδιών ανά κατεύθυνση και για τον λόγο αυτό ονομάζεται και ασυμμετρική.

Μερικές από τις πιο κοινές χρήσεις της ασυμμετρικής κρυπτογράφησης είναι:

– **η εξασφάλιση εμπιστευτικότητας στη μεταδιδόμενη πληροφορία**

– **η εξασφάλιση αυθεντικότητας**

Για να καταλάβουμε, πως διασφαλίζεται η εμπιστευτικότητα και η αυθεντικότητα με τη χρήση της ασυμμετρικής κρυπτογράφησης, θα αναλύσουμε βήμα προς βήμα την επικοινωνία μεταξύ του Α και του Β.

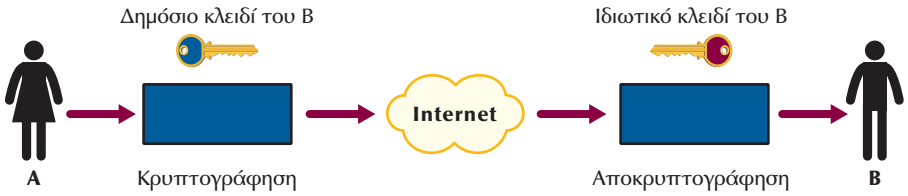


Σχήμα 8-13 Επικοινωνία με χρήση ασυμμετρικής κρυπτογράφησης

Εάν δύο άτομα ο Α και ο Β, θέλουν να επικοινωνήσουν, χρειάζεται πρώτα από όλα να έχει ο καθένας από ένα διαφορετικό ζευγάρι δημόσιο / ιδιωτικό κλειδί.

Επίσης, θα πρέπει ο καθένας να είναι γνώστης του δημοσίου κλειδιού του άλλου. Πρέπει να σημειώσουμε ότι η πληροφορία κρυπτογραφείται με το δημόσιο κλειδί και αποκρυπτογραφείται με το ιδιωτικό ή το αντίστροφο. Εδώ πάλι υπάρχει ζήτημα σχετικά με τον τρόπο, που θα μοιραστούν τα δημόσια κλειδιά πάνω από ένα μη ασφαλές δίκτυο.

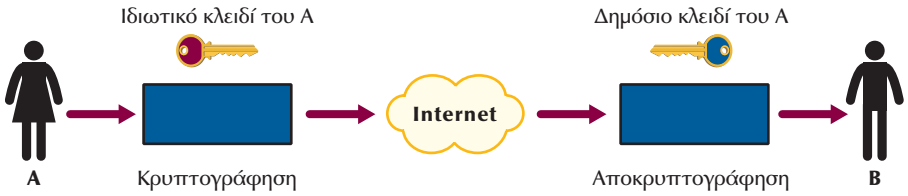
Εάν ο Α θέλει να εξασφαλίσει την εμπιστευτικότητα των δεδομένων, που θα στείλει προς τον Β, δηλαδή να εξασφαλίσει ότι μόνο ο Β θα μπορεί να καταλάβει το περιεχόμενο του μηνύματος, τότε θα κρυπτογραφήσει το μήνυμα, που πρόκειται να μεταδώσει με το δημόσιο κλειδί του Β.



Σχήμα 8-14 Εμπιστευτικότητα Δεδομένων με χρήση δημόσιου κλειδιού

Με τον τρόπο αυτό, έχουμε εξασφαλίσει ότι μόνο ο Β θα μπορέσει να αποκρυπτογραφήσει το μήνυμα κάνοντας χρήση του ιδιωτικού του κλειδιού, που γνώστης του είναι βέβαια μόνο ο Β.

Στη συνέχεια, θα δούμε με ποιόν τρόπο μπορεί να εξασφαλισθεί η αυθεντικότητα στην επικοινωνία μεταξύ του Α και Β. Για παράδειγμα, πως ο Β θα είναι σίγουρος ότι το μήνυμα έχει σταλεί από τον Α και όχι από κάποιον, που προσποιείται ότι είναι ο Α.



Σχήμα 8-15 Αυθεντικοποίηση αποστολέα με χρήση δημόσιου κλειδιού

Εάν ο Α κρυπτογραφήσει το μήνυμα με το ιδιωτικό του κλειδί, τότε ο Β θα μπορέσει να το αποκρυπτογραφήσει κάνοντας χρήση του δημοσίου κλειδιού του Α. Εάν η αποκρυπτογράφηση είναι επιτυχής τότε ο Β ξέρει ότι ο Α είναι αυτός που του έστειλε το μήνυμα, αφού μόνο αυτός έχει το ιδιωτικό κλειδί.

