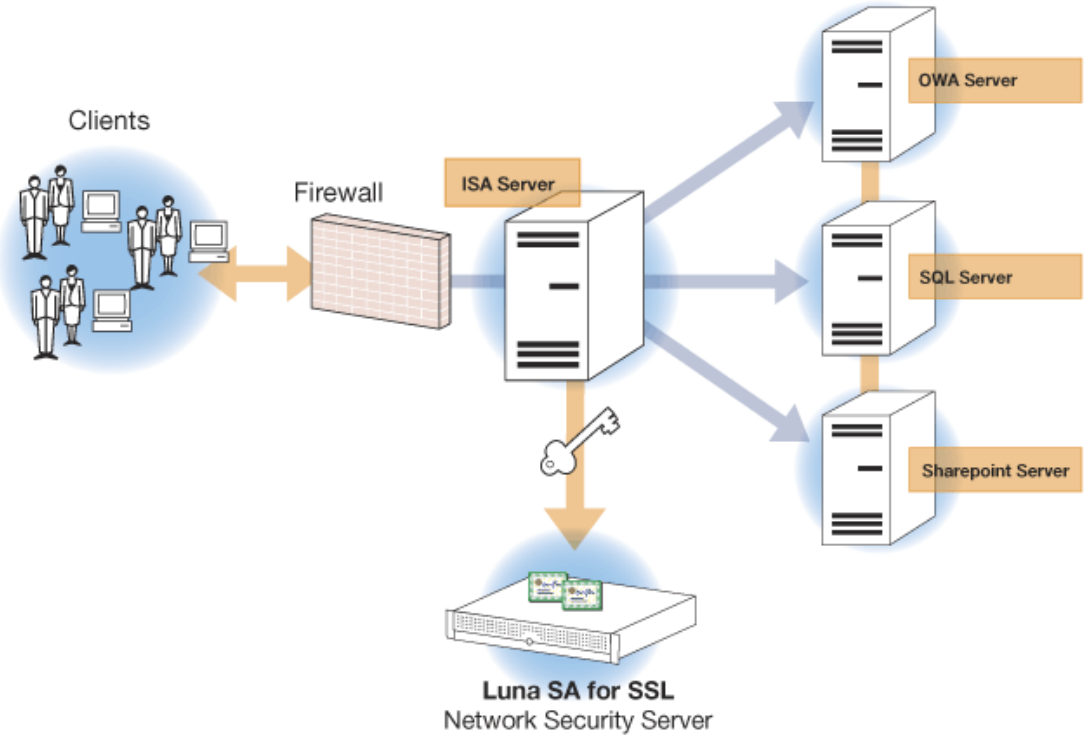
ΤΕΙ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ




# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ: ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΣΠΟΥΔΑΣΤΕΣ:
ΜΑΝΤΖΙΟΣ ΙΩΑΝΝΗΣ
ΜΠΑΝΤΙΑΣ ΣΠΥΡΙΔΩΝ

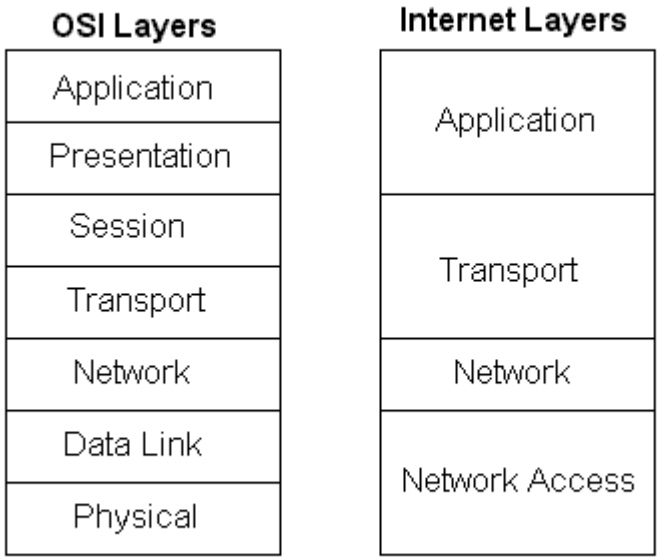
Περιεχόμενα

# 1. Σύντομη Αναφορά στο Διαδίκτυο

## *1.1 Εισαγωγή*

Η επικοινωνία δεδομένων έχει αναχθεί σε πρωταρχικής σημασίας κομμάτι της πληροφορικής. Δίκτυα εγκατεστημένα σε όλο το κόσμο, χρησιμοποιούνται για την συλλογή και διανομή δεδομένων πάνω σε ποικίλα θέματα. Από καιρό έχει κατανοηθεί η αναγκαιότητα διασύνδεσης όλων αυτών των επιμέρους δικτύων σε ένα ευρύτερο σύνολο, διευκολύνοντας και επιταχύνοντας την επικοινωνία. Οι προσπάθειες της κατασκευής αυτού του υπέρ – δικτύου ήταν επιτυχημένες και το αποτέλεσμα ήταν αυτό που σήμερα ξέρούμε σαν *Internet*. Το Internet (ή Διαδίκτυο) παρουσιάζει μεγάλη αποδοχή, πράγμα που οδηγεί στην συνεχή εξέλιξη και αναδιαμόρφωση του.

Ένα από τα μεγαλύτερα προβλήματα που έπρεπε να λυθούν ώστε το Διαδίκτυο να γίνει πραγματικότητα, ήταν η ύπαρξη πολλών τεχνολογιών δικτύων, καθεμιά από τις οποίες εξυπηρετεί μια συγκεκριμένη ομάδα ανθρώπων. Οι χρήστες του δικτύου διαλέγουν την τεχνολογία που είναι κατάλληλη για τις επικοινωνιακές τους ανάγκες. Η χρήση μίας και μόνο τεχνολογίας για την δημιουργία ενός παγκόσμιου δικτύου είναι αδύνατη, γιατί δεν υπάρχει τεχνολογία που να ικανοποιεί όλες τις απαιτήσεις. Για παράδειγμα, μερικοί χρήστες χρειάζονται δίκτυα υψηλών ταχυτήτων που καλύπτουν μικρές αποστάσεις. Για άλλους πάλι, πιο εξαπλωμένα δίκτυα, χαμηλών ταχυτήτων είναι πιο χρήσιμα.




Το Διαδίκτυο, παρ' όλα αυτά, καταφέρνει να συνενώσει όλες αυτές τις διαφορετικές τεχνολογίες, παρέχοντας ένα σύνολο συμβάσεων. Κρύβει τις λεπτομέρειες της υποκείμενης δικτυακής τεχνολογίας και επιτρέπει σε υπολογιστές από όλο τον κόσμο να βρίσκονται σε επαφή ανεξάρτητα από το δίκτυο στο οποίο συνδέονται. Το Διαδίκτυο βασίζεται σε μια συλλογή από τυποποιήσεις που καλούνται *πρωτόκολλα*.

Τα πρωτόκολλα (π.χ. TCP και IP) παρέχουν τους κανόνες για την επικοινωνία. Περιέχουν τις λεπτομέρειες των ανταλλασσόμενων μηνυμάτων, περιγράφουν πως ανταποκρίνεται ο υπολογιστής όταν λαμβάνει κάποιο μήνυμα και ορίζει πως διαχειρίζεται ο υπολογιστής της καταστάσεις λάθους. Κατά μία έννοια, τα πρωτόκολλα είναι για την επικοινωνία ότι είναι οι αλγόριθμοι για τον προγραμματισμό. Ένας αλγόριθμος επιτρέπει την κατανόηση της λογικής του προγράμματος, χωρίς να χρειάζεται να ξέρει την δομή και κατασκευή της CPU. Ομοίως, ένα πρωτόκολλο επιτρέπει στον χρήστη να καταλάβει τα δεδομένα μιας χωρίς να έχει γνώση του δικτυακού υλικού.

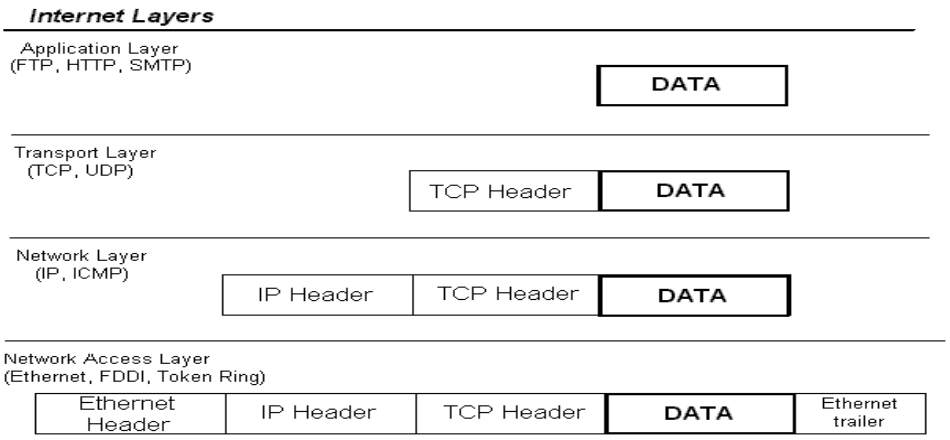
## *1.2 Αρχιτεκτονική του Διαδικτύου*

Το Διαδίκτυο αποτελεί παράδειγμα συστήματος τύπου *open system interconnection*. Καλείται ανοιχτό σύστημα *(open system)*, γιατί σε αντίθεση με προηγούμενα επικοινωνιακά συστήματα ανεπτυγμένα από ιδιωτικές εταιρίες, η περιγραφή του είναι δημόσια διαθέσιμη. Έτσι, οποιοσδήποτε μπορεί να γράψει λογισμικό που να συμβαδίζει με τις προδιαγραφές του συστήματος.

Σαν τέτοιο σύστημα, το Διαδίκτυο μπορεί να συγκριθεί με το μοντέλο *OSI (Open System Interconnection)*. Στο παραπάνω σχήμα βλέπουμε την δομή του Διαδικτύου σε σχέση με την αντίστοιχη δομή του OSI μοντέλου. Παρατηρούμε πως η αρχιτεκτονική του Διαδικτύου έχει λιγότερα επίπεδα από αυτή του OSI και τα δεδομένα από το επίπεδο εφαρμογής *(application)* ως το επίπεδο φυσικής πρόσβασης *(network access).*

Στο επίπεδο της φυσικής πρόσβασης *(network access)* ανήκουν τα πρωτόκολλα LAN όπως Ethernet, Token Ring, FDDI και πρωτόκολλα WAN όπως X.25, Frame Relay, SLIP, PPP που επιτρέπουν την φυσική διασύνδεση, την πρόσβαση στο μέσο και τον έλεγχο της ζεύξης.

Στο επίπεδο δικτύου *(network)* χρησιμοποιείται το πρωτόκολλο IP, του οποίου τα πακέτα δρομολογούνται με ειδικές συσκευές, τους δρομολογητές *(routers)*.Στο επίπεδο μεταφορά *(transport)* χρησιμοποιείται το πρωτόκολλο TCP και δευτερευόντως το UDP.




Στο επίπεδο εφαρμογών *(application)* ανήκουν μεταξύ άλλων και τα πρωτόκολλα FTP, Telnet, SMTP, HTTP για την παροχή διάφορων υπηρεσιών όπως την μεταφορά αρχείων, την πρόσβαση σε υπολογιστές, ηλεκτρονικό ταχυδρομείο και το Web.

# 2. Εισαγωγή στην Ασφάλεια

## *2.1 Υπηρεσίες Ασφάλειας*

Στο σημερινό κόσμο της διαδικτύωσης και του ηλεκτρονικού εμπορίου κάθε υπολογιστικό σύστημα είναι ένας πιθανός στόχος. Σπάνια περνάει ένας μήνας χωρίς ειδήσεις που να αφορούν την "κατάληψη" και το "τρύπημα" των υπολογιστικών συστημάτων μεγάλων εταιριών και οργανισμών. Αν και λέγεται, από ορισμένους hackers, ότι τέτοιες επιθέσεις αποτελούν παιχνίδια κάποιων εφήβων το φαινόμενο έχει γίνει πιο μεθοδικό και απειλητικό τα τελευταία χρόνια.

Ακόμα και αν τίποτα δεν αλλάξει ή τίποτα δεν αφαιρεθεί οι διαχειριστές των συστημάτων πρέπει να ξοδεύουν ώρες ατελείωτες για την επανεγκατάσταση και επαναρύθμιση ενός τρυπημένου συστήματος για να είναι φτάσουν πάλι σε ένα ικανοποιητικό επίπεδο εμπιστοσύνης προς αυτό. Δεν υπάρχει κανένας τρόπος να γνωρίζουμε τα κίνητρα του εισβολέα και έτσι πρέπει να υποθέτουμε το χειρότερο.

Πολλοί διαφορετικοί τύποι ανθρώπων μπαίνουν σε υπολογιστικά συστήματα τρυπώντας την ασφάλειά τους. Άλλοι το κάνουν για πλάκα και άλλοι αποσκοπώντας σε κάποιο κέρδος. Υπάρχουν επίσης στοιχεία οργανωμένου εγκλήματος και κατασκοπευτικής δράσης οδηγούμενα από κυβερνήσεις, οργανισμούς, εταιρίες ή και τρομοκρατικές ομάδες. Οι πιο επικίνδυνοι από όλους, για κάποιο δίκτυο, είναι οι νυν και πρώην χρήστες του ίδιου του δικτύου διότι αυτοί γνωρίζουν τα συστήματα ασφάλειας και το που πρέπει να χτυπήσουν ώστε να προκαλέσουν ζημιά.

Παρά την ύπαρξη όλων αυτών των κινδύνων το ενδιαφέρον για τη δικτύωση των υπολογιστικών συστημάτων και για το Internet δεν υπήρξε ποτέ μεγαλύτερο. Ο

αριθμός των υπολογιστών στο Internet διπλασιάζεται κάθε χρόνο για μια δεκαετία τώρα.

Όροι όπως ασφάλεια, προστασία και διασφάλιση του απορρήτου έχουν αποκτήσει παραπάνω από μία έννοιες. Ακόμα και οι επαγγελματίες του είδους δεν μπορούν να συμφωνήσουν στην ουσία αυτών των όρων. Μπορούμε, ωστόσο, να χρησιμοποιήσουμε μια πρακτική προσέγγιση και να πούμε ότι:

"ασφάλεια υπολογιστικού συστήματος έχουμε όταν μπορούμε να βασιστούμε σε αυτό και στο λογισμικό του να συμπεριφερθεί όπως περιμένουμε από αυτό".

# *3.Κρυπτογράφηση*

## *3.1Εισαγωγή*

Στο προηγούμενο κεφάλαιο παρουσιάσαμε και αναλύσαμε όλες τις έννοιες που περιλαμβάνει ο όρος "ασφάλεια". Ερευνήσαμε, λοιπόν, τις βασικές υπηρεσίες της ασφάλειας που είναι η ακεραιότητα των δεδομένων, η απόρρητη συναλλαγή, η πιστοποίηση ταυτότητας και η εγκεκριμένη πρόσβαση. Υπάρχουν δύο βασικά εργαλεία για την παροχή αυτών των υπηρεσιών της ασφάλειας: η κρυπτογραφία και η στεγανογραφία.

Η κρυπτογραφία αναφέρεται στην υλοποίηση μεθόδων τροποποίησης των μεταδιδομένων πληροφοριών, έτσι ώστε να γίνονται κατανοητά μόνο από τον προβλεπόμενο παραλήπτη ή παραλήπτες. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software. Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε hardware επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους. Το γεγονός ότι ο χρήστης δεν ανακατεύεται καθόλου στις διαδικασίες της κρυπτογραφίας, αυξάνει την αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Παρ' όλα αυτά, δεν έχει καθιερωθεί η κρυπτογραφία σε hardware λόγω του υψηλού κόστους της, που απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της. Τα ειδικά αυτά μηχανήματα βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου.

Η λογισμική κρυπτογραφία είναι φτηνότερη, πράγμα που την κάνει ευρέως αποδεκτή και εύκολα πραγματοποιήσιμη. Βέβαια, δεν είναι το ίδιο γρήγορη με την εκτέλεση της σε hardware, αλλά η ολοένα αυξανόμενη ανάγκη για διασφάλιση των επικοινωνιών εδραίωσε την χρήση της. Εμείς, στις ακόλουθες σελίδες θα συζητήσουμε αποκλειστικά για την λογισμική κρυπτογραφία.

Στεγανογραφία είναι η τεχνική της απόκρυψης της ίδιας της ύπαρξης της πληροφορίας. Όπως για την κρυπτογραφία, έτσι και για την στεγανογραφία υπάρχουν

δύο τρόποι υλοποίησης της: σε hardware και σε software. Η hardware εκτέλεση της είναι γρήγορη, αλλά πάρα πολύ ακριβή. Χρησιμοποιείται περισσότερο από κυβερνητικές υπηρεσίες και από τον στρατό, καθ' ότι οι τεχνολογίες που χρησιμοποιούνται είναι πολύ ανεπτυγμένες και καθόλου διαδεδομένες. Η εκτέλεση της σε software είναι πιο φθηνή και οι τεχνολογίες που απαιτούνται είναι σαφώς πιο εμπορικές. Στο Διαδίκτυο συναντάται η λογισμική στεγανογραφία για ευνόητους λόγους. Γι' αυτό το λόγο, θα σχολιάσουμε επί το πλείστον την λογισμική κρυπτογραφία στο υπόλοιπο κεφάλαιο.

## *3.2 Κρυπτογραφία*

Κρυπτογραφία *(cryptography)* είναι η μελέτη τεχνικών *cryptanalysis)* είναι η επίλυση αυτών των προβλημάτων και κρυπτολογία *(cryptology)* είναι ο συνδυασμός της κρυπτογραφίας και κρυπτολογίας σε ένα ενιαίο επιστημονικό κλάδο.

Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση. Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Σκοπός της κρυπτογράφησης είναι να εξασφάλιση το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά.

Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, όπως είπαμε, την χρήση κάποιας μυστικής πληροφορίας, το κλειδί. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν.

Στις μέρες μας κρυπτογραφία δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Εκτός από την διασφάλιση του απόρρητου *(privacy)*, η πιστοποίηση ταυτότητας *(authen*tication) είναι άλλη μία έννοια που έχει γίνει μέρος της ζωής μας. Πιστοποιούμε την ταυτότητα μας καθημερινά και ανεπαίσθητα, για παράδειγμα όταν υπογράφουμε ένα έγγραφο, όταν δείχνουμε την ταυτότητα μας. Καθώς ο κόσμος εξελίσσεται σε ένα περιβάλλον που όλες οι αποφάσεις και οι συναλλαγές θα γίνονται ηλεκτρονικά, χρειαζόμαστε ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας.

Η κρυπτογραφία παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι όσοι είναι σε θέση να το αναγνώσουν να είναι σίγουρη για το ποιος το έχει γράψει. Επίσης, μία ψηφιακή χρονοσφραγίδα *(digital timestamp)* συνδέει ένα έγγραφο με την ώρα της δημιουργίας του. Τέτοιο μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλής συναλλαγές μέσω του Διαδικτύου ή ακόμα και για σύνδεση με καλωδιακή τηλεόραση.

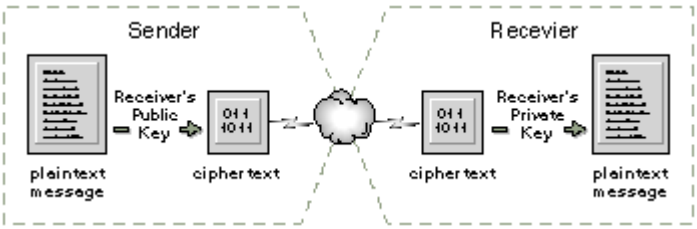
### 3.2.1 Είδη Κρυπτογραφίας

#### Ασύμμετρη Κρυπτογραφία *(Public-Key Cryptography)*

Η ασύμμετρη κρυπτογραφία χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσια κλείδα και το άλλο καλείται ιδιωτική κλείδα. Η δημόσια κλείδα δημοσιοποιείται, ενώ η ιδιωτική κλείδα κρατείται μυστική. Η ιδιωτική κλείδα δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στην δημόσια κλείδα. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών.

Η ιδιωτική κλείδα είναι μαθηματικά συνδεδεμένη με την δημόσια κλείδα. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας την ιδιωτική κλείδα από την δημόσια. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνο που γνωρίζει την ιδιωτική κλείδα.

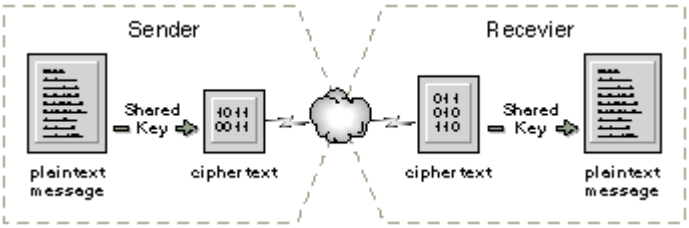



Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

## Συμμετρική Κρυπτογραφία (Symmetric Cryptography ή Secret-Key Cryptography)

Στην συνηθισμένη κρυπτογραφία, ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτή η μέθοδος

καλείται συμμετρική κρυπτογραφία ή κρυπτογραφία μυστικού κλειδιού. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας. Μία τέτοια τεχνική είναι η *Message Authentication Code (MAC)*.




Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

## Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέραμε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" σ το δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση της ιδιωτική του κλείδας και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος

ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής *(non-repudiation)*. Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς *(Certificate Authority)* ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στις περιπτώσεις που οι χρήστες μπορούν να συναντηθούν και να ανταλλάξουν τα κλειδιά ή όταν η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους.

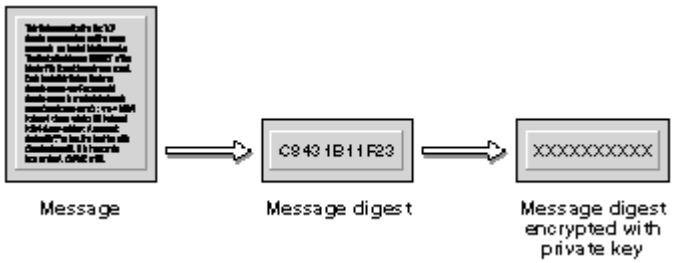
## *3.3 Απλές Εφαρμογές της Κρυπτογραφίας*

### 3.3.1 Διαφύλαξη του Απορρήτου και Κρυπτογράφηση

Η πιο φανερή εφαρμογή της κρυπτογραφίας είναι η εξασφάλιση του απορρήτου *(privacy)* μέσω της κρυπτογράφησης. Οι ευαίσθητες πληροφορίες κρυπτογραφούνται με κατάλληλο αλγόριθμο που εξαρτάται από τις ανάγκες της επικοινωνίας. Για να μπορέσει κάποιος να επαναφέρει τα κρυπτογραφημένα δεδομένα στην αρχική τους μορφή πρέπει να κατέχει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση τους, εάν μιλάμε για συμμετρική κρυπτογράφηση ή την ιδιωτική κλείδα που αντιστοιχεί στην δημόσια κλείδα που το κρυπτογράφησε, εάν μιλάμε για ασύμμετρη κρυπτογράφηση.

Αξίζει να σημειώσουμε ότι υπάρχουν περιπτώσεις όπου ότι οι πληροφορίες δεν πρέπει να είναι απροσπέλαστες από όλους και γι' αυτό αποθηκεύονται με τέτοιο τρόπο ώστε η αντιστροφή της κρυπτογραφική διαδικασίας που έχει εφαρμοστεί να είναι αδύνατη. Για παράδειγμα, σε ένα τυπικό περιβάλλον πολλών χρηστών, κανένας δεν πρέπει να έχει γνώση του αρχείου που περιέχει τους κωδικούς όλων των χρηστών. Συχνά, λοιπόν, αποθηκεύονται οι hash values των πληροφοριών (στην προηγούμενη περίπτωση θα ήταν οι κωδικοί) αντί για τις ίδιες τις πληροφορίες. Έτσι, οι χρήστες είναι σίγουροι για το απόρρητο των κωδικών τους, ενώ μπορούν να ακόμα να αποδεικνύουν την ταυτότητα τους με την παροχή του κωδικού τους. Ο υπολογιστής που έχει αποθηκευμένες τις hash values των κωδικών, σε κάθε εισαγωγή κωδικού υπολογίζει το hash του και το συγκρίνει με το αποθηκευμένο που αντιστοιχεί στον χρήστη που προσπαθεί να πιστοποιήσει τον εαυτό του.

### 3.3.2 Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές




Η ψηφιακή υπογραφή είναι ένα εργαλείο που παρέχει πιστοποίηση ταυτότητας *(authentication)*. Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων *(integrity)* και την ταυτότητα ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία του αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας hash function και της ιδιωτικής κλείδας του αποστολέα.

Ας δούμε πως λειτουργεί μία ψηφιακή υπογραφή. Έστω δύο χρήστες, ο Α και ο Β. Όταν ο Α θέλει να στείλει ένα υπογεγραμμένο έγγραφο στον Β. Το πρώτο βήμα είναι η παραγωγή του message digest του μηνύματος. Το message digest είναι κατά κανόνα μικρότερο σε μέγεθος από το αρχικό μήνυμα. Στο δεύτερο βήμα, ο Α κρυπτογραφεί το message digest με την ιδιωτική του κλείδα. Τέλος, στέλνει το κρυπτογραφημένο message digest στον Β μαζί με το έγγραφο. Για να μπορέσει ο Β να επαληθεύσει την υπογραφή πρέπει να γνωρίζει την δημόσια κλείδα του Α και τον hash function που χρησιμοποίησε ο Α. Πρώτα θα αποκρυπτογραφήσει το message digest με την δημόσια κλείδα του Α και θα πάρει το message digest που παρήγαγαι ο Α. Έπειτα, θα υπολογίσει το message digest του εγγράφου ξανά και θα το συγκρίνει με το παραληφθέν. Εάν τα δύο είναι ταυτόσημα τότε η υπογραφή επαληθεύτηκε επιτυχώς. Εάν δεν ταιριάζουν τότε ή κάποιος προσποιείται ότι είναι ο Α ή το μήνυμα τροποποιήθηκε κατά την μεταφορά του ή προέκυψε λάθος κατά την μετάδοση. Οποιοσδήποτε που γνωρίζει την δημόσια κλείδα του Α, την hash function και τον αλγόριθμο κρυπτογράφησης που χρησιμοποιήθηκε, μπορεί να επιβεβαιώσει το γεγονός ότι το μήνυμα προέρχεται από τον Α και ότι δεν αλλοιώθηκε μετά την υπογραφή του.

Για να έχει αποτέλεσμα η παραπάνω μέθοδος, πρέπει να τηρούνται δύο προϋποθέσεις: (α) η hash function πρέπει να είναι όσο το δυνατόν περισσότερο μη αντιστρέψιμη και (β) τα ζεύγη δημόσιας – ιδιωτικής κλείδας να είναι συσχετισμένα με τους νόμιμους κατόχους τους. Για την εξασφάλιση της δεύτερης προϋπόθεσης υπάρχουν ψηφιακά έγγραφα που καλούνται πιστοποιητικά *(certificates)* και συνδέουν ένα άτομο με μία συγκεκριμένη δημόσια κλείδα.

# *4.*Μοντέλο Ασφαλείας

## *4.1 Η Προσέγγιση*

## 4.1.1 Γενικά

Για την κατάταξη των νέων πρωτοκόλλων και συστημάτων που, είναι απαραίτητη η υιοθέτηση ενός μοντέλου, σαν αυτό του OSI, που θα βοηθήσει στην κατανόηση της λειτουργικότητας των και της συσχέτισης τους τόσο μεταξύ τους, όσο και με τα πρωτόκολλα του Internet. Η προσέγγιση μας βασίστηκε στο πολυεπίπεδο μοντέλο που ακολουθεί και προσομοιάζει τα επίπεδα του Διαδικτύου.

## 4.1.2 Το Μοντέλο

| | |
|---|---|
| . | *APPLICATIONS* |
| . | *INTERNET SERVICES* |
| . | *HIGHER INTERNET PROTOCOLS* |
| . | *TCP/IP* |
| . | *NETWORK ACCESS* |

## 4.1.3 Σύντομη Περιγραφή του Μοντέλου

Στο πρώτο επίπεδο του μοντέλου ασφαλείας, περιλαμβάνονται οι τεχνικές ασφάλισης του ηλεκτρικού σήματος. Οι τεχνικές αυτές έχουν να κάνουν με την κωδικοποίηση των bits για μετάδοση στο μέσο, την πολυπλεξία λογικών καναλιών με την χρήση διαφορετικών συχνοτήτων και τα bits ισοτιμίας. Οι τεχνικές διαφέρουν ανάλογα με την τεχνολογία τοπικών δικτύων που χρησιμοποιείται (Ethernet, Token Ring, FDDI), ενώ παρόμοιες μέθοδοι εφαρμόζονται και από τα modem στις dial-up συνδέσεις. Συγκεκριμένα, η λειτουργία των modem βασίζεται σε πρωτόκολλα που καθορίζουν τους αλγόριθμους που υλοποιούνται σε τσιπ σιλικόνης. Σε αυτό το επίπεδο ανήκουν και οι περιπτώσεις της hardware κρυπτογραφίας και στεγανογραφίας.

Στο επίπεδο TCP/IP κατατάσσονται τα συστήματα που εξασφαλίζουν την επικοινωνία με τα πρωτοκόλλα TCP και IP. Παράδειγμα συστημάτων αυτού του επιπέδου είναι IPSec και το NAT.

Στο αμέσως πιο πάνω επίπεδο, στο επίπεδο *HIGHER INTERNET PROTOCOLS* βρίσκουμε το SSL, πρωτόκολλο που στοχεύει στην διασφάλιση του πακέτου TCP/IP και των εφαρμογών που χρησιμοποιούν το TCP/IP. Το SSL προσθέτει δύο νέα επίπεδα στο OSI μοντέλο, γεγονός που το τοποθετεί ένα επίπεδο πάνω από το IPSec.

Στο επίπεδο των υπηρεσιών του Διαδικτύου ανήκουν όλα τα συστήματα που αποτελούν προεκτάσεις των υπαρχόντων πρωτοκόλλων υπηρεσιών, προσθέτοντας χαρακτηριστικά ασφαλείας. Οι υπηρεσίες που διασφαλίζονται είναι το ηλεκτρονικό ταχυδρομείο, το World Wide Web, το DNS και το remote login. Παράδειγμα αυτών των συστημάτων είναι το *S/MIME*, το *PEM*, το *S/HTTP*.

Τέλος, στο επίπεδο των εφαρμογών κατατάσσονται πιο ολοκληρωμένα συστήματα, που πολλές φορές χρησιμοποιούν πρωτόκολλα από το παρακάτω επίπεδο. Καλύπτουν πληθώρα αναγκών και συνήθως αναπτύσσονται από οργανισμούς για εσωτερική χρήση. Η επιτυχία του κάθε συστήματος καθορίζει της αποδοχή του από την κοινότητα του Διαδικτύου. Μερικά από αυτά είναι το *Kerberos*, το *S/KEY*, το *RADIUS*, ενώ υπάρχουν και πιο γενικές έννοιες όπως αυτή των *Firewalls*. Στα δύο τελευταία επίπεδα του μοντέλου ασφαλείας ανήκουν και τα περισσότερα από τα νέα πρωτόκολλα.

Στις σελίδες που ακολουθούν, θα επιχειρήσουμε να παρουσιάσουμε τα υπάρχοντα δικτυακά συστήματα ασφαλείας και συγχρόνως να τα κατατάξουμε σύμφωνα με το παραπάνω μοντέλο. Λόγω της φύσης των τεχνικών που χρησιμοποιούνται στο πρώτο επίπεδο, η οποίες εξαρτούνται από την εκάστοτε τεχνολογία δικτύων, δεν θα αναφερθούμε καθόλου σε αυτό. Οι τεχνικές αυτές έχουν να κάνουν περισσότερο με τα χαρακτηριστικά της σύνδεσης και δεν έχουν γίνει προσπάθειες για την περαιτέρω διασφάλιση τους. Ακόμα, οι περιπτώσεις της hardware κρυπτογραφίας και στεγανογραφίας, δεν εφαρμόζεται παρά σε ελάχιστες, εξειδικευμένες καταστάσεις, όπως στις στρατιωτικές και κυβερνητικές επικοινωνίες.

# *5.* Πρωτόκολλα Ασφάλειας

## *5.1 IPSec (IP Security)*

### 5.1.1 Εισαγωγή

Το Internet αποτελεί αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων συμπεριλαμβανομένων αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων, της πλαστοπροσωπίας και της άρνησης παροχής υπηρεσιών. Ο στόχος της IPSec είναι η αντιμετώπιση όλων αυτών των προβλημάτων μέσα στην ίδια την υποδομή του δικτύου χωρίς να είναι αναγκαία η εγκατάσταση και η ρύθμιση ακριβών μηχανών και λογισμικού.

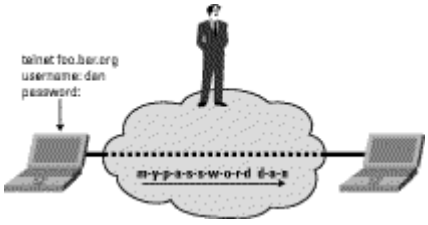
Η IPSec παρέχει κρυπτογράφηση στο επίπεδο του IP και για αυτό το λόγο αποτελεί ένα αξιοσημείωτο κομμάτι της συνολικής ασφάλειας. Οι προδιαγραφές της IPSec ορίζουν δύο νέους τύπους δεδομένων στα πακέτα: την επικεφαλίδα

πιστοποίησης *(AH-Authentication Header)*, για την παροχή υπηρεσίας ακεραιότητας δεδομένων και το φορτίο ενθυλάκωσης ασφάλειας *(ESP-Encapsulating Security Payload)* το οποίο παρέχει πιστοποίηση ταυτότητας και ακεραιότητα δεδομένων. Ορίζονται επίσης οι παράμετροι επικοινωνίας μεταξύ δύο συσκευών που είναι η διαχείριση των κλειδιών και η συσχετισμοί ασφάλειας *(security associations).*

# 5.1.2 Γιατί χρειαζόμαστε την IPSec

### Απώλεια του Απορρήτου (Loss of Privacy)

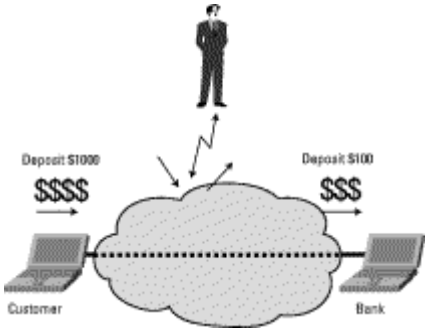
Κάποιος που έχει καταφέρει να εισχωρήσει σε κάποιο δίκτυο έχει τη δυνατότητα να παρακολουθεί εμπιστευτικά δεδομένα κατά τη διακίνηση των τελευταίων στο Internet. Αυτή η δυνατότητα είναι ίσως ο μεγαλύτερος ανασταλτικός παράγοντας στις επικοινωνίες μεταξύ των επιχειρήσεων σήμερα. Χωρίς τη χρήση κρυπτογραφικών μεθόδων κάθε μήνυμα είναι ανοικτό προς ανάγνωση από όποιον έχει τη δυνατότητα να το αιχμαλωτίσει, όπως φαίνεται στο σχήμα 1. Το CERT (Computer Emergency Response Team Coordination Center) αναφέρεται στα προγράμματα "packet sniffers" ως την πιο συνηθισμένη περίπτωση επίθεσης από αυτές που συναντώνται, λέγοντας :




"Οι εισβολείς συνηθίζουν να εγκαθιστούν packet sniffers σε συστήματα που έχουν εκτεθεί σε κάθε είδους κίνδυνο μετά την απώλεια της μυστικότητας του root password. Αυτά τα προγράμματα, που συλλέγουν ονόματα και κωδικούς, εγκαθίστανται σαν μέρος ενός kit το οποίο αντικαθιστά επιπλέον κοινά αρχεία του συστήματος με προγράμματα που δείχνουν ότι κάνουν αυτό που θα έπρεπε αλλά στην πραγματικότητα εκτελούν άλλες λειτουργίες (Trojan horse programs). Αυτά τα kit παρέχουν οδηγίες οι οποίες καθιστούν και τον αρχάριο χρήστη τους επικίνδυνο για την ασφάλεια ενός απροστάτευτου δικτύου".

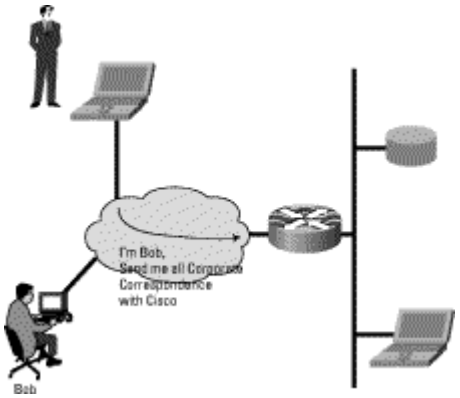
### Απώλεια της Ακεραιότητας των Δεδομένων (Loss of Data Integrity)

Ακόμα και για δεδομένα που δεν είναι εμπιστευτικά πρέπει να λαμβάνονται μέτρα διασφάλισης της ακεραιότητάς τους. Μπορεί να μην μας ενδιαφέρει εάν κάποιος "δει" τη κίνηση ρουτίνας της δουλείας μας, αλλά σίγουρα θα μας προβλημάτιζε εάν αυτός αλλοίωνε κατά οποιοδήποτε τρόπο τα δεδομένα αυτά. Για παράδειγμα το να μπορεί κάποιος να πιστοποιεί με ασφάλεια τον εαυτό του στη τράπεζα κάνοντας χρήση ψηφιακών πιστοποιητικών δεν είναι αρκετό εάν η κύρια εργασία του στη τράπεζα θα μπορούσε να αλλοιωθεί με κάποιο τρόπο όπως φαίνεται στο σχήμα 2.



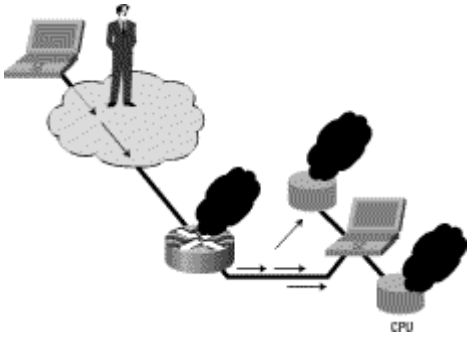

## Πλαστοπροσωπία (Identity Spoofing)

Εκτός της προστασίας των ίδιων των δεδομένων, θα πρέπει να παίρνουμε μέτρα ώστε να προστατεύεται και η ταυτότητά μας στο Internet. Όπως φαίνεται στο σχήμα 3, ένας εισβολέας μπορεί να αποδειχθεί ικανός να κλέψει τη ταυτότητα κάποιου και έτσι να αποκτήσει πρόσβαση σε εμπιστευτικές πληροφορίες . Πολλά συστήματα ασφάλειας, σήμερα, βασίζονται στην IP διεύθυνση για να αναγνωρίσουν μοναδικά τους χρήστες. Τα συστήματα αυτά είναι πολύ εύκολο να ξεγελαστούν και αυτό το γεγονός έχει οδηγήσει σε αναρίθμητα τρυπήματα διαφόρων συστημάτων. Το CERT έχει αναφερθεί σε αυτού του είδους την επίθεση : "Συνεχίζουμε να λαμβάνουμε αρκετές αναφορές που μιλάνε για επιθέσεις τύπου IP Spoofing. Οι εισβολείς επιτίθενται χρησιμοποιώντας αυτοματοποιημένα εργαλεία που κυκλοφορούν ελευθέρα στο Internet. Κάποια sites πίστευαν, λανθασμένα, ότι σταματούσαν τέτοιου είδους επιθέσεις ενώ άλλα σχεδίαζαν να το κάνουν αλλά δεν είχαν προλάβει να το εφαρμόσουν".