Από όσα έχουμε αναφέρει, γίνεται αντιληπτό, ότι η ασυμμετρική κρυπτογράφηση στηρίζεται στο ότι τα ιδιωτικά κλειδιά είναι γνωστά από τους πραγματικούς τους κατόχους και ότι δεν έχουν διαρρεύσει σε άλλα άτομα. Για να αποφευχθούν προβλήματα κλοπής των κλειδιών, που είναι αποθηκευμένα στα λειτουργικά συστήματα των υπολογιστών, έχουν αναπτυχθεί τεχνικές, που κάνουν χρήση έξυπνων καρτών (smartcard).

Οι μηχανισμοί παραγωγής των ζευγαριών δημοσίου / ιδιωτικού κλειδιού είναι σύνθετοι και οδηγούν στη δημιουργία δύο πολύ μεγάλων τυχαίων αριθμών. Η δημιουργία αυτή απαιτεί μεγάλη υπολογιστική ισχύ και πρέπει να τηρείται η εκπλήρωση αυστηρών μαθηματικών κριτηρίων.

Μερικοί από τους πιο κοινούς αλγόριθμους ασυμμετρικής κρυπτογράφησης είναι οι RSA (Rivest, Shamir, Adelman) και ElGamal.

- **Ψηφιακές υπογραφές**

Η ψηφιακή υπογραφή είναι σύνοψη μηνύματος η οποία προσκολλάται στο τέλος ηλεκτρονικού εγγράφου. Η ψηφιακή υπογραφή χρησιμοποιείται κύρια για την απόδειξη της ταυτότητας του αποστολέα καθώς και για την ακεραιότητα των δεδομένων.

Οι ψηφιακές υπογραφές προκύπτουν από το συνδυασμό αλγόριθμου κατατεμαχισμού και ασυμμετρικής κρυπτογραφίας. Οι αλγόριθμοι κατατεμαχισμού δέχονται συνήθως ως είσοδο μηνύματα τυχαίου μήκους και παράγουν συνόψεις μηνύματος συγκεκριμένου μήκους. Οι πλέον διαδεδομένοι αλγόριθμοι κατατεμαχισμού είναι: **Message Digest 4(MD4), Message Digest 5(MD5)** και **Secure Hash Algorithm (SHA**).

Στη συνέχεια, θα δούμε πως δημιουργείται η ψηφιακή υπογραφή και πως αυτή με τη σειρά της εξασφαλίζει την αυθεντικότητα και την ακεραιότητα, στην επικοινωνία μέσου του δικτύου δύο χρηστών, του Α και Β. Πρώτα από όλα, θα πρέπει οι Α και Β να έχουν συμφωνήσει σε αλγόριθμο δημοσίου κλειδιού (π.χ. τον Digital Signature Standard)και σε αλγόριθμο κατατεμαχισμού (π.χ. MD5). Θα πρέπει, επίσης, να έχουν δημιουργήσει οι Α και Β το ζευγάρι δημόσιου / ιδιωτικού κλειδιού και να ανταλλάξουν τα δημόσια κλειδιά τους. Ας υποθέσουμε, στη συνέχεια, ότι ο Α θέλει να στείλει έγγραφο στον Β κάνοντας χρήση ψηφιακής υπογραφής. Θα πρέπει ο Α να βάλει ως είσοδο στον αλγόριθμο κατατεμαχισμού το έγγραφο και να παράγει το message digest. Στη συνέχεια θα πρέπει να κρυπτογραφήσει το message digest με το ιδιωτικό του κλειδί. Το αποτέλεσμα της κρυπτογράφησης του message digest είναι η ψηφιακή υπογραφή του Α για το συγκεκριμένο έγγραφο και τίθεται στο τέλος του αρχικού εγγράφου. Στη συνέχεια, ο Α θα αποστείλει το αρχικό μήνυ-