## Άρνηση Παροχής Υπηρεσιών (Denial-of-Service)

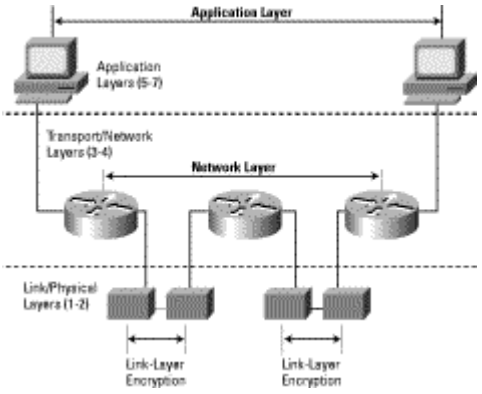
Εφόσον κάποιος οργανισμός εκμεταλλεύεται το Internet, πρέπει να λάβει κάποια μέτρα ώστε να διασφαλίσει τη διαθεσιμότητα του συστήματός του σε αυτό. Τα τελευταία χρόνια διάφοροι hackers έχουν βρει αδυναμίες στο πρωτόκολλο TCP/IP που τους δίνει τη δυνατότητα να "ρίχνουν" τις μηχανές (crash-σχήμα 4). Το CERT έχει μιλήσει για το θέμα : "Ο αριθμός των επιθέσεων εναντίον συστημάτων έχει αυξηθεί σημαντικά αφού υπάρχουν πλέον πακέτα που κυκλοφορούν ελευθέρα και που κάνουν εύκολη την πραγματοποίηση τέτοιου είδους επιθέσεων".




## 5.1.3 Ορισμός

Η IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών. Είναι βασισμένο στις προδιαγραφές που ανέπτυξε η ομάδα εργασίας του Internet (IETF). Η IPSec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο. Η IPSec παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφάλειας σε ένα δίκτυο.

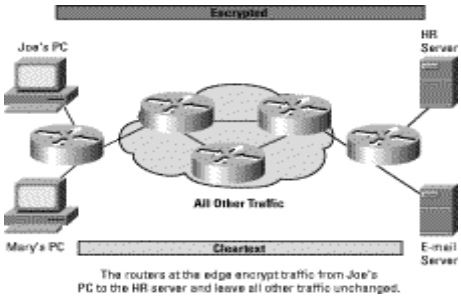
Έλεγχοι κρυπτογράφησης και πιστοποίησης ταυτότητας μπορούν να εφαρμοσθούν σε διάφορα επίπεδα στην δικτυακή υποδομή όπως φαίνεται και στο σχήμα 5.




Πριν την άφιξη της IPSec στο προσκήνιο, εφαρμόζονταν αποσπασματικές λύσεις που αντιμετώπιζαν μέρος μόνο του προβλήματος. Για παράδειγμα, το SSL(Secure Sockets Layer) παρέχει κρυπτογράφηση σε επίπεδο εφαρμογής για Web browsers και άλλες εφαρμογές. Το SSL προστατεύει την πιστότητα των δεδομένων που στέλνονται από κάθε εφαρμογή που το χρησιμοποιεί, αλλά δεν προστατεύει τα δεδομένα που αποστέλλονται από άλλες εφαρμογές. Κάθε σύστημα και εφαρμογή πρέπει να είναι προστατεμένη από το SSL για να του παρέχει το τελευταίο την προστασία.

Οργανισμοί όπως ο στρατός χρησιμοποιούσαν για χρόνια κρυπτογράφηση επιπέδου συνδέσμου. Σε αυτό το σχήμα κάθε σύνδεσμος επικοινωνιών προστατεύεται από ένα ζεύγος συσκευών κρυπτογράφησης - μια στο τέλος κάθε πλευράς του συνδέσμου. Αν και αυτό το σύστημα παρέχει εξαιρετική ασφάλεια δεδομένων είναι πολύ δύσκολο να παρακολουθηθεί και να διαχειριστεί. Επιπλέον απαιτεί η κάθε

πλευρά του συνδέσμου στο δίκτυο να είναι ασφαλής διότι τα δεδομένα είναι σε καθαρή μορφή σε αυτά τα σημεία. Φυσικά αυτό το σχήμα δεν μπορεί να δουλέψει καθόλου στο Internet όπου πιθανότατα κανένας από τους ενδιάμεσους συνδέσμους δεν είναι προσβάσιμος σε κανέναν και δεν εμπιστεύεται κανέναν.




Η IPSec υλοποιεί κρυπτογράφηση και πιστοποίηση επιπέδου δικτύου όπως φαίνεται στο σχήμα 6, παρέχοντας μια λύση ασφαλείας μέσα στην ίδια την αρχιτεκτονική του δικτύου. Έτσι τα συστήματα και οι εφαρμογές που βρίσκονται στις άκρες δεν χρειάζονται αλλαγές ή ρυθμίσεις για να έχουν το πλεονέκτημα της ισχυρής ασφάλειας. Επειδή τα κρυπτογραφημένα πακέτα μοιάζουν με κανονικά IP πακέτα μπορούν εύκολα να δρομολογηθούν μέσα από οποιοδήποτε IP δίκτυο, όπως το Internet, χωρίς καμία αλλαγή στον ενδιάμεσο δικτυακό εξοπλισμό. Οι μόνες συσκευές οι οποίες γνωρίζουν για την κρυπτογράφηση είναι αυτές στα ακραία σημεία. Αυτό το χαρακτηριστικό μειώνει δραστικά τόσο το κόστος της υλοποίησης όσο και το κόστος της διαχείρισης.

## Πρωτόκολλο Διαχείρισης Κλειδιών Internet

Η IPSec μπορεί να θεωρήσει ότι ένας συσχετισμός ασφάλειας υπάρχει αλλά δεν έχει το μηχανισμό να τον δημιουργήσει. Η IETF επέλεξε να σπάσει τη διαδικασία αυτή σε δύο μέρη : η IPSec παρέχει την επεξεργασία των πακέτων επιπέδου IP και το πρωτόκολλο διαχείρισης κλειδιών Internet *(IKMP—Internet Key Management Protocol)*, ασχολείται με ότι έχει να κάνει με τους συσχετισμούς ασφάλειας. Μετά από εξέταση πολλών εναλλακτικών λύσεων συμπεριλαμβανομένων και των SKIP (Simple Key Management Protocol) και Photouris, η IETF επέλεξε το IKE σαν το τρόπο ρύθμισης των συσχετισμών ασφάλειας για την IPSec.

Το IKE δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι – τούνελ μεταξύ δύο οντοτήτων και κατόπιν διαπραγματεύεται τους συσχετισμούς ασφάλειας για την IPSec. Αυτή η διαδικασία απαιτεί από τις δύο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν κλειδιά.

### *Πιστοποίηση Ταυτότητας*

Τα δύο μέρη πρέπει να πιστοποιήσουν το ένα το άλλο. Το IKE είναι πολύ ευέλικτο και υποστηρίζει πολλές διαφορετικές μεθόδους πιστοποίησης της ταυτότητας. Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μιας κατάλληλης διαδικασίας. Σε αυτή τη φάση υλοποιούνται συνήθως οι παρακάτω μηχανισμοί :

- Προ-Μοιρασμένα Κλειδιά—το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας hash συνάρτησης) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.
- Κρυπτογράφηση Δημοσίων Κλειδιών—κάθε μηχανή "γεννάει" έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το public key (δημόσιο κλειδί) της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια hash συνάρτηση του τυχαίου αριθμού αποκρυπτογραφώντας με τα private keys (ιδιωτικά κλειδιά) ότι λαμβάνουν από το συνομιλητή τους. Το σύστημα παρέχει ακόμα και δυνατότητα άρνησης συμμετοχής σε οποιαδήποτε διαδικασία πιστοποίησης. Προς το παρόν μόνο ο αλγόριθμος δημοσίων κλειδιών της RSA υποστηρίζεται.
- Ψηφιακές Υπογραφές—κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Αυτή η μέθοδος είναι παρόμοια με την προηγούμενη μόνο που δεν παρέχει μηχανισμό άρνησης της εμπλοκής της σε κάποια προσπάθεια πιστοποίησης. Προς το παρόν υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

Τόσο η διαδικασία κρυπτογράφησης όσο και αυτή των ψηφιακών υπογραφών απαιτεί τη χρήση ψηφιακών πιστοποιητικών για την επικύρωση της δημόσιας σε ιδιωτική αντιστοίχησης. Το IKE επιτρέπει την ανεξάρτητη ανταλλαγή των ψηφιακών πιστοποιητικών με τη χρήση για παράδειγμα του DNSSEC ή την ανταλλαγή τους σαν μέρος του IKE.

***Ανταλλαγή Κλειδιών***

Τα δύο μέρη πρέπει να έχουν ένα κοινό, έστω προσωρινό, κλειδί έτσι ώστε να κρυπτογραφήσουν το IKE τούνελ. Το πρωτόκολλο Diffie-Helman χρησιμοποιείται για τη συμφωνία σε ένα κοινό κλειδί. Η ανταλλαγή πιστοποιείται όπως περιγράφηκε παραπάνω για τη αποφυγή επιθέσεων παρεμβολών.

## Χρησιμοποίηση του IKE στην IPSec

Αυτά τα δύο βήματα, πιστοποίηση και ανταλλαγή κλειδιών, δημιουργούν το IKE SA—ένα ασφαλές κανάλι μεταξύ των δύο συσκευών. Το ένα μέρος του τούνελ προσφέρει ένα σύνολο αλγορίθμων ενώ το άλλο πρέπει να κάνει αποδεκτή μία από τις προσφορές ή να απορρίψει ολόκληρη τη σύνδεση. Όταν πλέον τα δύο μέρη συμφωνήσουν στη χρήση συγκεκριμένων αλγορίθμων αντλούν το υλικό των κλειδιών για χρήση από την IPSec μαζί με μία ή και τις δύο επικεφαλίδες (AH και ESP). Η IPSec χρησιμοποιεί διαφορετικό κλειδί από αυτό του IKE. Το κλειδί της IPSec μπορεί να προέλθει από την επαναχρησιμοποίηση της ανταλλαγής Diffie-Helman για την επίτευξη υψηλού βαθμού ασφάλειας, ή με την χρησιμοποίηση της αρχικής ανταλλαγής Diffie-Helman η οποία και παρήγαγε το IKE SA, αφού αυτή πρώτα συσχετισθεί μέσω μιας hash συνάρτησης με κάποιους τυχαίους αριθμούς. Η πρώτη

μέθοδος παρέχει μεγαλύτερη ασφάλεια αλλά είναι πολύ πιο αργή. Αφού όλα τα παραπάνω τελειώσουν το IPSec SA έχει εγκαθιδρυθεί.

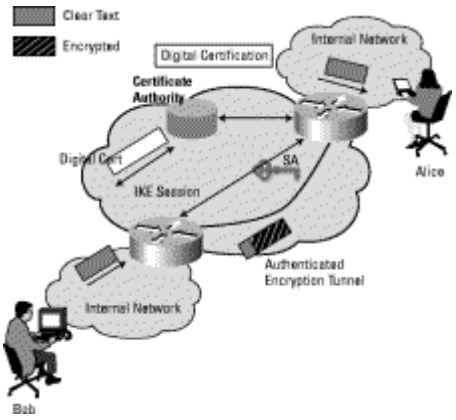
Το σχήμα 9 δείχνει πως η IPSec χρησιμοποιεί το IKE για την εγκαθίδρυση μιας ασφαλούς συσχέτισης ασφάλειας. Στο παράδειγμα, το πρώτο πακέτο της Alice προς τον Bob, το οποίο πρέπει να είναι κρυπτογραφημένο, ενεργοποιεί την διαδικασία IKE. Αυτή, με τη σειρά της, φτιάχνει ένα ασφαλές κανάλι μεταξύ του Bob και της Alice. Η IPSec SA διαπραγματεύονται μέσα σε αυτό το κανάλι-τούνελ. Κατόπιν η Alice μπορεί να χρησιμοποιήσει αυτό το συσχετισμό ασφάλειας για να στείλει δεδομένα στο Bob με ασφάλεια.

Επειδή η όλη διαδικασία δείχνει κάπως σύνθετη στη θεωρία, ας δούμε το παρακάτω παράδειγμα (σχήμα 11):

Σε αυτό το παράδειγμα ο Bob προσπαθεί να επικοινωνήσει με ασφάλεια, με την Alice. Οι κινήσεις που γίνονται είναι οι παρακάτω:

1. Ο Bob στέλνει τα δεδομένα του προς την Alice
2. Όταν ο δρομολογητής του Bob δει τα πακέτα ελέγχει τη πολιτική ασφάλειάς τους και αντιλαμβάνεται ότι αυτά πρέπει να είναι κρυπτογραφημένα.
3. Η προ-ρυθμισμένη πολιτική ασφάλειας λέει επιπλέον ότι ο δρομολογητής της Alice πρέπει να είναι το τελικό σημείο του IPSec τούνελ.
4. Ο δρομολογητής του Bob κοιτάει να δει εάν έχει εγκαθιδρυμένη μια IPSec SA με το δρομολογητή της Alice.
5. Σε περίπτωση που μια τέτοια δεν υπάρχει, τότε ζητάει μία από το IKE.

Εάν οι δύο δρομολογητές έχουν έτοιμη μια IKE SA τότε μπορεί γρήγορα να ξεκινήσει μια IPSec SA. Εάν δεν έχουν, τότε πρέπει να περιμένουν να δημιουργηθεί μία πρώτα. Σαν μέρος αυτής της διαδικασίας, οι δύο δρομολογητές ανταλλάσσουν ψηφιακά πιστοποιητικά. Αυτά θα πρέπει να είναι υπογεγραμμένα από πριν από κάποιον τρίτο τον οποίο εμπιστεύεται τόσο ο Bob όσο και η Alice (οι δρομολογητές αυτών). Όταν ενεργοποιηθεί το IKE κανάλι οι δρομολογητές μπορούν να ξεκινήσουν τις διαπραγματεύσεις για την IPSec SA. Όταν αυτή πια, ενεργοποιηθεί τότε θα έχει συμφωνηθεί ένας αλγόριθμος κρυπτογράφησης (για παράδειγμα ο DES) και ένας αλγόριθμος πιστοποίησης (για παράδειγμα ο MD5) και θα έχει επιπλέον γίνει και η ανταλλαγή κάποιου κλειδιού. Τώρα πλέον ο δρομολογητής του Bob μπορεί να κρυπτογραφήσει τα IP πακέτα του και να τα τοποθετήσει σε νέα IPSec πακέτα για να τα στείλει στο δρομολογητή της Alice. Όταν ο τελευταίος τα λαμβάνει, κοιτάει την IPSec SA και κατόπιν αποθυλακώνει και επεξεργάζεται κατάλληλα το αρχικό πακέτο το οποίο και προωθεί στην Alice. Όσο και σύνθετα αν ακούγονται όλα αυτά, στην πραγματικότητα συμβαίνουν εντελώς αυτόματα και χωρίς να φαίνεται το παραμικρό στα μάτια τόσο του Bob όσο και της Alice.




## *5.2 Secure Socket Layer (SSL)*

## 5.2.1 Γενικά

Το πρωτόκολλο SSL αναπτύχθηκε από την *Netscape Communications Corporation* για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση *(version 1.0)* και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή *RFC (Request For Comments)*. Τον Δεκέμβριο του 1994 εκδίδεται μια επαναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του *(version 2.0)*. Η παρούσα έκδοση του SSL, version 3.0, παρουσιάσθηκε στο κοινό στα τέλη του 1995, ενώ από τα μέσα του 1995 είχε αρχίσει να εφαρμόζεται σε προϊόντα της εταιρίας, όπως τον *Netscape Navigator*.

Επειδή η *Netscape* επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου γεγονός που ερχόταν σε σύγκρουση με τους νόμους των Ηνωμένων Πολιτειών περί εξαγωγή κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει την χρήση ασθενών αλγορίθμων στις εξαγόμενες εφαρμογές. Πιο συγκεκριμένα, δημιούργησε παραλλαγές των αλγόριθμων RC4-128 και RC2-128 που στην πραγματικότητα χρησιμοποιούν κλειδιά των 40 bits.

## 5.2.2 Εισαγωγή στο SSL

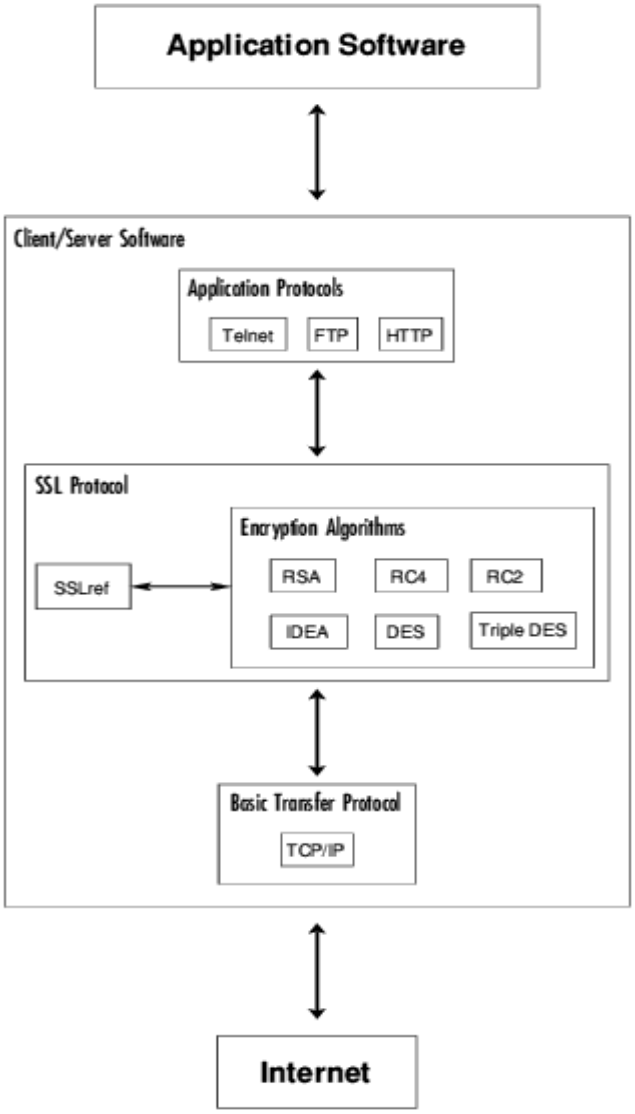
Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των

Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Όλα τα παραπάνω γίνονται με τρόπο διαφανές και απλό.

Η έκδοση 3 του πρωτοκόλλου κάλυψε πολλές αδυναμίες της δεύτερης. Οι σημαντικότερες αλλαγές έχουν να με την μείωση των απαραίτητων μηνυμάτων κατά το *handshake* για την εγκαθίδρυση της σύνδεσης, την επιλογή των αλγόριθμων συμπίεσης και κρυπτογράφησης από τον server και την εκ νέου διαπραγμάτευση του *master-key* και *session-id*. Ακόμα αυξάνονται οι διαθέσιμοι αλγόριθμοι και προστίθενται νέες τεχνικές για την διαχείριση των κλειδιών.

Συμπερασματικά μπορούμε να πούμε πως η έκδοση 3 του SSL είναι πιο ολοκληρωμένη σχεδιαστικά, με μεγαλύτερο εύρος υποστήριξης εφαρμογών και λιγότερες ατέλειες. Παρ' όλο που είναι συμβατή με την δεύτερη έκδοση, η χρήση της τελευταίας δεν πρέπει να προτιμάται.

Το SSL μπορεί να τοποθετηθεί στην κορυφή οποιουδήποτε πρωτοκόλλου μεταφοράς, δεν εξαρτάται από την ύπαρξη του TCP/IP και τρέχει κάτω από πρωτόκολλα εφαρμογών όπως το HTTP, FTP και TELNET. Μια αναπαράσταση του πρωτοκόλλου SSL βλέπουμε παρακάτω.




## 5.2.3 Υποστηριζόμενοι Αλγόριθμοι

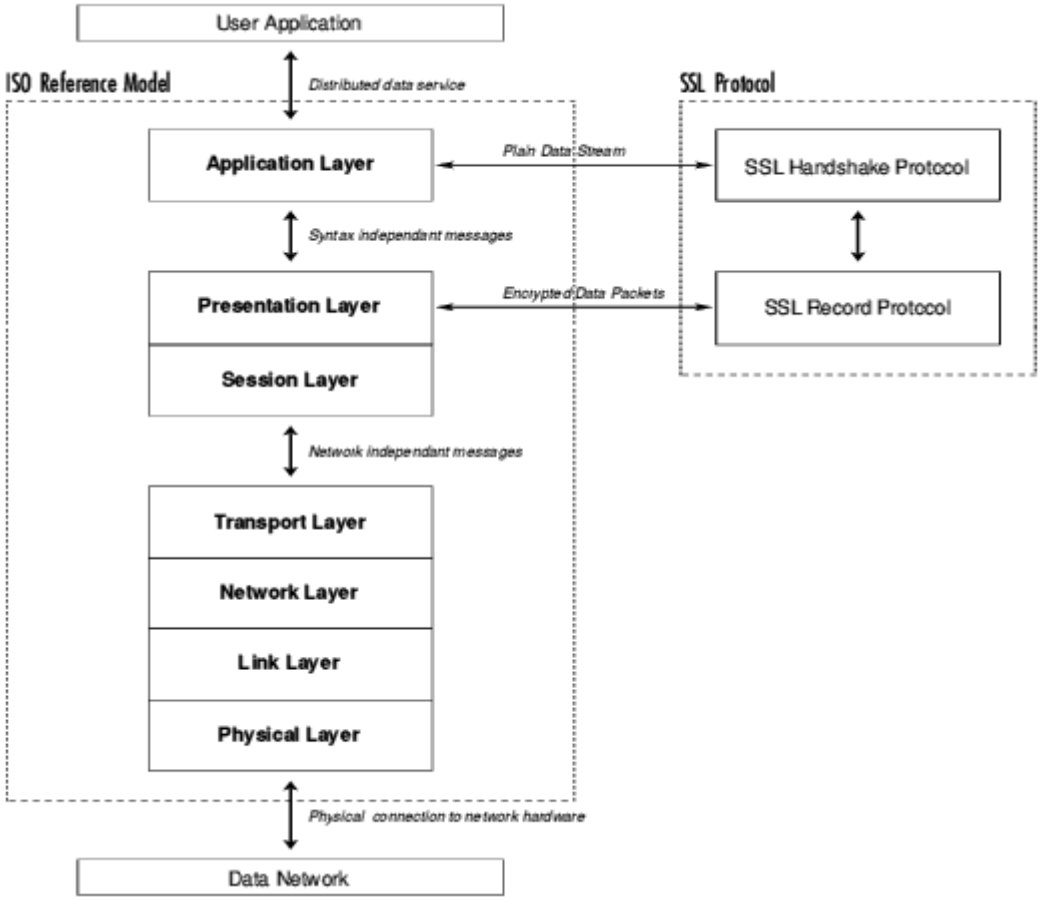
Οι αλγόριθμοι κρυπτογράφησης χωρίζονται στους stream ciphers και στους block ciphers. Στους stream ciphers ανήκουν οι RC4 με κλειδιά 40 bits και 128 bits. Στους block ciphers ανήκουν οι RC2 με κλειδιά 40 και 128 bits, οι DES, DES40, Triple DES και οι IDEA και Fortezza.

Οι αλγόριθμοι για την παραγωγή των hash και digest values για τα MACs είναι ο MD5 (128-bit hash) και ο SHA (160-bit hash).

Οι τεχνικές διαχείρισης των κλειδιών (key management) διακρίνονται στους: την ασύμμετρη κρυπτογραφία με RSA, την τεχνική Diffie-Hellman. Τα πιστοποιητικά είναι της μορφής X.509. Ο RSA μαζί με τον DSS και τον Fortezza μπορούν να χρησιμοποιηθούν για την ψηφιακή υπογραφή των κλειδιών κρυπτογράφησης.

Προσφέρεται και η δυνατότητα επιλογής ανασφάλιστης επικοινωνίας, αλλά δεν συνιστάται.

## 5.2.4 Το SSL και το OSI μοντέλο



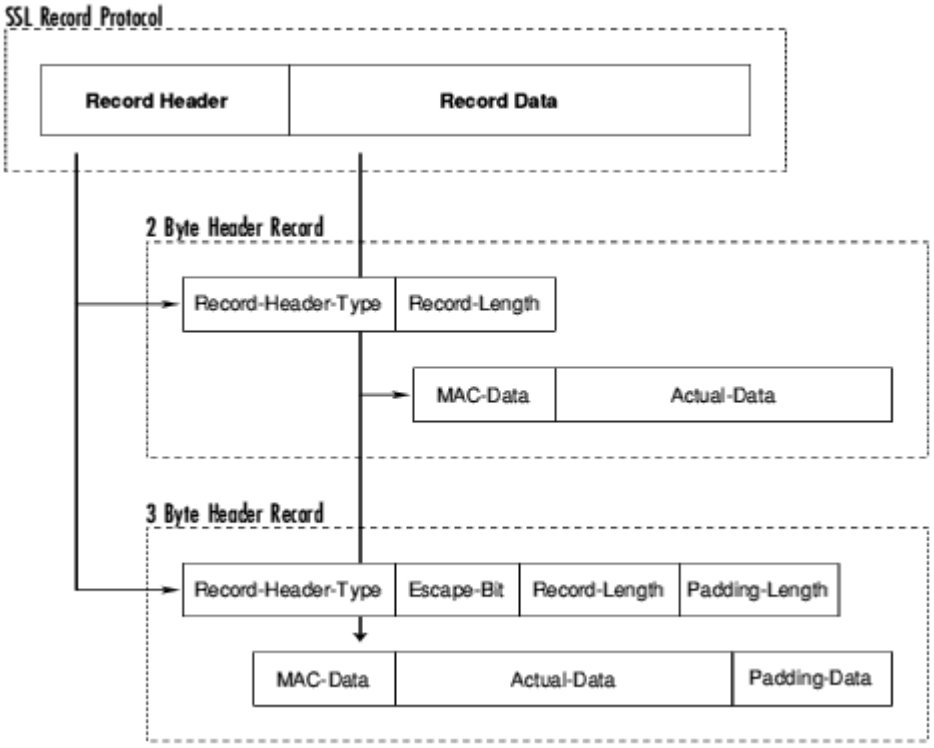

Είναι σημαντικό κάθε νέο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το OSI μοντέλο, έτσι ώστε να μπορεί εύκολα να αντικαταστήσει κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων.

Το SSL χωρίζεται σε δύο μέρη, το SSL Handshake Protocol (SSLHP) και το SSL Record Protocol (SSLRP). Το SSLHP διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και εάν ζητηθεί και του client. Το SSLRP συλλέγει τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει και αποκρυπτογραφεί τα παραλαμβανόμενα πακέτα.

Βλέπουμε πως το SSL λειτουργεί επιπρόσθετα της υπάρχουσας δομής του OSI και όχι σαν πρωτόκολλο αντικατάστασης. Επίσης είναι πασιφανές ότι η χρήση του SSL δεν αποκλείει την χρήσης άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο Εφαρμογών, πάνω από το SSL.

# 5.2.5 Λειτουργία του SSL

## SSL Record Protocol




Ένα πακέτο SSL αποτελείται από δύο μέρη, την επικεφαλίδα και τα δεδομένα. Η επικεφαλίδα μπορεί να είναι είτε 3 bytes είτε 2 bytes, από τις οποίες περιπτώσεις η δεύτερη χρησιμοποιείται όταν τα δεδομένα χρειάζονται συμπλήρωμα (padding). Το πεδίο escape-bit στην περίπτωση των 3 bytes υπάρχει μόνο σε εκδόσεις μετά την δεύτερη του πρωτοκόλλου και προβλέπεται για ρύθμιση πληροφοριών out-of-band. Για την επικεφαλίδα των 2 bytes το μέγεθος του πακέτου είναι 32767 bytes, ενώ για την επικεφαλίδα των 3 bytes το μέγεθος είναι 16383 bytes.

Το κομμάτι των δεδομένων αποτελείται από ένα Message Authentication Code (MAC), τα πραγματικά δεδομένα και δεδομένα συμπλήρωσης, εάν χρειάζονται. Αυτό το κομμάτι είναι που κρυπτογραφείται κατά την μετάδοση. Τα συμπληρωματική δεδομένα απαιτούνται όταν οι αλγόριθμοι κρυπτογράφησης εν χρήση είναι τύπου block ciphers και ο ρόλος τους είναι να συμπληρώνουν τα πραγματικά δεδομένα ώστε το μέγεθος τους είναι πολλαπλάσιου του μεγέθους που δέχεται σαν είσοδο ο block cipher. Εάν χρησιμοποιούνται stream ciphers τότε δεν απαιτείται συμπλήρωμα και μπορεί αν χρησιμοποιηθεί η επικεφαλίδα των 2 bytes.

Το MAC είναι η digest ή hash value των secret-write key (βλέπε παρακάτω) του αποστολέα του πακέτου, των πραγματικών δεδομένων, των συμπληρωματικών δεδομένων και ενός αριθμού ακολουθίας, στην σειρά που δίνονται.

Προβλέπεται και η συμπίεση των δεδομένων *(data compression)* με κατάλληλους μηχανισμούς που επιλέγονται κατά το handshake, ενώ δεν αποκλείεται να χρειαστεί και τεμαχισμός της πληροφορίας σε πολλά πακέτα *(fragmentation)*.

## SSL Handshake Protocol

Το πρωτόκολλο SSL Handshake διαχωρίζεται σε δύο επιμέρους φάσεις: η πρώτη φάση αφορά την επιλογή των αλγόριθμων, την ανταλλαγή ενός master key και την πιστοποίηση της ταυτότητας του server. Η δεύτερη φάση διαχειρίζεται την πιστοποίηση της ταυτότητας του client (εάν ζητηθεί) και ολοκληρώνει την διαδικασία του handshaking. Όταν το ολοκληρωθούν και οι δύο φάσεις, το στάδιο του handshake τελειώνει και η μεταφορά μεταξύ των δύο άκρων αρχίζει. Όλα τα μηνύματα κατά την διάρκεια του handshaking και μετά στέλνονται σύμφωνα με το SSL Record Protocol.

Το πακέτο των αλγορίθμων κρυπτογράφησης *(Cipher Suite)* περιλαμβάνει την μέθοδο για την ανταλλαγή των κλειδιών, τον αλγόριθμο κρυπτογράφησης και τον μηχανισμό για την παραγωγή του MAC.

Παρακάτω θα δούμε τρεις διαφορετικές περιπτώσεις επικοινωνίας.

**1**. Πρώτα θα εξετάσουμε την περίπτωση της αρχικής σύνδεσης, χωρίς πιστοποίηση ταυτότητας του client. Χρησιμοποιείται η σύμβαση "{data}key" για να υποδηλώσουμε κρυπτογραφημένα δεδομένα με το κλειδί "key".

Ας δούμε βήμα προς βήμα την ακολουθία μηνυμάτων.

| *Τύπος Μηνύματος* | *Κατεύθυνση* | *Δεδομένα που μεταφέρονται* |
|---|---|---|
| client-hello | C ➿ S | challenge-data, cipher-suite-specs, compressions |
| server-hello | C ✍ S | connection-id, server-certificate, cipher-kind, compression-kind |
| client-master-key | C ➿ S | clear-master-key,{secret-master-key}server-public-key |
| client-finish | C ➿ S | {connection-id}client-write-key |
| server-verify | C ✍ S | {challenge-data}server-write-key |
| server-finish | C ✍ S | {session-id}server-write-key |

Με το μήνυμα **client-hello** στέλνει ο client στον server μια λίστα με τους αλγόριθμους που υποστηρίζει και τα challenge-data που θα χρησιμοποιηθούν αργότερα για την πιστοποίηση της ταυτότητας του.

Το μήνυμα **server-hello** επιστρέφει στον client ένα αναγνωριστικό της σύνδεσης (connection-id), την επιλογή του server όσον αναφορά πακέτο των αλγόριθμων κρυπτογράφησης και συμπίεσης (που και οι δύο υποστηρίζουν) και το πιστοποιητικό του server που θα χρησιμοποιηθεί από τον client για την απόκτηση της δημόσιας κλείδας του server. Στην τελευταία έκδοση του

Το **client-master-key** και το master-key, που ανάλογα με το που βρίσκεται κάθε υπολογιστής, μπορεί να έχει δυο διαφορετικές μορφές. Για SSL εφαρμογές έξω από τις Ηνωμένες Πολιτείες, τα 88 bits του master-key μεταδίδονται μη κρυπτογραφημένα και κρυπτογραφούνται τα υπόλοιπα 40 bits με την δημόσια κλείδα του server. Αντίθετα για SSL εφαρμογές εντός των Ηνωμένων Πολιτειών, κρυπτογραφείται όλο το master-key και το clear-master-key είναι άδειο.

Από αυτό το σημείο και μετά όλα τα μηνύματα κρυπτογραφούνται στο επίπεδο του SSL Record Protocol. Το master-key δεν χρησιμοποιείται άμεσα για κρυπτογράφηση, αλλά για την παραγωγή δύο ζευγάρια κλειδιών. Το ένα ζευγάρι ανήκει στον client και αποτελείται από το *client-write-key* που χρησιμοποιεί ο client για να κρυπτογραφήσει τα μηνύματα προς τον server και το *client-read-key* για να αποκρυπτογραφήσει ότι λαμβάνει από αυτόν. Το δεύτερο ζευγάρι ανήκει στον server και αποτελείται από το *server-write-key* για κρυπτογράφηση μηνυμάτων προς τον client και το *server-read-key* για αποκρυπτογράφηση των παραληφθέντων. Για την ακρίβεια, το client-write-key είναι το ίδιο με το server-read-key και το client-read-key είναι το ίδιο με το server-write-key.

Το **client-finish** περιέχει το αναγνωριστικό της σύνδεσης που αρχικά είχε σταλεί από τον server κρυπτογραφημένο με το client-write-key.

Το **server-verify** περιέχει τα challenge-data που είχε στείλει ο client στον server κατά την αρχή της σύνδεσης, κρυπτογραφημένα με το server-write-key. Η παραλαβή και αποκρυπτογράφηση αυτού του μηνύματος είναι το τελικό στάδιο για την επιβεβαίωση της ταυτότητας του server καθ' ότι μόνο ο αληθινός server θα μπορούσε να αποκρυπτογραφήσει με την ιδιωτική του κλείδα το master-key.

Τέλος, το μήνυμα **server-finish** τερματίζει το handshake. Περιέχει το session-id που χρησιμοποιείται σε επόμενες διαδικασίες handshake για την αποφυγή επανάληψης της φάσης επιλογής αλγορίθμων και ανταλλαγής του master-key. Το session-id αποθηκεύεται και από τους δύο και η προτεινόμενη διάρκεια ζωής είναι 100 δευτερόλεπτα. Έπειτα, αχρηστεύεται.

**2**. Όταν ένα προηγούμενο session-id από τον client χρησιμοποιείται για να επαναεγκαταστήσει την σύνδεση, το handshake γίνεται ως εξής:

| *Τύπος Μηνύματος* | *Κατεύθυνση* | *Δεδομένα που μεταφέρονται* |
|---|---|---|
| client-hello | C ➲ S | challenge-data, session-id, cipher-suite-specs, compressions |
| server-hello | C ✍ S | connection-id |
| client-finish | C ➲ S | {connection-id}client-write-key |
| server-verify | C ✍ S | {challenge-data}server-write-key |
| server-finish | C ✍ S | {session-id}server-write-key |

Αλλάζει το **client-hello** που περιέχει επιπλέον το session-id και χρησιμοποιείται από τον server για να καθορίσει τους αλγόριθμους και το master-key. Η λίστα με τους αλγόριθμους στέλνεται ξανά για την περίπτωση όπου έχει λήξει το session-id.

Το **server-hello** στέλνεται μόνο όταν το session-id ισχύει ακόμα.

**3**. Όταν ζητείται πιστοποίηση της ταυτότητας του client και έχει προηγουμένως εκδοθεί session-id, η ακολουθία των μηνυμάτων του handshaking γίνεται:

| *Τύπος Μηνύματος* | *Κατεύθυνση* | *Δεδομένα που μεταφέρονται* |
|---|---|---|
| client-hello | C ♋ S | challenge-data, session-id, cipher-suite-specs |
| server-hello | C ✍ S | connection-id, server-certificate, cipher-kind |
| client-master-key | C ♋ S | clear-master-key,{secret-master-key}server-public-key |
| client-finish | C ♋ S | {connection-id}client-write-key |
| server-verify | C ✍ S | {challenge-data}server-write-key |
| request-certificate | C ✍ S | {auth-type, cert-chal-data}server-write-key |
| client-certificate | C ♋ S | {cert-type, client-cert, resp-data}client-write-key |
| server-finish | C ✍ S | {session-id}server-write-key |

Παρατηρούμε ότι τα προστίθονται δύο νέα μηνύματα στην προηγούμενη ακολουθία.

Το **request-certificate** στέλνεται από τον server και περιέχει μια δήλωση για την συνάρτηση που θα χρησιμοποιήσει ο client για την παραγωγή της digest value και τον τύπο της συμμετρική κρυπτογράφησης (auth-type). Επίσης, αποστέλλονται και δεδομένα που θα υπογράψει ο client για να αποδείξει την ταυτότητα του (cert-chal-data).

Το **client-certificate** επιστρέφει στον server το πιστοποιητικό του client, μαζί με μια δήλωση του τύπου αυτού (cert-type )και την υπογραφή των δεδομένων cert-chal-data. Ο server θα χρησιμοποιήσει την δημόσια κλείδα που περιέχεται στο πιστοποιητικό του client για να αποκρυπτογραφήσει την υπογραφή. Έπειτα, θα υπολογίσει το message digest των cert-chal-data και θα το συγκρίνει με το message digest που προήλθε από την αποκρυπτογράφηση της υπογραφής.

Κατά την διάρκεια όλων των παραπάνω ανταλλαγών μηνυμάτων, μηνύματα λάθους μπορούν να σταλούν σαν απάντηση σε μηνύματα που δεν βγάζουν νόημα. Η διαδικασία αναγνώρισης λάθους και αποστολή του κατάλληλου μηνύματος αναλαμβάνεται από το πρωτόκολλο SSL Alert Protocol και είναι μέρος του SSL Handshake Protocol. Έτσι, το μήνυμα **no-cipher-error** στέλνεται όταν ο server δεν υποστηρίζει κανένα από τους αλγόριθμους που προτείνει ο client, το μήνυμα **no-certificate-error** όταν δεν είναι διαθέσιμο το ζητηθέν πιστοποιητικό, το μήνυμα **bad-certificate** αν το πιστοποιητικό είναι άκυρο και τέλος το **unsupported-certificate-type-error**, όταν ο τύπος ενός πιστοποιητικού δεν υποστηρίζεται από κανέναν.

## 5.2.6 Αντοχή του SSL σε Γνωστές Επιθέσεις

### Dictionary Attack

Αυτό το είδος της επίθεσης λειτουργεί όταν ένα μέρος του μη κρυπτογραφημένου κειμένου είναι στην κατοχή του ανέντιμων προσώπων. Το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί.

Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα των 128 bit. Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bit κλειδιά και παρ' όλο που τα 88 bit αυτών μεταδίδονται ανασφάλιστα, ο υπολογισμός $2^{40}$ διαφορετικών ακολουθιών κάνει την επίθεση αδύνατο να επιτύχει.

### Brute Force Attack

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι τελείως ανούσια. Μόνο ο DES56 bit cipher είναι ευαίσθητος σε αυτήν την επίθεση, αλλά η χρήση του δεν συνιστάται.

### Replay Attack

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση replay attack. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id και το σύνολο των είδη χρησιμοποιημένων μηνυμάτων δεν γίνονται δεκτά από τον server. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.

### Man-In-The-Middle-Attack

Η επίθεση Man-In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα.

Το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατον. Μην ξεχνάμε την δυνατότητα επικοινωνίας των κλειδιών υπογεγραμμένα.

## 5.2.7 Αδυναμίες του SSL

### Brute Force Attack Εναντίον Αδύναμων Αλγορίθμων

Η μεγαλύτερη αδυναμία του πρωτοκόλλου είναι η ευαισθησία των αλγόριθμων που χρησιμοποιούν μικρά κλειδιά. Συγκεκριμένα, οι RC4-40, RC2-40 και DES-56 εισάγουν σοβαρά προβλήματα ασφαλείας και θα πρέπει να αποφεύγονται.