μα μαζί με τη ψηφιακή υπογραφή στον Β. Με την σειρά του, ο Β θα πάρει το κρυπτογραφημένο μέρος και θα το αποκρυπτογραφήσει με το δημόσιο κλειδί του Α. Το αποτέλεσμα της αποκρυπτογράφησης είναι το message digest του εγγράφου. Στη συνέχεια, ο Β θα πάρει το αρχικό έγγραφο και θα το περάσει από τον αλγόριθμο κατατεμαχισμού και θα παράγει message digest, το οποίο θα συγκρίνει, εάν είναι το ίδιο με το message digest που προέκυψε από την αποκρυπτογράφηση. Εάν τα δύο message digest είναι ίδια, ο Β μπορεί να είναι σίγουρος, ότι το μήνυμα έχει σταλεί από τον Α αφού μπόρεσε να κάνει αποκρυπτογράφηση με το δημόσιο κλειδί του Α και ότι το έγγραφο δεν έχει υποστεί αλλαγές από τρίτους κατά την αποστολή, αφού τα δύο message digest είναι τα ίδια.

8.3.5 Τεχνολογίες ασφάλειας

Όπως αναφέραμε και στην αρχή της παραγράφου 8.3.4, υπάρχει πληθώρα τεχνικών, που προσπαθούν να εξασφαλίσουν λύσεις για τα βασικά στοιχεία που συνθέτουν πολιτική ασφάλειας. Ταυτόχρονα, στην αγορά κυκλοφορούν πολλά προϊόντα ασφάλειας. Επιγραμματικά θα αναφερθούμε ορισμένες από τις πιο δημοφιλείς λύσεις για την εμπιστευτικότητα των δεδομένων και την πιστοποίηση των χρηστών:

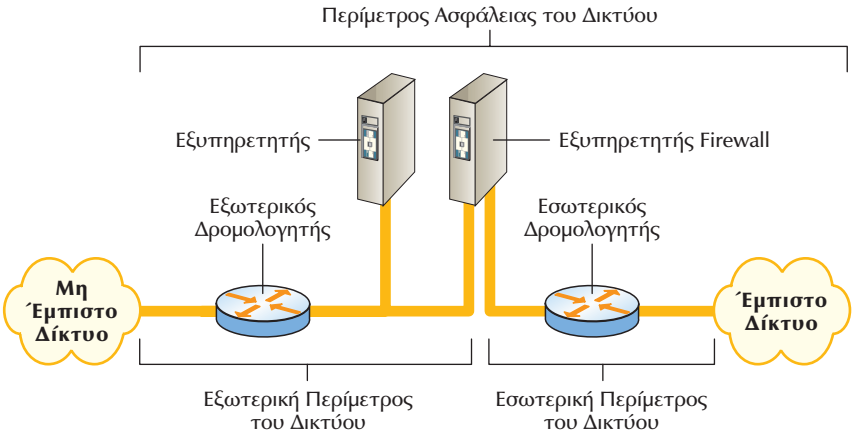
- **Σταθερά passwords και passwords μιας χρήσης για πιστοποίηση χρηστών**
- **SSL / SSH / SOCKS** – συστήματα κρυπτογράφησης δεδομένων για την εξασφάλιση της ακεραιότητας και εμπιστευτικότητας των δεδομένων
- **Radius / Tacacs** – συστήματα για πιστοποίηση dial up χρηστών και εκχώρηση συγκεκριμένων δικαιωμάτων
- **PAP / CHAP** – συστήματα για πιστοποίηση δικτυακών συσκευών αλλά όχι χρηστών σε συνδέσεις point to point
- **Single Sign On** – βασίζεται σε πιστοποιήσεις ενός παράγοντα. Είναι συνήθως, λιγότερο ασφαλές από τη χρήση πολλαπλών passwords
- **Κέρβερος** – κρυπτογράφηση για τη διασφάλιση της εμπιστευτικότητας των δεδομένων και πιστοποίηση χρηστών
- **IPSec (IP Security)** – Το Internet Protocol Security είναι αναπτυσσόμενο πρότυπο για ασφάλεια στο επίπεδο του δικτύου. Προηγούμενες προσεγγίσεις ασφάλειας εστιάζονταν στο επίπεδο της εφαρμογής με βάση το OSI μοντέλο. Το IPSec παρέχει δύο επιλογές ασφάλειας:

– Αυθεντικότητα της Επικεφαλίδας των Ip πακέτων (Authentication Header – AH), όπου παρέχεται η δυνατότητα αυθεντικοποίησης του αποστολέα των πακέτων

– ESP (Encapsulation Security Payload), όπου υποστηρίζει την αυθεντικότητα τόσο της επικεφαλίδας των πακέτων όσο και των δεδομένων.