### Renegotiation of Session Keys (μόνο στην 2 έκδοση)

Από την στιγμή που μία σύνδεση δημιουργηθεί, το ίδιο master key χρησιμοποιείται καθ' όλη την διάρκεια της. Όταν το SSL χρησιμοποιείται πάνω από μια μακρόχρονη σύνδεση (π.χ. μιας TELNET εφαρμογής), η αδυναμία αλλαγής του master key γίνεται επικίνδυνη. Η καλύτερη μέθοδος επίλυσης αυτού του προβλήματος είναι η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα, μειώνοντας έτσι την πιθανότητα μιας επιτυχής Brute Force Attack.

## 5.2.8 Χρήσεις του SSL

Η πιο κοινή του εφαρμογή είναι για την διασφάλιση HTTP επικοινωνιών μεταξύ του browser και του web server. Η ασφαλή έκδοση του HTTP χρησιμοποιεί URLs που ξεκινούν με "https" αντί του κανονικού "http" και διαφορετική πόρτα *(port)* που είναι η προκαθορισμένη στην 443. Ο browser αποθηκεύει τα ιδιωτικά κλειδιά του χρήστη και με κατάλληλο τρόπο υποδεικνύει την διενέργεια ασφαλών συνδέσεων.

Παρ' όλο που μπορεί κανείς να γράψει μια εφαρμογή του SSL ακολουθώντας τα *Internet drafts* και RFCs, είναι προτιμότερο να χρησιμοποιήσει μία από τις υπάρχοντες βιβλιοθήκες εργαλείων του SSL *(SSL toolkit Libraries)*. Τέτοιες βιβλιοθήκες περιέχούν ρουτίνες για κρυπτογράφηση, digestion, και διαχείριση πιστοποιητικών και διακρίνονται στις ακόλουθες:

- SSLRef
- SSLPlus
- SSLava
- SSLeay

## *5.3 S/MIME (Secure MIME)*

Το S/MIME είναι μια εξειδίκευση του πρωτοκόλλου MIME και αναπτύχθηκε για την ασφαλή ανταλλαγή ηλεκτρονικών μηνυμάτων. Σκοπός του είναι η καταπολέμηση της πλαστογραφίας και της υποκλοπής ηλεκτρονικών μηνυμάτων καθώς και η ευκολία στην χρήση. Σχεδιάστηκε ώστε να μπορεί εύκολα να ενοποιηθεί σε προϊόντα ηλεκτρονικού ταχυδρομείου, επεκτείνοντας το πρωτόκολλο MIME σύμφωνα με ένα σύνολο κρυπτογραφικών τυποποιήσεων, το *Public Key Cryptography Standards (PKCS).*

Η παγκόσμια υιοθέτηση του S/MIME θα επωφελήσει τους χρήστες, αφού έννοιες όπως η ακεραιότητα των δεδομένων, η αυθεντικότητα και η διαφύλαξη του απόρρητου των συναλλαγών *(privacy)*, θα είναι διαθέσιμες σε όλους.

Πριν προχωρήσουμε σε λεπτομέρειες για το S/MIME, και για να γίνουν κατανοητά αυτά που θα ακολουθήσουνε, θα πρέπει να περιγράψουμε σε γενικές γραμμές το πρωτόκολλο MIME.

## 5.3.1 Εισαγωγή στο S/MIME

Το S/MIME είναι ένα πρωτόκολλο που χρησιμοποιείται από προγράμματα ηλεκτρονικού ταχυδρομείου για την εφαρμογή κρυπτογραφικών υπηρεσιών σε αποστέλλοντα μηνύματα και για την επεξεργασία προστατευμένων παραληφθέντων. Η δεύτερη έκδοση του S/MIME είναι επί του παρόντος ενσωματωμένη σε πολλά δημοφιλή προϊόντα, όπως τα *Lotus Domino, Netscape Communicator, Novell GroupWise* και *Microsoft Exchange*. Το S/MIME δίνει την δυνατότητα σε εταιρίες που σχεδιάζουν λογισμικό να αναπτύσσουν προγράμματα τέτοια ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί από ένα άλλο.

Η ομάδα *Internet Engineering Task Force (IETF)* αναπτύσσει την $3^{η}$ έκδοση του S/MIME που περιλαμβάνει την εξειδίκευση *Cryptographic Message Syntax (CMS)* που ορίζει μια τυποποιημένη σύνταξη για την επικοινωνία των κρυπτογραφικών πληροφοριών που είναι ανεξάρτητες από την μορφή των ενθυλακωμένων περιεχομένων ή από τον μηχανισμό μεταφοράς. Κάθε τύπος δεδομένων μπορεί να προστατευθεί από το CMS. Εκτός από τις εφαρμογές S/MIME, το CMS μπορεί να χρησιμοποιηθεί με τα πρωτόκολλα HTTP, X.400, FTP, SSL και SET. Η στρατηγική ανάπτυξης της τρίτης έκδοσης είναι τέτοια ώστε να διατηρείται η συμβατότητα με την προηγούμενη έκδοση (version 2). Αυτό επιτυγχάνεται με την πρόσθεση νέων, προαιρετικών στοιχείων στην νέα έκδοση, των οποίων η απουσία στις επικεφαλίδες επιτρέπει την συνεργασία των δύο εκδόσεων.

Επίσης, η έκδοση 3 του S/MIME απαιτεί την ύπαρξη ενός ελάχιστου συνόλου κρυπτογραφικών αλγορίθμων που διασφαλίζουν την συνεργασίας μεταξύ διαφορετικών εφαρμογών.

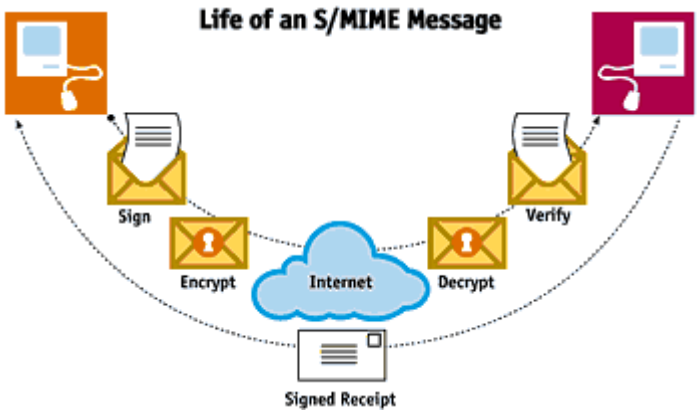
Η περιγραφή του S/MIME v3, που αναπτύχθηκε από την ομάδα IETF περιλαμβάνει τα εξής έγγραφα:

- *Cryptographic Message Syntax (CMS)*: Όπως προείπαμε, το CMS ορίζει ένα τυποποιημένο τρόπο σύνταξης για την ανταλλαγή κρυπτογραφικών πληροφοριών που σχετίζονται με τα προστατευμένα περιεχόμενα. Το CMS βασίζεται στο PKCS #7 Version 1.5 που χρησιμοποιείται στα τρέχοντα προϊόντα S/MIME. στο τελευταίο έχουν ενσωματωθεί προαιρετικά χαρακτηριστικά ασφάλειας όπως η ακεραιότητα δεδομένων (integrity), η πιστοποίηση ταυτότητας (authentication), η εξασφάλιση της μη αποκήρυξης της προέλευσης (non-repudiation of origin) και της διασφάλισης του απόρρητου (privacy).

| ***Security Services*** | ***Security Mechanism*** |
|---|---|
| *Authentication, Integrity, Non-repudiation* | *Digital Signature* |
| *Confidentiality* | *Encryption* |

- *S/MIME Version 3 Message Specification*: Ορίζει την MIME κωδικοποίηση που χρησιμοποιείται για την μεταφορά περιεχομένων προστατευμένων από το CMS. Συγκεκριμένα, καθορίζει τις διάφορες επιλογές για την ενθυλάκωση αυτών των περιεχομένων στα MIME μηνύματα και προστίθενται οι νέοι τύποι περιεχομένων multipart/signed και application/pkcs7-siganture. Όλα τα προγράμματα με εφαρμοσμένο το S/MIME πρέπει να συμμορφώνονται με αυτό το έγγραφο.
- *S/MIME Version 3 Certificate Handling System*: Υποχρεώνει την υποστήριξη των πιστοποιητικών X.509, που μαζί με τις Λίστες Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists) χρησιμοποιούνται για την πιστοποίηση ταυτότητας και την διαχείριση κλείδων.
- *Enhanced Security Services*: Το έγγραφο αυτό περιγράφει προαιρετικές υπηρεσίες ασφάλειας που μπορούν να παρέχονται σε συνδυασμό με την CMS προστασία. Οι προβλεπόμενες προαιρετικές υπηρεσίας είναι:

1. Υπογεγραμμένες αποδείξεις *(Signed Receipts)*: παρέχει αυθεντικές αποδείξεις παραλαβής μηνυμάτων.
2. Ετικέτες Ασφαλείας *(Security Labels)*: παρέχει την δυνατότητα ιεράρχησης των επιπέδων ασφάλειας, συνδέοντας τα δεδομένα με ετικέτες ευαισθησίας.
3. Ταχυδρομικές Λίστες *(Mail Lists)*: επιτρέπει στις ταχυδρομικές λίστες να διαχειρίζονται ασφαλισμένα μηνύματα.
4. Υπογεγραμμένα Πιστοποιητικά *(Signing Certificates)*: εξασφαλίζει την αυθεντικότητα των πιστοποιητικών.




## 5.3.2 Δημιουργία S/MIME μηνυμάτων

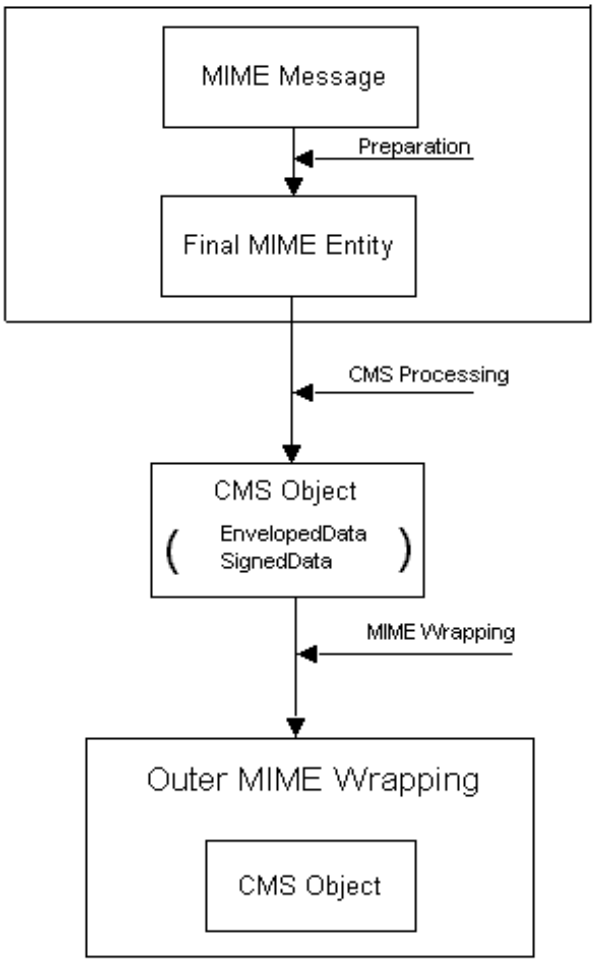
Τα μηνύματα S/MIME είναι συνδυασμός MIME μηνυμάτων και CMS αντικειμένων. Τα *CMS* αντικείμενα περιγράφουν το είδος της ασφάλειας που θέλουμε να εφαρμόσουμε και μπορεί να είναι Ψηφιακός Φάκελος *(Enveloped-Data)*, Υπογεγραμμένα δεδομένα *(Signed-Data)* και άλλα. Μπορούν να χρησιμοποιηθούν όλοι οι τύποι δεδομένων του MIME, χωρίς κανένα περιορισμό. Το *MIME* μήνυμα, μαζί με άλλες πληροφορίες (πιστοποιητικά, αναγνωριστικά αλγόριθμων κ.α.), επεξεργάζονται από τις διαδικασίες του CMS και παράγεται το CMS αντικείμενο. Τέλος, το CMS αντικείμενο τυλίγεται σε εξωτερικό MIME μήνυμα με κατάλληλες επικεφαλίδες.

### Προετοιμασία

Η MIME οντότητα που θα ασφαλιστεί από το S/MIME μπορεί να είναι είτε μέρος ενός μηνύματος, είτε ολόκληρο μήνυμα. Σε περίπτωση που η MIME οντότητα ισοδυναμεί με ολόκληρό το μήνυμα, περιλαμβάνονται σ' αυτήν όλες τις MIME επικεφαλίδες (δεν περιλαμβάνονται οι επικεφαλίδες του RFC822) και φυσικά τα περιεχόμενα.

Η διαδικασία που προετοιμάζει το μήνυμα/οντότητα για επεξεργασία από το CMS αποτελείται από 3 βασικά βήματα:

1. : Η MIME οντότητα κατασκευάζεται σύμφωνα με τις υποδείξεις του τοπικού περιβάλλοντος. Το σύνολο χαρακτήρων και οι χαρακτήρες οριοθέτησης γραμμών *(line delimiters)* καθορίζονται από το τοπικό σύστημα.
2. : Η MIME οντότητα μετατρέπεται σε κανονική μορφή *(canonical form)*. Η μορφή αυτή είναι διεθνώς αναγνωρίσιμη και παρουσιάσιμη είναι ανεξάρτητη από την πλατφόρμα του εκάστοτε χρήστη. Ανάλογα με τον τύπο δεδομένων, οι ενέργειες που πρέπει να γίνουν ώστε να προκύψει αυτή η μορφή, διαφέρουν. Για παράδειγμα, για περιεχόμενα τύπου κειμένου ο χαρακτήρας οριοθέτησης γραμμών πρέπει να είναι το ζευγάρι <CR>CLF>, και το σύνολο χαρακτήρων πρέπει να είναι ένα από τα τυποποιημένα.




3.

4. : Εφαρμόζεται κατάλληλη κωδικοποίηση μεταφοράς *(transfer encoding)*. Απαιτείται όλες οι MIME οντότητες που πρόκειται να ασφαλιστούν με το S/MIME, να είναι σε κωδικοποίηση 7bit, για σίγουρη και σωστή μεταφορά. Αυτό συμβαίνει γιατί δεν είναι βέβαιο κατά πόσο υποστηρίζεται η μεταφορά μηνυμάτων με κωδικοποίηση 8bit ή binary σε όλο το μονοπάτι από τον αποστολέα στον παραλήπτη. Εάν ένα τέτοιο μήνυμα συναντήσει ενδιάμεσο σύστημα που δεν μπορεί να μεταδώσει 8bit ή binary δεδομένα, τότε υπάρχουν τρεις επιλογές: (α) το σύστημα θα μπορούσε να αλλάξει το κωδικοποίηση μεταφοράς, ακυρώνοντας την υπογραφή, (β) το σύστημα θα μπορούσε να προωθήσει το μήνυμα όπως και να' χει, με καταστροφή του $8^{ου}$ bit και συνεπώς ακύρωσης της υπογραφής και (γ) το σύστημα θα μπορούσε να επιστρέψει το μήνυμα. Και τρεις επιλογές είναι απαράδεκτες. Οι μηχανισμοί, λοιπόν, Quoted-Printable και Base64 είναι απαραίτητοι.

## CMS Αντικείμενα και CMS Επεξεργασία

Σ' αυτό το κεφάλαιο θα περιγράψουμε τα αντικείμενα ασφαλείας του CMS και πως αυτά κατασκευάζονται. Τα υποστηριζόμενα αντικείμενα είναι EnvelopedData, SignedData, DigestedData, EncryptedData και AuthenticatedData. Για κάθε αντικείμενο ο τύπος των περιεχομένων αλλάζει. Έτσι, το αντικείμενο EnvelopedData

περιέχει δεδομένα σε ψηφιακό φάκελο (θα δούμε παρακάτω τι σημαίνει αυτό), το SignedData περιέχει υπογεγραμμένα δεδομένα, το EncryptedData περιέχει κρυπτογραφημένα δεδομένα, το DigestedData περιλαμβάνει την digest τιμή των δεδομένων και τέλος, το AuthenticatedData περιέχει πιστοποιημένα δεδομένα. Τα σημαντικότερα και περισσότερο χρησιμοποιούμενα αντικείμενα είναι τα SignedData και τα EnvelopedData, τα οποία και θα αναλύσουμε πιο πολύ. Εξάλλου, η υποστήριξη των υπόλοιπων αντικείμενων είναι προαιρετική.

Τα ασφαλισμένα περιεχόμενα δεν είναι η μόνη πληροφορία που περικλείεται σε ένα αντικείμενο. Υπάρχουν και άλλες πληροφορίες που προορίζονται για επεξεργασία από τα προγράμματα S/MIME και εισάγονται σε πεδία που καλούνται ιδιότητες (attributes). Πολλές φόρες, ίσως, αυτές οι ιδιότητες να απαιτούν προστασία είτε μέσω υπογραφής, είτε μέσω κρυπτογράφησης.

Επίσης, πρέπει να διευκρινιστεί, ότι όπου στο παρών κεφάλαιο αναφερόμαστε σε "περιεχόμενα οποιουδήποτε τύπου", εννοούμε δεδομένα απλά, κρυπτογραφημένα, υπογεγραμμένα, πιστοποιημένα ή συνοψισμένα (digested). Τα απλά δεδομένα ισοδυναμούν με την MIME οντότητα, που είναι η είσοδος στην CMS επεξεργασία, ενώ οι υπόλοιποι τύποι αναφέρονται σε αντικείμενα του CMS, δηλαδή είδη προστατευμένα MIME στοιχεία.

**SignedData**: Αποτελείται από περιεχόμενα οποιουδήποτε τύπου και μηδέν ή περισσότερες υπογραφές αυτών. Τα περιεχόμενα μπορούν να υπογραφούν παράλληλα από πολλούς χρήστες και τυπική εφαρμογή αυτού του τύπου είναι για την υπογραφή απλών δεδομένων ή για την μεταφορά πιστοποιητικών.

Η διαδικασία σύμφωνα με την οποία κατασκευάζονται τα υπογεγραμμένα δεδομένα έχει ως εξής:

1. Για κάθε υπογράφοντα, παράγεται η συνοπτική τιμή (digest value) των περιεχομένων βάση αλγόριθμου που εξαρτάται από τον υπογράφοντα. Εάν μαζί με τα περιεχόμενα υπογράφονται και συγκεκριμένες ιδιότητες τότε παράγεται η digest value των περιεχομένων, εισάγεται σε ειδικό πεδίο των προς υπογραφή ιδιοτήτων και το τελικό message digest είναι η digest value των ιδιοτήτων.
2. Το message digest που προκύπτει από το προηγούμενο βήμα για κάθε υπογράφοντα, κρυπτογραφείται με την ιδιωτική κλείδα κάθε υπογράφοντα ξεχωριστά.
3. Για κάθε υπογράφοντα, το αποτέλεσμα της υπογραφής και άλλες πληροφορίες σχετικές με αυτόν συλλέγονται στο πεδίο SignerInfo. Το πεδίο αυτό υπάρχει μια φορά για κάθε χρήστη και αποτελείται από καταχωρήσεις που περιλαμβάνουν τα πιστοποιητικά της ταυτότητας του χρήστη (μαζί και την δημόσια κλείδα αυτού), τους αλγόριθμούς που χρησιμοποιήθηκαν και την υπογραφή αυτού.
4. Όλα τα πεδία SignerInfo, τα περιεχόμενα και επιπλέον πληροφορίες συλλέγονται και φτιάχνουν το αντικείμενο SignedData.

Ο παραλήπτης του μηνύματος/αντικειμένου υπολογίζει το message digest των περιεχομένων και με την δημόσια κλείδα του αποστολέα ανακτεί το

κρυπτογραφημένο message digest που παρέλαβε με το μήνυμα. Συγκρίνει αυτά δύο, και εάν είναι ταυτόσημα, τότε έχει επαληθεύσει επιτυχώς την υπογραφή.

**EnvelopedData**: Αποτελείται από κρυπτογραφημένα περιεχόμενα οποιουδήποτε τύπου και κρυπτογραφημένα κλειδιά-κρυπτογράφησης για έναν ή περισσότερους αποδέκτες. Ο συνδυασμός των κρυπτογραφημένων περιεχομένων και του κρυπτογραφημένου κλειδιού, είναι ένας "ψηφιακός φάκελος". Για την επικοινωνία του κλειδιού-κρυπτογράφησης (του κλειδιού δηλαδή που χρησιμοποιήθηκε κατά την κρυπτογράφηση των περιεχομένων) υπάρχουν τρεις (3) τεχνικές και για κάθε παραλήπτη μπορεί να χρησιμοποιηθεί οποιαδήποτε από αυτές:

- *key transport*: το κλειδί κρυπτογραφείται με την δημόσια κλείδα του παραλήπτη.
- *key agreement*: η δημόσια κλείδα τού παραλήπτη και η ιδιωτική κλείδα τού αποστολέα χρησιμοποιούνται για να παράγουν (μέσω κατάλληλου αλγόριθμου) ένα συμμετρικό κλειδί το οποίο κρυπτογραφεί το κλειδί κρυπτογράφησης. Λόγω της μαθηματικής σχέσης που συνδέει την δημόσια κλείδα με την ιδιωτική κλείδα και της φύσης του αλγόριθμου, το ίδιο συμμετρικό κλειδί μπορεί να παράγει ο παραλήπτης, χρησιμοποιώντας την ιδιωτική του κλείδα και την δημόσια του αποστολέας.
- *symmetric key-agreement*: το κλειδί-κρυπτογράφησης, κρυπτογραφείται με συμμετρικό κλειδί που έχει πρωτύτερα διανεμηθεί.

Η διαδικασία κατασκευής των ψηφιακών φακέλων είναι:

1. Παράγεται το τυχαίο κλειδί κρυπτογράφησης.
2. Για κάθε παραλήπτη, κρυπτογραφείται το κλειδί-κρυπτογράφησης. Οι λεπτομέρειες αυτής της κρυπτογράφησης, εξαρτούνται από το ποία από τις παραπάνω τεχνικές χρησιμοποιείται.
3. Το κρυπτογραφημένο κλειδί και άλλες πληροφορίες που αφορούν κάθε παραλήπτη συλλέγονται στο πεδίο RecipientInfo. Το τελευταίο, όπως και το SignerInfo, περιέχει τα πιστοποιητικά κάθε χρήστη, την τεχνική που χρησιμοποιήθηκε, τους αλγόριθμους και το κρυπτογραφημένο κλειδί. Υπάρχει αριθμό ίσο με τον αριθμό των παραληπτών.
4. Τα περιεχόμενα κρυπτογραφούνται με το κλειδί-κρυπτογράφησης. Τα περιεχόμενα, ίσως, να χρειαστούν συμπλήρωμα (padding).
5. Τα πεδία RecipientInfo για όλους τους παραλήπτες, μαζί με τα κρυπτογραφημένα περιεχόμενα αποτελούν το αντικείμενο EnvelopedData.

Ο εκάστοτε παραλήπτης, αφού ανακτήσει το κρυπτογραφημένο κλειδί ακολουθώντας την τεχνική που υποδεικνύεται στο RecipientInfo πεδίο, αποκρυπτογραφεί τα περιεχόμενα του μηνύματος.

Θα αναφερθούμε σύντομα και στα υπόλοιπα, προαιρετικά αντικείμενα. Το **DigestData** συνίσταται από περιεχόμενα οποιουδήποτε τύπου και την digest value αυτών. Το **EncryptedData** διαφέρει από το EnvelopedData στο ότι το πρώτο δεν περιέχονται τα κλειδιά –κρυπτογράφησης κρυπτογραφημένα και δεν έχει παραλήπτες. Προορίζεται για τοπική κρυπτογράφηση αρχείων. Τέλος, το **AuthenticatedData** μοιάζει με το SignedData, με την διαφορά, ότι αντί για την υπογραφή του μηνύματος περιέχεται το Message Authentication Code (MAC).

## MIME Wrapping

Μέχρι τώρα έχουμε περιγράψει, πως προετοιμάζεται η MIME οντότητα και πως δημιουργούνται τα CMS αντικείμενα από αυτήν. Το τελικό στάδιο παραγωγής ενός S/MIME μηνύματος είναι η περιτύλιξη του CMS αντικειμένου με ένα εξωτερικό MIME επίπεδο και ασχοληθούμε με αυτό σε αυτό το κεφάλαιο.

### *Οι Νέες Επικεφαλίδες*

Όπως αναφέραμε στην εισαγωγή, προστίθενται δύο νέες επικεφαλίδες, στις είδη υπάρχουσες επικεφαλίδες του MIME: η multipart/signed και η application/pkcs7-mime. Αυτές οι νέες επικεφαλίδες χρησιμοποιούνται κατά την περιτύλιξη και εσωκλείουν τα CMS αντικείμενα.

Η **multipart/signed** υποδηλώνει μήνυμα με δυο body parts. Το πρώτο μέρος περιέχει αυτούσια την MIME οντότητα που ασφαλίζεται, αφού υποστεί την προεργασία που περιγράφηκε προηγουμένως. Το δεύτερο μέρος περιέχει την υπογραφή της MIME οντότητας και η επικεφαλίδα του body part είναι application/pkcs7-signature (βλέπε παρακάτω παράγραφο).

Η **application/pkcs7-mime** χρησιμοποιείται για να μεταφέρει CMS αντικείμενα διάφορων τύπων (Ψηφιακός Φάκελος, Υπογεγραμμένα Δεδομένα, κ.α.), τα οποία εμπεριέχουν μία MIME οντότητα. Καθ' ότι τα CMS αντικείμενα είναι δυαδικά δεδομένα, ο κατάλληλος μηχανισμός κωδικοποίησης που πρέπει να χρησιμοποιηθεί είναι ο Base64, ειδικά όταν το πρωτόκολλο μεταφοράς είναι το SMTP. Εδώ πρέπει να πούμε ότι η κωδικοποίηση αυτή αναφέρεται στο CMS αντικείμενο και όχι στην MIME οντότητα. Συνεπώς δεν υπάρχει σχέση με το 3$^{ο}$ βήμα της προετοιμασίας του MIME μηνύματος.

Όταν η τιμή της επικεφαλίδας είναι application/pkcs7-mime και η επέκταση του αρχείου το οποίο αποτελείται από το CMS αντικείμενο είναι .p7m τότε το αντικείμενο είναι είτε Ψηφιακός Φάκελος, είτε Υπογεγραμμένα Δεδομένα. Εάν η επέκταση είναι .p7c και η τιμή η ίδια με προηγουμένως, το αντικείμενο είναι μόνο πιστοποιητικά. Τέλος, εάν η τιμή είναι application/pkcs7-signature και η επέκταση .p7s, το αντικείμενο είναι σκέτη υπογραφή.

### *Φακελωμένο Μήνυμα (Enveloped Message)*

Συνδυάζοντας τα παραπάνω, τα βήματα για την παρασκευή φακελωμένου μηνύματος θα είναι:

I. Η MIME οντότητα προετοιμάζεται κατάλληλα.
II. Η MIME οντότητα και άλλες απαραίτητες πληροφορίες επεξεργάζονται για την κατασκευή του αντικειμένου EnvelopedData.
III. Στο CMS αντικείμενο EnvelopedData, προστίθεται η επικεφαλίδα application/pkcs7-mime και πραγματοποιείται η περιτύλιξη του τελικού σταδίου.

Παράδειγμα ενός S/MIME μηνύματος ασφαλισμένο κατά αυτόν τον τρόπο είναι:

Η παράμετρος smime-type καθορίζει το είδος του αντικείμενου και η επέκταση του μεταφερόμενου αρχείου είναι ".p7m". Ένα τέτοιο μήνυμα ,όμως, δεν προσφέρει ακεραιότητα δεδομένων.

***Υπογεγραμμένο Μήνυμα (Signed Message)***

Υπάρχουν δύο δυνατότητες για την παρασκευή υπογεγραμμένων μηνυμάτων. Η πρώτη περίπτωση περιλαμβάνει την χρήση της επικεφαλίδας application/pkcs7-mime και η δεύτερη την χρήση της multipart/signed.

application/pkcs7-mime: Τα βήματα είναι παρόμοια με αυτά του φακελωμένου μηνύματος.

I. Η MIME οντότητα προετοιμάζεται κατάλληλα.
II. Η MIME οντότητα και άλλες απαραίτητες πληροφορίες επεξεργάζονται για την κατασκευή του αντικειμένου SignedData.
III. Στο SignedData, προστίθεται η επικεφαλίδα application/pkcs7-mime και πραγματοποιείται η περιτύλιξη του τελικού σταδίου.

Παράδειγμα ενός τέτοιου S/MIME μηνύματος:

Και εδώ, η παράμετρος smime-type καθορίζει το είδος του αντικείμενου και η επέκταση του μεταφερόμενου αρχείου είναι ".p7m".

multipart/signed: Σε αυτήν την MIME επικεφαλίδα, το περιεχόμενο SignedData αντικείμενο αποτελείται μόνο από την υπογραφή της MIME οντότητας. Αυτό συμβαίνει γιατί όπως θα δούμε, το πρώτο body part περικλείει το αυθεντικό MIME στοιχείο.

I. Η MIME οντότητα προετοιμάζεται κατάλληλα.
II. Έπειτα, η MIME οντότητα οδηγείται στην CMS επεξεργασία και προκύπτει ένα αντικείμενο SignedData, από το οποίο όμως αφαιρείται το υπογεγραμμένο περιεχόμενο (η MIME οντότητα δηλαδή).
III. Το αποτέλεσμα του πρώτου βήματος, εισάγεται στο πρώτο μέρος του multipart μηνύματος.
IV. Αφού κωδικοποιηθεί κατάλληλα για μεταφορά η υπογραφή (που αποκτήθηκε στο δεύτερο βήμα), εισάγεται στο δεύτερο μέρος του multipart μηνύματος με επικεφαλίδα body part, application/pkcs7-signature.

Στο παρακάτω σχήμα παρατηρούμε στο δεύτερο body part, την επέκταση του αρχείου, ".p7s" και την κωδικοποίηση μεταφοράς Base64.

Τις περισσότερες φορές, χρησιμοποιείται η περιτύλιξη με multipart/signed. Το εσωτερικό ενός τέτοιου μηνύματος μπορεί να αναγνωστεί και από χρήστες των οποίων τα προγράμματα δεν ενσωματώνουν τις S/MIME λειτουργίες. Βέβαια, αναγνώριση και επαλήθευση της υπογραφής στο δεύτερο body part δεν είναι δυνατόν να γίνει και άρα δεν μπορεί να επιβεβαιωθεί η ακεραιότητα των δεδομένων ούτε η ταυτότητα του αποστολέα.

***Μήνυμα με Πιστοποιητικά (Certificate-only Message)***

Αυτό το μήνυμα μεταφέρει πιστοποιητικά και Λίστες Ανάκλησης Πιστοποιητικών. Κατασκευάζεται σε δύο βήματα:

I. Τα πιστοποιητικά δίνονται για CMS επεξεργασία και προκύπτει αντικείμενο SignedData χωρίς υπογεγραμμένο περιεχόμενο και υπογραφή.
II. Προστίθεται η επικεφαλίδα application/pkcs7-mime και ολοκληρώνεται η MIME περιτύλιξη.

Η παράμετρος smime-type, που είδαμε στα προηγούμενα παραδείγματα, είναι certs-only και η επέκταση του αρχείου είναι ".p7c".

***Υπογράφοντας και Κρυπτογραφώντας***

Για μέγιστη διασφάλιση της μεταφερόμενη πληροφορίας, επιτρέπεται ένα μήνυμα διαδοχικά να υπογραφεί και να κρυπτογραφηθεί και αντίστροφα. Μια εφαρμογή του S/MIME πρέπει να είναι σε θέση να παραλάβει και να επεξεργαστεί ένα μήνυμα με αυθαίρετο αριθμό φωλιασμένων υπογραφών και κρυπτογραφήσεων.

Το μήνυμα μπορεί είτε να υπογραφεί πρώτα και να κρυπτογραφηθεί έπειτα, είτε να κρυπτογραφηθεί και μετά να υπογραφεί. Στην πρώτη περίπτωση, οι υπογραφές ασφαλίζονται και η μετάδοση γίνεται με απόλυτη εμπιστευτικότητα. Στην δεύτερη περίπτωση, εξασφαλίζεται η ακεραιότητα του κρυπτογραφημένου μηνύματος και επιτρέπεται η επαλήθευση των υπογραφών, χωρίς την αποκρυπτογράφηση του.

# *5.4 PGP (Pretty Good Privacy)*

## 5.4.1 Εισαγωγή

Το λογισμικό Pretty Good Privacy (PGP), το οποίο σχεδιάστηκε από τον Phill Zimmerman, είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX/VMS και για άλλες πλατφόρμες. Το PGP επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.

*Διασφάλιση* του απορρήτου σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το διαβάσει.

*Πιστοποίηση της* ταυτότητας σημαίνει ότι μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο.

Ευκολία σημαίνει ότι η διασφάλιση του απόρρητου και η πιστοποίησης της ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία. Δεν είναι αναγκαία ασφαλή κανάλια για την ανταλλαγή κλειδιών μεταξύ χρηστών κάτι που κάνει το PGP πολύ ευκολότερο στη χρήση από κάθε άλλο αντίστοιχο πακέτο. Αυτό συμβαίνει διότι το PGP είναι

βασισμένο σε μια δυναμική νέα τεχνολογία που καλείται κρυπτογράφηση "δημοσίων κλειδιών" (public key).

Το PGP συνδυάζει την ευκολία του RSA κρυπτοσυστήματος δημοσίων κλειδιών με την ταχύτητα της συμβατικής κρυπτογράφησης, περιλήψεις μηνυμάτων για ψηφιακές υπογραφές, συμπίεση δεδομένων πριν την κρυπτογράφηση, καλός εργονομικός σχεδιασμός και υψηλού επιπέδου διαχείριση κλειδιών. Επιπλέον το PGP εκτελεί τις λειτουργίες των δημοσίων κλειδιών γρηγορότερα από τα περισσότερα αντίστοιχα προγράμματα. Το PGP είναι κρυπτογράφηση δημοσίων κλειδιών για τις μάζες.

Σήμερα εάν η κυβέρνηση θελήσει να παραβιάσει το απόρρητο των πολιτών πρέπει να καταβάλλει ένα συγκεκριμένο ποσό χρημάτων και εργασίας για να υποκλέψει και να διαβάσει το συμβατικό ταχυδρομείο και να ακούσει ή να υποκλέψει τηλεφωνικές συνομιλίες. Αυτός ο τρόπος της παρακολούθησης δεν είναι πρακτικός σε μεγάλο επίπεδο. Αυτό συμβαίνει μόνο σε σημαντικές περιπτώσεις όπου φαίνεται ότι αξίζει.

Όλο και μεγαλύτερο ποσοστό από τις ιδιωτικές μας επικοινωνίες δρομολογείται μέσω ηλεκτρονικών καναλιών. Το ηλεκτρονικό ταχυδρομείο σταδιακά αντικαθιστά το συμβατικό ταχυδρομείο. Τα μηνύματα e-mail είναι πολύ εύκολο να υποκλέπτουν και να περάσουν από διαδικασία ανίχνευσης βάσει καθορισμένων λέξεων-κλειδιών (keywords). Αυτό μπορεί να γίνει εύκολα, αυτόματα και χωρίς να πέσει στην αντίληψη κανενός σε μεγάλο επίπεδο. Οι διεθνείς συνδέσεις βρίσκονται ήδη κάτω από μια τέτοια διαδικασία παρακολούθησης από την NSA.

Κινούμαστε προς ένα μέλλον όπου οι υπολογιστές διεθνώς θα ενώνονται με δίκτυα οπτικών ινών υψηλής χωρητικότητας. Το e-mail θα είναι κάτι το αυτονόητο για όλους και όχι η καινοτομία που θεωρείται σήμερα. Οι κυβερνήσεις θα προστατεύουν το e-mail των πολιτών με πρωτόκολλα σχεδιασμένα από τις ίδιες. Πιθανότατα οι περισσότεροι άνθρωποι θα συμβιβαστούν με αυτή τη λύση αλλά ίσως μερικοί προτιμήσουν να πάρουν τα δικά τους μέτρα ασφάλειας.

## 5.4.2 Λειτουργία Του PGP

Για να κατανοήσουμε τη λειτουργία του PGP θα πρέπει να αναφέρουμε λίγα λόγια πάνω στην ορολογία που χρησιμοποιείται. Ας θεωρήσουμε ότι θέλει κάποιος να στείλει ένα μήνυμα αλλά δεν θέλει να το διαβάσει κανένας άλλος εκτός από τον παραλήπτη. Μπορεί να το κρυπτογραφήσει με τη χρήση ενός κλειδιού το οποίο θα πρέπει να χρησιμοποιηθεί στην αποκρυπτογράφηση του μηνύματος από τον παραλήπτη του—τουλάχιστον έτσι δουλεύει η συμβατική κρυπτογραφία ενός κλειδιού.

Στα συμβατικά κρυπτοσυστήματα, όπως το DES, ένα και μόνο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτό σημαίνει ότι το κλειδί θα πρέπει να μεταδοθεί αρχικά μέσα από ένα ασφαλές κανάλι έτσι ώστε και τα δυο μέρη να το γνωρίζουν προτού αρχίσει η αποστολή κρυπτογραφημένων μηνυμάτων μέσω ασφαλών καναλιών. Αυτό δεν είναι και τόσο

βολικό διότι αν έχεις ένα ασφαλές κανάλι για να ανταλλάζεις κλειδιά τότε τι χρειάζεσαι την κρυπτογραφία;

Στα κρυπτοσυστήματα δημοσίων κλειδιών ο καθένας έχει δυο συμπληρωματικά κλειδιά. Ένα που δίδεται δημόσια (public key) και ένα μυστικό (secret key ή private key). Το κάθε κλειδί ξεκλειδώνει τον κώδικα που το άλλο φτιάχνει. Η γνώση του δημοσίου κλειδιού δεν βοηθάει στην εξαγωγή του αντίστοιχου μυστικού κλειδιού. Το δημόσιο κλειδί μπορεί να διατεθεί σε ένα δίκτυο επικοινωνιών. Αυτό το πρωτόκολλο παρέχει διασφάλιση του απόρρητου χωρίς την ανάγκη ύπαρξης ασφαλών καναλιών, όπως απαιτεί η συμβατική κρυπτογραφία.

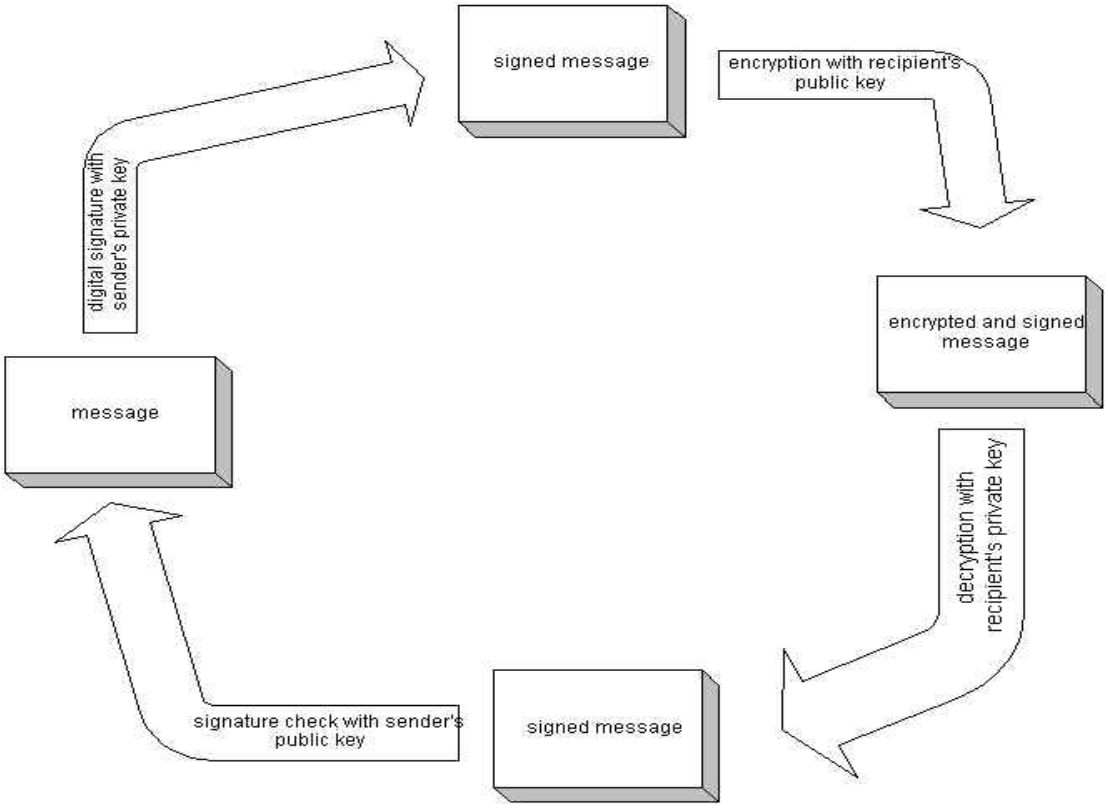
Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη ενός μηνύματος για να κρυπτογραφήσει ένα μήνυμα προς αυτό το άτομο ενώ ο παραλήπτης μπορεί να χρησιμοποιήσει με τη σειρά του το αντίστοιχο μυστικό κλειδί για να αποκρυπτογραφήσει το μήνυμα. Κανένας άλλος εκτός από τον παραλήπτη δεν μπορεί να το αποκρυπτογραφήσει διότι κανένας άλλος δεν έχει πρόσβαση στο μυστικό κλειδί - ακόμη και το άτομο που κρυπτογράφησε το μήνυμα.

Επίσης παρέχεται υπηρεσία πιστοποίησης του μηνύματος. Το μυστικό κλειδί του αποστολέα μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος άρα και για την υπογραφή του. Έτσι δημιουργείται μια ψηφιακή υπογραφή του μηνύματος την οποία ο παραλήπτης ή οποιοσδήποτε άλλος μπορεί να ελέγξει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να την αποκρυπτογραφήσει. Αυτό αποδεικνύει ότι ο αποστολέας ήταν ο πραγματικός δημιουργός του μηνύματος και ότι το μήνυμα δεν αλλοιώθηκε από κάποιον άλλον διότι μόνο ο αποστολέας έχει στην κατοχή του το μυστικό κλειδί που έφτιαξε την υπογραφή. Η πλαστογράφηση ενός υπογεγραμμένου μηνύματος δεν είναι εφικτή και ο αποστολέας δεν μπορεί μετά να απαρνηθεί την υπογραφή του.

Αυτές οι δυο διαδικασίες μπορούν να συνδυαστούν για την παροχή τόσο διασφάλισης του απόρρητου όσο και πιστοποίησης της ταυτότητας αφού μπορεί κάποιος πρώτα να υπογράψει ένα μήνυμα με το μυστικό κλειδί του και μετά να το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης αντιστρέφει αυτά τα βήματα αποκρυπτογραφώντας πρώτα το μήνυμα με το μυστικό κλειδί του και κατόπιν ελέγχοντας την ψηφιακή υπογραφή που περιέχεται σε αυτό με το δημόσιο κλειδί του αποστολέα. Αυτές οι διαδικασίες γίνονται αυτόματα από το λογισμικό του παραλήπτη.

Επειδή ο αλγόριθμος της κρυπτογράφησης δημοσίων κλειδιών είναι πολύ πιο αργός από τη συμβατική κρυπτογράφηση ενός κλειδιού η κρυπτογράφηση επιτυγχάνεται καλύτερα με τη χρήση ενός υψηλής ποιότητας γρήγορου αλγόριθμου συμβατικής κρυπτογράφησης ενός κλειδιού για την κρυπτογράφηση του μηνύματος. Το αρχικό μη κρυπτογραφημένο μήνυμα καλείται "απλό κείμενο". Σε μια διαδικασία αόρατη στο χρήστη ένα προσωρινό τυχαίο κλειδί, το οποίο έχει δημιουργηθεί μόνο για τη συγκεκριμένη φορά, χρησιμοποιείται για να κρυπτογραφηθεί συμβατικά το αρχείο "απλό κείμενο". Μετά το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για να κρυπτογραφηθεί αυτό το προσωρινό κλειδί. Αυτό το συμβατικά δημιουργημένο κλειδί μιας φοράς (session key) το οποίο έχει κρυπτογραφηθεί και με τη διαδικασία του δημόσιου κλειδιού αποστέλλεται μαζί με το κρυπτογραφημένο κείμενο (κρυπτοκείμενο) στον παραλήπτη. Ο παραλήπτης χρησιμοποιεί το δικό του μυστικό

κλειδί για να ανακτήσει το session key και μετά χρησιμοποιεί αυτό κλειδί για να τρέξει τον γρήγορο συμβατικό αλγόριθμο ενός κλειδιού έτσι ώστε να αποκρυπτογραφήσει το κρυπτοκείμενο. Η όλη διαδικασία φαίνεται στο παρακάτω σχήμα:




Τα δημόσια κλειδιά φυλάσσονται σε ξεχωριστά πιστοποιητικά κλειδιών (key certificates) τα οποία περιλαμβάνουν την ταυτότητα του ιδιοκτήτη τους (το όνομα του ιδιοκτήτη), μια σφραγίδα χρόνου που δείχνει πότε το ζεύγος των κλειδιών δημιουργήθηκε και τέλος το ίδιο το υλικό του κλειδιού. Τα πιστοποιητικά δημοσίων κλειδιών περιλαμβάνουν το υλικό των δημοσίων κλειδιών ενώ τα πιστοποιητικά των μυστικών κλειδιών περιλαμβάνουν το υλικό των μυστικών κλειδιών. Κάθε μυστικό κλειδί κρυπτογραφείται επιπλέον με τον κωδικό του σε περίπτωση που κλαπεί. Ένα αρχείο κλειδιών ή ένα μπρελόκ κλειδιών (key ring) περιέχει ένα ή περισσότερα από αυτά τα πιστοποιητικά κλειδιών. Τα δημόσια μπρελόκ περιέχουν τα δημόσια πιστοποιητικά κλειδιών ενώ τα ιδιωτικά μπρελόκ περιέχουν τα ιδιωτικά πιστοποιητικά κλειδιά.

Τα κλειδιά χαρακτηρίζονται από ένα "key id" (ταυτότητα κλειδιού) η οποία είναι μια συντομογραφία του δημόσιου κλειδιού (τα 64 λιγότερο σημαντικά bits του δημοσίου κλειδιού). Όταν αυτή η ταυτότητα παρουσιάζεται μόνο τα 32 λιγότερο σημαντικά bits δίνονται για επιπλέον ελαχιστοποίηση του όγκου της ταυτότητας. Καθώς πολλά κλειδιά μπορεί να μοιράζονται το ίδιο user id (ταυτότητα χρήστη), για πρακτικούς λόγους κανένα κλειδί δεν μοιράζεται το ίδιο key id με κανένα άλλο.

Το PGP χρησιμοποιεί τις περιλήψεις μηνυμάτων (message digests) για να δημιουργήσει υπογραφές. Μια περίληψη μηνύματος είναι μια κρυπτογραφικά πολλή δυνατή μονόδρομη (hash) συνάρτηση 128 bit του μηνύματος. Είναι κάτι ανάλογο με το "check sum" ή CRC κώδικα ελέγχου στο ότι αντιπροσωπεύουν συμπαγώς το μήνυμα και χρησιμοποιούνται για την ανίχνευση αλλαγών σε αυτό. Αντίθετα βέβαια με το CRC είναι υπολογιστικά αδύνατο για κάποιον επιτιθέμενο να φτιάξει ένα υποκατάστατο μήνυμα το οποίο θα μπορούσε να παράγει την ίδια περίληψη μηνύματος. Η περίληψη μηνύματος κρυπτογραφείται με το μυστικό κλειδί και έτσι σχηματίζει την ψηφιακή υπογραφή.

Τα κείμενα υπογράφονται με την εισαγωγή στην αρχή τους ψηφιακών πιστοποιητικών υπογραφών οι οποίες περιέχουν το key id του κλειδιού που χρησιμοποιήθηκε για την υπογραφή τους, μια υπογεγραμμένη με το μυστικό κλειδί περίληψη του κειμένου και μια χρονική σφραγίδα της δημιουργίας της υπογραφής. Το key id χρησιμοποιείται από τον παραλήπτη για την ανεύρεση του δημόσιου κλειδιού του αποστολέα έτσι ώστε να ελέγξει την ψηφιακή υπογραφή. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το δημόσιο κλειδί του αποστολέα και το user id του στο μπρελόκ δημοσίων κλειδιών που έχει στην κατοχή του ο παραλήπτης.

Τα κρυπτογραφημένα αρχεία περιέχουν στην αρχή τους το key id του δημοσίου κλειδιού που χρησιμοποιήθηκε στην κρυπτογράφησή τους. Ο παραλήπτης χρησιμοποιεί αυτό το key id για την ανεύρεση του μυστικού κλειδιού που απαιτείται για την αποκρυπτογράφηση του μηνύματος. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το απαραίτητο μυστικό κλειδί αποκρυπτογράφησης στο μπρελόκ μυστικών κλειδιών του παραλήπτη.

Αυτοί οι δυο τύποι μπρελόκ κλειδιών είναι η κύρια μέθοδος της αποθήκευσης και διαχείρισης των δημόσιων και ιδιωτικών κλειδιών. Αντί να κρατάμε ξεχωριστά κλειδιά σε ξεχωριστά αρχεία κλειδιών τα μαζεύουμε σε μπρελόκ κλειδιών έτσι ώστε να διευκολύνουμε την αυτόματη ανεύρεσή τους είτε με τη χρήση του key id είτε με τη χρήση του user id. Κάθε χρήστης διατηρεί το δικό του ζεύγος μπρελόκ. Ένα ξεχωριστό δημόσιο κλειδί αποθηκεύεται προσωρινά σε ένα ξεχωριστό αρχείο μόνο για το χρόνο που χρειάζεται για την αποστολή του σε κάποιο φίλο ο οποίος κατόπιν θα το προσθέσει στο δικό του μπρελόκ κλειδιών.

## 5.4.3 Προστασία Δημοσίων Κλειδιών

Σε ένα κρυπτοσύστημα δημοσίων κλειδιών δεν υπάρχει ανάγκη προστασίας των δημοσίων κλειδιών, διότι το επιδιωκόμενο είναι η όσο το δυνατόν ευρύτερη διάδοσή τους. Το σημαντικό και αυτό που θα πρέπει να διασφαλίζεται είναι το να είμαστε σίγουροι ότι κάποιο δημόσιο κλειδί που φαίνεται ότι ανήκει σε κάποιον, όντως να ανήκει σε αυτόν. Αυτό μπορεί να είναι και το πιο σημαντικό μειονέκτημα του κρυπτοσυστήματος δημόσιων κλειδιών. Ας εξετάσουμε το λόγο:

Ας υποθέσουμε ότι ο Bob θέλει να στείλει ένα προσωπικό μήνυμα στην Alice. Για να το κάνει αυτό κατεβάζει το πιστοποιητικό δημοσίων κλειδιών από κάποιο σύστημα ηλεκτρονικού πίνακα ανακοινώσεων (BBS). Κατόπιν, κρυπτογραφεί το γράμμα προς την Alice με αυτό δημόσιο κλειδί και το στέλνει σε αυτήν μέσω της λειτουργίας e-mail του BBS.

Ατυχώς, τόσο για τον αποστολέα (Bob) όσο και για την Alice κάποιος τρίτος χρήστης – ας υποθέσουμε ο Charlie - έχει δημιουργήσει ένα δημόσιο κλειδί με το user id της Alice και το έχει βάλει στη θέση του πραγματικού κλειδιού της Alice. Ο Bob χρησιμοποίησε αυτό το πλαστογραφημένο κλειδί για να κρυπτογραφήσει το μήνυμα προς την Alice αντί του αληθινού κλειδιού της Alice. Όπως φαίνεται όλα δείχνουν φυσιολογικά διότι το πλαστογραφημένο κλειδί έχει το user id της Alice. Έτσι ο Charlie μπορεί να αποκρυπτογραφήσει το μήνυμα που προοριζόταν για την Alice μια και έχει το κλειδί που αντιστοιχεί στο πλαστογραφημένο δημόσιο κλειδί της Alice. Όμως το πρόβλημα δεν τελειώνει εδώ. Ο Charlie μπορεί επιπλέον να επανακρυπτογραφήσει το μήνυμα και να το προωθήσει στην Alice οπότε κανείς δεν πρόκειται να υποπτευθεί τίποτα. Εάν θέλει, μπορεί να προχωρήσει στη δημιουργία ψηφιακών υπογραφών της Alice με το πλαστογραφημένο κλειδί μια και όλοι θα το χρησιμοποιούν για να ελέγχουν τις υπογραφές της.

Όπως τελικά φαίνεται ο κίνδυνος είναι πολύ μεγάλος. Ο μόνος τρόπος να αποτραπούν τέτοιες καταστάσεις είναι η αποφυγή της υποκλοπής και του μπερδέματος των δημοσίων κλειδιών. Εάν κάποιος έχει πάρει το δημόσιο κλειδί της Alice κατευθείαν από την ίδια τότε δεν υπάρχει πρόβλημα. Αυτό βέβαια μπορεί να είναι πολύ δύσκολο εάν η Alice είναι χιλιάδες χιλιόμετρα μακριά ή απλά προσωρινά απρόσιτη.

Μία διέξοδος σε αυτό το πρόβλημα είναι η χρήση κάποιου τρίτου κοινά αποδεκτού "φίλου" ο οποίος έχει στη κατοχή του ένα καλό αντίγραφο του δημόσιου κλειδιού της Alice. Για παράδειγμα ας θεωρήσουμε ότι αυτός είναι ο David ο οποίος μπορεί να υπογράψει το δημόσιο κλειδί της Alice με τη δικό του μυστικό κλειδί και να εγγυηθεί με αυτό το τρόπο την αυθεντικότητα του κλειδιού της Alice.

Αυτή η διαδικασία θα παρήγαγε ένα υπογεγραμμένο πιστοποιητικό δημόσιου κλειδιού που θα αποδείκνυε την ακεραιότητα του κλειδιού της Alice. Αυτή η διαδικασία,βέβαια, προϋποθέτει την δυνατότητα ελέγχου του κλειδιού του David άρα την κατοχή ενός γνήσιου αντίγραφου του δημόσιου κλειδιού του. Ο David θα μπορούσε επιπλέον να στείλει στην Alice ένα υπογεγραμμένο αντίγραφο του δημόσιου κλειδιού του Bob. Με αυτό το τρόπο λειτουργεί σαν μεσάζοντας (introducer) μεταξύ του Bob και της Alice.

Το υπογεγραμμένο κλειδί για την Alice μπορεί να σταλεί από τον David ή την Alice στο BBS και από εκεί να το πάρει αργότερα όποιος το χρειαστεί. Αυτός το μόνο που θα χρειαστεί να κάνει, για να σιγουρευτεί για την ακεραιότητα του δημόσιου κλειδιού της Alice, είναι να την ελέγξει μέσω του δημόσιου κλειδιού του David. Κανένας δεν μπορεί να ξεγελάσει πλέον όποιον έχει το υπογεγραμμένο από τον David δημόσιο κλειδί της Alice διότι κανείς δεν μπορεί να πλαστογραφήσει την υπογραφή του David.

Κάποιο άτομο που τυγχάνει ευρείας εμπιστοσύνης θα μπορούσε να εξειδικευτεί στην παροχή αυτής της υπηρεσίας, δηλαδή της παροχής υπογραφών σε πιστοποιητικά δημοσίων κλειδιών άλλων χρηστών. Αυτό το κοινά αποδεκτό άτομο θα μπορούσε να είναι κάποιος "key server" ή κάποια υπηρεσία πιστοποίησης. Κάθε πιστοποιητικό δημόσιου κλειδιού που φέρει την υπογραφή αυτού του key server θα μπορεί να θεωρείται γνήσιο και έτσι άξιο της εμπιστοσύνης κάποιου. Το μόνο που χρειάζεται να κάνουν όσοι χρήστες θα ήθελαν να συμμετέχουν σε αυτή τη διαδικασία είναι να

αποκτήσουν ένα καλό αντίγραφο του δημοσίου κλειδιού του key server έτσι ώστε να είναι σε θέση να επιβεβαιώσουν την υπογραφή αυτού.

Κάποιος κεντρικός key server ή μια υπηρεσία πιστοποίησης, θα ήταν κατάλληλη για κάποια μεγάλη και απρόσωπη επιχείρηση ή κυβερνητική υπηρεσία.

Η αποκεντρωμένη έκδοση του σχήματος αυτού είναι εκείνη που επιτρέπει σε όλους τους χρήστες να δρουν σαν μεσάζοντες, ο ένας για τον άλλο,κάτι που έχει καλύτερα αποτελέσματα από έναν και μοναδικό key server. Το PGP τείνει προς αυτή τη κατεύθυνση διότι αντανακλά καλύτερα το φυσικό τρόπο με τον οποίο αλληλεπιδρούν μεταξύ τους οι άνθρωποι στις σχέσεις τους και ταυτόχρονα επιτρέπει σε αυτούς να διαλέξουν ποιόν εμπιστεύονται για τη διαχείριση των κλειδιών τους.

Αυτή ολόκληρη η διαδικασία της προστασίας των δημοσίων κλειδιών είναι το μοναδικό δύσκολο πρόβλημα στις πρακτικές εφαρμογές της κρυπτογράφησης δημοσίων κλειδιών. Θα μπορούσαμε να πούμε ότι είναι η Αχίλλειος φτέρνα της κρυπτογράφησης δημοσίων κλειδιών και έχει καταβληθεί μεγάλη προσπάθεια για τη λύση αυτού του προβλήματος.

Η χρήση ενός δημόσιου κλειδιού δεν θα πρέπει να ξεκινάει εάν δεν είμαστε σίγουροι ότι πρόκειται για ένα καλό δημόσιο κλειδί το οποίο ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει. Μπορούμε να είμαστε σίγουροι για την προέλευση του κλειδιού εάν έχουμε κάποιο πιστοποιητικό από τον ιδιοκτήτη του ή κάποιον άλλο που εμπιστευόμαστε,από τον οποίο όμως έχουμε ήδη ένα εγγυημένο δημόσιο κλειδί. Επιπλέον το user id θα πρέπει να έχει ολόκληρο το όνομα του ιδιοκτήτη και όχι απλά το μικρό του ή κάποιο άλλο ψευδώνυμο.

Δεν έχει σημασία πόσο σίγουροι μπορεί να αισθανόμαστε για κάποιο δημόσιο κλειδί που κατεβάσαμε από κάποιον ηλεκτρονικό πίνακα ανακοινωθέντων—ΠΟΤΕ δεν θα πρέπει να εμπιστευόμαστε οτιδήποτε δεν έχει την υπογραφή κάποιου που εμπιστευόμαστε. Ένα δημόσιο κλειδί που απλά κατεβάσαμε δίχως να το ελέγξουμε είναι πιθανόν να έχει αλλοιωθεί από κάποιον τρίτο, ακόμα και από το διαχειριστή του ηλεκτρονικού πίνακα. Εάν ποτέ μας ζητηθεί να υπογράψουμε το δημόσιο κλειδί κάποιου άλλου θα πρέπει να σιγουρευτούμε ότι αυτό πραγματικά του ανήκει. Αυτό πρέπει να γίνει διότι η υπογραφή μας στο δημόσιο κλειδί εγγυάται την αυθεντικότητά του. Εάν έχουμε κάνει λάθος,τότε όσοι μας εμπιστεύονται θα εμπιστευτούν και το κλειδί με αβέβαια αποτελέσματα. Ο κανόνας λέει ότι υπογράφουμε δημόσια κλειδιά για τα οποία έχουμε ιδία γνώση της αυθεντικότητάς τους. Για να αποκτήσουμε αυτή τη γνώση μπορούμε για παράδειγμα να μιλήσουμε στον ιδιοκτήτη του κλειδιού στο τηλέφωνο και να επιβεβαιώσουμε τα στοιχεία που έχουμε στα χέρια μας. Με το να βάλουμε την υπογραφή μας σε ένα δημόσιο κλειδί για το οποίο ήμαστε σίγουροι δεν χάνουμε την αξιοπιστία μας ακόμα και αν αυτό ανήκει σε κάποιον ψυχοπαθή. Αυτό συμβαίνει διότι με την υπογραφή μας δεν λέμε τίποτα παραπάνω από το ότι αυτό το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει—το ότι κάποιος μπορεί να εμπιστευθεί το κλειδί δεν έχει καμία σχέση με το αν μπορεί να εμπιστευθεί ή όχι τον ιδιοκτήτη του.

Η εμπιστοσύνη δεν είναι αναγκαστικά κάτι μεταβιβάσιμο. Για παράδειγμα μπορεί έχουμε κάποιον φίλο που εμπιστευόμαστε και ξέρουμε ότι δεν λέει ψέματα. Αυτός μπορεί να εμπιστεύεται τον πρόεδρο της κυβέρνησης. Όπως είναι αυτονόητο αυτό

δεν σημαίνει ότι και εμείς εμπιστευόμαστε τον πρόεδρο της κυβέρνησης – κοινή λογική. Ανάλογα εάν εμπιστευόμαστε την υπογραφή της Alice σε ένα δημόσιο κλειδί και η Alice με τη σειρά της εμπιστεύεται την υπογραφή του Charlie σε κάποιο άλλο κλειδί, αυτό δεν σημαίνει ότι και εμείς εμπιστευόμαστε την υπογραφή του Charlie σε εκείνο το κλειδί.

Θα ήταν καλή ιδέα, οι χρήστες να κρατούσαν το δημόσιο κλειδί τους μαζί με ένα σύνολο από πιστοποιητικά για αυτό από διαφόρους μεσάζοντες με την ελπίδα ότι οι περισσότεροι χρήστες εμπιστεύονται κάποιον από αυτούς. Μπορεί λοιπόν, κάποιος χρήστης να ανακοινώσει το δημόσιο κλειδί του μαζί με τη συλλογή των πιστοποιητικών που διαθέτει για αυτό. Όταν υπογράφουμε το δημόσιο κλειδί κάποιου πρέπει να του το επιστρέφουμε μαζί με την υπογραφή μας ώστε να την προσθέσουνε στη συλλογή πιστοποιητικών για το δημόσιο κλειδί τους.

Το PGP κρατάει στοιχεία για το ποια από τα δημόσια κλειδιά που έχουμε στην κατοχή μας είναι πιστοποιημένα με υπογραφές που εμπιστευόμαστε. Το μόνο που εμείς πρέπει να κάνουμε είναι να πούμε στο PGP ποιους εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας. Το PGP αναλαμβάνει από εκεί και πέρα να κρίνει αυτόματα κάποιο δημόσιο κλειδί ως έγκυρο ή όχι.

Πρέπει να διασφαλίσουμε ότι κανένας δεν πρόκειται να αλλοιώσει το μπρελόκ με τα κλειδιά μας. Ο έλεγχος ενός νέου υπογεγραμμένου δημοσίου κλειδιού πρέπει να εξαρτάται ολοκληρωτικά από την ακεραιότητα των κλειδιών τα οποία ήδη έχουμε στο μπρελόκ μας και τα οποία φυσικά εμπιστευόμαστε. Πρέπει να διατηρούμε συνεχή φυσικό έλεγχο των μπρελόκ δημοσίων κλειδιών μας σε κάποιο PC εκτός δικτύου όπως ακριβώς θα κάναμε και με το μυστικό κλειδί μας. Επιπλέον πρέπει να κρατάμε ένα αντίγραφο του δημόσιου και μυστικού κλειδιού μας σε κάποιο προστατευμένο μέσο όπου αποκλείεται ποτέ να τα σβήσουμε κατά λάθος. Από τη στιγμή κατά την οποία το δημόσιο κλειδί μας χρησιμοποιείται ως ο τελικός κριτής για τη πιστοποίηση ή μη όλων των άλλων κλειδιών του μπρελόκ είναι σημαντική για την ασφάλεια όλου του συστήματος η διασφάλισή του. Το PGP μπορεί αυτόματα να συγκρίνει το δημόσιο κλειδί μας με ένα αντίγραφό του σε κάποιο προστατευμένο φυσικό μέσο.

Το PGP γενικά θεωρεί ότι διατηρούμε το σύστημά μας, τα μπρελόκ και το PGP ασφαλές σε φυσικό επίπεδο. Εάν κάποιος έχει πρόσβαση στο σκληρό δίσκο του συστήματός μας τότε θεωρητικά μπορεί να αλλοιώσει το ίδιο το PGP έτσι ώστε αυτό να αδυνατεί να ανιχνεύσει οποιαδήποτε αλλοιώσει σε άλλα κλειδιά.

Ένας ακόμα τρόπος να προστατεύσουμε ολόκληρο το μπρελόκ με τα κλειδιά μας είναι να το υπογράψουμε ολόκληρο με το μυστικό μας κλειδί. Βέβαια θα έπρεπε πάλι να έχουμε κάπου αλλού προστατευμένο ένα αντίγραφο του δημοσίου κλειδιού μας για να είμαστε σε θέση να ελέγξουμε την υπογραφή μας. Όπως είναι φυσικό δεν μπορούμε να βασιστούμε στο δημόσιο κλειδί μας, που βρίσκεται στο μπρελόκ, για τον έλεγχο της υπογραφής μας διότι αυτό είναι μέρος αυτού που πάμε να προστατέψουμε.

## 5.4.4 Διαδικασία Αναγνώρισης Έγκυρων Κλειδιών

Το PGP παρακολουθεί ποια από τα κλειδιά που υπάρχουν στο μπρελόκ δημοσίων κλειδιών είναι πιστοποιημένα και ποια όχι με υπογραφές χρηστών που εμπιστευόμαστε. Το μόνο που πρέπει να κάνουμε είναι να "πούμε" στο PGP ποιους χρήστες εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας κλειδί. Το PGP αναλαμβάνει από εκεί να κινήσει αυτόματα διαδικασίες ελέγχου της εγκυρότητας κλειδιών που είναι υπογεγραμμένα από τους μεσάζοντες που εμείς ορίσαμε. Υπάρχει βέβαια πάντα η δυνατότητα να υπογράψουμε κλειδιά και εμείς οι ίδιοι.

Υπάρχουν δύο διαφορετικά κριτήρια βάση των οποίων το PGP κρίνει τη χρησιμότητα των κλειδιών και τα οποία δεν πρέπει να συγχέουμε:

1. Το κλειδί ανήκει σε αυτόν που ισχυρίζεται ότι ανήκει; (έχει πιστοποιηθεί από κάποιον του οποίου την υπογραφή εμπιστευόμαστε;)
2. Ανήκει σε κάποιον που μπορούμε να εμπιστευθούμε για την πιστοποίηση άλλων κλειδιών;

Το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση. Η απάντηση στη δεύτερη πρέπει να δοθεί αποκλειστικά από το χρήστη. Όταν ο χρήστης δώσει την απάντηση στην δεύτερη ερώτηση τότε το PGP μπορεί να υπολογίσει την απάντηση στην πρώτη ερώτηση για άλλα κλειδιά τα οποία υπογράφονται από αυτόν που έχουμε ορίσει σαν έμπιστο. Κλειδιά τα οποία έχουν πιστοποιηθεί από κάποιον που έχουμε ορίσει ως έμπιστο θεωρούνται έγκυρα από το PGP. Τα κλειδιά που ανήκουν σε έμπιστους μεσάζοντες πρέπει να πιστοποιηθούν από είτε από εμάς τους ίδιους είτε από κάποιον άλλο που έχουμε ορίσει ως έμπιστο.

Το PGP δίνει επιπλέον τη δυνατότητα ορισμού διαφορετικών επιπέδων εμπιστοσύνης για διαφορετικούς μεσάζοντες. Το ότι εμπιστευόμαστε κάποιον να δράσει ως μεσάζοντας δεν σημαίνει μόνο ότι τον εμπιστευόμαστε αλλά επιπλέον ότι τον θεωρούμε αρκετά ικανό να διαχειριστεί κλειδιά επιλέγοντας ποια από αυτά πρέπει και ποια όχι να υπογράψει. Μπορεί να ορίσουμε έναν χρήστη - μεσάζοντα στο PGP σαν άγνωστο, μη έμπιστο, μερικώς έμπιστο και εντελώς έμπιστο για να πιστοποιεί δημόσια κλειδιά. Αυτή η πληροφορία, που αφορά το βαθμό εμπιστοσύνης κάποιου μεσάζοντα, περιέχεται στο μπρελόκ των κλειδιών μαζί με το αντίστοιχο κλειδί (του μεσάζοντα) και δεν αντιγράφεται σε καμία περίπτωση κατά την αντιγραφή κάποιου κλειδιού του μπρελόκ διότι θεωρείται εμπιστευτική πληροφορία μια και αντικατοπτρίζει την άποψη του κατόχου του για τους μεσάζοντες - απόλυτα προσωπικό στοιχείο.

Όταν το PGP ελέγχει την εγκυρότητα ενός κλειδιού αυτό που κάνει είναι να ελέγχει τον βαθμό εμπιστοσύνης όλων των συνημμένων υπογραφών πιστοποίησής του. Κατόπιν υπολογίζει ένα μέσο επίπεδο εμπιστοσύνης - για παράδειγμα δύο μερικώς έμπιστες υπογραφές ισοδυναμούν με μία πλήρως έμπιστη. Το σκεπτικό λειτουργίας του PGP προσαρμόζεται στις απαιτήσεις του χρήστη και ρυθμίζεται αναλόγως (για παράδειγμα μπορούμε να ρυθμίσουμε το PGP να θεωρεί ένα κλειδί έγκυρο μόνο εάν αυτό φέρει δύο πλήρως έμπιστες υπογραφές ή τρεις μερικώς έμπιστες).

Το δικό μας κλειδί θεωρείται έγκυρο από το PGP αξιωματικά και για αυτό το λόγο δεν χρειάζεται την πιστοποίηση από κανέναν. Το PGP γνωρίζει ποια δημόσια κλειδιά είναι δικά μας κοιτάζοντας να βρει τα αντίστοιχα μυστικά κλειδιά στο μπρελόκ τους. Το PGP θεωρεί επιπλέον ότι εμπιστευόμαστε τους εαυτούς μας για να πιστοποιούν άλλα κλειδιά.

Όσο θα περνάει ο καιρός θα λαμβάνουμε όλο και περισσότερα κλειδιά από χρήστες που ίσως να θέλουμε να ορίσουμε ως μεσάζοντες. Κάθε ένας από αυτούς θα έχει τους δικούς του μεσάζοντες των οποίων τα πιστοποιητικά - υπογραφές θα μοιράζει μαζί με το κλειδί του με την ελπίδα ότι όποιος τα λάβει να εμπιστεύεται κάποιο από όλα. Έτσι δημιουργείται ένα αποκεντρωμένο δίκτυο εμπιστοσύνης για όλα τα δημόσια κλειδιά.

Αυτή η μοναδική προσέγγιση έρχεται σε αντίθεση με τα κατεστημένα κυβερνητικά σχήματα διαχείρισης κλειδιών, όπως το PEM (Internet Privacy Enhanced Mail), τα οποία βασίζονται σε συστήματα κεντρικού ελέγχου και υποχρεωτικής εμπιστοσύνης σε αυτά. Τα σχήματα αυτά απαρτίζονται από ιεραρχικές οντότητες που υπαγορεύουν ποιόν πρέπει να εμπιστευόμαστε. Αυτό είναι φανερό ότι έρχεται σε πλήρη αντίθεση με τη σχεδιαστική αρχή του PGP η οποία επιτρέπει στον καθένα και ανεξάρτητα από οποιονδήποτε και οτιδήποτε άλλο να καθορίσει ο ίδιος την πολιτική που θέλει να ακολουθήσει στη διαχείριση των κλαδιών του. Έτσι το PGP βάζει το χρήστη και όχι το σύστημα στην κορυφή της προσωπική του πυραμίδα πιστοποίησης.

## 5.4.5 Προστασία του Μυστικού Κλειδιού

Η προστασία του μυστικού κλειδιού και της φράσης-κλειδί του, είναι κάτι το αυτονόητο στο οποίο πρέπει να δοθεί μεγάλη προσοχή. Εάν ποτέ το μυστικό κλειδί πέσει σε λάθος χέρια – τα οποία είναι οποιαδήποτε άλλα εκτός των δικών μας—τότε θα πρέπει άμεσα, τόσο για τη δική μας ασφάλεια όσο και των άλλων, να ειδοποιήσουμε τους πάντες για το γεγονός προτού κάποιος αρχίσει να υπογράφει με το "όνομά" μας. Θα μπορούσε, για παράδειγμα, να υπογράψει ένα σύνολο από δημόσια κλειδιά δημιουργώντας έτσι πρόβλημα σε πολλούς χρήστες ειδικά εάν η υπογραφή μας τυγχάνει ευρείας εμπιστοσύνης και αποδοχής. Φυσικά, κίνδυνο διατρέχουμε και από το γεγονός της έκθεσης όλων των μηνυμάτων μας στα μάτια αυτού που έχει το προσωπικό μας κλειδί.

Η προστασία του μυστικού κλειδιού πρέπει να αρχίζει με τη φυσική του διασφάλιση. Μπορούμε να το κρατάμε σε κάποιο PC στο σπίτι ή κάποιο υπολογιστή notebook μια και αυτά τα έχουμε υπό την επίβλεψή μας συνεχώς. Εάν ποτέ υπάρξει ανάγκη χρησιμοποίησης υπολογιστή στο γραφείο ή οπουδήποτε αλλού τότε θα πρέπει να μεταφέρουμε το μυστικό κλειδί μας σε αυτόν μέσο κάποιας δισκέτας ενδεχομένως και για όσο χρειάζεται ενώ όταν τελειώσουμε τη δουλεία μας δεν πρέπει να αφήσουμε πίσω οτιδήποτε μπορεί να οδηγήσει στην αποκάλυψη του. Δεν είναι επίσης σωστό να αφήνουμε το μυστικό κλειδί μας σε κάποιο απομακρυσμένο μηχάνημα (ένας Unix dial-in server) διότι μπορεί κάποιος που παρακολουθεί τις επικοινωνίες μέσω modem να υποκλέψει τη μυστική φράση (pass phrase) και να αποκτήσει το μυστικό από το απομακρυσμένο σύστημα. Συμπερασματικά λέμε ότι θα πρέπει να γίνεται χρήση του μυστικού κλειδιού μόνο σε συστήματα στα οποία έχουμε φυσικό έλεγχο.

Επιπρόσθετα, πρέπει να προσέξουμε πού αποθηκεύουμε τη μυστική φράση-κλειδί. Δεν πρέπει ποτέ αυτή να βρίσκεται στον ίδιο υπολογιστή με αυτόν που έχει το αρχείο του μυστικού κλειδιού μας. Η αποθήκευση τόσο του μυστικού κλειδιού όσο και της μυστικής φράσης στον ίδιο υπολογιστή είναι το ίδιο επικίνδυνη με την φύλαξη του PIN ενός τραπεζικού ATM λογαριασμού στο ίδιο πορτοφόλι με την κάρτα ATM. Ένα πράγμα είναι σίγουρο - δεν θέλουμε σε καμία περίπτωση αυτός που θα έχει στα χέρια του τον σκληρό δίσκο με το μυστικό μας κλειδί να έχει στη διάθεσή του και τη μυστική φράση. Το ιδανικό θα ήταν να απομνημονεύαμε τη μυστική φράση και να μην την φυλάγαμε σε κανένα άλλο μηχάνημα εκτός του εγκεφάλου μας. Εάν, ωστόσο, νιώθουμε ότι πρέπει να τη γράψουμε κάπου θα πρέπει να την ασφαλίσουμε καλλίτερα ίσως και από το ίδιο το μυστικό μας κλειδί.

Κάτι άλλο επίσης σημαντικό, που πρέπει να κάνουμε, είναι να παίρνουμε backup του μυστικού μπρελόκ μας διότι μόνο εμείς έχουμε το μοναδικό αντίγραφο αυτού και πιθανή απώλειά του θα ισοδυναμούσε με αχρήστευση όλων των δημοσίων κλειδιών που διανείμαμε στον κόσμο.

Το αποκεντρωτικό σχήμα φιλοσοφίας αλλά και λειτουργίας που έχει επιλέξει να χρησιμοποιήσει το PGP εκτός από τα πλεονεκτήματα στη διαχείριση των κλειδιών έχει και τα μειονεκτήματα του. Δεν υπάρχει μία κεντρική λίστα που να περιέχει τα μη έγκυρα κλειδιά κάνοντας πιο δύσκολη την γνώση τους. Έτσι αν κάτι πάει στραβά η διαδικασία γνωστοποίησής του είναι επίπονη. Εάν τελικά το μυστικό κλειδί και η μυστική φράση πέσουν στα χέρια άλλων θα πρέπει να φτιάξουμε και να διανείμουμε ένα "πιστοποιητικό απολεσθέντος κλειδιού" (key compromise certificate). Αυτός ο τύπος πιστοποιητικού χρησιμοποιείται για να προειδοποιεί άλλους χρήστες να σταματήσουν να χρησιμοποιούν το αντίστοιχο δημόσιο κλειδί μας. Μπορούμε να χρησιμοποιήσουμε το PGP στη δημιουργία αυτού του πιστοποιητικού και κατόπιν να το στείλουμε σε όλους τους φίλους και συνεργάτες μας σε όλο τον κόσμο. Η έκδοση του PGP που τρέχει σε αυτούς θα αναλάβει να εγκαταστήσει το πιστοποιητικό του απολεσθέντος κλειδιού στα δημόσια μπρελόκ τους και από εκείνη τη στιγμή θα αποτρέπεται αυτόματα η επαναχρησιμοποίησή τους. Μπορούμε κατόπιν να δημιουργήσουμε ένα νέο ζεύγος μυστικού/δημοσίου κλειδιού και να αρχίσουμε πλέον να δουλεύουμε με αυτά.

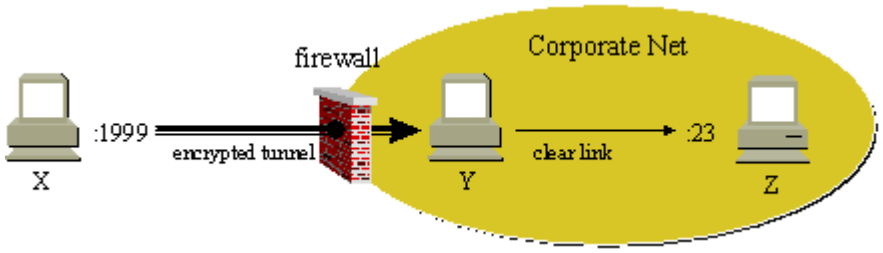
# *5.5 SSH (Secure Shell)*

## 5.5.1 Εισαγωγή

Τα εργαλεία απομακρυσμένης επικοινωνίας *(rsh, rcp, rlogin)* είναι γνωστά για την ευκολία χρήσης τους και την παροχή γρήγορης πρόσβασης σε άλλες μηχανές. Το πρόβλημα, όμως, είναι ότι βασίζονται σε IP διευθύνσεις ή host names για την πιστοποίηση της ταυτότητας των μηχανών, γεγονός που τα καθιστά ανασφαλή καθ' ότι οι υπηρεσίες του DNS δεν είναι άξιες εμπιστοσύνης. Επίσης, η μετάδοση των κωδικών χωρίς κανένα είδος προστασίας οξύνει τις τρύπες ασφαλείας. Για να μπορούν, λοιπόν, να χρησιμοποιούνται σε ασφαλή περιβάλλοντα πρέπει να διαθέτουν πιο καλύτερους μηχανισμούς πιστοποίησης ταυτότητας. Η εισαγωγή της έννοιας της κρυπτογράφησης και των ψηφιακών υπογραφών στα εργαλεία rsh, rcp και rlogin, δημιούργησε το *Secure Shell (SSH).*

Το SSH σχεδιάστηκε για να αντικαταστήσει τα εργαλεία rsh, rcp και rlogin με τα αντίστοιχα ssh, scp και slogin, με επιπλέον χαρακτηριστικά αυτά της ισχυρής από άκρη σε άκρη κρυπτογράφηση, της βελτιωμένης πιστοποίησης ταυτότητας χρήστη και μηχανής και την προώθηση TCP πορτών και X11 συνδέσεων.