Το IPSec είναι ιδιαίτερα χρήσιμο για δίκτυα VPN καθώς επίσης και για χρήστες που συνδέονται στο δίκτυό με χρήση επιλεγόμενων τηλεφωνικών γραμμών.

- **Firewall** – Με την έννοια Firewall αναφερόμαστε στο σύνολο των προγραμμάτων / φίλτρων, που έχουμε εγκαταστήσει σε πύλες (σημεία σύνδεσης) του εσωτερικού μας δικτύου με άλλα δίκτυα, π.χ το Internet ή άλλο ιδιωτικό / δημόσιο δίκτυο, που δεν ελέγχονται από εμάς. Οι συσκευές που εγκαθίστανται τα προγράμματα / φίλτρα και συνθέτουν ένα Firewall, είναι δρομολογητές και εξυπηρετητές ειδικοί για τον σκοπό αυτόν.



Σχήμα 8-16 Παράδειγμα δικτύου με χρήση firewall

Στο παραπάνω Σχήμα 8-16 βλέπουμε διαχωρισμό του εσωτερικού δικτύου επιχείρησης με τα υπόλοιπα δίκτυα με την βοήθεια αρχιτεκτονικής βασισμένης σε δρομολογητές και εξυπηρετητές. Οι χρήστες, που βρίσκονται στο τμήμα του δικτύου ευρείας περιοχής πίσω από τον εσωτερικό δρομολογητή, θεωρούμε, ότι ανήκουν στο λεγόμενο έμπιστο δίκτυο αφού συνδέονται άμεσα σε δομή που ελέγχεται, διαχειρίζεται και γενικότερα διέπεται από κανόνες ασφάλειας, που καθορίζονται πλήρως από την επιχείρηση, που κατέχει το δίκτυο. Αντίθετα, το τμήμα του δικτύου ευρείας περιοχής, που συνδέεται στον εξωτερικό δρομολογητή ονομάζεται μη έμπιστο δίκτυο. Η επιχείρηση δεν διαχειρίζεται χρήστες, που ανήκουν στο μη έμπιστο δίκτυο, δηλαδή δεν διέπονται από τις ίδιες διαδικασίες ελέγχου αυθεντικότητας με τους χρήστες του εσωτερικού δικτύου.

Στην παραπάνω τοπολογία, το firewall δημιουργείται από φίλτρα στους δύο δρομολογητές καθώς και από προγράμματα στον firewall server.

Με τους κανόνες, που έχουμε επιβάλει στο firewall, μπορούμε να επιτρέψουμε την πρόσβαση από τα μη έμπιστα δίκτυα προς συγκεκριμένους εξυπηρετη-

τές του εσωτερικού μας δικτύου, καθώς επίσης και το είδος των εφαρμογών, που επιτρέπεται να χρησιμοποιήσουν οι μη έμπιστοι χρήστες, για να συνδεθούν σε αυτούς. Για παράδειγμα μπορούμε να επιτρέψουμε πρόσβαση σε συγκεκριμένες IP διευθύνσεις του εσωτερικού δικτύου και με συγκεκριμένα πρωτόκολλα, όπως HTTP, ενώ προσπάθειες σύνδεσης με άλλα πρωτόκολλα όπως telnet, ftp, tftp rlogin κ.λ.π να απορρίπτονται από το firewall. Το φιλτράρισμα των πρωτοκόλλων γίνεται με βάση τον αριθμό πόρτας που χρησιμοποιούν στην TCP/IP δομή. Στη συνέχεια, το firewall εξετάζει τις επικεφαλίδες των πακέτων από τα μη έμπιστα δίκτυα προς τα έμπιστο δίκτυο, ανιχνεύοντας και απορρίπτοντας άμεσα τα πακέτα με προορισμούς προς απαγορευμένες TCP πόρτες και IP διευθύνσεις. Υπάρχουν αρκετές αρχιτεκτονικές στην τοπολογία διασύνδεσης δρομολογητών και εξυπηρετητών, που συνθέτουν ένα firewall. Ανάλογα με την πολυπλοκότητα της τοπολογίας τόσο πιο δύσκολη είναι η παραβίαση της ασφάλειας του εσωτερικού δικτύου επιχείρησης.