Σε αυτό το σημείο είναι απαραίτητο να εξηγήσουμε τον όρο "προώθηση TCP πορτών". Ας θεωρήσουμε τις τρεις μηχανές του παρακάτω παραδείγματος. Η μηχανή X είναι ο client και εγκαθιστά σύνδεση με τον server Y μέσω SSH. Μια πόρτα ρου X, ας πούμε η 1999, ρυθμίζεται για προώθηση σε μια άλλη πόρτα στο απομακρυσμένο σύστημα Z, ας πούμε την 23. Η πόρτα προωθείται μέσω του κρυπτογραφημένου καναλιού στον Y και από εκεί προωθείται στην πόρτα 23 του Z. Έτσι, η εντολή telnet localhost 1999 θα έχει σαν αποτέλεσμα μια telnet σύνδεση με τον Z.

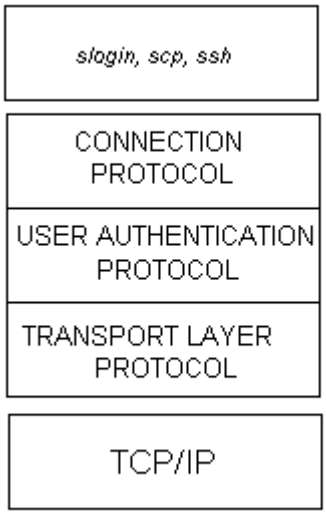



Η τρέχοντα έκδοση του πρωτοκόλλου είναι η 2 (version 2.0).

## 5.5.2 Περιγραφή του SSH πρωτοκόλλου

Το SSH είναι ένα πρωτόκολλο που παρέχει ασφαλή απομακρυσμένη σύνδεση σε υπολογιστές πάνω από μη ασφαλές δίκτυο. Αποτελείται από τρία βασικά στοιχεία:

- Το Transport layer protocol παρέχει πιστοποίηση της ταυτότητας του server, ακεραιότητα των δεδομένων και εξασφάλιση του απόρρητου της συναλλαγής. Προαιρετικά μπορεί να εφαρμόσει και συμπίεση δεδομένων. Τυπικά τρέχει πάνω από μία TCP/IP σύνδεση.
- Το User Authentication protocol πιστοποιεί την ταυτότητα του πελάτη-χρήστη στον server. Τρέχει πάνω από το Transport layer protocol.
- Το Connection protocol πολυπλέκει το κρυπτογραφημένο φυσικό κανάλι σε αρκετά λογικά κανάλια και τρέχει πάνω από το User Authentication protocol.




*Σχηματική αναπαράσταση των επιμέρους πρωτοκόλλων του SSH.*

# 5.5.3 Δομή του SSH

## Ιδιωτικά Και Δημόσια Κλειδιά

Κάθε server και client πρέπει να έχει ένα ζευγάρι ιδιωτικής – δημόσιας κλείδας για να μπορεί να επαλήθευση την ταυτότητα του στο άλλο άκρο. Επιτρέπεται η κατοχή περισσότερων του ενός ζευγάρια κλειδιών, όταν χρησιμοποιούνται με διαφορετικούς αλγόριθμους, ενώ η από κοινού χρήση ενός ζεύγους από πολλούς server δεν απαγορεύεται.

Για να μπορεί ο client με ευκολία να επαληθεύει την ταυτότητα του server είναι απαραίτητο να γνωρίζει την δημόσια κλείδα που αντιστοιχεί στον server που θέλει να συνδεθεί. Υπάρχουν δυο διαφορετικά μοντέλα που εξασφαλίζουν την προηγούμενη προϋπόθεση:

- Πρώτον, ο client έχει αποθηκευμένα σε μια τοπική βάση δεδομένων τα ονόματα των server και τις σχετιζόμενες με αυτά δημόσιες κλείδες. Αυτή η μέθοδος δεν απαιτεί μια κεντρική διαχείριση των κλειδιών από τρίτους. Το μειονέκτημα είναι ότι το μέγεθος μιας τέτοιας βάσης δεδομένων μπορεί να εξελιχθεί σημαντικά και συνεπώς η συντήρηση της να γίνει δύσκολη.
- Στην δεύτερη περίπτωση, σχέση μεταξύ του ονόματος του server και του κλειδιού του πιστοποιείται από μια άξια εμπιστοσύνης Certification Authority. Το πρόγραμμα του πελάτη γνωρίζει μόνο την δημόσια κλείδα της Certification Authority και μπορεί να επιβεβαιώσει την εγκυρότητα των κλείδων που έχουν πιστοποιηθεί από την CA. Εδώ δεν υπάρχει το πρόβλημα της διατήρησης μεγάλων βάσεων δεδομένων από τα τοπικά συστήματα, αφού μόνο ένα κλειδί χρειάζεται να αποθηκεύει ο client. Από την άλλη μεριά, όμως, δεν είναι δυνατή η απόλυτη εμπιστοσύνη στις διαδικασίες της Certification Authority. Επίσης, πιστοποίηση κάθε κλειδιού μπορεί να είναι μια χρονοβόρα και περίπλοκή διαδικασία.

Οι εφαρμογές του SSH μπορούν να παρέχουν επιπρόσθετες μεθόδους επικύρωσης των δημόσιων κλειδιών, όπως για παράδειγμα την παραγωγή ενός δεκαεξαδικού

"αποτυπώματος" της κλείδας και από τα δύο άκρα και την σύγκριση τους μέσω εξωτερικών καναλιών επικοινωνίας (π.χ. τηλέφωνο). Κλείδες που δεν επαληθεύονται, κανονικά δεν πρέπει να γίνονται δεκτές.

## Επεκτασιμότητα

Βασικός στόχος της σχεδίασης είναι η διατήρηση του πρωτοκόλλου όσο το δυνατόν απλό γίνεται, με όσο το δυνατόν λιγότερους αλγόριθμους. Όλες οι εφαρμογές πρέπει να υποστηρίζουν ένα ελάχιστο σύνολο αλγόριθμων για να εξασφαλιστεί η δια – λειτουργικότητα. Στο μέλλον αναμένεται η πρόσθεση και άλλων αλγορίθμων.

## Θέματα Πολιτικής

Το πρωτόκολλο επιτρέπει την διαπραγμάτευση όλων των χρησιμοποιούμενων αλγορίθμων. Έτσι, οι αλγόριθμοι κρυπτογράφησης, ανταλλαγή κλειδιών και συμπίεσης καθώς επίσης και οι μηχανισμοί ασύμμετρων κλειδιών και παροχής ακεραιότητας, μπορούν να επιλεγούν από λίστες που παρέχουν ο client και ο server ο ένας στον άλλο και μάλιστα διαφορετικοί για κάθε κατεύθυνση. Η πολιτική ασφαλείας κάθε συστήματος καθορίζει ποιοι προτιμούνται.

Τα παρακάτω θέματα πολιτικής θα πρέπει υπολογίζονται κατά την ρύθμιση SSH εφαρμογών:

- Οι αλγόριθμοι και οι μηχανισμοί που πρόκειται να χρησιμοποιηθούν για κάθε κατεύθυνση (client ♋ server ή client ✍ server). Πρέπει να ορίζεται ποιος προτιμάται.
- Η μέθοδοι πιστοποίησης της ταυτότητας, ξεχωριστοί για κάθε χρήστη που θα εφαρμόζει ο server. Η πολιτική του server μπορεί να ζητά πολλαπλές διαδικασίες πιστοποίησης για μερικού ή όλους τους χρήστες, ενώ οι απαιτούμενοι αλγόριθμοι μπορούν να εξαρτώνται από την τοποθεσία από όπου προσπαθεί να συνδεθεί ο χρήστης.
- Οι ενέργειες που επιτρέπονται σε κάθε χρήστη και στον server. Η πολιτική ασφαλείας δεν θα πρέπει να επιτρέπει στον server να εκτελεί εντολές στην μηχανή του χρήστη ούτε στον χρήστη να συνδέεται στον authentication server.

## Ιδιότητες Ασφάλειας

Ο πρωταρχικός στόχος του SSH πρωτοκόλλου είναι η βελτίωση της ασφάλειας στο Internet και ο τρόπος με τον οποίο προσπαθεί να το επιτύχει αυτό βασίζεται στο εξής σκεπτικό:

- Όλοι οι αλγόριθμοι κρυπτογράφησης, παροχής ακεραιότητας και ανταλλαγής κλειδιών έχουν δοκιμαστεί και
- Οι αλγόριθμοι χρησιμοποιούν κλειδιά μεγέθους ικανού να παρέχει προστασία απέναντι στις ισχυρότερες επιθέσεις κρυπτοανάλυσης.
- Στην περίπτωση που κάποιος αλγόριθμος "σπάσει", είναι εύκολη η αντικατάσταση του από κάποιον άλλο χωρίς αλλαγές στις βάσεις του SSH.

Για την ταχεία ανάπτυξη και υιοθέτηση του πρωτοκόλλου, κάποιες έχουν γίνει παραχωρήσεις. Σημαντικότερη από αυτές είναι η καθιέρωση της επαλήθευσης των κλείδων με υποχρεωτική, γεγονός όμως που δεν συνιστάται.

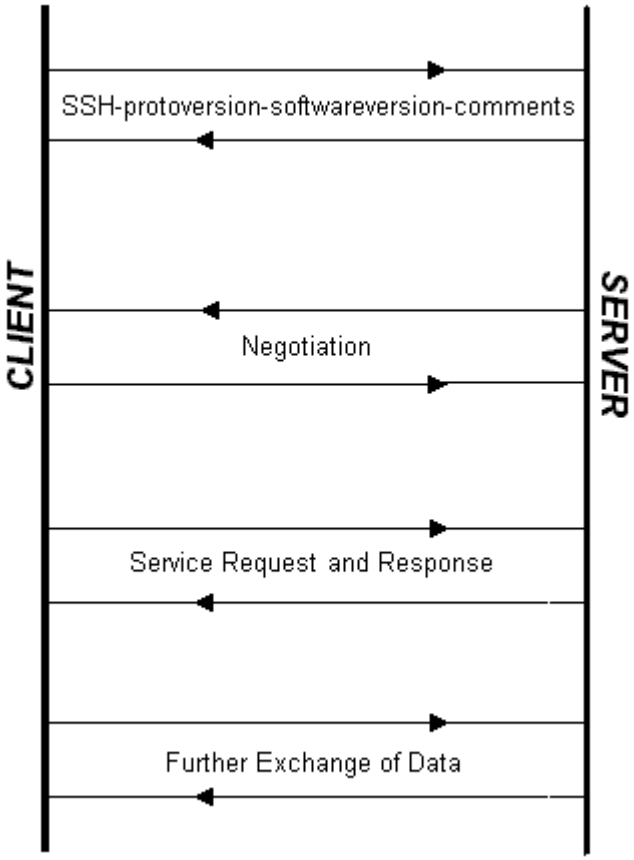
## 5.5.4 Transport Layer Protocol

Το Transport Layer Protocol είναι ένα ασφαλές χαμηλού επιπέδου πρωτόκολλο μεταφοράς, που παρέχει ισχυρή κρυπτογράφηση, πιστοποίηση του server και ακεραιότητα των δεδομένων. Σε αυτό το επίπεδο γίνεται η διαπραγμάτευση των αλγόριθμων ανταλλαγής κλειδιών, συμμετρικής κρυπτογράφησης, ασύμμετρης κρυπτογράφησης, hash και MAC. Συνήθως τρέχει πάνω από TCP/IP. Η πιστοποίηση ταυτότητας σε αυτό το επίπεδο αναφέρεται μόνο σε πιστοποίηση υπολογιστικών μηχανών και όχι χρηστών. Το User Authentication Protocol αναλαμβάνει την επιβεβαίωση της ταυτότητας των χρηστών.

Έχει σχεδιαστεί για να είναι απλό, ευέλικτο, να επιτρέπει την διαπραγμάτευση παραμέτρων και να χρησιμοποιεί ένα ελάχιστο αριθμό απαραίτητων μηνυμάτων για την εγκαθίδρυση της σύνδεσης. Για τα περισσότερα περιβάλλοντα, έχει υπολογιστεί ότι ένας αριθμός 2 ανταλλαγών *(round-trips)* είναι αρκετός για πλήρη επικοινωνία όλων των απαραίτητων πληροφοριών. Η χειρότερη περίπτωση είναι 3 round-trips.

### Εγκατάσταση της Σύνδεσης

Την διαδικασία ξεκινά ο client, ενώ ο server χρησιμοποιεί την πόρτα *(port)* 22 για ανταποκρίνεται τις επερχόμενες κλήσεις για σύνδεση. Όταν επιτευχθεί η ζεύξη των επικοινωνούντων σημείων, τα δύο άκρα πρέπει να στείλουν μια ακολουθία χαρακτήρων της μορφής "SSH-protoversion-softwareversion-comments" ακολουθούμενη από χαρακτήρες αλλαγής γραμμής και επιστροφής του κέρσορα (*carriage return* and *newline characters*). Το μέγιστο μήκος αυτής της ακολουθίας είναι 255 χαρακτήρες περιλαμβανομένων και των χαρακτήρων ελέγχου. Οι αριθμοί έκδοσης πρέπει να αποτελούνται από εκτυπώσιμους ASCII χαρακτήρες εκτός του κενού διαστήματος και του σήματος της αφαίρεσης (-). Χρησιμοποιείται για συμβατότητα μεταξύ παλιών εκδόσεων και για να υποδηλώσει τις δυνατότητες του συστήματος. Το πεδίο comments περιέχει επιπρόσθετες πληροφορίες που μπορεί να είναι χρήσιμες στην επίλυση διάφορων προβλημάτων.




Η διαπραγμάτευση για των αλγορίθμων ξεκινά μόλις σταλεί και από τις δύο μεριές αυτό το αναγνωριστικό. Όλα τα πακέτα που ακολουθούν χρησιμοποιούν το *Binary Packet Protocol* που θα περιγράψουμε αργότερα.

Συνοπτικά, τα βήματα εγκαθίδρυσης της σύνδεσης είναι:

1. Ζεύξη των δύο σημείων.
2. Ανταλλαγή της ακολουθίας "SSH-protoversion-softwareversion-comments".
3. Διαπραγμάτευση αλγορίθμων κρυπτογράφησης και MAC και πιστοποίηση ταυτότητας του server.
4. Αίτηση εξυπηρέτησης από τον client στον sever.
5. Ανταλλαγή περαιτέρω δεδομένων.

Τα δύο πρώτα βήματα συζητήθηκαν στο παρών κεφάλαιο. Παρακάτω θα αναφερθούμε στα υπόλοιπα βήματα.

## Διαπραγμάτευση Αλγορίθμων

Η διαδικασία αυτή ξεκινά με την αποστολή από κάθε πλευρά λίστας των υποστηριζόμενων αλγόριθμων, στην κορυφή της οποίας υπάρχει αυτός που προτιμάται περισσότερο. Δίνεται η δυνατότητα σε κάθε σύστημα να μαντέψει τους

αλγόριθμους που χρησιμοποιεί το ανταποκρινόμενο σύστημα υπηρεσία και μπορεί να στείλει ένα αρχικό πακέτο χρησιμοποιώντας αυτούς. Εάν οι αλγόριθμοι είχαν προβλεφθεί σωστά, τότε χρησιμοποιούνται κατά την διάρκεια της υπόλοιπης σύνδεσης και το πακέτο λαμβάνεται σαν το πρώτο πακέτο διαπραγμάτευσης. Διαφορετικά το πακέτο πρέπει αν αγνοηθεί και η διαδικασία να ξαναρχίσει με το κανονικό αρχικό πακέτο.

Η πιστοποίηση της ταυτότητας μπορεί να είναι υπονοούμενη και μετά από αυτήν ακολουθεί η αίτηση εξυπηρέτησης του client.

Το αρχικό πακέτο, που σηματοδοτεί την αρχή αυτού του βήματος, έχει την παρακάτω δομή:

byte SSH_MSG_KEXINIT

byte[16] cookie (random bytes)

string kex_algorithms

string server_host_key_algorithms

string encryption_algorithms_client_to_server

string encryption_algorithms_server_to_client

string mac_algorithms_client_to_server

string mac_algorithms_server_to_client

string compression_algorithms_client_to_server

string compression_algorithms_server_to_client

string languages_client_to_server

string languages_server_to_client

boolean first_kex_packet_follows

uint32 0 (reserved for future extension)

Στην πρώτη στήλη αναφέρεται η μορφή των δεδομένων κάθε πεδίου (δυαδικά, boolean κτλ.), ενώ η δεύτερη στήλη περιγράφει την χρησιμότητα αυτών. Με τον όρο byte περιγράφουμε ποσότητα 8 bits (octet) και ομοίως ο γενικός όρος byte[n] περιγράφει μονοδιάστατο πίνακα bytes, όπου n ο αριθμός των bytes του πίνακα. Ο όρος boolean υποδηλώνει μοναδικό byte που παίρνει τις τιμές 0 ή 1. Η τιμή 0 φανερώνει "ΛΑΘΟΣ" και η τιμή 1 φανερώνει "ΑΛΗΘΕΙΑ". Ο όρος uint32 αναφέρεται σε ακέραιο 32 bit αποθηκευμένος σαν 4 bytes με το Most Significant Bit (MSB) πρώτο. Τέλος, ο όρος string παρουσιάζει δυαδικά δεδομένα αυθαίρετου μήκους.

Ακολουθεί μια σύντομη περιγραφή των πεδίων:

`SSH_MSG_KEXINIT`

Το πεδίο αυτό προσδιορίζει την ταυτότητα του πακέτου.

`cookie:`

Είναι μια τυχαία τιμή που παράγεται από τον server.

`kex_algorithms`

Περιέχει λίστα με τους διαθέσιμους αλγόριθμους ανταλλαγής κλειδιών. Ο πρώτος στην λίστα είναι αυτός που προτιμάται. Η μία και μοναδική μέθοδος που απαιτείται είναι η Diffie-Hellman με hash αλγόριθμο τον SHA-1.

`server_host_key_algorithms`

Περιέχει λίστα με τους υποστηριζόμενους αλγόριθμους για την ασύμμετρη κρυπτογραφία, δηλαδή για το ζεύγος ιδιωτικής και δημόσιας κλείδας. Ο server δηλώνει τους αλγόριθμους για τους οποίου έχει κλείδες και ο client δηλώνει τους αλγόριθμους που δέχεται. Η επιλογή του αλγόριθμου εξαρτάται από το κατά πόσο απαιτείται από την μέθοδο ανταλλαγής κλειδιών ψηφιακή υπογραφή ή κρυπτογράφηση. Επιλέγεται ο πρώτος από την λίστα του client που ικανοποιεί όλες τις απαιτήσεις και που υποστηρίζεται από τον server. Εάν δεν υπάρχει τέτοιος αλγόριθμος πρέπει να τερματιστεί η σύνδεση.

`encryption_algorithms`

Περιέχει λίστα με τους αποδεκτούς συμμετρικούς αλγόριθμους με σειρά προτεραιότητας. Ο αλγόριθμος που επιλέγεται για την κάθε κατεύθυνση πρέπει να είναι ο πρώτος στην λίστα του client που υπάρχει και στην λίστα του server. Εάν δεν υπάρχει τέτοιος αλγόριθμος πρέπει να τερματιστεί η σύνδεση.

`mac_algorithms`

Περιέχονται όλοι οι αποδεκτοί MAC αλγόριθμοι σε σειρά προτεραιότητας. Επιλέγεται ο πρώτος στην λίστα του client που υπάρχει και στην λίστα του server. Εάν δεν υπάρχει τέτοιος αλγόριθμος πρέπει να τερματιστεί η σύνδεση. Οι αλγόριθμοι που υποστηρίζονται είναι:

`compression_algorithms`

Περιέχονται οι αποδεκτοί αλγόριθμοι συμπίεσης με πρώτο αυτόν που προτιμάται. Επιλέγεται ο πρώτος στην λίστα του client που υπάρχει και στην λίστα του server. Εάν δεν υπάρχει τέτοιος αλγόριθμος πρέπει να τερματιστεί η σύνδεση.

`languages`

Λίστα χωρισμένοι με κόμμα υποστηριζόμενων γλωσσών. Αυτή η λίστα μπορεί να αγνοηθεί και από τους δύο.

`first_kex_packet_follows`

Υποδηλώνει κατά πόσο ακολουθεί πακέτο με αλγόριθμους που έχουν μαντέψει ο client και ο server. Εάν θα σταλεί τέτοιο πακέτο, τότε η τιμή είναι "ΑΛΗΘΕΙΑ" (TRUE) εάν όχι τότε είναι "ΛΑΘΟΣ" (FALSE). Μετά την παραλαβή του πακέτου SSH_MSG_KEYINIT από την αντίστοιχη πλευρά, το κάθε σύστημα θα γνωρίζει κατά πόσο έπεσε μέσα στις προβλέψεις του.

Με το πέρας αυτού του βήματος, παράγονται δύο τιμές που έχουν στην κατοχή τους και τα δύο συστήματα: ένα μυστικό κλειδί K και μια hash value. Από αυτά τα δύο και με κατάλληλο αλγόριθμο προκύπτουν κλειδιά κρυπτογράφησης και πιστοποίησης. Η hash value χρησιμοποιείται και σαν session identifier, τιμή που ταυτίζει με μοναδικό τρόπο την σύνδεση.

Μετά την καθιέρωση των χρησιμοποιούμενων αλγόριθμων, υποχρεούται ο server να αποδείξει την ταυτότητα του. Αυτό επιτυγχάνεται με την υπογραφή του session identifier με την ιδιωτική τού κλείδα και αποστολή του αποτελέσματος στον client. Μαζί αποστέλλονται και κατάλληλος αριθμός πιστοποιητικών που εμπεριέχούν την δημόσια κλείδα του server.

## Αίτηση Εξυπηρέτησης

Αφού ληφθούν όλες οι απαραίτητες αποφάσεις σχετικά με τους χρησιμοποιούμενους μηχανισμούς, ο client στέλνει πακέτο που περιέχει αίτηση για συγκεκριμένη υπηρεσία. Το πακέτο έχει την εξής μορφή:

```
byte SSH_MSG_SERVICE_REQUEST

string service name
```

όπου η πρώτη γραμμή ταυτίζει το πακέτο σαν πακέτο αίτησης εξυπηρέτησης και η δεύτερη γραμμή δηλώνει το όνομα της υπηρεσίας που ζητείται. Τα ονόματα ssh-useraut και ssh-connection είναι κρατημένα για της υπηρεσίες του πρωτοκόλλου User Authentication και Connection αντίστοιχα.

Εάν ο server απορρίψει την αίτηση, στέλνει κατάλληλο μήνυμα αποσύνδεσης και η σύνδεση τερματίζεται. Διαφορετικά, εάν η υπηρεσία υποστηρίζεται και επιτρέπεται στον client, απαντά με

```
byte SSH_MSG_SERVICE_ACCEPT

string service name
```

Ο client περιμένει για την απάντηση του server πριν προχωρήσει σε αποστολή άλλων δεδομένων.

## Binary Packet Protocol

Κάθε πακέτο είναι της μορφής:

```
uint32 packet_length

byte padding_length
```

```
byte[n1] payload; n1 = packet_length - padding_length - 1

byte[n2] random padding; n2 = padding_length

byte[m] mac (message authentication code); m = mac_length
```

Αναλυτικά για το κάθε πεδίο έχουμε:

`packet_length`

Το μήκος του πακέτου, εξαιρουμένου των MAC bytes και του παρών πεδίου.

`padding_length`

Το μήκος των συμπληρωματικών bytes.

`payload`

Τα χρήσιμα περιεχόμενα του πακέτου. Εάν έχει βρεθεί αλγόριθμος συμπίεσης, τα περιεχόμενα είναι συμπιεσμένα. Αρχικά, δεν υπάρχει συμπίεση.

`random padding`

Συμπληρωματικά bytes των χρήσιμων περιεχομένων, εάν χρειάζεται

`mac (message authentication code)`

Περιέχει τα bytes του Message Authentication Code (MAC). Το πεδίο αυτό είναι άδειο πριν να συμφωνηθεί ο MAC αλγόριθμος.

Το ελάχιστο μήκος του πακέτου είναι 16 bytes και το μέγιστο 35000 bytes. Όλες οι εφαρμογές πρέπει να μπορούν να επεξεργάζονται πακέτα με ασυμπίεστο payload 23768 bytes ή λιγότερο. Πακέτα με μεγαλύτερο μήκος, θα στέλνονται μόνο όταν η έκδοση του πρωτοκόλλου στο "SSH-protoversion-softwareversion-comments" υποδηλώνει ότι υποστηρίζονται.

## Κατηγορίες Αλγόριθμων

### *Αλγόριθμοι Συμπίεσης*

Εάν έχει διαπραγματευθεί ο αλγόριθμος συμπίεσης, τότε συμπιέζονται μόνο τα περιεχόμενα του πεδίου payload σε κάθε πακέτο. Το μήκος του πακέτου και το MAC υπολογίζονται από το συμπιεσμένο payload. Ορίζεται ο αλγόριθμος GNU ZLIB (LZ77), η υποστήριξή του οποίου είναι προαιρετική, ενώ υπάρχει πάντα η δυνατότητα μη συμπίεσης. Η συμπίεση για κάθε κατεύθυνση πρέπει να είναι ανεξάρτητη του αλγόριθμου που χρησιμοποιείται στην άλλη αντίθετη φορά.

### *Αλγόριθμοι Κρυπτογράφησης*

Όταν χρησιμοποιείται κρυπτογράφηση, το μήκος του πακέτου, το μήκος των συμπληρωματικών bytes, τα περιεχόμενα και τα συμπληρωματικά bytes

κρυπτογραφούνται με το αλγόριθμο που έχει προεπιλεχθεί. Οι αλγόριθμοι επιλέγονται ανεξάρτητα για κάθε κατεύθυνση και για κάθε κατεύθυνση μπορεί να τρέχει διαφορετικός αλγόριθμος.

Οι ακόλουθοι ciphers υποστηρίζονται επί του παρόντος:

- Triple DES in CBC mode.
- Blowfish in CBC mode.
- ARCFOUR stream cipher (συμβατός με τον RC4).
- IDEA in CBC mode.
- CAST-128 in CBC mode.
- Καμία κρυπτογράφηση.

Από αυτούς ο Triple DES είναι υποχρεωτικά υποστηριζόμενος, ο Blowfish απλά συνιστάται, ενώ οι υπόλοιποι είναι προαιρετικοί.

***Αλγόριθμοι MAC***

Η ακεραιότητα των δεδομένων εξασφαλίζεται με την παραγωγή του MAC του μυστικού κλειδιού K, του αύξοντα αριθμού του πακέτου και των χρήσιμων περιεχομένων του πακέτου. Αρχικά, πριν την διαπραγμάτευση του αλγόριθμου, δεν υπάρχει MAC. Η παραγωγή του γίνεται πριν την κρυπτογράφηση των περιεχομένων. Τα MAC bytes μεταδίδονται στο τέλος του πακέτου, χωρίς κρυπτογράφηση.

Ο αύξοντας αριθμός του πακέτου είναι ένας ακέραιος που σε μορφή uint32 και είναι μηδέν για το πρώτο πακέτο. Αυξάνεται με την αποστολή κάθε πακέτου και μηδενίζεται κάθε $2^{32}$ πακέτα, ενώ ο ίδιος δεν περιλαμβάνεται στο πακέτο ποτέ.

Οι αλγόριθμοι MAC επιλέγονται ανεξάρτητα για κάθε κατεύθυνση και για κάθε κατεύθυνση μπορεί να τρέχει διαφορετικός αλγόριθμος.

Οι αλγόριθμοι που υποστηρίζονται είναι:

- HMAC σε συνδυασμό με τον SHA1.
- HMAC σε συνδυασμό με τον MD5.
- Χωρίς MAC.

Ο πρώτος είναι απαιτούμενος, ο δεύτερος προαιρετικός και ο τρίτος δεν συνιστάται.

***Αλγόριθμοι Ανταλλαγής Κλειδιών***

Ένας τέτοιος αλγόριθμος καθορίζει πως παράγονται και ανταλλάσσονται κλειδιά κρυπτογράφησης μίας χρήσης και πως γίνεται η πιστοποίηση της ταυτότητας του server. Η μία και μοναδική μέθοδος που υποστηρίζεται είναι η Diffie-Hellman με hash αλγόριθμο τον SHA-1.

***Αλγόριθμοι Ασύμμετρων Κλειδιών***

Υπάρχουν τρία διαφορετικά στοιχεία που απαρτίζουν ένα ζεύγος ιδιωτικής-δημόσιας κλείδας:

- *Key format*: Πως κωδικοποιείται η κλείδα και πως παρουσιάζονται τα πιστοποιητικά, που περιέχουν την δημόσια κλείδα.
- *Signature and/or encryption algorithms*: Μερικοί τύποι κλείδων δεν υποστηρίζουν και ψηφιακές υπογραφές και κρυπτογραφία.
- *Encoding of signatures and/or encrypted data*: Περιλαμβάνει το απαραίτητο συμπλήρωμα και μορφή των υπογραφών και κρυπτογραφήσεων.

Οι υποστηριζόμενοι αλγόριθμοι για αυτήν την κατηγορία είναι:

- DSS
- X.509 Certificates
- SPKI Certificates
- PGP Certificates

Η υποστήριξη του DSS είναι απαιτούμενη, του X.509 συνιστάται και οι υπόλοιποι δύο είναι προαιρετικοί.

## 5.5.5 User Authentication Protocol

Σε αυτό το πρωτόκολλο γίνεται η πιστοποίηση της ταυτότητας του χρήστη που χειρίζεται το μηχανή του client. Προορίζεται να τρέχει πάνω από το SSH Transport Layer Protocol, το οποίο παρέχει ακεραιτότητα δεδομένων και απόρρητη επικοινωνία. Η πρώτη αίτηση εξυπηρέτησης από τον client μετά την διαπραγμάτευση των αλγορίθμων και πιστοποίηση της ταυτότητας του server, είναι για την υπηρεσία με το όνομα "ssh-userauth"και αναφέρεται σε αυτό το πρωτόκολλο.

Όταν το πρωτόκολλο ξεκινά, λαμβάνει από το Transport Layer Protocol το session identifier που χρησιμοποιείται για να προσδιορίζει την σύνδεση με μοναδικό τρόπο. Ο server οδηγεί την διαδικασία της επαλήθευσης της ταυτότητας του χρήστη, λέγοντας στον client ποιες μέθοδοι μπορούν να εφαρμοστούν. Ο server έχει τον απόλυτο έλεγχο της διαδικασίας, αλλά παράλληλα παρέχει στον client την ευελιξία να επιλέξει τον αλγόριθμο που υποστηρίζει περισσότερο ή που είναι πιο βολική στον χρήστη. Οι υποστηριζόμενες μέθοδοι είναι τρεις: (α) με χρήση των δημοσίων κλείδων των χρηστών, (β) με χρήση μυστικών κωδικών και (γ) με χρήση των δημοσίων κλείδων των μηχανών που εργάζονται οι χρήστες. Θα αναλυθούν και οι τρεις παρακάτω.

### Αιτήσεις για Πιστοποίηση Ταυτότητας

Ο server θα πρέπει να έχει ένα προκαθορισμένο χρονικό όριο κατά την διάρκεια του οποίου πρέπει να έχει ολοκληρωθεί η πιστοποίηση της ταυτότητας του χρήστη. Εάν η πιστοποίηση δεν έχει γίνει δεκτή μέσα στο διάστημα αυτό, η σύνδεση θα πρέπει να διακοπεί. Ο χρόνος που συνιστάται είναι 10 λεπτά. Επιπλέον, η SSH εφαρμογή θα πρέπει να περιορίζει τον αριθμό των αποτυχημένων προσπαθειών κατά

την διάρκεια μιας συγκεκριμένης σύνδεσης. Ο αριθμός αυτό συνιστάται στις 20 προσπάθειες.

Όλες αιτήσεις για πιστοποίηση του χρήστη πρέπει να έχουν την ακόλουθη μορφή:

```
byte SSH_MSG_USERAUTH_REQUEST

string user name (in ISO-10646 UTF-8 encoding)

string service name (in US-ASCII)

string method name (US-ASCII)

rest of the packet is method-specific
```

Στο πεδίο `user name` δίνεται το όνομα του χρήστη. Εάν είναι άκυρο ο server μπορεί να συνδεθεί αμέσως ή να στείλει μια λίστα με τους αποδεκτές μεθόδους πιστοποίησης ταυτότητας, αλλά πότε να μην δεχθεί κανέναν από αυτούς. Με αυτόν τον τρόπο αποφεύγει να δώσει πληροφορίες με το ποια ονόματα υπάρχουν και ποια όχι.

Το πεδίο `service name` καθορίζει την υπηρεσία που θα ξεκινήσει μετά από την πιστοποίηση. Εάν δεν είναι διαθέσιμη ο server μπορεί να αποσυνδεθεί αμέσως ή οποιαδήποτε στιγμή αργότερα και η πιστοποίηση του χρήστη δεν πρέπει να γίνει δεκτή.

Το πεδίο `method name` περιέχει την μέθοδο που επιθυμεί να χρησιμοποιήσει ο χρήστης. Μπορεί να χρησιμοποιηθεί η τιμή "none", αλλά τότε η προσπάθεια θα απορριφθεί από τον server. Σκοπός της, κυρίως, είναι η αποστολή των υποστηριζόμενων μεθόδων στον client.

Ακολουθούν δεδομένα που σχετίζονται με την μέθοδο πιστοποίησης που ζητήθηκε από τον χρήστη και αποτελούν την προσπάθεια του να αποδείξει την ταυτότητα του.

### Απάντηση σε Αιτήσεις Πιστοποίησης Ταυτότητας

Εάν ο server απορρίψει την αίτηση, πρέπει να απαντήσει με το ακόλουθου μήνυμα:

```
byte SSH_MSG_USERAUTH_FAILURE

string authentications that can continue

boolean partial success
```

Η δεύτερη γραμμή περιέχει λίστα από μεθόδους που μπορούν να συνεχίσουν αυτόν τον διάλογο.

Το πεδίο `partial success` θα είναι "ΑΛΗΘΕΙΑ" όταν η προηγούμενη προσπάθεια ήταν επιτυχής, αλλά απαιτούνται και επιπλέον πιστοποιήσεις. Θα είναι "ΛΑΘΟΣ" όταν η αρχική προσπάθεια ήταν αποτυχημένη.

Όταν ο server δεχθεί την πρώτη προσπάθεια, τότε απαντά με:

```
byte SSH_MSG_USERAUTH_SUCCESS
```

Ο client μπορεί να στείλει πολλές αιτήσεις χωρίς να περιμένει για απάντηση από τον server. Ο server πρέπει να είναι σε θέση να αναγνωρίζει τις αποτυχημένες αιτήσεις και να στέλνει μηνύματα αποτυχίας, ενώ όταν δεχθεί μήνυμα που να μπορεί να επαληθεύσει την ταυτότητα του χρήστη να αποκρίνεται με μήνυμα επιτυχίας. Το τελευταίο μπορεί να στέλνεται μόνο μια φορά. Όταν ο server στείλει αυτό το μήνυμα, η διαδικασία έχει ολοκληρωθεί και ξεκινά την ζητούμενη υπηρεσία.

## Μέθοδοι Πιστοποίησης

### *Χρήση της Δημόσιας Κλείδας του Χρήστη (Public Key Authentication)*

Είναι η μόνη απαιτούμενη μέθοδος και όλες οι εφαρμογές πρέπει να την υποστηρίζουν. Σε αυτήν, η κατοχή μίας ιδιωτικής κλείδας χρησιμεύει σαν αποδεικτικό στοιχείο της ταυτότητας του χρήστη, σε συνδυασμό με τη σχετιζόμενη δημόσια κλείδα. Λειτουργεί με την αποστολή από τον client, της υπογραφής του χρήστη που έχει δημιουργηθεί με χρήση της ιδιωτικής του κλείδας. Οι ιδιωτικές κλείδες συχνά αποθηκεύονται κρυπτογραφημένες στον client και ο χρήστης πρέπει να δώσει μία φράση – κλειδί για να αποκτήσει πρόσβαση σε αυτήν. Επειδή η διαδικασία της υπογραφής περιλαμβάνει χρονοβόρους υπολογισμούς, χρησιμοποιείται το παρακάτω μήνυμα για να ερευνηθεί εάν είναι αποδεκτή η πιστοποίηση με την συγκεκριμένη κλείδα, ώστε να αποτραπεί άχρηστη και ασύμφορη επεξεργασία.

```
byte SSH_MSG_USERAUTH_REQUEST

string user name

string service

string "publickey"

boolean FALSE

string public key algorithm name

string public key blob (=certificates)
```

Οι αλγόριθμοι ασύμμετρων κλειδιών αποφασίσθηκαν στο Transport Layer Protocol. Ανταποκρίνονταν, όμως, στα ασύμμετρα κλειδιά που χρησιμοποιήθηκαν κατά την πιστοποίηση της ταυτότητας του server. Οπότε, είναι δυνατόν κάποιοι από αυτούς να μην ισχύουν για αυτήν την περίπτωση πιστοποίησης. Εάν συμβαίνει κάτι τέτοιο, ο server απαντά με ένα από τα δύο μηνύματα:

`SSH_MSG_USERAUTH_FAILURE` ή με

```
byte SSH_MSG_USERAUTH_PK_OK

string public key algorithm name from the request

string public key blob from the request
```

Για να πραγματοποιήσει ουσιαστική πιστοποίηση, ο client στέλνει μία υπογραφή του χρήστη που έχει δημιουργηθεί με την ιδιωτική του κλείδα. Ο client μπορεί να στείλει το παρακάτω μήνυμα χωρίς πρώτα να επαληθεύσει κατά πόσο η κλείδα είναι αποδεκτή.

```
byte SSH_MSG_USERAUTH_REQUEST

string user name

string service

string "publickey"

boolean TRUE

string public key algorithm name

string public key to be used for authentication

string signature
```

Η υπογραφή γίνεται πάνω στα έξης δεδομένα: (α) το session identifier και (β) στο πεδίο payload του πακέτου. Όταν ο server παραλάβει το μήνυμα, πρέπει πρώτα να ελέγξει εάν το είναι αποδεκτή η δημόσια κλείδα και έπειτα να ελέγξει εάν είναι σωστή η υπογραφή. Δεδομένου ότι και οι δύο έλεγχοι επιτύχουν, η μέθοδος έχει θετικό αποτέλεσμα και μήνυμα επιτυχίας αποστέλλεται στον client. Υπάρχει περίπτωση, όμως, ο server να απαιτεί και επιπλέον πιστοποιήσεις. Η τελική απάντηση, λοιπόν, του server πρέπει να είναι είτε SSH_MSG_USERAUTH_SUCCESS (όταν δεν χρειάζεται περαιτέρω πιστοποίηση και η υπογραφή ήταν έγκυρη) είτε SSH_MSG_USERAUTH_FAI-

LURE (όταν περισσότερες πιστοποιήσεις χρειάζονται ή η αίτηση απέτυχε).

### *Χρήση Μυστικού Κωδικού (Password Authentication)*

Όλες οι SSH εφαρμογές θα πρέπει να υποστηρίζουν αυτή την μέθοδο. Τα παρακάτω πακέτα χρησιμοποιούνται:

```
byte SSH_MSG_USERAUTH_REQUEST

string user name

string service
```

```
string "password"

boolean FALSE

string plaintext password (ISO-10646 UTF-8)
```

Παρ' όλο που ο κωδικό μεταδίδεται μη κρυπτογραφημένος μέσα στο πακέτο, ολόκληρο το πακέτο κρυπτογραφείται από το Transport Layer Protocol. Κανονικά, θα πρέπει να ελεγχθεί κατά πόσο είναι ενεργοποιημένος κάποιος αλγόριθμος κρυπτογράφησης. Εάν δεν εξασφαλίζεται η εμπιστευτικότητα της επικοινωνίας, τότε αυτή η μέθοδος θα πρέπει να πάψει να θεωρείται διαθέσιμη.