8.3.6 Αποφυγή καταστροφών

Κάθε επιχείρηση που έχει αναπτύξει πληροφοριακό σύστημα και βασίζει την λειτουργία της στην εύρυθμη και απρόσκοπτη λειτουργία του πληροφοριακού συστήματός της, θα πρέπει να είναι σε ετοιμότητα να αντιμετωπίσει προβλήματα μικρά ή μεγάλα, που πιθανόν θα προκύψουν.

Τα προβλήματα ενός μοντέρνου και κατανεμημένου πληροφοριακού συστήματος δεν περιορίζονται μόνο στις βλάβες του ενεργού ή παθητικού εξοπλισμού, αλλά συμπεριλαμβάνουν και δυσλειτουργίες των λειτουργικών συστημάτων, των πρωτοκόλλων επικοινωνίας καθώς και των ίδιων των δεδομένων. Τα προβλήματα μπορεί να προέρχονται από συνηθισμένες αστοχίες του εξοπλισμού ενεργού ή παθητικού (π.χ αστοχία σκληρού δίσκου, κάψιμο τροφοδοτικού), από κακές ρυθμίσεις – προγραμματισμούς, από εγγενείς δυσλειτουργίες του εξοπλισμού ή λογισμικού (π.χ bugs), από φυσικές καταστροφές (π.χ πλημμύρες, σεισμούς) αλλά και από κακόβουλες ενέργειες (π.χ επιθέσεις από χάκερ, ή τρομοκρατικές επιθέσεις). Μια επιχείρηση, που σέβεται τους πελάτες της αλλά και το όνομα της, θα πρέπει να είναι σε θέση να αντεπεξέλθει στα προβλήματα, ανεξάρτητα από το μέγεθος και την προέλευση τους, στον ελάχιστο δυνατό χρόνο και με τις λιγότερες συνέπειες, τόσο για την ίδια την εταιρεία όσο και για τους πελάτες της. Για παράδειγμα φανταστείτε τι πλήγμα είναι για την αξιοπιστία μίας τράπεζας ή μιας χρηματιστηριακής εταιρείας η μη εξυπηρέτηση των πελατών της, λόγω τεχνικών προβλημάτων για μεγάλο χρονικό διάστημα. Από όλα όσα έχουμε αναφέρει, οδηγούμαστε στο συμπέρασμα, ότι είναι απαραίτητη η ύπαρξη σχεδίων αποφυγής καταστροφών.

Στο σημείο αυτό, θα αναφερθούμε σε κάποιες έννοιες που σχετίζονται άμεσα με το σχεδιασμό της αποφυγής καταστροφών πληροφοριακού συστήματος:

- **Ανάκαμψη (Recovery)** – Η αποκατάσταση της λειτουργίας πληροφοριακού συστήματος σε επιθυμητό επίπεδο μετά από κάποιο δυσλειτουργία.
- **Σχέδιο Συνέχειας (Continuity Plan)** –Η σαφής και πλήρης περιγραφή των ενεργειών που θα πραγματοποιηθούν, ώστε να επιτευχθεί ανάκαμψη μετά από σοβαρή παραβίαση.
- **Εφεδρικό Αντίγραφο Πληροφοριών (Information back up**) –Η τήρηση αντιγράφου των πληροφοριών, που θα μπορεί να χρησιμοποιηθεί, για να επιτευχθεί ανάκαμψη. Θα μπορούσαμε να συμπεράνουμε ότι απαίτηση για ανάκαμψη πληροφοριακού συστήματος σε μηδέν χρόνο, δηλαδή στην ουσία να μην σταματά ποτέ η λειτουργία του, συνεπάγεται κλωνοποίηση δομής του δικτύου δύο ή ίσως και παραπάνω φορές. Αυτό, όσο και να φαίνεται υπερβολικό, συμβαίνει σε επιχειρήσεις, που βασίζουν την παροχή υπηρεσιών σε πελάτες εξολοκλήρου στο πληροφοριακό τους σύστημα. Αυτό, βέβαια, συνεπάγεται για την επιχείρηση πολύ υψηλό κόστος εγκατάστασης, λειτουργίας και συντήρησης.

Μια επιχείρηση πρέπει να προβεί στη διαβάθμιση της κρισιμότητας των επιμέρους στοιχείων, που συνθέτουν το πληροφοριακό της σύστημα. Με βάση την ανάλυση των κινδύνων που θα προκύψουν, σε περίπτωση καταστροφής κάποιων βαθμίδων του πληροφοριακού συστήματος, θα πρέπει να ληφθούν και τα αντίστοιχα μέτρα προστασίας. Τα περισσότερα πληροφοριακά συστήματα, σήμερα, είναι κατανεμημένα και οι εφαρμογές τους κάνουν χρήση της αρχιτεκτονικής client – server. Στις περιπτώσεις αυτές, το κτίριο με τον κεντρικό υπολογιστή (main site) αποτελεί το πιο κρίσιμο σημείο του συστήματος. Για το λόγο αυτό υπάρχουν πολλοί οργανισμοί που έχουν υλοποιήσει δύο κεντρικά sites, έτσι ώστε σε περίπτωση καταστροφής του ενός αυτόματα να αναλάβει το δεύτερο. Η ύπαρξη δύο site προϋποθέτει δύο κεντρικά σχεδόν ισοδύναμα υπολογιστικά συστήματα, καθώς και την κατάλληλη τηλεπικοινωνιακή υποδομή για την πρόσβαση των διαφόρων κατανεμημένων σημείων με τα δύο κεντρικά site. Επίσης, τα κεντρικά site θα πρέπει να περιλαμβάνουν πρόβλεψη για επαλληλία των κεντρικών switches, routers καθώς και εναλλακτικότητα στη διασύνδεση των διαφόρων εσωτερικών LAN. Βέβαια πέρα από τις προβλέψεις για την εναλλακτικότητα της δικτυακής υποδομής, θα πρέπει να έχουν καταστρωθεί και σχέδια για αντίστοιχες εφεδρικές λύσεις τόσο για τη τα συστήματα εξοπλισμού του πληροφοριακού συστήματος όσο και για τις εφαρμογές και τα δεδομένα (π.χ. την πολιτική των back up).

Γενικά, δεν υπάρχει καθιερωμένη συνταγή, για τη μορφή σχέδιου αποφυγής καταστροφών για μια επιχείρηση, αφού αυτό ποικίλει με βάση τη δομή του πληροφοριακού συστήματος, τη σπουδαιότητά του καθώς και το χρηματικό ποσό, που είναι διατεθειμένη να ξοδέψει η επιχείρηση. Το σίγουρο είναι ότι πρόκειται για πολύ σοβαρό έργο, η αναβολή ή ο κακός σχεδιασμός του οποίου μπορεί να αποδειχθεί μοιραίο κάποια στιγμή για την ίδια την επιχείρηση.

ΑΝΑΚΕΦΑΛΑΙΩΣΗ

Στο κεφάλαιο αυτό παρουσιάσθηκαν θέματα σχετικά, με τη διαχείριση των συστημάτων, καθώς και με την ασφάλεια τους. Αρχικά, παρουσιάσθηκαν οι πέντε περιοχές, που πρέπει να καλύπτει η πλήρης διαχείριση κατανεμημένου πληροφοριακού συστήματος. Στη συνέχεια, έγινε παρουσίαση των δύο σημαντικότερων μοντέλων διαχείρισης, του **CMIP** και του **SNMP**. Μεγαλύτερη έμφαση δόθηκε στο μοντέλο **SNMP**, που είναι το πιο διαδεδομένο. Επίσης, έγινε ανάλυση του τρόπου δόμησης της διαχειριζόμενης πληροφορίας στη δομή του **MIB**. Αναφορά έγινε στη διαχειριζόμενη πληροφορία που παρέχεται από τα πρότυπα **MIB II**, **RMON** και **RMON2**.

Μετά την παρουσίαση των θεμάτων, που αφορούν τη διαχείριση των πληροφοριακών συστημάτων, ακολούθησε η παρουσίαση των θεμάτων ασφάλειας αυτών.

Στην αρχή έγινε ανάλυση των εννοιών, που αφορούν την ασφάλεια γενικότερα. Στη συνέχεια, έγινε επεξήγηση της ορολογίας που χρησιμοποιείται στις τεχνικές ασφάλειας. Μετά, ακολούθησε παρουσίαση των σημαντικότερων μεθόδων, που υπάρχουν, προκειμένου να παραβιασθεί η ασφάλεια των πληροφοριακών συστημάτων. Ακολούθως έγινε επεξήγηση των βασικότερων μεθόδων για την εξασφάλιση της αυθεντικότητας και ακεραιότητας της μεταδιδόμενης πληροφορίας σε δίκτυο υπολογιστών. Μετά αναφέρθηκαν οι πιο διαδεδομένες τεχνολογίες για την εξασφάλιση της ασφάλειας, και αναφέρθηκε πιο τμήμα καλύπτει η κάθε τεχνολογία. Τέλος, αναλύθηκε η κρισιμότητα της πρόβλεψης και υλοποίησης αποφυγής καταστροφών στα πληροφοριακά συστήματα.