Ο server μπορεί να ζητήσει από τον χρήστη να αλλάξει κωδικό με το παρακάτω μήνυμα:

```
byte SSH_MSG_USERAUTH_PASSWD_CHANGEREQ

string prompt (ISO-10646 UTF-8)

string language tag (as defined in RFC 1766)
```

Ο client, μετά από υπόδειξη του χρήστη, μπορεί να ανταποκριθεί με τον καινούργιο κωδικό. Ο χρήστης μπορεί να αλλάξει τον κωδικό του χωρίς να του ζητηθεί από τον server.

```
byte SSH_MSG_USERAUTH_REQUEST

string user name

string service

string "password"

boolean TRUE

string plaintext old password (ISO-10646 UTF-8)

string plaintext new password (ISO-10646 UTF-8)
```

### *Χρήση της Δημόσιας Κλείδας του Client (Host-Based Authentication)*

Μερικά sites επιθυμούν να επιτρέψουν πιστοποίηση του χρήστη, βασιζόμενη στην μηχανή-client που βρίσκεται αυτός σε συνδυασμό με το όνομα του. Παρ' όλο που δεν συνιστάται δίκτυα υψηλής ασφάλειας, μπορεί να είναι πολύ βολική για μερικά περιβάλλοντα. Είναι προαιρετική η υποστήριξη της μεθόδου και πρέπει να τηρείται προσοχή ώστε ο χρήστης να μην έχει την δυνατότητα να αποκτήσει την δημόσια κλείδα του client.

Η μέθοδος λειτουργεί με την αποστολή υπογραφής που έχει δημιουργηθεί με την ιδιωτική κλείδα του client, την οποία ελέγχει ο server με την δημόσια κλείδα του client. Το μήνυμα έχει ως εξής:

```
byte SSH_MSG_USERAUTH_REQUEST

string user name

string service

string "hostbased"

string public key algorithm for host key

string public host key and certificates for client host

string client host name (FQDN; US-ASCII)

string client user name on the remote host (ISO-10646 UTF-8)

string signature
```

Οι αλγόριθμοι έχουν διαπραγματευτεί στο Transport Layer Protocol. Η υπογραφή προκύπτει από το session identifier και τα περιεχόμενα του payload του πακέτου. Ο server πρέπει να επιβεβαιώσει η δημόσια κλείδα ανήκει όντως στον client, ότι ο χρήστης επιτρέπεται να συνδεθεί και ότι η υπογραφή είναι έγκυρη.

# 5.5.6 Connection Protocol

Το Connection Protocol έχει σχεδιαστεί για να τρέχει πάνω από το SSH Transport Layer Protocol και το User Authentication Protocol. Παρέχει interactive login session, απομακρυσμένη εκτέλεση εντολών, προώθηση TCP/IP και X11 συνδέσεων. Οι υπηρεσίες του έπονται των υπηρεσιών του User Authentication Protocol και αναγνωρίζονται από το όνομα "ssh-connection".

### Ο Μηχανισμός των Καναλιών

Όλες τερματικές sessions, οι προωθημένες TCP/IP και X11 συνδέσεις, η απομακρυσμένη εκτέλεση εντολών κ.α. αποτελούν κανάλια. Οποιαδήποτε πλευρά μπορεί να ανοίξει ένα κανάλι και πολλαπλά λογικά κανάλια πολυπλέκονται σε ένα φυσικό.

Τα κανάλια αναγνωρίζονται από μοναδικούς αριθμούς διαφορετικούς σε κάθε πλευρά. Όταν οποιοδήποτε άκρο επιθυμεί την δημιουργία καναλιού, ετοιμάζει αίτηση που περιέχει τον αριθμό που έχει αντιστοιχήσει τοπικά στο κανάλι, ώστε ο αποδέκτης της αίτησης να μπορεί στην συνέχεια για να προσδιορίζει το κανάλι χρησιμοποιώντας αυτόν τον αριθμό.

Τα κανάλια είναι ελεγχόμενης ροής δεδομένων (flow-controlled), που σημαίνει ότι δεν αποστέλλονται δεδομένα έως ότου παραληφθεί μήνυμα που να δηλώνει ότι υπάρχει ελεύθερος χώρος στο παράθυρο.

### Δημιουργία Καναλιών

Όταν επιθυμείται η δημιουργία καναλιού και αφού το καινούργιο κανάλι έχει αντιστοιχηθεί με κατάλληλο αριθμό αναγνώρισης, στέλνεται το ακόλουθο μήνυμα στο άλλο άκρο:

```
byte SSH_MSG_CHANNEL_OPEN

string channel type (restricted to US-ASCII)

uint32 sender channel

uint32 initial window size

uint32 maximum packet size

... channel type specific data follows
```

Το πεδίο `channel type` περιγράφει τον τύπο του καναλιού που επιθυμεί ο αποστολέας να δημιουργήσει. Στο πεδίο `sender channel` περιέχεται ο αριθμός που έχει αντιστοιχήσει ο αποστολέας στο κανάλι. Στο `initial window size` καθορίζεται πόσα bytes Δεδομένων μπορούν να σταλούν μέσα από το κανάλι αρχικά, χωρίς να χρειάζεται να ξαναρυθμιστεί το μέγεθος του. Τέλος, το `maximum packet size` καθορίζει τον μέγιστο μέγεθος κάθε πακέτου που δέχεται ο αποστολέας της αίτησης.

Το απομακρυσμένο σύστημα αποφασίζει κατά πόσο μπορεί να ανοίξει το κανάλι και ανταποκρίνεται είτε με

```
byte SSH_MSG_CHANNEL_OPEN_CONFIRMATION

uint32 recipient channel

uint32 sender channel

uint32 initial window size

uint32 maximum packet size

... channel type specific data follows
```

όπου recipient channel είναι ο αριθμός καναλιού του συστήματος που ξεκίνησε την διαδικασία και sender channel είναι ο αριθμός του αποστολέα του παρών μηνύματος, είτε με

```
byte SSH_MSG_CHANNEL_OPEN_FAILURE

uint32 recipient channel

uint32 reason code

string additional textual information (ISO-10646 UTF-8

[RFC-2044])
```

```
string language tag (as defined in [RFC-1766])
```

Εάν ο αποδέκτης του αρχικού SSH_MSG_CHANNEL_OPEN μηνύματος δεν υποστηρίζει το ζητούμενο κανάλι, τότε απλά απαντά με το SSH_MSG_CHANNEL_O- PEN_FAILURE. Στο πεδίο reason code περιέχεται ακέραιος που υποδηλώνει την αιτία που δεν μπορούσε να δημιουργηθεί το κανάλι. Στο παρακάτω πίνακα βλέπουμε τους κωδικούς με την σημασία τους.

```
SSH_OPEN_ADMINISTRATIVELY_PROHIBITED 1

SSH_OPEN_CONNECT_FAILED 2

SSH_OPEN_UNKNOWN_CHANNEL_TYPE 3

SSH_OPEN_RESOURCE_SHORTAGE 4
```

## Μεταφορά Δεδομένων

Το μέγεθος του παραθύρου *(window size)* καθορίζει πόσα bytes μπορεί να στείλει η άλλη οντότητα χωρίς να χρειάζεται η εκ νέού ρύθμιση του μεγέθους του. Το ακόλουθο μήνυμα χρησιμοποιείται για την ρύθμιση του παραθύρου.

```
byte SSH_MSG_CHANNEL_WINDOW_ADJUST

uint32 recipient channel

uint32 bytes to add
```

Με αυτό το μήνυμα το μέγεθος του παραθύρου αυξάνεται σύμφωνα με το ποσό που ορίζεται στο πεδίο bytes to add. Η μεταφορά δεδομένων γίνεται με μηνύματα του τύπου:

```
byte SSH_MSG_CHANNEL_DATA

uint32 recipient channel

string data
```

Το μέγιστο πόσο δεδομένων που επιτρέπεται να σταλεί είναι ίσο με το μέγεθος του παραθύρου, το οποίο μειώνεται με κάθε αποστολή. Και οι δύο πλευρές μπορούν να αγνοήσουν τα δεδομένα που στέλνονται όταν το παράθυρο έχει γεμίσει.

## Κλείσιμο Καναλιών

Όταν κάποιος από τους συνδιαλλέγοντες δεν θα στείλει άλλα δεδομένα στο κανάλι, θα πρέπει να στείλει το εξής μήνυμα:

```
byte SSH_MSG_CHANNEL_EOF

uint32 recipient_channel
```

Η σύνδεση δεν διακόπτεται, απλά τερματίζεται η αποστολή δεδομένων σε μία από τις δύο κατευθύνσεις. Στην άλλη κατεύθυνση η ροή των δεδομένων συνεχίζεται κανονικά. Για το μήνυμα αυτό δεν υπάρχει σαφής απάντηση και το ίδιο δεν καταλαμβάνει χώρο από το παράθυρο και μπορεί να σταλεί ακόμα και αν δεν υπάρχει διαθέσιμος χώρος.

Όταν οποιοσδήποτε από τους δύο επιθυμεί να τερματίσει το κανάλι, στέλνει το μήνυμα

```
byte SSH_MSG_CHANNEL_CLOSE

uint32 recipient_channel
```

το οποίο πρέπει να απαντηθεί με παρόμοιο μήνυμα από τον παραλήπτη του. Το κανάλι θεωρείται ότι έχει κλείσει για ένα άκρο όταν έχει στείλει και παραλάβει το μήνυμα αυτό και συνεπώς ο αριθμός του καναλιού μπορεί να ξαναχρησιμοποιηθεί. Η αποστολή του μηνύματος δεν προϋποθέτει την αποστολή του SSH_MSG_CHANNEL_EOF. Ομοίως, το μήνυμα δεν καταλαμβάνει χώρο από το παράθυρο.

## Αιτήσεις Σχετικές με Κανάλια

Για πολλούς τύπους καναλιών, υπάρχουν αιτήσεις εξυπηρέτησης που είναι συγκεκριμένες για κάθε κανάλι. Αυτές οι αιτήσεις αναφέρονται σε υπηρεσίες που μπορεί αν προσφέρει το κανάλι. Παράδειγμα είναι η αίτηση για ένα pseudo terminal για ένα κανάλι interactive session.

Όλες οι αιτήσεις έχουν την εξής μορφή:

```
byte SSH_MSG_CHANNEL_REQUEST

uint32 recipient channel

string request type (restricted to US-ASCII)

boolean want reply

... type-specific data
```

Εάν το πεδίο want reply είναι "FALSE", τότε δεν θα σταλεί απάντηση στην αίτηση. Διαφορετικά, η απάντηση θα είναι μία από τις παρακάτω:

```
byte SSH_MSG_CHANNEL_SUCCESS

uint32 recipient_channel
```

ή

```
byte SSH_MSG_CHANNEL_FAILURE

uint32 recipient_channel
```

Εάν η αίτηση δεν αναγνωρίζεται ή δεν υποστηρίζεται για το κανάλι το SSH_MSG_CHANNEL_FAILURE επιστρέφεται. Όλα τα παραπάνω μηνύματα δεν καταναλώνουν τον διαθέσιμο χώρο του παραθύρου.

Στον παρακάτω πίνακα παρουσιάζονται όλοι οι κυριότεροι τύποι καναλιών και οι αντίστοιχες αιτήσεις.

| ***Channel*** | ***Channel Type*** | ***Request*** | ***Request Type*** |
|---|---|---|---|
| INTERACTIVE SESSION | "session" | PSEUDO TERMINAL | "pty-req" |
| | | X11 FORWARDING | "x11-req" |
| | | AUTHENTICATION AGENT | "auth-agent-req" |
| | | ENVIRONMENT VARIABLE PASSING | "env" |
| | | SHELL | "shell" |
| | | COMMAND | "exec" |
| | | SUBSYSTEM | "subsystem" |
| | | SIGNAL | "signal" |
| | | RETURNING EXIT STATUS | "exit-status" |
| X11 CHANNEL | "x11" | - | - |
| AUTHENTICATION AGENT | "auth=agent" | - | - |
| TCP/IP FORWARDING | "forwarded-tcpip" | | |
| - | - | PORT FORWARDING | "tcpip-forward" |

Τα κανάλια X11 και AUTHENTICATION AGENT έπονται πάντα των αιτήσεων X11 FORWARDING και AUTHENTICATION AGENT REQUEST, διαφορετικά δεν γίνονται δεκτά. Ομοίως και το κανάλι TCP/IP FORWARDING το οποίο ακολουθεί πάντα μία αίτηση PORT FORWARDING.

## 5.5.7 Παρεχόμενη Προστασία

Το SSH προστατεύει απέναντι στις εξής επιθέσεις:

- *IP spoofing* (όταν μια μηχανή προσποιείται ότι είναι κάποια άλλη, που μπορεί να εμπιστευτεί).

- *IP source routing* (όταν μία μηχανή μπορεί να προσποιηθεί ότι ένα πακέτο προέρχεται από μηχανή)
- *DNS spoofing* (όταν κάποιος απατεώνας πλαστογραφεί τα αρχεία ενός DNS sever).
- Απόκτηση μυστικών κωδικών και άλλων ευαίσθητων πληροφοριών από ενδιάμεσα συστήματα.
- Τροποποίηση δεδομένων από ανθρώπους που χειρίζονται ενδιάμεσα συστήματα.
- Επιθέσεις που βασίζονται στην παράνομη καταγραφή X11 δεδομένων που κατευθύνονται σε X11 server.

Με άλλα λόγια, το SSH δεν εμπιστεύεται ποτέ το δίκτυο και κάποιος που έχει καταλάβει το δίκτυο μπορεί μόνο να αναγκάσει το SSH να αποσυνδεθεί.

Όλα αυτά ισχύουν όμως με την προϋπόθεση ότι δεν είναι δυνατή η απόκτηση *root access* με άλλα μέσα. Σε αυτήν την περίπτωση το SSH δεν μπορεί να βοηθήσει σε τίποτα.

### 5.5.8 Θέματα Ασφάλειας

Όσο αναφορά το SSH Transport Layer Protocol, είναι αναμενόμενο ότι μερικές φορές θα χρησιμοποιείται χωρίς αξιόπιστη συσχέτιση μεταξύ των δημοσίων κλείδων των μηχανών και της ταυτότητας των μηχανών. Τέτοια χρήση του πρωτοκόλλου είναι ανασφαλής, άλλα μπορεί να παρέχει ικανοποιητική ασφάλεια σε κάποια συστήματα.

Όταν το SSH Transport Layer Protocol δεν υποστηρίζει την κρυπτογράφηση των πακέτων, τότε οι μέθοδοι πιστοποιήσεις ταυτότητας του SSH User Authentication Protocol βασίζονται στην ανταλλαγή μυστικών δεδομένων, θα πρέπει να απαγορεύονται.

Τέλος, παρά την ασφάλεια που προστίθεται στις X11 συνδέσεις και στην προώθηση των TCP/IP πορτών, είναι προτιμότερο οι εφαρμογές του SSH να αποφεύγουν την υποστήριξη τους, καθ' ότι τα firewalls δεν μπορούν να εξετάσουν την κυκλοφορία λόγω του κρυπτογραφημένου καναλιού.

## *5.6 S/HTTP (Secure Hyper-Text Transfer Protocol)*

### 5.6.1 Εισαγωγή

Το WWW είναι ένα διανεμημένο σύστημα πολυμέσων το οποίο χαίρει μεγάλης αποδοχής από πολλούς χρήστες. Το βασικό και περισσότερο χρησιμοποιούμενο πρωτόκολλο μεταξύ WWW clients και WWW servers είναι το Hyper Text Transfer Protocol. Η ευκολία της χρήσης του WWW έχει προκαλέσει το παγκόσμιο ενδιαφέρον και χρησιμοποιείται σαν η υποδομή client / server για πολλές δικτυακές εφαρμογές. Τέτοιες εφαρμογές απαιτούν την αμοιβαία πιστοποίηση της ταυτότητας

των δύο επικοινωνούντων υπολογιστών και την ικανότητα ανταλλαγής ευαίσθητων πληροφοριών. Οι τρέχοντες, όμως, HTTP εφαρμογές έχουν μέτρια έως και μηδαμινή υποστήριξη για τους κρυπτογραφικούς μηχανισμούς που είναι απαραίτητοι για τέτοιες συναλλαγές.

Το πρωτόκολλο Secure HTTP παρέχει ασφαλής μηχανισμούς επικοινωνίας μεταξύ ένα ζευγάρι HTTP server – client με σκοπό να επιτρέψει αυθόρμητες εμπορικές συναλλαγές. Στόχος της σχεδίασης ήταν ένα ευέλικτο πρωτόκολλο που διαθέτει πολλαπλούς μηχανισμούς και αλγόριθμους, και την δυνατότητα διαπραγμάτευσης αυτών. Σχεδιάστηκε από τους E. Rescorla και A. Schiffman του EIT και αποτελεί υπερσύνολο του HTTP.

## 5.6.2 Χαρακτηριστικά του S/HTTP

1. Το S/HTTP υποστηρίζει μία ποικιλία μηχανισμών ασφαλείας στους HTTP clients και servers. Το πρωτόκολλο παρέχει συμμετρικές δυνατότητες στον client και server που σημαίνει ότι τα μηνύματα και οι προτιμήσεις και των δύο πλευρών μεταχειρίζονται με τον ίδιο τρόπο, ενώ παράλληλα διατηρούνται το μοντέλο συναλλαγής και τα χαρακτηριστικά επικοινωνίας του HTTP.
2. Αρκετά κρυπτογραφικά στάνταρντς ενσωματώνονται στους S/HTTP clients και servers συμπεριλαμβανομένων των PEM, PGP, Kerberos και PKCS-7 (ο πρόγονος του CMS). Είναι συμβατό με το HTTP.
3. Το S/HTTP δεν απαιτεί πιστοποιητικά δημοσίων κλείδων από την μεριά του client, καθ' ότι υποστηρίζει και τα συμμετρικά κλειδιά. Αυτό είναι σημαντικό γιατί αυθόρμητες ιδιωτικές συναλλαγές μπορούν να λάβουν χώρα, χωρίς την απαίτηση από τους χρήστες να έχουν ένα έγκυρο ζεύγος δημόσιας – ιδιωτικής κλείδας. Βέβαια, είναι σε θέση να εκμεταλλευτεί την υπάρχουσα υποδομή πιστοποιητικών και ασύμμετρων κλειδιών.
4. Το S/HTTP υποστηρίζει απ' άκρη σ' άκρη ασφαλής συναλλαγές, σε αντίθεση με το HTTP που προϋποθέτει μία αποτυχημένη προσπάθεια πρόσβασης του χρήστη πριν την εφαρμογή οποιωνδήποτε μηχανισμών ασφαλείας. Με το S/HTTP, σε καμία περίπτωση ευαίσθητα δεδομένα θα μεταδοθούν στο δίκτυο απροστάτευτα.
5. Επιτρέπει πλήρη ευελιξία όσον αναφορά τους κρυπτογραφικούς αλγόριθμούς και τις παραμέτρους αυτών. Το είδος της παρεχόμενης προστασίας (κρυπτογράφηση, ψηφιακή υπογραφή, και τα δύο), οι αλγόριθμοι και τα πιστοποιητικά μπορούν να διαπραγματευτούν.
6. Οι χρήστες αναμένονται να έχουν (αν και δεν συνιστάται) πολλαπλά πιστοποιητικά.

## 5.6.3 Είδη Προστασίας

Η προστασία ενός μηνύματος εφαρμόζεται με τρεις διαφορετικούς τρόπους: με υπογραφή, με κρυπτογράφηση και με παραγωγή MACs. Κάθε μήνυμα μπορεί να υπογραφεί, να κρυπτογραφηθεί ή οποιοσδήποτε συνδυασμός αυτών, συμπεριλαμβανομένων της παραγωγής και της παροχής καμίας προστασίας.

Υποστηρίζονται αρκετές τεχνικές διαχείρισης κλειδιών όπως συμμετρικά μυστικά κλειδιά, ασύμμετρη διαχείριση και το σύστημα Key Distribution Center (KDC) του Kerberos. Επιπλέον, ένας μηχανισμός *challenge-response* παρέχει στους επικοινωνούντες υπολογιστές την δυνατότητα να αναγνωρίζουν τις επιθέσεις επανάληψης (replay attacks).

### Υπογραφές

Όταν υπογράφεται ψηφιακά, ένα κατάλληλο πιστοποιητικό μεταφέρεται με το μήνυμα ή ο αποστολέας μπορεί να αφήσει τον παραλήπτη να αποκτήσει το απαιτούμενο πιστοποιητικό από μόνος του.

### Κρυπτογράφηση

Εκτός από την βασική κρυπτογράφηση, το S/HTTP καθορίζει δύο μηχανισμούς ανταλλαγής κλειδιών: (α) χρήση ασύμμετρης διαχείρισης κλειδιών και (β) χρήση ενός προκαθορισμένου κλειδιού.

Στην πρώτη περίπτωση, οι παράμετροι και το κλειδί του συμμετρικού κρυπτοσυστήματος κρυπτογραφούνται με την δημόσια κλείδα του παραλήπτη.

Στην δεύτερη περίπτωση, τα ίδια στοιχεία κρυπτογραφούνται με κλειδί που έχει προαποφασιστεί νωρίτερα. Τα κλειδιά αυτά μπορούν να προέλθουν και από τα tickets του Kerberos.

### Παραγωγή Message Authentication Codes (MACs)

Το S/HTTP παρέχει επιπλέον μέσα για την επαλήθευση της ακεραιότητας των δεδομένων και την πιστοποίηση της ταυτότητας του αποστολέα. Χρησιμοποιεί το MAC του μηνύματος, το οποίο υπολογίζεται από hash αλγόριθμο σε συνδυασμό με ένα κοινό μυστικό κλειδί (π.χ. MD5). Αυτή η τεχνική δεν απαιτεί την χρήση ασύμμετρης διαχείρισης ούτε την χρήση κρυπτογράφησης.

## 5.6.4 Μοντέλο Επεξεργασίας

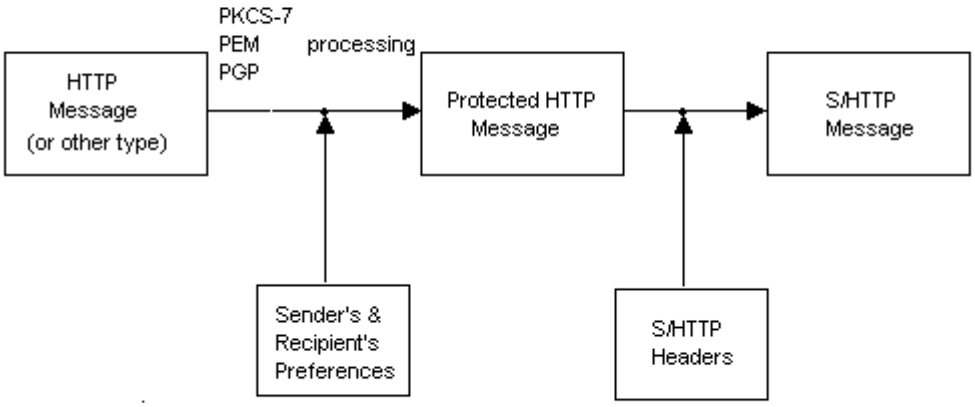
### Προετοιμασία Μηνύματος

Η δημιουργία ενός S/HTTP μηνύματος μπορεί να θεωρηθεί σαν μια συνάρτηση με τρεις εισόδους:

1. Το μήνυμα που πρόκειται να προστατευτεί. Μπορεί να είναι ένα HTTP μήνυμα ή κάποιο άλλο αντικείμενο. Το HTTP μήνυμα μπορεί να είναι οποιασδήποτε έκδοσης του HTTP πρωτοκόλλου.
2. Οι κρυπτογραφικές προτιμήσεις του παραλήπτη. Αυτές είτε έχουν καθοριστεί σε προηγούμενη επικοινωνία, είτε βασίζονται σε προρυθμίσεις.
3. Οι κρυπτογραφικές προτιμήσεις του αποστολέα.

Ο αποστολέας συνδυάζει τις προτιμήσεις και των δύο πλευρών και αποφαίνεται για τους αλγόριθμους και μηχανισμούς που θα χρησιμοποιηθούν καθώς και για την

μορφή των κλειδιών. Ίσως χρειαστεί η επέμβαση του χρήστη σε περίπτωση πολλών επιλογών. Στο προστατευμένο HTTP μήνυμα, έπειτα, προστίθονται κατάλληλες S/HTTP επικεφαλίδες και παράγεται το τελικό S/HTTP μήνυμα.




### Παραλαβή του Μηνύματος

Η επεξεργασία του παραληφθέντος S/HTTP μηνύματος, με την σειρά της, μπορεί να θεωρηθεί σαν συνάρτηση με τέσσερις διακριτές εισόδους:

1. Το S/HTTP μήνυμα.
2. Οι πρωτύτερα δηλωμένες κρυπτογραφικές προτιμήσεις του παραλήπτη.
3. Οι τρέχοντες κρυπτογραφικές προτιμήσεις του παραλήπτη.
4. Οι πρωτύτερα δηλωμένες κρυπτογραφικές προτιμήσεις του αποστολέα. Ο αποστολέας μπορεί να έχει δηλώσει το είδος των κρυπτογραφικών διαδικασιών που θα εφήρμοζε στο μήνυμα.

Για να μπορέσει να επεξεργαστεί το S/HTTP μήνυμα, ο παραλήπτης διαβάζει τις S/HTTP επικεφαλίδες για να ανακαλύψει τι κρυπτογραφικοί μετασχηματισμοί εφαρμόστηκαν στο μήνυμα και με την βοήθεια των προσυμφωνημένων κλειδιών τις αφαιρεί. Το αποτέλεσμα είναι το HTTP μήνυμα (ή κάποιο άλλο αντικείμενο).

Ο παραλήπτης μπορεί να επιλέξει να επαληθεύσει ότι οι εφαρμοσμένοι μηχανισμοί ταιριάζουν με αυτούς που είχε δηλώσει ο αποστολέας (είσοδος 4), με αυτούς που είχε ζητήσει ο παραλήπτης (είσοδος 2) καθώς και με τις τρέχοντες προτιμήσεις του τελευταίου (είσοδος 3), με σκοπό να αποφανθεί εάν το μήνυμα είχε μετασχηματιστεί κατάλληλα.

## 5.6.5 HTTP Ενθυλάκωση

Ένα S/HTTP μήνυμα αποτελείται από μία γραμμή αίτησης *(request line)* ή απάντησης *(status line)*, ακολουθούμενη από μια σειρά από επικεφαλίδες τύπου RFC822 και τα ασφαλισμένα ενθυλακωμένα περιεχόμενα. Τα ενθυλακωμένα περιεχόμενα μπορεί να είναι είτε ένα ακόμα S/HTTP μήνυμα, είτε ένα HTTP μήνυμα, είτε απλά δεδομένα.

## Request Line

Για τις HTTP αιτήσεις η γραμμή που ξεκινά το μήνυμα είναι:

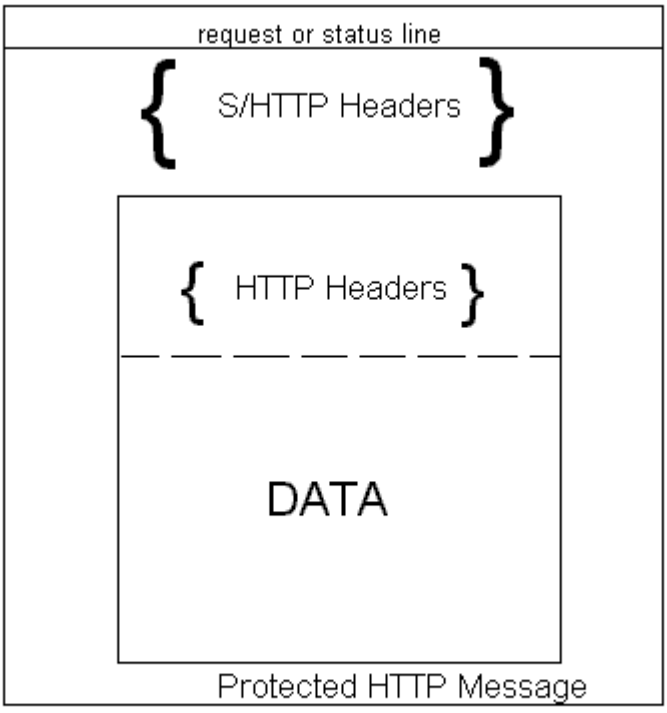
```
Secure * Secure-HTTP/1.1
```

## Status Line

Στις απαντήσεις του server η πρώτη γραμμή πρέπει να είναι:

```
Secure-HTTP/1.1 200 OK
```

Παρατηρούμε ότι δεν δηλώνεται κατά πόσο έγινε δεκτή ή όχι η αίτηση του client. Η ίδια γραμμή χρησιμοποιείται και στην περίπτωση αποτυχίας και στην περίπτωση επιτυχίας, γεγονός που αποτρέπει την επίγνωση της περίπτωσης.




**S/HTTP Message**

## 5.6.6 Οι Επικεφαλίδες του S/HTTP

Το πρωτόκολλο καθορίζει μία σειρά από νέες επικεφαλίδες που πηγαίνουν στο πεδίο των επικεφαλίδων του S/HTTP μηνύματος. Από αυτές, όλες εκτός των "Content-Type" και "Content-Privacy-Domain" είναι προαιρετικές. Τα κυρίως περιεχόμενα του μηνύματος διαχωρίζονται από τις επικεφαλίδες με δύο συνεχόμενες ακολουθίες των χαρακτήρων ελέγχου <CR><LF>.

### Content-Privacy-Domain

Αυτή η επικεφαλίδα υπάρχει για να παρέχει συμβατότητα με τα S/HTTP εφαρμογές που βασίζονται στο PEM. Οι τιμές της είναι "PEM", "PKCS-7" και "PGP".

Όταν χρησιμοποιείται η επικεφαλίδα "Content-Privacy-Domain: PKCS-7", η προστασία του μηνύματος γίνεται με τους εξής τρόπους, βάσει του PKCS-7: με υπογραφή και με κρυπτογράφηση. Κάθε HTTP μήνυμα μπορεί να κρυπτογραφηθεί, να υπογραφεί ή και τα δύο. Το μήνυμα που υπογράφεται συνήθως συνοδεύεται από πιστοποιητικό ή από αλυσίδα πιστοποιητικών. Οι επικεφαλίδες "Content-Privacy-Domain: PGP" και "Content-Privacy-Domain: PEM" υποδηλώνουν εφαρμογή των κανόνων του PGP ή του PEM, αντίστοιχα.

### Content-Transfer-Encoding

Εδώ καθορίζεται η κωδικοποίηση των περιεχομένων και οι τιμές που μπορεί να πάρει η επικεφαλίδα είναι "8-bit", "7-bit" και "BASE64". Η τιμή εξαρτάται από την επικεφαλίδας "Content-Privacy-Domain ".

Για την περίπτωση που είναι "Content-Privacy-Domain: PKCS-7", οι μόνες επιτρεπτές τιμές της "Content-Transfer-Encoding" είναι "BASE64" ή "8-bit".

Για την περίπτωση που είναι "Content-Privacy-Domain: PEM", η μόνη επιτρεπτή τιμή είναι η "7-bit".

Για την περίπτωση που είναι "Content-Privacy-Domain: PGP" , όλες οι παραπάνω τιμές επιτρέπονται ανάλογα με την μορφή του PGP μηνύματος.

### Content-Type

Υπό κανονικές συνθήκες, τα ενθυλακωμένα περιεχόμενα μετά την αφαίρεση όλων κρυπτογραφικών μέτρων ασφαλείας, θα είναι ένα HTTP μήνυμα. Σε αυτήν την περίπτωση η επικεφαλίδα θα είναι:

```
Content-Type: application/http
```

Δεν αποκλείεται, όμως, τα ενθυλακωμένα περιεχόμενα να είναι κάποιου άλλου τύπου με την προϋπόθεση ότι αυτός ο τύπος δηλωθεί σωστά με την χρήση κατάλληλης επικεφαλίδας "Content-Type".

### Prearranged-Key-Info

Η επικεφαλίδα αυτή έχει σαν σκοπό να συνοδεύσει πληροφορίες σχετικά με κλειδί που έχει προκανονιστεί με κάποιον τρόπο έκτος της εσωτερικής κρυπτογράφησης. Μία χρήση της επικεφαλίδας είναι η in-band επικοινωνία ενός session key στην περίπτωση που κάποια από τις δύο πλευρές δεν κατέχει ένα.

Ορίζονται τρεις μέθοδοι για την ανταλλαγή session keys: (α) Inband, (β) Kerberos και (γ) Outband. Οι δύο πρώτες μέθοδοι, Inband και Kerberos, υποδηλώνουν ότι το κλειδί έχει ανταλλαγεί πρωτύτερα, με χρήση μιας HTTP επικεφαλίδας "Key-Assign". Η Outband μέθοδος υπονοεί ότι ο client και ο server έχουν πρόσβαση σε κλειδιά που σχετίζονται με ονόματα χρηστών, είτε μέσω μιας βάσης δεδομένων, είτε από την εισαγωγή ενός κωδικού από τον χρήστη μέσω του πληκτρολόγιου.

### MAC-Info

Μεταφέρει ένα Message Authentication Code (MAC), παρέχοντας πιστοποίηση ταυτότητας και ακεραιότητας. Το MAC υπολογίζεται από τα ενθυλακωμένα περιεχόμενα, την ώρα (προαιρετικό – αποτρέπει τις επιθέσεις replay attacks) και κάποιού κοινού μυστικού που μοιράζονται ο client και ο server. Έστω ότι χρησιμοποιείται hash αλγόριθμος H, τότε η εξίσωση που περιγράφει την διαδικασία είναι (οι δύο κάθετες παύλες || σημαίνουν συνένωση):

```
MAC = hex(H(Message||<time>||<shared key>))
```

## 5.6.7 Διαπραγματεύσεις

Και δύο πλευρές πρέπει να είναι σε θέση να εκφράσουν τις προτιμήσεις και τις απαιτήσεις τους σχετικά με ποίες κρυπτογραφικές ενισχύσεις επιτρέπουν ή απαιτούν. Το σύνολο των πληροφοριών που διαπραγματεύονται, χωρίζεται σε τέσσερα μέρη:

*Property*: Το είδος της προστασίας (κρυπτογράφηση, υπογραφές, κτλ.).

*Value*: Ο αλγόριθμος που προσφέρει την παραπάνω προστασία.

*Direction*: Η κατεύθυνση για την οποία αναφέρονται οι συγκεκριμένες προτιμήσεις (*reception, origination*).

*Strength*: Πόσο ισχυρή είναι η επιλογή (*required, optional, refused*).

Η τιμή *optional* του τελευταίου πεδίου φανερώνει ότι οι αλγόριθμοι και το είδος της προστασίας που αναφέρονται στο Value και στο Property είναι προαιρετικές. Κατά την παραλαβή (*reception*) μηνύματος ασφαλισμένου με προαιρετικούς μηχανισμούς, ο παραλήπτης θα επιλέξει να το επεξεργαστεί αλλά δεν περιορίζεται στην επεξεργασία μόνο τέτοιων μηνυμάτων. Ο αποστολέας (*origination*) ο οποίος ορίζει κάποιες προτιμήσεις προαιρετικές, μπορεί να τις χρησιμοποιήσει όταν βρίσκονται σε συμφωνία με τις προτιμήσεις του παραλήπτη και δεν μπορεί όταν δεν είναι αποδεκτές.

Η τιμή *required* υποδηλώνει ότι ο παραλήπτης (*reception*) θα δέχεται S/HTTP μηνύματα μόνο με αυτές τις κρυπτογραφικές ενισχύσεις, ενώ ο αποστολέας (*origination*) θα χρησιμοποιεί μόνο αυτές ανεξάρτητα με τις προτιμήσεις του παραλήπτη.

Τέλος, η τιμή refused υποδηλώνει ότι ο παραλήπτης (*reception*) δεν θα δέχεται S/HTTP μηνύματα με τέτοιες κρυπτογραφικές ενισχύσεις, ενώ ο αποστολέας (*origination*) δεν θα παράγει ποτέ τέτοια μηνύματα.

## Επικεφαλίδες Διαπραγμάτευσης

Η τιμή του πεδίου *Property* συμπληρώνεται με κατάλληλες επικεφαλίδες που προσδιορίζουν ποια κρυπτογραφική ιδιότητα βρίσκεται υπό συζήτηση.

1. **SHTTP-Privacy-Domains**: Καθορίζει την διαδικασία που θα ασφαλίσει το HTTP μήνυμα (ή οποιουδήποτε άλλου τύπου δεδομένα). Οι δεκτές τιμές είναι "PEM", "PGP" και "PKCS-7". Οι υπόλοιπες επικεφαλίδες μπορούν είτε να αναφέρονται σε ένα από τα PEM", "PGP", "PKCS-7" οπότε ακολουθούν την SHTTP-Privacy-Domains, είτε να αναφέρονται και στις τρεις τιμές οπότε βρίσκονται πριν από την SHTTP-Privacy-Domains. Επιτρέπονται πολλαπλές τέτοιες επικεφαλίδες με σκοπό την υποστήριξη πολλαπλών συνδυασμό παραμέτρων.
2. **SHTTP-Certificate-Types**: Υποδηλώνει τον τύπο των πιστοποιητικών που θα γίνονται ή δεν θα γίνονται δεκτά (ανάλογα με το πεδίο *Strength*).
3. **SHTTP-Key-Exchange-Algorithms**: Υποδηλώνει τους αλγόριθμους που μπορεί να χρησιμοποιηθούν για την διαχείριση και ανταλλαγή κλειδιών.
4. **SHTTP-Signature-Algorithms**: Υποδηλώνει τους αλγόριθμους ψηφιακών υπογραφών που μπορεί να χρησιμοποιηθούν.
5. **SHTTP-Message-Digest-Algorithms**: Υποδηλώνει τους αλγόριθμους παραγωγής message digest.
6. **SHTTP-Symmetric-Contents-Algorithms**: Εδώ καθορίζονται οι αλγόριθμοι συμμετρικής κρυπτογράφησης του HTTP μηνύματος (ή οποιουδήποτε άλλου τύπου δεδομένα).
7. **SHTTP-Symmetric-Header-Algorithms**: Οι επικεφαλίδες ενός HTTP μηνύματος ασφαλίζονται ξεχωριστά από το υπόλοιπο μήνυμα. Οι αλγόριθμοι συμμετρικής κρυπτογράφησης που μπορεί να χρησιμοποιηθούν καθορίζονται με αυτήν την επικεφαλίδα.
8. **SHTTP-Privacy-Enhancement**: Υποδηλώνει εάν θα εφαρμοστεί κρυπτογράφηση ("encrypt"), ψηφιακή υπογραφή ("sign") ή MAC ("auth").

## 5.6.8 Νέες Επικεφαλίδες HTTP

Το πρωτόκολλο S/HTTP καθορίζει μία συλλογή νέων επικεφαλίδων που τοποθετούνται στις επικεφαλίδες του HTTP μηνύματος. Με τον τρόπο αυτό οι νέες επικεφαλίδες μοιράζονται την κρυπτογραφική προστασία που παρέχεται στις υπάρχουσες. Οι νέες επικεφαλίδες παρουσιάζονται παρακάτω.

1. **Security-Scheme**: Είναι απαραίτητη επικεφαλίδα που καθορίζει την έκδοση του S/HTTP πρωτοκόλλου. Η τρέχουσα έκδοση είναι η 1.4.
2. **Encryption-Identity**: Προσδιορίζει την ταυτότητα μιας οντότητας για την οποία το μήνυμα θα μπορούσε να κρυπτογραφηθεί.
3. **Certificate-Info**: Περιέχει πληροφορίες για τα πιστοποιητικά της οντότητας που προσδιορίζεται στην "Encryption-Identity".
4. **Key-Assign**: Αυτή η επικεφαλίδα υποδηλώνει ότι το σύστημα επιθυμεί να συνδέσει ένα κλειδί με ένα συμβολικό όνομα, για μελλοντική του χρήση. Στην επικεφαλίδα περιέχεται το συμβολικό όνομα, το κλειδί, η μέθοδος σύμφωνα με την οποία θα αποκτηθεί το κλειδί (Inband και Kerberos), η διάρκεια ζωής του και τέλος τους αλγόριθμους με τους οποίους προορίζεται για χρήση το κλειδί. Στην περίπτωση Inband ανταλλαγής, το κλειδί μεταφέρεται σαν παράμετρος της επικεφαλίδας, ενώ στην περίπτωση Kerberos ανταλλαγής, το κλειδί μεταφέρεται στο εσωτερικό ενός ticket.
5. **Nonce**: Περιέχει τιμή που χρησιμοποιείται για το ταίριασμα αίτησης και απάντησης. Σκοπός της είναι η διατήρηση της επικαιρότητας της σύνδεσης (freshness) και η αποφυγή replay attacks.