Ερωτήσεις – Ασκήσεις

1. Αναφέρατε τις πέντε περιοχές που καλύπτει η διαχείριση δικτύου, καθώς και λεπτομέρειες για την κάθε περιοχή.
2. Ποια είναι η αλληλουχία των SNMP εντολών μεταξύ του σταθμού διαχείρισης και διαχειριζόμενου agent για το διάβασμα μεταβλητής του MIB και στη συνέχεια αλλαγής της τιμής του.
3. Σε τι χρειάζονται τα communities στο SNMP;
4. Με ποιο τρόπο μπορούμε να αποτρέψουμε τη διαχείριση των agents από σταθμούς που προσπαθούν να διαχειριστούν τους agents με χρήση του σωστού community name, αλλά στην πραγματικότητα δεν είναι οι πραγματικοί managers;
5. Ποιο γκρουπ του RMON δίνει πληροφορίες και για τα εφτά επίπεδα του μοντέλου OSI;

6. Περιγράψτε με δικά σας λόγια τις έννοιες: αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα και εγκυρότητα.
7. Ποιοι μπορεί να είναι οι λόγοι, για τους οποίους αρκετές φορές δεν λαμβάνουμε μέτρα ασφάλειας για όλους τους πιθανούς κινδύνους, που αντιμετωπίζει το πληροφοριακό μας σύστημα;
8. Αναφέρατε τους τρόπους που μπορεί να γίνει αποκάλυψη των σταθερών passwords, που χρησιμοποιούνται για την πρόσβαση στα συστήματα.
9. Ποια μέθοδος εξασφαλίζει καλύτερα την αυθεντικότητα των μηνυμάτων:
   α) η συμμετρική κρυπτογράφηση.
   β) η ασυμμετρική κρυπτογράφηση.
10. Τι εννοούμε με τον όρο εικονικά ιδιωτικά δίκτυα;
11. Τι ρόλο αναλαμβάνει ο firewall μέσα σε δίκτυο και σε ποια σημεία του δικτύου μας συνήθως τον τοποθετούμε;
12. Αναφέρατε ενδεικτικά μέτρα στο δικτυακό – τηλεπικοινωνιακό εξοπλισμό για την αποφυγή καταστροφών κατανεμημένου πληροφοριακού συστήματος.

Βιβλιογραφία

1. Αλεξόπουλος Α., Λαγογιάννης Γ., *Τηλεπικοινωνίες και Δίκτυα Υπολογιστών*, 1997.
2. Γκρίτζαλης Δ., Τμ. Πληροφορικής Οικονομικό Παν/μιο Αθηνών, Επιτροπή των Ευρωπαϊκών Κοινοτήτων,Αθήνα 1996, *Ασφάλεια στις Τεχνολογίες Πληροφοριών & Επικοινωνιών*.
3. ΕΠΥ 1995, *Ασφάλεια Πληροφοριών Τεχνικά Νομικά & Κοινωνικά Θέματα*.
4. Breyer Robert and Riley Sean, *Switched and Fast Ethernet*: *How It Works and How to Use It, Ziff*– Davis Press 1995.
5. Brown Steven, *Implementing Virtual Private Networks,* McGraw Hill, 1999.
6. Doraswamy Naganand, Harkins Dan, *IPSec The New Security Standard for the Internet,* Intranets, Virtual Private Networks, PTR PH,1999.
7. Manuals, *White papers και Tutorials από site εταιρειών δικτυακών προϊόντων,* όπως:
   α) Cisco: www.cisco.com
   β) Nortel: http://www.nortelnetworks.com/
   γ) Lucent: www.lucent.com
   δ) Cabletron: www.cabletron.com
   ε) Rad: www.rad.com
   στ) 3Com: www.3com.com
8. Tanebaum A., *Computer Networks,* Prentice Hall, 1994.