## 5.6.9 Υποστηριζόμενοι Αλγόριθμοι

Οι αλγόριθμοι που υποστηρίζει το S/HTTP χωρίζονται σε κατηγορίες, ανάλογα με είδος της παρεχόμενης προστασίας με την οποία χρησιμοποιούνται.

### Αλγόριθμοι Διαχείριση Κλειδιών

Οι μηχανισμοί που καθορίζονται για την διαχείριση και ανταλλαγή κλειδιών (key management, key exchange) είναι οι RSA, Inband, Outband και Kerberos. Οι δύο ς μέθοδοι Inband και Kerberos, υποδηλώνουν ότι το κλειδί έχει ανταλλαγεί πρωτύτερα, με χρήση μιας HTTP επικεφαλίδας "Key-Assign". Η Outband μέθοδος υπονοεί ότι ο client και ο server έχουν πρόσβαση σε κλειδιά που σχετίζονται με ονόματα χρηστών, είτε μέσω μιας βάσης δεδομένων, είτε από την εισαγωγή ενός κωδικού από τον χρήστη μέσω του πληκτρολόγιου. Η RSA χρησιμοποιεί την ιδιωτική κλείδα του αποστολέα για την κρυπτογράφηση του κλειδιού κρυπτογράφησης των ενθυλακωμένων περιεχομένων που συνοδεύεται από πιστοποιητικό τύπου X.509 με την δημόσια κλείδα του αποστολέα.

## Αλγόριθμοι Ψηφιακής Υπογραφής και Παραγωγής Message Digest

Το S/HTTP υποστηρίζει δύο αλγόριθμους για την παραγωγή ψηφιακών υπογραφών: RSA και DSS. Για την παραγωγή message digest υποστηρίζονται οι MD2, MD5 και SHS.

## Αλγόριθμοι Συμμετρικής Κρυπτογράφησης

Οι αλγόριθμοι αυτοί διαχωρίζονται σε αυτούς που χρησιμοποιούνται στην κρυπτογράφηση των ενθυλακωμένων περιεχομένων και σε αυτούς που χρησιμοποιούνται στην κρυπτογράφηση των ενθυλακωμένων HTTP επικεφαλίδων.

Οι αλγόριθμοι για την κρυπτογράφηση των περιεχομένων είναι:

*DES-CBC*: Ο DES σε Cipher Block Chaining (CBC) mode.

*DES-EDE-CBC*: Ο Triple DES χρήση 2 κλειδιών σε Encrypt-Decrypt-Encrypt mode και σε CBC mode.

*DES-EDE3-CBC*: Ο Triple DES με χρήση 3 κλειδιών σε Encrypt-Decrypt-Encrypt mode και σε CBC mode.

*DESX-CBC*: Ο DESX της RSA.

*IDEA-CFB*: Ο IDEA σε Cipher Feedback mode.

*RC2-CBC*: Ο RC2 της RSA σε Cipher Block Chaining (CBC) mode.

*RC4*: Ο RC4 της RSA.

*CDMF-CBC*: Ο CDMF της IBM σε Cipher Block Chaining (CBC) mode.

Οι αλγόριθμοι για την κρυπτογράφηση των επικεφαλίδων είναι:

*DES-ECB*: Ο DES σε Electronic Codebook (ECB) mode.

*DES-EDE-ECB*: Ο Triple DES χρήση 2 κλειδιών σε Encrypt-Decrypt-Encrypt mode και σε ECB mode.

*DES-EDE3-ECB*: Ο Triple DES με χρήση 3 κλειδιών σε Encrypt-Decrypt-Encrypt mode και σε ECB mode.

*DESX-ECB*: Ο DESX της RSA.

*IDEA-ECB*: Ο IDEA σε Electronic Codebook (ECB) mode.

*RC2-ECB*: Ο RC2 της RSA σε Electronic Codebook (ECB) mode.

*CDMF-ECB*: Ο CDMF της IBM σε Electronic Codebook (ECB) mode.

## 5.6.10 Προστασία Από Γνωστές Επιθέσεις

Το S/HTTP, όπως και το SSL, παρέχει προστασία έναντι των επιθέσεων Man-In-The-Middle-Attack, Replay Attack και Dictionary Attack. Είναι πιο σταθερό, όμως από το SSL γιατί επιτρέπεται η επαναδιαπραγμάτευση των μηχανισμών και αλγορίθμων. Επιπλέον, οι αλγόριθμοι που υποστηρίζει το S/HTTP είναι πιο ανθεκτικοί σε επιθέσεις. Συγκεκριμένα, το κόστος ανάλυσης του DES (ο προρυθμισμένος αλγόριθμος του S/HTTP) είναι πολύ υψηλότερο από το αντίστοιχο κόστος του RC4 με 40 bit κλειδί (προρυθμισμένος αλγόριθμος του SSL).

## 5.6.11 Αδυναμίες του S/HTTP

Η χρήση της μεθόδου Inband για ανταλλαγή κλειδιών είναι προβληματική. Η μεταφορά των κλειδιών δεν γίνεται με αρκετή ασφάλεια και μπορούν εύκολα να πέσουν στα χέρια εισβολέων. Επίσης, άλλη μια αδυναμία του S/HTTP είναι η εξαιρετική του ευελιξία στην επιλογή μηχανισμών και αδυναμία κρυπτογράφησης όλων των ανταλλαγών μηνυμάτων. Σε αντίθεση το SSL εφαρμόζει την άποψη της κρυπτογράφησης των πάντων.

# *5.7 RADIUS & TACACS+*

## 5.7.1 Εισαγωγή

Καθώς τα δίκτυα εξαπλώνονται πέρα από το φυσικό χώρο των επιχειρήσεων η έννοια της ασφάλειας γίνεται πιο σημαντική και σύνθετη. Οι εταιρίες πρέπει να προστατέψουν τα δίκτυά και τους δικτυακούς τους πόρους από απομακρυσμένους χρήστες που μπαίνουν παράνομα στο σύστημα αποκτώντας πρόσβαση με κάποιο τρόπο. Τα συστήματα της Cisco χρησιμοποιούν μία στρατηγική που είναι γνωστή σαν Πιστοποίηση, Έγκριση και Παρακολούθηση (authentication, authorization, accounting-AAA) για να εκτελέσει τις λειτουργίες της πιστοποίησης της ταυτότητας του χρήστη, τη παροχή ή όχι πρόσβασης και την παρακολούθηση των κινήσεων των απομακρυσμένων χρηστών αντίστοιχα. Στα σημερινά δίκτυα χρησιμοποιούνται τα πρωτοκολλά0 TACACS+ (Terminal Access Controller Access Control System plus) και RADIUS (Remote Access Dial-In User Service) για τη παροχή AAA λύσεων. Η υποστήριξη των RADIUS και TACACS+ δίνει τη δυνατότητα στη Cisco να προτείνει μία πολύ ευέλικτη και αποδοτική AAA λύση.

## 5.7.2 Ανάλυση των Απαιτήσεων Ασφάλειας (AAA)

**Authentication - Πιστοποίηση**

Η Πιστοποίηση είναι η διαδικασία με την οποία καθορίζεται ποιος έχει πρόσβαση στο LAN. Απλές μέθοδοι έγκρισης χρησιμοποιούν μια βάση δεδομένων που αποτελείται από usernames και passwords στον server πρόσβασης. Πιο εξελιγμένα συστήματα χρησιμοποιούν μεθόδους όπως το TACACS και το Kerberos.

Ωστόσο, το ότι πιστοποιείται η ταυτότητα κάποιου χρήστη δε σημαίνει ότι αυτός έχει αποκτήσει πρόσβαση σε όλες τις υπηρεσίες του δικτύου—είναι πιθανό να του ζητηθεί εκ νέου κάποιος κωδικός από κάποια συγκεκριμένη υπηρεσία UNIX, NetWare ή AppleShare. Ένας καλός NAS server υποστηρίζει μία πλειάδα επιλογών πιστοποίησης.

## Authorization - Έγκριση

Η Έγκριση είναι η ικανότητα του περιορισμού των δικτυακών υπηρεσιών σε διαφορετικούς χρήστες βάση μιας δυναμικά εφαρμοζόμενης λίστας πρόσβασης (access list) που μερικές φορές αναφέρεται και ως "προφίλ χρήστη" και που βασίζεται στο δίδυμο username/password. Αυτό το χαρακτηριστικό είναι σημαντικό για δύο λόγους: βοηθάει στη μείωση της έκθεσης του εσωτερικού δικτύου στον έξω κόσμο και απλοποιεί τη μορφή του δικτύου για τον τελικό χρήστη που αγνοεί τις τεχνικές του λεπτομέρειες.

Το χαρακτηριστικό της έγκρισης επιτρέπει στους χρήστες να κινούνται. Κινούμενοι και προσωρινοί χρήστες (χρήστες με φορητά από ξενοδοχεία και τηλεργαζόμενοι με modems και ISDN συνδέσεις από το σπίτι) θέλουν να συνδεθούν στη πιο κοντινή τοπική σύνδεση διατηρώντας ωστόσο όλα τα προνόμιά των LAN τους.

Ο Διαχειριστής του δικτύου (Network Administrator) πρέπει να είναι σε θέση να περιορίζει τη πρόσβαση στο δίκτυο για όλα τα πρωτόκολλα και τις υπηρεσίες (Telnet, IP, IPX και AppleTalk) όσο οι χρήστες συνδέονται (dial-in) από τη την ίδια "πηγή" modem (pool). Η διαδικασία έγκρισης με τη χρήση access list για κάθε χρήστη δεν περιορίζεται σε συγκεκριμένα interfaces αλλά ανατίθεται δυναμικά στη συγκεκριμένη πόρτα στην οποία συνδέεται ο χρήστης. Για παράδειγμα όταν ο χρήστης Α συνδέεται στη πόρτα 1, μπορεί να δει τα υπο-δίκτυα 1, 2, 3 και τις AppleTalk ζώνες bldg D, bldg E και bldg F. Όταν ο χρήστης 2 συνδέεται στη πόρτα 1, τότε το προφίλ του τον περιορίζει στο υπο-δίκτυο 1 και στη ζώνη bldg D.

Από τη στιγμή που το NAS υποστηρίζει πολύ περισσότερους απομακρυσμένους χρήστες από τις φυσικές γραμμές που έχει στη διάθεσή του κάθε χρήστης ή group, μπορεί να τηλεφωνήσει στο ίδιο περιστροφικό κέντρο και να πάρει πρόσβαση στο δίκτυο. Αυτή η access list βασίζεται στο username και σαν τέτοια κάθε NAS μπορεί να υποστηρίξει χιλιάδες χρήστες στη βάση δεδομένων που έχει για τα usernames και passwords.

## Accounting—Παρακολούθηση

Η παρακολούθηση είναι το τρίτο κύριο συστατικό ενός ασφαλούς συστήματος. Οι διαχειριστές του συστήματος μπορεί από το να θέλουν να χρεώσουν τους πελάτες τους για την ώρα που παρέμειναν συνδεδεμένοι στο δίκτυο μέχρι να παρακολουθήσουν ύποπτες προσπάθειες σύνδεσης στο δίκτυο.

# 5.7.3 Το Πρωτόκολλο RADIUS

Το πρωτόκολλο RADIUS αναπτύχθηκε από την Livingston Enterprises ως ένας server πρόσβασης, πιστοποίησης και παρακολούθησης. Από τότε έχει υλοποιηθεί από διάφορους άλλους πωλητές και έχει κερδίσει ευρεία υποστήριξη ανάμεσα ακόμα και στους παροχείς υπηρεσιών (ISPs).

Το RADIUS είναι βασισμένο στο client/server μοντέλο. Οι servers πρόσβασης (NAS-Network Access Servers) λειτουργούν σαν clients του RADIUS. Ο client είναι υπεύθυνος για την προώθηση της πληροφορίας του χρήστη στον αρμόδιο RADIUS server και την εκτέλεση των εντολών που θα του σταλούν πίσω από το server.

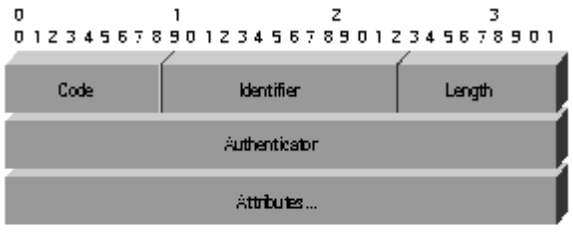
Ο RADIUS server ή daemon παρέχει υπηρεσίες πιστοποίησης και παρακολούθησης σε έναν ή περισσότερους RADIUS clients δηλαδή συσκευές NAS. Οι RADIUS servers είναι υπεύθυνοι για το να λαμβάνουν τις αιτήσεις σύνδεσης των χρηστών, να τους πιστοποιούν και τέλος να επιστρέφουν όλη τη πληροφορία με τις απαιτούμενες ρυθμίσεις για τους clients ώστε να δοθούν οι αιτούμενες υπηρεσίες στους χρήστες. Ο RADIUS server πρόσβασης είναι συνήθως ένας αφιερωμένος σταθμός εργασίας συνδεδεμένος με το δίκτυο.

## Λειτουργία Πρωτοκόλλου

Η επικοινωνία μεταξύ ενός NAS και ενός RADIUS server βασίζεται στο User Datagram Protocol (UDP). Το σχήμα 1 δείχνει τη μορφή ενός πακέτου RADIUS.

Οι δημιουργοί του RADIUS επέλεξαν το UDP ως το πρωτόκολλο μεταφοράς για τεχνικούς λόγους. Γενικά το RADIUS θεωρείται μία υπηρεσία άνευ συνδέσεως(connectionless). Θέματα που σχετίζονται με τη διαθεσιμότητα του server, την επανεκπομπή και τα timeouts διαχειρίζονται από διάφορες συσκευές του RADIUS και όχι από το πρωτόκολλο μεταφοράς.

A summary of the RADIUS data format is shown below.
The fields are transmitted from left to right.




Code

The Code field is one octet, and identifies the type of RADIUS packet.
When a packet is received with an invalid Code field, it is silently discarded.
Radius Codes (decimal) are assigned as follows:

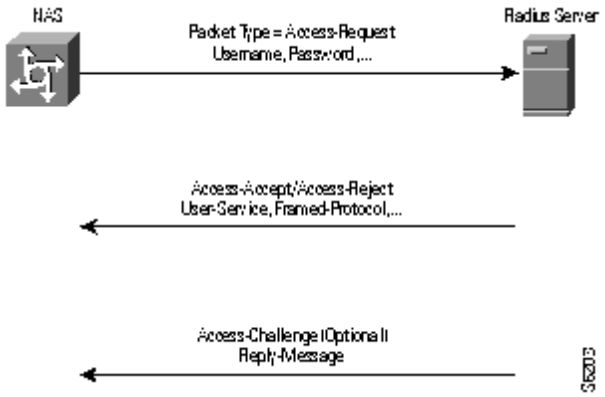
| | |
|---|---|
| 1 | Access-Request |
| 2 | Access-Accept |
| 3 | Access-Reject |
| 4 | Accounting-Request |
| 5 | Accounting-Response |
| 11 | Access-Challenge |
| 12 | Status-Server (experimental) |
| 13 | Status-Client (experimental) |
| 255 | Reserved |

*Σχήμα 1:RADIUS Packet Format from RFC 2058*

Τυπικά μία αίτηση για login αποτελείται από μία αίτηση (Access Request) από το NAS server στον RADIUS server και μια απάντηση, θετική ή αρνητική, του τελευταίου (Access-Accept ή Access-Reject). Το πακέτο αίτησης που στέλνει ο NAS server περιέχει το username, το κρυπτογραφημένο password, την IP διεύθυνση του NAS server και τη πόρτα. Η μορφή της αίτησης παρέχει επιπλέον πληροφορίες για τον τύπο της σύνδεσης την οποία ο χρήστης θέλει να ξεκινήσει. Για παράδειγμα εάν η αίτηση παρουσιάζεται σε mode χαρακτήρων τότε το "Service-Type = Exec-User" αλλά εάν παρουσιάζεται σε mode PPP πακέτου τότε το "Service-Type = Framed User" και "Framed-Type = PPP"

Όταν ο RADIUS server λαμβάνει μια αίτηση από κάποιον NAS, ψάχνει σε μια βάση δεδομένων για το username που υπάρχει στην αίτηση. Εάν το username δεν υπάρχει στη βάση δεδομένων τότε είτε ένα τυπικό προφίλ φορτώνεται και ο RADIUS server αποστέλλει μήνυμα αποδοχής (Access-Accept) είτε αποστέλλει μήνυμα απόρριψης (Access-Reject) το οποίο μπορεί να συνοδεύεται και από κάποιο επεξηγηματικό μήνυμα του λόγου απόρριψης.

Στην περίπτωση που το username βρεθεί και το password είναι σωστό ο RADIUS server επιστρέφει μία Access-Accept απάντηση η οποία περιλαμβάνει μια λίστα των χαρακτηριστικών των ρυθμίσεων που πρέπει να χρησιμοποιηθούν από τη μεριά του NAS για τη σύνδεση. Τυπικές παράμετροι περιλαμβάνουν το τύπο της υπηρεσίας (shell ή framed), το τύπο του πρωτοκόλλου, την IP διεύθυνση που θα δοθεί στο χρήστη (στατική ή δυναμική), την access list που πρέπει να εφαρμοστεί ή τη στατική διεύθυνση που πρέπει να εγκατασταθεί στον πίνακα δρομολογίων του NAS. Το σχήμα 2 δείχνει τη διαδικασία του RADIUS login και authentication.




*Σχήμα 2:RADIUS Login and Authentication Process*

## Χαρακτηριστικά Διαδικασίας Πιστοποίησης και Έγκρισης

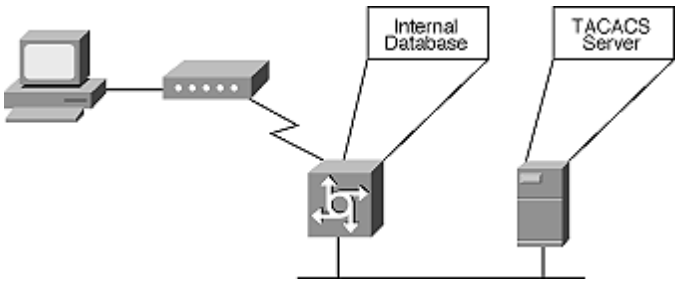
Η πιστοποίηση είναι η πιο απαιτητική πλευρά της ασφάλισης απομακρυσμένων χρηστών λόγω της δυσκολίας που σχετίζεται με τη σίγουρη αναγνώριση του χρήστη.

Για τη διασφάλιση της ταυτότητας ενός απομακρυσμένου χρήστη το πρωτόκολλο RADIUS υποστηρίζει πολλές μεθόδους πιστοποίησης περιλαμβανομένων των Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) και token cards. Προς το παρόν όλες οι εκδόσεις του RADIUS απαιτούν να τρέχει ένας server για τα token cards επιπρόσθετα του RADIUS server. Όταν βγει στην αγορά η έκδοση υποστήριξης του RADIUS, CiscoSecure, θα περιέχει OEM υποστήριξη για CryptoCard token κάρτες και έτσι δεν θα είναι απαραίτητος επιπλέον server για τα token cards.

### Ενεργοποίηση της Πιστοποίησης, Έγκρισης και παρακολούθησης RADIUS

Για κάθε τύπο login που χρειάζεται πιστοποίηση και έγκριση, πρέπει να εισαχθεί μια γραμμή εντολών. Αυτή η γραμμή είναι η λίστα που χρησιμοποιείται για login μέσω του RADIUS εκτός αν υπάρχει κάποια άλλη λίστα που έχει ρυθμιστεί. Η παρακολούθηση μπορεί να χρησιμοποιηθεί ανεξάρτητα από τις άλλες διαδικασίες και επιτρέπει την αποστολή δεδομένων στην αρχή και στο τέλος των συνδέσεων καταδεικνύοντας τη ποσότητα των πόρων που χρησιμοποιήθηκαν κατά τη σύνδεση. Ένας ISP θα μπορούσε να χρησιμοποιήσει το RADIUS για να καλύψει ειδικές απαιτήσεις ασφάλειας και χρέωσης.

## 5.7.4 Το πρωτόκολλο TACACS+




Το TACACS+ επιτρέπει σε ένα ξεχωριστό server πρόσβασης (τον TACACS+ server) να παρέχει τις υπηρεσίες πιστοποίησης, έγκρισης και παρακολούθησης με ανεξάρτητο τρόπο. Κάθε υπηρεσία μπορεί να συνδυαστεί με τη δική της βάση δεδομένων ή μπορεί να χρησιμοποιήσει τις άλλες υπηρεσίες που είναι διαθέσιμες στο δίκτυο.

Η φιλοσοφία σχεδίασης του TACACS+ είναι ο καθορισμός μιας μεθόδου για την διαχείριση όχι όμοιων server πρόσβασης (NAS) από ένα και μόνο σύνολο διαχειριστικών υπηρεσιών όπως μια βάση δεδομένων. Ένας NAS παρέχει πρόσβαση σε έναν χρήστη, σε ένα δίκτυο ή υποδίκτυο ή και σε διασυνδεδεμένα δίκτυα.

Το TACACS+ αποτελείται από τρία κύρια μέρη: την υποστήριξη του πρωτοκόλλου από servers πρόσβασης και δρομολογητές, τα χαρακτηριστικά του πρωτοκόλλου και την κεντρική βάση δεδομένων. Παρόμοια με μια εσωτερική βάση δεδομένων, το TACACS+ υποστηρίζει τα παρακάτω τρία απαιτούμενα χαρακτηριστικά ενός ασφαλούς συστήματος.

## Authentication - Πιστοποίηση

Το TACACS+ προωθεί πολλούς τύπους πληροφοριών που αφορούν τα usernames και passwords. Αυτή η πληροφορία κρυπτογραφείται με τον αλγόριθμο MD5. Το TACACS+ μπορεί να προωθήσει πληροφορία για τους παρακάτω τύπους passwords (κωδικών): ARA, SLIP, PAP, CHAP, Telnet, μέχρι και τον νέο τύπο KCHAP με επέκταση. Αυτό επιτρέπει στους χρήστες να χρησιμοποιήσουν το ίδιο username/password για διαφορετικά πρωτόκολλα.

## Authorization - Έγκριση

Το TACACS+ παρέχει ένα μηχανισμό με τον οποίο μπορεί να πει στον access server ποια access list χρησιμοποιεί ο χρήστης που είναι συνδεδεμένος στη πόρτα 1. Ο TACACS+ server και η τοποθεσία της πληροφορίας username/password καθορίζουν την access list μέσω της οποίας ο χρήστης φιλτράρεται. Οι access list(s) βρίσκονται στον access server. Ο TACACS+ server απαντά σε ένα username με μια απάντηση αποδοχής και με έναν αριθμό της λίστας πρόσβασης ο οποίος προκαλεί και την εφαρμογή της λίστας.

## Accounting - Παρακολούθηση

Το TACACS+ παρέχει πληροφορίες παρακολούθησης μέσω σε μια βάση δεδομένων μέσω TCP για τη διασφάλιση ενός ασφαλούς και ολοκληρωμένου ημερολογίου.

Το τμήμα παρακολούθησης του TACACS+ περιλαμβάνει τη δικτυακή διεύθυνση του χρήστη, το username, το πρωτόκολλο που ενεργοποιήθηκε, η υπηρεσία που επιχειρήθηκε να χρησιμοποιηθεί, ημέρα και ώρα και το πακέτο-φίλτρο που ενεργοποίησε το ημερολόγιο. Για συνδέσεις Telnet, περιέχει επιπλέον τις πόρτες πηγής και προορισμού, τις ενέργειες που πραγματοποιήθηκαν και τον τύπο συναγερμού.

Οι πληροφορίες χρέωσης περιλαμβάνουν τον χρόνο σύνδεσης, τη ταυτότητα του χρήστη, την τοποθεσία από την οποία συνδέθηκε, το χρόνο εκκίνησης και το χρόνο λήξης. Αναγνωρίζει επίσης το πρωτόκολλο που χρησιμοποιείται από το χρήστη και μπορεί να περιλαμβάνει εντολές που πρέπει να τρέξουν εάν το τελευταίο είναι το Telnet ή το exec. Οι μελλοντικές εκδόσεις του TACACS+ θα περιλαμβάνουν πρόσθετα στοιχεία παρακολούθησης όπως η ανανέωση του χρόνου, που θα στέλνει νέα στοιχεία για τον χρόνο σύνδεσης κάθε x λεπτά. Αυτό το χαρακτηριστικό επιτρέπει στους παροχείς υπηρεσιών Internet να χρεώνουν το πελάτη ακόμα και αν ο access server επανεκκινηθεί και έτσι χάσει τον αρχικό χρόνο εκκίνησης.

Το πρωτόκολλο παρέχει αρκετές πληροφορίες ώστε ένας server να μπορεί να παράγει ρουτίνες ανίχνευσης εισβολέων, να δίνει αναφορές στατιστικών, αριθμούς πακέτων και αριθμό bytes.

Οι χρήστες επιδιώκουν την αποφυγή χρήσεως του ίδιου username/password έτσι ώστε οι πελάτες να μην μοιράζονται το λογαριασμό τους με άλλους. Αν και η τελική απόφαση λαμβάνεται από τον server, το πρωτόκολλο είναι αρκετά ικανό να δώσει ικανά στοιχεία ανίχνευσης πολλαπλών εμφανίσεων του ίδιου κωδικού.

# 5.7.5 Σύγκριση RADIUS & TACACS+

Το RADIUS είναι απλώς ένα πρωτόκολλο που παρέχει λειτουργίες πιστοποίησης και έγκρισης για υπηρεσίες μέσω τηλεφωνικών γραμμών. Ένα άλλο ευρέως διαδεδομένο πρωτόκολλο είναι το TACACS+ το οποίο είναι η τελευταία εξέλιξη του Cisco TACACS πρωτοκόλλου. Αν και αυτά τα πρωτόκολλα παρέχουν παρόμοια λειτουργικότητα έχουν αρκετές σημαντικές διαφορές.

## Μηχανισμός Μεταφοράς

Η πιο ουσιαστική διαφορά μεταξύ των RADIUS και TACACS+ είναι το δικτυακό πρωτόκολλο μεταφοράς που το καθένα χρησιμοποιεί. Το RADIUS χρησιμοποιεί το UDP για την ανταλλαγή πληροφοριών μεταξύ των NAS και των server πρόσβασης, ενώ το TACACS+ χρησιμοποιεί το TCP.

Το TCP είναι ένα πρωτόκολλο σύνδεσης connection oriented, ενώ το UDP προσφέρει best effort υπηρεσία (καλύτερης δυνατής σύνδεσης). Το RADIUS χρησιμοποιεί επιπρόσθετες προγραμματιζόμενες μεταβλητές για να ελέγξει θέματα όπως:προσπάθειες επανεκπομπής και timeouts έτσι ώστε να αντισταθμίσει τα κενά που αφήνει το UDP σε αυτούς τους τομείς. Το TACACS+ χρησιμοποιώντας το TCP δεν χρειάζεται αυτές τις επιπλέον μεταβλητές διότι τα θέματα σύνδεσης διαχειρίζονται προφανώς από το TCP.

Η χρησιμοποίηση του TCP παρέχει μια ξεχωριστή υπηρεσία αναγνώρισης, μέσω ενός TCP πακέτου αναγνώρισης, που χρησιμοποιείται για την επιβεβαίωση της λήψης μιας αίτησης προς το server πρόσβασης εντός συγκεκριμένου χρόνου. Αυτή η διαδικασία λαμβάνει χώρα ανεξάρτητα από τη συμφόρηση που πιθανόν να υπάρχει στο server πρόσβασης.

Με τη χρησιμοποίηση των TCP keep alives (ένδειξη "ζωντανής" σύνδεσης) μπορούν να ανιχνευθούν οι "πτώσεις" των servers. Επιπλέον μπορούν να διατηρηθούν πολλές ταυτόχρονες συνδέσεις και μηνύματα χρειάζεται να αποστέλλονται μόνο σε servers που είναι γνωστό ότι τρέχουν.

## Εμπιστευτικότητα

Το RADIUS κρυπτογραφεί μόνο τον κωδικό στο πακέτο Access-Request (αίτησης πρόσβασης) από τον client στον server. Το υπόλοιπό πακέτο μένει ανέπαφο. Άλλες πληροφορίες όπως το username, υπηρεσίες έγκρισης και παρακολούθησης μπορούν να αιχμαλωτιστούν από κάποιον τρίτο κάνοντας έτσι τα δίκτυα RADIUS πιθανούς στόχους για τους hackers που χρησιμοποιούν μεθόδους υποκλοπής μιας ολόκληρης σύνδεσης και επανάληψής της. Εξαιτίας αυτού του μειονεκτήματος τα δίκτυα RADIUS πρέπει να σχεδιάζονται έτσι που να ελαχιστοποιούν τη πιθανότητα εκδήλωσης επίθεσης.

Το TACACS+ κρυπτογραφεί ολόκληρο το πακέτο και αφήνει εκτός κρυπτογράφησης μόνο την επικεφαλίδα TACACS+ . Μέσα σε αυτήν υπάρχει ένα πεδίο που δείχνει εάν το πακέτο είναι ή όχι κρυπτογραφημένο. Η συνήθης διαδικασία κρυπτογραφεί ολόκληρο το πακέτο για ασφαλέστερη επικοινωνία.

## Διανομή Λειτουργιών

Το πρωτόκολλο RADIUS συνδυάζει τις διαδικασίες της πιστοποίησης και της έγκρισης. Τα πακέτα Access-Accept (αποδοχής της αίτησης πρόσβασης) που αποστέλλονται από τον RADIUS server στο client περιέχουν όλη τη πληροφορία που χρειάζεται η έγκριση, κάνοντας έτσι το διαχωρισμό των λειτουργιών της πιστοποίησης και της έγκρισης δύσκολο. Η χρήση του RADIUS πρέπει να προτιμάται όταν απαιτείται απλή πιστοποίηση και έγκριση ενός βήματος, όπως συμβαίνει με τα δίκτυα των περισσότερων παροχέων υπηρεσιών (ISPs).

Το TACACS+ χρησιμοποιεί την αρχιτεκτονική των τριών άλφα (AAA) της Cisco, η οποία διαχωρίζει τις διαδικασίες πιστοποίησης, έγκρισης και παρακολούθησης. Το setup επιτρέπει ξεχωριστές λύσεις πιστοποίησης που μπορούν να χρησιμοποιούν το TACACS+ για έγκριση και παρακολούθηση. Για παράδειγμα είναι δυνατό να χρησιμοποιηθεί το Kerberos για πιστοποίηση και το TACACS+ για έγκριση και παρακολούθηση. Αφού ένας server πρόσβασης στο δίκτυο (NAS) πιστοποιηθεί από τον Kerberos server, ζητάει πληροφορίες έγκρισης από τον TACACS+ server χωρίς να είναι αναγκαία η επαναπιστοποίηση. Αυτό γίνεται όταν ο NAS πληροφορεί τον TACACS+ server για το γεγονός ότι έχει πιστοποιηθεί επιτυχώς από το Kerberos και τότε ο server παρέχει την πληροφορία έγκρισης.

Κατά τη διάρκεια μιας σύνδεσης και εάν επιπλέον έλεγχος πιστοποίησης είναι αναγκαίος, ο server πρόσβασης ελέγχει με τη βοήθεια του TACACS+ εάν ο χρήστης έχει πάρει άδεια χρήσης μιας συγκεκριμένης εντολής. Αυτό το χαρακτηριστικό παρέχει μεγαλύτερο έλεγχο των εντολών που μπορούν να εκτελεστούν στον server πρόσβασης την ίδια στιγμή που αποδεσμεύει το μηχανισμό πιστοποίησης από τον μηχανισμό έγκριση. Για τους παραπάνω λόγους το TACACS+ είναι πιο κατάλληλο για περιβάλλον σύνθετου δικτύου όπου χρησιμοποιείται σχήμα πολλαπλών πιστοποιήσεων. Αυτό το σενάριο χρησιμοποιούνται κυρίως σε δίκτυα μεγάλων επιχειρήσεων.

Εξαιτίας της συνεχούς εξέλιξης των προϊόντων ασφάλειας, που είναι μάλιστα ανταγωνιστικά μεταξύ τους, η αρχιτεκτονική θα πρέπει να είναι βαθμωτή ώστε να διαχωρίζει τα τρία άλφα (AAA) που αποτελούν μαζί τη λύση στο πρόβλημα της και να ανοίγει τις πόρτες σε μελλοντικές επιλογές.

## Υποστήριξη Πολλαπλών Πρωτοκόλλων

Το RADIUS υποστηρίζει ελάχιστα πρωτόκολλα εκτός του TCP/IP. Για παράδειγμα δεν υποστηρίζει τα:

- AppleTalk Remote Access (ARA)
- NetBios frame protocol control
- Novell Asynchronous Services Interface (NASI)
- Packet assembler/disassembler (PAD) connection

Τα παραπάνω πρωτόκολλα υποστηρίζονται από το TACACS+.

Η Cisco με το Cisco IOS παρέχει τη δυνατότητα επιλογής του πρωτοκόλλου που ο χρήστης θέλει να χρησιμοποιήσει. Οι Cisco servers πρόσβασης είναι μοναδικοί επειδή μπορούν να υλοποιήσουν τόσο το RADIUS όσο και το TACACS+.

## *5.8 Cisco NetSonar*

### 5.8.1 Περιγραφή Προϊόντος

Το Cisco NetSonar είναι ένα προϊόν Ανίχνευσης Αδυναμιών Ασφάλειας και Χαρτογράφησης Δικτύου. Αποτελεί το πρώτο τέτοιο προϊόν που συνδυάζει τεχνολογία αιχμής στην ανίχνευση αδυναμιών ασφάλειας, ευέλικτη ανάλυση δεδομένων και είναι φιλικότατο προς το χρήστη τόσο στη λειτουργία του όσο και στους όρους της άδειάς του. Στοχεύει στην αγορά των Διαχειριστών Συστημάτων (Network Administrators) σε επιχειρησιακά περιβάλλοντα όπως επίσης αποτελεί εργαλείο και για συμβούλους ασφάλειας δικτύων. Αυτό που κάνει είναι να ψάχνει στα βάθη ενός δικτύου για τρύπες στην ασφάλειά του. Χαρτογραφεί γρήγορα όλα τα συστήματα στο δίκτυο, τα λειτουργικά τους συστήματα και τις υπηρεσίες τους και τέλος τις σχετιζόμενες με αυτά αδυναμίες όσον αφορά το βαθμό ασφάλειας που προσφέρουν. Επιπλέον ερευνά ενεργά για να διαπιστώσει τις όποιες τρύπες στο σύστημα συγκεντρώνοντας αναλυτικές πληροφορίες διασφαλίζοντας την ακρίβεια των δεδομένων. Με την παρουσίαση των αποτελεσμάτων, που γίνεται με ένα πολύ διαμορφώσιμο τρόπο – ανάλογα με τις ανάγκες του ενδιαφερόμενου – το NetSonar δίνει την ευκαιρία στο χρήστη του να αποκτήσει μοναδική αίσθηση για τη λειτουργία και την ασφάλεια του συστήματός του. Το NetSonar αναγνωρίζει ακόμα και λειτουργικά συστήματα που δεν είναι συμβατά με το έτος 2000.

Για να κατανοήσουμε τη λειτουργία και τελικά τη χρησιμότητα του NetSonar θα πρέπει να εξετάσουμε που επεμβαίνει και τι κάνει.

### 5.8.2 Ανίχνευση Αδυναμιών Ασφάλειας

Η ανίχνευση αδυναμιών στην ασφάλεια ενός δικτύου είναι διαδικασία κατά την οποία γίνεται αναγνώριση του δικτυακού εξοπλισμού και των κινδύνων για την ασφάλεια του δικτύου που προκύπτουν από τη χρήση του. Αυτή η πληροφορία μπορεί να χρησιμοποιηθεί για την αξιολόγηση του επιπέδου ασφάλειας και την ελαχιστοποίηση των απειλών προτού κάποιος τρυπήσει τη δικτυακή δομή. Το πρόβλημα με πολλά από τα σημερινά εργαλεία ανίχνευσης είναι το ότι βρίσκουν τις τρύπες μόνο εάν τους δίνεται η δυνατότητα να διεισδύσουν φυσικά στο δίκτυο. Ατυχώς, καταστάσεις όπως καθυστερήσεις του δικτύου, λάθη στις ρυθμίσεις ή και προγραμματιστικά λάθη μπορούν να εμφανίσουν εικονική εικόνα για την ασφάλεια του δικτύου αφού μία επίθεση μπορεί να αποτύχει εξαιτίας τους χωρίς όμως αυτό να σημαίνει ότι η τρύπα δεν υφίσταται. Το NetSonar προσπαθεί να αναγνωρίσει πιθανές καταστάσεις αστάθειας και να δώσει τη δυνατότητα στο χρήστη να αποφασίσει ο ίδιος εάν και σε ποίο επίπεδο διείσδυσης θέλει να φτάσει.

## 5.8.3 Θέση του NetSonar στη Πολιτική Ασφάλειας της Cisco

Το προϊόν NetSonar είναι συστατικό στοιχείο της πολιτικής ασφάλειας που ακολουθεί η Cisco στα απ' άκρη σε άκρη δίκτυά της. Η στρατηγική της στο τομέα της ενεργούς παρακολούθησης περιλαμβάνει τόσο ανίχνευση αδυναμιών όσο και ανακάλυψη εισβολής, οπότε αντιλαμβανόμαστε τη σημασία του NetSonar για το πρώτο μέρος αυτή της πολιτικής.

## 5.8.4 Μεθοδολογία – Τρόπος Λειτουργίας

Το NetSonar ανιχνεύει τις τρύπες στην ασφάλεια ενός δικτύου μέσω μιας διαδικασίας τεσσάρων βημάτων:

1. ***Συλλογή Πληροφοριών:*** Το NetSonar προγραμματίζεται από τους χρήστες να ελέγχει συγκεκριμένες διευθύνσεις, περιοχή διευθύνσεων ή και τα δύο σε ένα δίκτυο. Μέσα σε αυτό το πλαίσιο το NetSonar αναγνωρίζει όλες τις συνδεδεμένες στο δίκτυο συσκευές και τις υπηρεσίες που αυτές τρέχουν.
2. ***Αναγνώριση Πιθανών Αδυναμιών:*** Το NetSonar χρησιμοποιεί τεχνικές παθητικής ανάλυσης και τη Βάση Ασφάλειας Δικτύου (NSDB) για να συγκρίνει τα συγκεντρωμένα δεδομένα με γνωστές καταστάσεις που οδηγούν σε τρυπήματα της ασφάλειας. Η Cisco έχει καθορίσει επιπλέον βαθμίδες αδυναμίας έτσι ώστε αυτές που βρίσκονται σε επίπεδο δικτύου (όπως αυτές που επιδρούν στους δρομολογητές) να αντιμετωπίζονται με μεγαλύτερη σοβαρότητα από αυτές που αφορούν μεμονωμένους σταθμούς εργασίας.
3. ***Επιβεβαίωση Επιλεγμένων Αδυναμιών:*** Με τη χρησιμοποίηση τεχνικών ενεργούς, πλέον, έρευνας το NetSonar μπορεί να επιβεβαιώσει την ύπαρξη μιας πιθανολογούμενης αδυναμίας του συστήματος για να διασφαλίσει ότι καμιά ζημιά δεν πρόκειται να συμβεί στο δίκτυο.
4. ***Δημιουργία Αναφορών Αποτελεσμάτων:*** Το NetSonar ενοποιεί τις συλλεγμένες πληροφορίες και τις παρουσιάζει σε αναφορές κατάλληλες κάθε φορά για το κοινό που πρόκειται να τις χρησιμοποιήσει. Η δημιουργία τέτοιων αναφορών είναι απλή διαδικασία που δεν περιέχει κανενός είδους προγραμματισμό και που μπορεί να δώσει διαγράμματα και γραφήματα απόλυτα διαμορφώσιμα.

## 5.8.5 Τι Ανιχνεύει το NetSonar

Συλλέγει και αναλύει πληροφορίες για:

- ***Δικτυωμένους Υπολογιστές:*** Σε αντίθεση με άλλους ανιχνευτές, που αναγνωρίζουν μόνο IP διευθύνσεις, το NetSonar αναγνωρίζει τους υπολογιστές του δικτύου, το λειτουργικό τους σύστημα και την έκδοσή του. Επιπλέον καταλαβαίνει από το domain name(όνομα περιοχής) τους υπολογιστές του δικτύου. Αναγνωρίζει την υποδομή του δικτύου, δηλαδή routers, switches και servers απομακρυσμένης πρόσβασης. Τέλος το NetSonar

θα βρει και θα αναγνωρίσει servers κλειδιά του δικτύου όπως Web servers, Firewalls, e-mail servers και File Transfer Protocol (FTP) servers.

- ***Αδυναμίες Δικτύου:*** Το NetSonar κάνει χρήση της Βάσης Δεδομένων Ασφάλειας Δικτύου (NSDB) στην οποία θα γίνει πιο εκτεταμένη αναφορά παρακάτω, από τη Cisco, για να βρει οποιοδήποτε ελάττωμα στη λειτουργία του.
- ***Internet, Συστήματα Δικτύου, Firewall:*** Το NetSonar μπορεί να πραγματοποιήσει έρευνα στις ρυθμίσεις του δικτύου για τι Internet, για όλα τα συστήματα του δικτύου και το Firewall του χωρίς να είναι αναγκαία κάποια άλλη έκδοση του προγράμματος ή κάποιο επιπρόσθετο βοήθημα. Σημαντικό είναι και πρέπει να τονισθεί ότι το NetSonar δεν περιορίζεται στην ανίχνευση συστημάτων που προέρχονται από τη Cisco αποκλειστικά αλλά είναι συμβατό με σχεδόν κάθε πλατφόρμα.

## 5.8.6 Επίδραση των Firewall στη Λειτουργία του NetSonar

Οι Firewalls μπορεί να μειώσουν τον αριθμό των συστημάτων που το NetSonar μπορεί να ανιχνεύσει. Εάν υπάρχει firewall μεταξύ του NetSonar και του δικτύου στο οποίο προσπαθεί να πραγματοποιήσει έρευνα τότε το πιθανότερο είναι ότι δεν θα δει πίσω από το firewall υποθέτοντας ότι έχουν γίνει οι σωστές ρυθμίσεις σε αυτό. Για το λόγο αυτό δεν θα μπορέσει να συγκεντρώσει όλες τις απαραίτητες πληροφορίες για τη σύναξη πλήρους αναφοράς για το εξεταζόμενο δίκτυο. Βεβαίως όταν εφαρμοσθεί πίσω από το firewall τότε θα συλλέξει ότι πληροφορία του λείπει και αφορά την τοπολογία που προστατεύει το firewall. Επιπλέον με το NetSonar μπορεί να ελεγχθεί και το ίδιο το firewall.

## 5.8.7 Επίδραση του NetSonar στη Λειτουργία του Συστήματος

Το NetSonar κατά τη λειτουργία και τις διάφορες φάσεις ανίχνευσης, επηρεάζει το φόρτο εργασίας του δικτύου σε κάποιο μικρό ποσοστό. Κυρίως κατά τη διάρκεια της χαρτογράφησης του δικτύου που συντελείται με τη διαδικασία του ping τη συλλογή banner—σημαιών και τις φάσεις ενεργούς ανίχνευσης. Ο φόρτος που επιβάλλει το NetSonar στο δίκτυο είναι συνάρτηση της διάρκειας και του βαθμού διείσδυσης που επιτυγχάνει στο δίκτυο. Το NetSonar επιτρέπει στους χρήστες να προγραμματίζουν ανιχνεύσεις—έρευνες εκτός ωρών αιχμής ή σε τέτοιο επίπεδο ώστε να μην έχουν επίδραση στο δίκτυο.

## 5.8.8 NetSonar και Java

Το NetSonar έχει προγραμματισθεί σε Java η οποία είναι γλώσσα που έχει ενσωματώσει την έννοια της ασφάλειας στο κώδικά της. Τα προβλήματα με την Java περιορίζονται στο download καταστροφικού κώδικα και πουθενά αλλού. Οι διαδικασίες Αναφοράς, Ανάλυσης και Παρουσίασης έχουν γραφεί σε Java αλλά δεν απαιτούν ιδιαίτερα δικαιώματα. Έτσι εάν υπάρχει περίπτωση τρύπας στη Java το

NetSonar δεν θα επηρεαστεί ούτε περισσότερο ούτε λιγότερο από οποιαδήποτε άλλη εφαρμογή του συστήματος.

## 5.8.9 Βάση Δεδομένων Ασφαλείας Δικτύου (NSDB)

Οι χρήστες του NetSonar κερδίζουν μοναδική γνώση για αδυναμίες που συνιστούν προβλήματα ασφάλειας χρησιμοποιώντας τη Βάση Δεδομένων Ασφαλείας Δικτύου (NSDB). Αυτή η εκτεταμένη βάση δεδομένων:

- Περιέχει περιγραφές προβλημάτων ασφάλειας και επιλογές για τη βελτίωση ή και τη λύση τους.
- Παρέχει βαθμούς σοβαρότητας και ανοικτή γραμμή συνδέσμων για περισσότερο εκτεταμένες τεχνικές πληροφορίες.

Η Βάση Δεδομένων Ασφάλειας Δικτύου βρίσκεται υπό τη διαρκή παρακολούθηση και υποστήριξη του Cisco Countermeasure Research Team έτσι ώστε να αναβαθμίζεται διαρκώς με τη συνεχή προσθήκη νέων μηχανισμών ελέγχου ασφάλειας.

## 5.8.10 Περίληψη Χαρακτηριστικών και Πλεονεκτημάτων

| Χαρακτηριστικά | Πλεονεκτήματα |
|---|---|
| Ευέλικτη άδεια χρήσης προϊόντος | • Οι χρήστες δεν χρειάζεται να εγγραφούν για συγκεκριμένη περιοχή IP διευθύνσεων και μπορούν εύκολα να αλλάξουν τις δικτυακές συσκευές που πρόκειται να ελεγχθούν<br>• Ελέγχει όλα τα συστήματα σε ένα δίκτυο,συμπεριλαμβανομένων και των firewalls, Web servers, routers, switches και άλλων συστημάτων |
| Έλεγχος Αδυναμιών Ασφάλειας και Χαρτογράφηση Δικτύου | • Αναγνωρίζει το δικτυακό εξοπλισμό και τις αδυναμίες στην ασφάλεια που προκύπτουν από τη χρήση του και σχετίζονται με αυτόν<br>• Αναγνωρίζει τρύπες στην ασφάλεια προτού αυτές χρησιμοποιηθούν εναντίον του οργανισμού<br>• Κυρώνει τις πολιτικές ασφάλειας όταν εγκαθιστά νέες |

| | |
|---|---|
| | συσκευές ασφάλειας |
| Ανακάλυψη Hosts/Υπηρεσιών | • Συλλέγει διαφανώς ακριβής πληροφορίες από όλες τις συσκευές που ενώνονται στο εξεταζόμενο δίκτυο συμπεριλαμβανομένων των server του δικτύου και των συσκευών υποδομής<br>• Παρέχει δυνατότητα χαρτογράφησης του δικτύου,επιτρέποντας στους χρήστες να συντάξουν ένα ηλεκτρονικό κατάλογο με τα στοιχεία του δικτύου που περιέχει συσκευές, τύπους συσκευών, λειτουργικό σύστημα και έκδοση του τελευταίου<br>• Καταγράφει με ακρίβεια τις ενεργές υπηρεσίες του δικτύου χρησιμοποιώντας τόσο τη μέθοδο εξέτασης πόρτας TCP/UDP όσο και SNMP τεχνικές αναζήτησης<br>• Επιτρέπει στους χρήστες να συλλέξουν πολύτιμες πληροφορίες αναγκαίες για την ανάπτυξη ή την επαλήθευση πολιτικών ασφάλειας |
| Αναγνώριση και Επαλήθευση Αδυναμιών του Δικτύου | • Χρησιμοποιεί την, εν αναμονή πατέντας , δομημένη γλώσσα ασφάλειας και την τεχνολογία ενεργούς έρευνας για την εύκολη αναγνώριση των αδυναμιών του δικτύου στις παρακάτω κατηγορίες:<br>1. TCP/IP hosts του δικτύου<br>2. UNIX hosts<br>3. Windows NT hosts<br>4. Web Servers<br>5. Mail Servers<br>6. FTP Servers<br>7. Firewalls<br>8. Routers<br>9. Switches<br>• Χρησιμοποιεί τόσο παθητικές όσο και ενεργές μεθόδους έρευνας για να αναγνωρίσει αδυναμίες ασφάλειας , αυξάνοντας την αποτελεσματικότητα |

| | |
|---|---|
| | της διαδικασίας αναγνώρισης αδυναμιών ασφάλειας μειώνοντας με αυτό το τρόπο τη πιθανότητα εσφαλμένων αποτελεσμάτων<br><br>• Διαχωρίζει τις αδυναμίες ασφάλειας μεταξύ των συσκευών της δικτυακής υποδομής (όπως routers-δρομολογητές switches και firewalls) από συσκευές hosts (workstations, server π.χ. e-mail και Web Servers) |
| Εξέταση και Παρουσίαση των Δεδομένων | • Παρέχει μία πλειάδα τύπων διαχείρισης δεδομένων,αναζήτησης και παρουσίασης συμπεριλαμβανομένων και πινάκων βασισμένων σε browsers που επιτρέπουν στους χρήστες να αναζητούν δεδομένα από πολλές πλευρές δηλαδή με τη χρήση λίστας τύπων δικτυακών αδυναμιών που αναφέρονται σε hosts με συγκεκριμένη αδυναμία<br>• Δημιουργεί σύνολο γραφημάτων εύκολα και γρήγορα οι οποίες είναι όλες διαμορφώσιμες ώστε να παρέχουν προοπτική σε κάθε πιθανή δικτυακή κατάσταση ασφάλειας |
| Ευέλικτες Αναφορές | • Δημιουργεί τρεις τύπους διαμορφωμένων και εξαιρετικά hyper-διασυνδεδεμένων αναφορών προσαρμοσμένων κάθε φορά στις ανάγκες του κοινού για το οποίο δημιουργήθηκαν – από τεχνικές περιλήψεις έως πλήρεις αναφορές για την κατάσταση ασφαλείας του δικτύου – για εύκολη επικοινωνία και κατανόηση των αποτελεσμάτων<br>• Περιλαμβάνει δεδομένα σε κείμενα,διαγράμματα, και γραφήματα τα οποία είναι εύκολα επεξεργάσιμα από τους χρήστες διότι οι συνήθεις φόρμες του NetSonar είναι εύκολα διαμορφώσιμες<br>• Υποστηρίζει HTML για |

| | |
|---|---|
| | συμβατότητα μεταξύ διαφορετικών πλατφόρμων και ευελιξία του συστήματος |
| Συνήθεις,καθοριζόμενοι<br><br>από το χρήστη,κανόνες | • Χρησιμοποιεί μία εν αναμονή πατέντας κανονιστική γλώσσα η οποία δίνει τη δυνατότητα στο χρήστη να διαμορφώσει τους κανόνες έρευνας βάση των μοναδικών αναγκών του χώρου και της πολιτικής ασφάλειάς του<br>• Επιτρέπει πολύ υψηλού επιπέδου διαμόρφωση για εφαρμογές κληροδότησης και συγκεκριμένων πολιτικών των εταιριών όσον αφορά την έρευνα δικών τους ιδιαίτερων χαρακτηριστικών<br>• Τα διαμορφωμένα αρχεία κανόνων μπορούν να διανεμηθούν σε όλη την επιχείρηση και έτσι να διασφαλίσουν μόνιμη ανίχνευση αδυναμιών σε αυτή |
| Δομημένη Γλώσσα Ασφάλειας | • Επιτρέπει στους χρήστες να εισάγουν παλαιότερα αποτελέσματα ανάλυσης έτσι ώστε να ελέγχεται σε αυτά η αποδοτικότητα των όποιων νέων κανόνων και πολιτικών ασφάλειας ένα βήμα πριν την εφαρμογή τους |
| Εκσυγχρονισμοί Αδυναμιών Συστήματος σε Σταθερή Βάση | • Επιτρέπει τον εκσυγχρονισμό του συστήματος με νέους κανόνες απλώς κατεβάζοντάς τους από το ανάλογο site της Cisco,διαχωρίζοντας έτσι την διαδικασία εκσυγχρονισμού από την αγορά της νέας έκδοσης του προϊόντος και μετατρέποντάς την σε υπόθεση ρουτίνας<br>• Οι συνεχείς αναβάθμιση και ανανέωση των κανόνων ασφάλειας επιτρέπει την τεχνολογική προπορεία του συγκεκριμένου συστήματος από αυτήν που χρησιμοποιεί η κοινότητα των hackers<br>• Επιτρέπει στους πελάτες της |

| | |
|---|---|
| | Cisco να μένουν στην επικαιρότητα των εξελίξεων στα θέματα ασφάλειας |
| Εύκολο στη Χρήση Περιβάλλον Εργασίας Χρήστη | • Επιτρέπει στους χρήστες να κινήσουν γρήγορα και εύκολα τις διαδικασίες ανίχνευσης χωρίς να πρέπει να γνωρίζουν το δίκτυο ή τις αδυναμίες ασφάλειας που αυτό πιθανόν έχει<br>• Χρησιμοποιεί ειδικές φόρμες<br>• Επιτρέπει την αυτόματη παρακολούθηση προτού της ενεργοποιήσεως του NetSonar κάτι που μπορεί να γίνει σε καθορισμένη ώρα ή σε τυχαίο χρόνο.Επιτρέπει στους χρήστες να πραγματοποιήσουν πολλαπλές έρευνες για διαφορετικές κάθε φορά ανιχνεύσεις |
| Βάση Δεδομένων<br><br>Ασφάλειας Δικτύου | • Παρέχει στους χρήστες—πελάτες μοναδική γνώση των αδυναμιών του δικτύου τους<br>• Περιλαμβάνει περιγραφές προβλημάτων ασφάλειας και επιλογές για την βελτίωση ή ολική απάλειψή τους. Παρέχει βαθμούς σοβαρότητας και ανοικτή γραμμή συνδέσμων για περισσότερο εκτεταμένες τεχνικές πληροφορίες.<br>• Συνεχώς ενημερώνεται καθώς κάθε νέα λειτουργία προστίθεται εύκολα στην υπάρχουσα δομή |

# 5.8.11 Ελάχιστες Απαιτήσεις Συστήματος

### NetSonar για NT 2.0:

- Pentium 266 MHz επεξεργαστής
- Windows NT 4.0 (με το Service Pack 3)
- 64 MB RAM (96 MB RAM ενδείκνυται)
- 2—GB σκληρός δίσκος
- TCP/IP δικτυακή υποδομή
- CD-ROM
- Netscape Navigator 2.0 ή νεότερος , Microsoft Internet Explorer 4.0 και νεότερος

**NetSonar για Solaris x86 1.0.1**

- Pentium 266 MHz επεξεργαστής με Solaris x86 V.2.5x ή V.2.6

- 64 MB RAM (96 MB RAM ενδείκνυται)
- 2—GB σκληρός δίσκος
- TCP/IP δικτυακή υποδομή
- CD-ROM

- Netscape Navigator 2.0 ή νεότερος

**NetSonar για SPARC Solaris 1.0.1**

- Sun SPARC Solaris V.2.5.x ή V.2.6

- 64 MB RAM (96 MB RAM ενδείκνυται)
- 2—GB σκληρός δίσκος
- TCP/IP δικτυακή υποδομή
- CD-ROM

- Netscape Navigator 2.0 ή νεότερος

## 5.8.12 Έλεγχοι Ανάλυσης Αδυναμιών Ασφάλειας

- Domain Name Server (DNS)
- Finger Service
- File Transfer Protocol (FTP)
- HTTP
- NetBios
- Network File System (NFS)
- Windows NT
- POP Server
- Rlogin Remote System
- Remote Procedure Call (RPC)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SMTP)
- Telnet Service
- Trivial File Transfer Protocol (TFTP)
- X-Windows
- Server Message Block (SMB)
- Internet Mail Access Protocol (IMAP)
- Network News Transport Protocol (NNTP)
- Remote Shell (RSH)
- IDENT Service
- Rwho Servic

## 5.8.13 Άδειες Χρήσης Λογισμικού

Επιχειρήσεις ή τελικοί χρήστες – διατίθεται βάση βαθμίδων IP διευθύνσεων

- Αφιερωμένα C Class ,250, 500, 1000, 1500, 2000 και 5000 διευθύνσεων

Σύμβουλοι ή Παροχείς Υπηρεσιών – διαθέσιμοι σε ετήσια βάση συμβολαίου

- Απεριορίστου αριθμού διευθύνσεων ή συμβουλευτική άδεια 500 διευθύνσεων

## *5.9 Cisco NetRanger*

Το σύστημα NetRanger είναι μια διαδικασία η οποία ανιχνεύει και αντιδρά σε κάθε παραβίαση ή κατάχρηση που γίνεται στην πολιτική ασφάλειας ενός δικτύου. Τοποθετώντας σε κατάλληλα επιλεγμένα σημεία του δικτύου αισθητήρες, παρακολουθείται η κίνηση και συγκρίνεται με γνωστά σχέδια ή υπογραφές που αντιπροσωπεύουν ύποπτη δραστηριότητα, κατάχρηση του συστήματος ή ακόμα και επίθεση σε αυτό. Ο αισθητήρας μπορεί να στείλει σήματα προειδοποίησης – κινδύνου στον υπεύθυνο, σε ένα σύστημα διαχείρισης ασφάλειας, και υπό συγκεκριμένες συνθήκες να πάρει τη πρωτοβουλία να στείλει εντολές αντιμετώπισης της κατάστασης κατευθείαν στον δικτυακό εξοπλισμό, όπως σε routers και firewalls, τροποποιώντας τις ρυθμίσεις τους έτσι ώστε να μην επιτρέψουν την είσοδο του εισβολέα στο σύστημα. Το σύστημα αυτόματα και γρήγορα απαντά, λοιπόν, προειδοποιώντας ή αναλαμβάνοντας δράση σε αληθινό χρόνο βάση οδηγιών που έχει πάρει από το χρήστη του.

### 5.9.1 Ανίχνευση Εισβολής σε Επίπεδο Δικτυωμένου Υπολογιστή και Δικτύου

Η ανίχνευση εισβολής σε επίπεδο δικτυωμένου υπολογιστή είναι μία διαδικασία που παρακολουθεί τη δραστηριότητα σε ένα μεμονωμένο σύστημα ενώ σε επίπεδο δικτύου έχουμε παρακολούθηση όλης της δραστηριότητας στο δίκτυο ή σε συγκεκριμένο κομμάτι του.

Σε επίπεδο δικτυωμένων υπολογιστικών συστημάτων χρησιμοποιούμε τα συστήματα ανίχνευσης εισβολής για να προστατέψουμε σημαίνοντες servers ή άλλα μεμονωμένα συστήματα που περιέχουν ευαίσθητη πληροφορία. Η εφαρμογή τέτοιων συστημάτων γίνεται με τη μορφή μικρών προγραμμάτων client ή εφαρμογών. Η εφαρμογή αυτών των προγραμμάτων γίνεται με τη χρήση χώρου, μνήμης και CPU χρόνου από τον server στον οποίο ανήκει ο υπό προστασία υπολογιστής με φυσικό επακόλουθο την πτώση της απόδοσής του. Οι εισβολές γίνονται αντιληπτές από τα αποτελέσματα της ανάλυσης των διαφόρων αρχείων καταγραφής στοιχείων του λειτουργικού συστήματος ή και συγκεκριμένων εφαρμογών όπως επίσης και από άλλες δραστηριότητες του συστήματος. Η παρακολούθηση ενός συστήματος σε αυτό το επίπεδο είναι αποδοτική όταν πρόκειται να προστατέψουμε περιορισμένο αριθμό servers ενώ σε αντίθετη περίπτωση δεν δίνουν καλά αποτελέσματα.

Στο επίπεδο της ανίχνευσης εισβολής σε δίκτυο, το σύστημα που έχει αναλάβει τη λειτουργία αυτή τρέχει σε μία αφιερωμένη σε αυτό το σκοπό πλατφόρμα. Το σύστημα λειτουργεί βάση κανόνων που έχει ορίσει ο διαχειριστής του ή της τεχνικής ανάλυσης έμπειρων συστημάτων (expert systems) της διακινούμενης πληροφορίας χρησιμοποιώντας παραμέτρους καθορισμένες πάλι από το διαχειριστή και τις υπογραφές που σηματοδοτούν υποψία εισβολής. Το σύστημα αναλύει τις επικεφαλίδες των πακέτων που διακινούνται στο δίκτυο και παίρνει αποφάσεις για την ασφάλεια βασισμένες στην πηγή, τον προορισμό και τον τύπο του πακέτου, όπως επίσης και τα ίδια τα δεδομένα των πακέτων για τα οποία έχει σχετικές οδηγίες απόρριψής τους ή μη. Το σύστημα αυτό ανταποκρίνεται στις απαιτήσεις δικτύου με μεγάλο πλήθος υπολογιστών και servers διότι δεν έχει σημασία ο αριθμός τους αλλά ο όγκος της διακινούμενης πληροφορίας. Επιπρόσθετα, οι αισθητήρες που έχουν τοποθετηθεί στα διάφορα σημεία του δικτύου μπορούν να ρυθμιστούν ώστε να δίνουν τις αναφορές τους σε ένα κεντρικό σημείο του δικτύου παρέχοντας έτσι τη δυνατότητα σε ένα μικρό αριθμό ειδικών ασφάλειας να ελέγχουν και να υποστηρίζουν από εκεί όλο το δίκτυο της επιχείρησης.

Το NetRanger είναι ένα τέτοιο σύστημα που δίνει τη δυνατότητα στους διαχειριστές της ασφάλειας ενός δικτύου να το ασφαλίσουν αποδοτικά.

## 5.9.2 Κρυπτογράφηση και NetRanger

Ο αισθητήρας του NetRanger αναλύει τόσο την επικεφαλίδα όσο και το περιεχόμενο ενός πακέτου για να αποφασίσει εάν αυτό αποτελεί απειλή ή όχι. Οι αλγόριθμοι που εκτελούν κρυπτογράφηση σε αυτό το επίπεδο κρυπτογραφούν το περιεχόμενο των πακέτων. Έτσι, εφόσον το NetRanger μπορεί να επεξεργαστεί μόνο ότι μπορεί να δει, ο αισθητήρας δεν μπορεί να ανιχνεύσει επιθέσεις που απαιτούν την έρευνα κρυπτογραφημένων πακέτων. Ωστόσο θα προειδοποιήσει και θα απαντήσει σε επιθέσεις που ανιχνεύθηκαν από τη μη κρυπτογραφημένη επικεφαλίδα του πακέτου. Όλα τα συστήματα αντιμετώπισης εισβολής σε αυτό το σημείο "υποφέρουν". Η σωστή χρησιμοποίηση των αισθητήρων απαιτεί αυτοί να τοποθετούνται σε σημεία όπου η πληροφορία είναι καθαρή και όχι κρυπτογραφημένη.

## 5.9.3 Τύποι Ύποπτων Δραστηριοτήτων που Ανιχνεύονται από το NetRanger

Η μηχανή ανίχνευσης εισβολών του NetRanger χρησιμοποιεί μία μεθοδολογία αναγνώρισης υπογραφών η οποία μπορεί να είναι "γενικού πλαισίου" και "περιεχομένου".

Οι "γενικού πλαισίου" υπογραφές επιθέσεων αποτελούνται από γνωστές αδυναμίες δικτυακών υπηρεσιών οι οποίες μπορούν να ανιχνευθούν με τη εξέταση των επικεφαλίδων των πακέτων. Σε αυτές συμπεριλαμβάνονται τύποι επιθέσεων SATAN, πειρατείες του TCP και απάτες στο IP.

Οι υπογραφές επιθέσεων "περιεχομένου" απαιτούν την εξέταση του φορτίου του πακέτου και των πεδίων δεδομένων για να καθορίσουν εάν υπάρχει επίθεση ή παραβίαση της πολιτικής ασφάλειας σε επίπεδο εφαρμογής

Αυτές περιλαμβάνουν για παράδειγμα e-mail και Web τύποι επιθέσεις.

Οι υπογραφές του NetRanger μπορούν να χωριστούν στις παρακάτω κατηγορίες:

- *Επιθέσεις Ονομασίας*: αυτές με συγκεκριμένα ονόματα όπως Smurf και PHF.
- *Επιθέσεις Γενικής Κατηγορίας*: επιθέσεις με πολλές παραλλαγές, βασισμένες όμως στα ίδια χαρακτηριστικά όπως δεδομένα εκτός εύρους(Teardrop) ή αποκερματισμένα IP πακέτα. Το γεγονός αυτό απλοποιεί τη διαχείριση υπογραφών και παρέχει συνεχή προστασία από νέες παραλλαγές επιθέσεων κάτι που σε διαφορετική περίπτωση δεν θα ανιχνεύεται.
- *Ασυνήθιστες Επιθέσεις*: Εξαιρετικά σύνθετες υπογραφές όπως Simplex-Mode πειρατεία TCP, Loki, ή e-mail Spam.

Το σύστημα NetRanger επιτρέπει επιπλέον την δημιουργία, από πλευράς χρήστη, συγκεκριμένων τύπων υπογραφών που χρησιμοποιούν τεχνικές σύγκρισης χαρακτήρων για να καλύψουν τις ιδιαίτερες ανάγκες τους. Για παράδειγμα η εταιρία "Χ-Ψ" θα μπορούσε να ρυθμίσει εύκολα το NetRanger να "χτυπάει" συναγερμό και να αποκλείει κάθε σύνδεση που μεταδίδει τη φράση "Χ-Ψ εμπιστευτικό" στο e-mail ή το ftp.

Στην περίπτωση που κάποια επίθεση χρησιμοποιεί υπογραφές που δεν βρίσκονται στη βάση δεδομένων υπογραφών, η ανίχνευσή της εξαρτάται από το τύπο της επίθεσης αλλά τις περισσότερες φορές το αποτέλεσμα θα είναι θετικό. Είναι πολύ δύσκολο για κάποιον hacker να σπάσει το NetRanger με τη χρήση υπογραφών που δεν αναγνωρίζονται από το σύστημα διότι αυτό έχει αναπτυχθεί κατά τέτοιο τρόπο που να ανιχνεύει τις "αναγνωριστικές πτήσεις" και τις προσπάθειες έρευνας των hackers, τυπικές διαδικασίες και προάγγελοι επιθέσεων. Το μεγαλύτερο μέρος υπογραφών της *Γενικής Κατηγορίας Επιθέσεων* έχει αναπτυχθεί αποκλειστικά για το σκοπό αυτό – την ανίχνευση κοινών παραλλαγών για την εκμετάλλευση ενός συστήματος.

## 5.9.4 Ασφάλεια Συστήματος NetRanger

Ο αισθητήρας του NetRanger έχει φτιαχτεί ώστε να προστατεύει το ίδιο το σύστημα από επιθέσεις. Πρώτα από όλα μόνο υπηρεσίες που απαιτούνται από τον αισθητήρα ενεργοποιούνται. Δευτερεύοντος, οι TCP Wrappers διασφαλίζουν ότι η επικοινωνία επιτρέπεται μόνο με τον Director – στον οποίο θα γίνει παρακάτω εκτενέστερη αναφορά. Κατά τρίτον, ο αισθητήρας ανιχνεύει επιθέσεις στο υπό παρακολούθηση κομμάτι του δικτύου (segment), συμπεριλαμβανομένων και αυτών που μπορεί να κατευθύνονται προς αυτόν. Τέλος, ο αισθητήρας μπορεί να είναι "αόρατος" για το δίκτυο, όταν η διάταξη που χρησιμοποιεί για την παρακολούθηση του βρίσκεται στην "αδιάκριτη" κατάσταση λειτουργίας και η διάταξη ελέγχου και εντολών είναι προσαρμοσμένη σε μία αφιερωμένη, για το σκοπό αυτό, είσοδο ενός router ή συνδέεται στο προστατευόμενο δίκτυο πίσω από έναν firewall. Ο Director είχε σχεδιαστεί για να τοποθετείται σε ένα αξιόπιστο δίκτυο οπότε και χρησιμοποιεί ασφάλεια επιπέδου λειτουργικού συστήματος και εφαρμογής. Ο Director μπορεί να ρυθμιστεί έτσι ώστε να χρησιμοποιεί τρίτα προϊόντα για πιστοποίηση μέσο

certificates κατά τη διαδικασία του log on της κονσόλας. Η τοποθέτησή του πρέπει να γίνει σε σημείο που να είναι είτε άμεσα είτε έμμεσα παρακολουθούμενο από έναν αισθητήρα για μεγαλύτερη προστασία.

## 5.9.5 Επικοινωνία Αισθητήρα *(Sensor)* - Διευθυντή *(Director)*

Το NetRanger δεν υποστηρίζει, προς το παρόν, κρυπτογράφηση δεδομένων από τον αισθητήρα στο διευθυντή, αλλά βασίζεται στην κρυπτογράφηση επιπέδου IP (IPSec) που υπάρχει στις επικοινωνίες των δρομολογητών, για τη προστασία των δεδομένων που κινούνται στο WAN. Ωστόσο, όλες οι επικοινωνίες αισθητήρα - διευθυντή πιστοποιούνται για την αποφυγή πειρατειών και άλλων απατών.

## 5.9.6 Αναλυτική Περιγραφή και Τεχνική Ανασκόπηση

### Συστατικά Στοιχεία του NetRanger

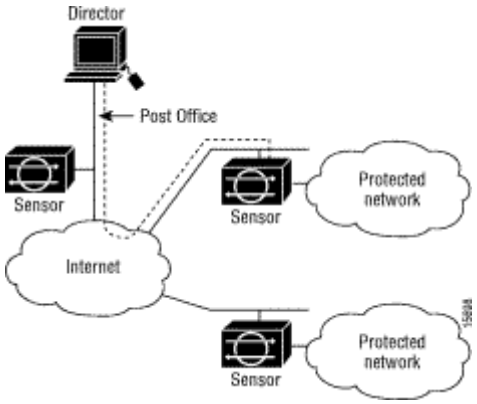
Το σύστημα NetRanger αποτελείται από δύο μέρη: τους αισθητήρες (Sensors), αόρατα όργανα που δρουν όπως οι "sniffers" και τον Διευθυντή (Director), μία κεντρική κονσόλα διαχείρισης. Ο Director μαζεύει τα εισερχόμενα, από τον Sensor, δεδομένα τα μεταφράζει και τα παρουσιάζει στο προσωπικό ασφάλειας με γραφικό τρόπο χαρτογραφώντας το δίκτυο. Οι χρήστες μπορούν να έχουν πρόσβαση σε επιπλέον πληροφορίες για το είδος της επίθεσης από την Βάση Δεδομένων Ασφάλειας Δικτύου του Director. Ο Director επιτρέπει στο προσωπικό ασφάλειας να διαχειριστεί τις ρυθμίσεις των απομακρυσμένων αισθητήρων. Τέλος, ο Director μπορεί να διαχειριστεί τα δεδομένα των αισθητήρων εξάγοντάς τα σε σχετικές βάσεις δεδομένων τρίτων.

### NetRanger—Ανάλυση υποσυστημάτων

- ***Sensor—Αισθητήρας:*** Ο αισθητήρας είναι ένα δικτυακό όργανο που συνδυάζει την υψηλή αξιοπιστία με την απλότητα και ευκολία της εγκατάστασης και συντήρησης. Κάθε κομμάτι του δικτύου που παρακολουθείται απαιτεί έναν αφιερωμένο σε αυτό αισθητήρα, συμπεριλαμβανομένων του Internet, των intranets και των extranets. Ο αισθητήρας είναι ρυθμισμένος για συγκεκριμένους ρυθμούς δεδομένων και interfaces όπως: Ethernet(10BaseT), Fast Ethernet(100BaseT), Token Ring(4-16 Mbps) και FDDI(Fiber Distributed Data interface) σε single ή dual mode. Χρησιμοποιεί ένα έμπειρο σύστημα βασισμένο σε κανόνες για να διυλίσει μεγάλους όγκους δικτυακής κίνησης IP πακέτων και να τους μετατρέψει σε στοιχεία ασφάλειας με νόημα. Ενσωματώνει μία μοναδική τριών—βημάτων δυνατότητα ανίχνευσης επιθέσεων για να επισημάνει παράνομη δραστηριότητα συμπεριλαμβανομένων ονοματικών, γενικής κατηγορίας και τέλος ασυνήθιστου τύπου επιθέσεις. Ο αισθητήρας μπορεί, επίσης, να παρακολουθεί τα ημερολόγια των routers για στοιχεία που φανερώνουν παραβιάσεις της δεδομένης πολιτικής, να κρατάει ο ίδιος ημερολόγιο ασφάλειας, να "σκοτώνει" TCP συνόδους και να διαχειρίζεται δυναμικά τις

λίστες πρόσβασης των router για να αποκλείει από το σύστημα τους επίδοξους εισβολείς.

- ***Director—Διευθυντής:*** Ο διευθυντής παρέχει χαρτογραφημένο γραφικό interface που δίνει τοπικά κεντραρισμένη ή διανεμημένη διαχείριση για ένα πλήθος εκατοντάδων αισθητήρων σε ένα διαμοιρασμένο δίκτυο. Ο διευθυντής αναπτύχθηκε για να παράσχει ένα φιλικό περιβάλλον επιχειρήσεων για συνεχή απάντηση στα διάφορα θέματα ασφάλειας. Μπορεί επίσης να εκτελέσει και άλλες σημαντικές λειτουργίες: διαχείριση δεδομένων με τη χρήση εργαλείων που προέρχονται από άλλα συστήματα, απόκτηση πρόσβασης σε μία βάση δεδομένων ασφάλειας δικτύου, απομακρυσμένη παρακολούθηση και διαχείριση αισθητήρων και αποστολή των δεδομένων σε οποιοδήποτε σύστημα αντιμετώπισης κρίσεων, pager ή e-mail για την προειδοποίηση του προσωπικού ασφάλειας.
- ***Post Office—Ταχυδρομείο:*** Το Post Office είναι η αρχιτεκτονική επικοινωνίας που παρέχει εύρωστες, αξιόπιστες και αποτελεσματικές επικοινωνίες μεταξύ των αισθητήρων και των διευθυντών του NetRanger. Όλες οι επικοινωνίες υποστηρίζονται από ένα ιδιόκτητο connectionless πρωτόκολλο το οποίο μπορεί να μεταπηδήσει από δρομολόγιο σε δρομολόγιο για να διατηρήσει τις point-to-point συνδέσεις.




## Δυνατότητες Αισθητήρων

Οι δυνατότητες των αισθητήρων περιλαμβάνουν:

1. Αντίληψη του Δικτύου
2. Συνήθεις Υπογραφές
3. Απάντηση σε Επίθεση
4. Διαχείριση Συσκευών

### *Αντίληψη του Δικτύου*

Η αντίληψη του δικτύου περιλαμβάνει την ανίχνευση σε αληθινό χρόνο εισβολών, την παρακολούθηση των διακινούμενων πακέτων και των δεδομένων που καταχωρούνται από τους routers στα ημερολόγιά τους. Η διαδικασία που τρέχει το NetRanger αιχμαλωτίζει, ανιχνεύει και αναλύει τα πακέτα στο δίκτυο. Επιπλέον παρακολουθεί την κατάσταση των συνδέσεων των χρηστών για την ανίχνευση επιθέσεων μεγάλου όγκου πακέτων ή την ύπαρξη παράνομων γραμμών σε αυτά. Ο αισθητήρας αιχμαλωτίζει τα πακέτα με κάποιο από τα interfaces του, τα

επανασυναρμολογεί και συγκρίνει τα δεδομένα τους με αυτά που υπάρχουν σε ένα σύνολο κανόνων που καταδεικνύουν τυπική προσπάθεια εισβολής.

Η υψηλή απόδοση των αισθητήρων τους επιτρέπει να ερευνούν σχεδόν κάθε πακέτο στο τμήμα του δικτύου του οποίου έχουν αναλάβει την παρακολούθηση. Έτσι ο χρήστης δεν χρειάζεται να φτιάχνει προφίλ και να παραλείπει υπογραφές , κάτι που απαιτεί πολύ καλή γνώση του δικτύου ώστε να διασφαλίσει ότι οι πρέπουσες υπογραφές επιθέσεων έχουν ενεργοποιηθεί. Όταν το NetRanger αναλύει δεδομένα ψάχνει για στοιχεία κατάχρησης. Τα στοιχεία αυτά μπορεί να είναι τόσο απλά όσο μία προσπάθεια πρόσβασης συγκεκριμένης πόρτας σε συγκεκριμένο υπολογιστή ή τόσο σύνθετα όσο σειρά ενεργειών διαμοιρασμένων σε υπολογιστές του δικτύου για αυθαίρετο χρονικό διάστημα. Ο πρώτος τύπος λέγεται "ατομικός" ενώ ο δεύτερος "σύνθετος".

Το NetRanger ερευνά εξετάζοντας τα δεδομένα της επικεφαλίδας ή του φορτίου των πακέτων. Επιθέσεις από το περιεχόμενο προέρχονται από το τμήμα των δεδομένων του πακέτου ενώ επιθέσεις γενικού πλαισίου από το τμήμα της επικεφαλίδας. Ο παρακάτω πίνακας παρουσιάζει παραδείγματα τύπων επίθεσης και σχήματα που το NetRanger αναγνωρίζει.

*Πίνακας 1: Τύποι επιθέσεων και σχημάτων*

| Επίθεση | Σχήμα | |
|---|---|---|
| | Ατομικό | Σύνθετο |
| Γενικού Πλαισίου<br><br>(επικεφαλίδα) | • Ping θανάτου<br>• Finger | • Σάρωση Πόρτας<br>• Επίθεση SYN<br>• Πειρατεία TCP |
| Περιεχομένου<br><br>(δεδομένα) | • Επίθεση MS IE<br>• Επίθεση e-mail | • Επίθεση Telnet |

Ένας άλλος τρόπος να εξετάσουμε τη μεθοδολογία πίσω από τις επιθέσεις γενικού πλαισίου και περιεχομένου είναι μέσω της ιδιότητας ανίχνευσης εισβολής τριών βημάτων του NetRanger. Σαν παραδείγματα μπορούμε να αναφέρουμε:

- Ονομαστικές Επιθέσεις – μεμονωμένες επιθέσεις που έχουν συγκεκριμένα ονόματα ή κοινές ταυτότητες (Smurf, PHF, Land)

- Γενικής Κατηγορίας Επιθέσεις – έρχονται σε παραλλαγές κρατώντας όμως σταθερή τη βασική φιλοσοφία τους

- Impossible IP πακέτο
- Κατακερματισμός IP
- Ασυνήθιστες Επιθέσεις – Εξαιρετικά σύνθετες ή πολυπρόσωπες
- Πειρατεία IP
- E-mail Spam

Η φιλοσοφία σχεδίασης του έμπειρου NetRanger συστήματος του επιτρέπει να ανιχνεύει επιθέσεις γενικής κατηγορίας σε πραγματικό χρόνο ακόμα και αν οι hackers χρησιμοποιούν παραλλαγές για να ξεγελάσουν τα συστήματα ασφάλειας. Για παράδειγμα υπάρχουν πολλές παραλλαγές της επίθεσης "Land", η οποία ανήκει στην κατηγορία των αφόρητων IP πακέτων. Έτσι παρατηρούμε ότι οι υπογραφές επιθέσεων εξελίσσονται μαζί με τις επιθέσεις. Αυτή η βάση δεδομένων επιθέσεων διαχειρίζεται, ελέγχεται και αναβαθμίζεται από μια ειδική ομάδα που περιλαμβάνει μερικούς από τους πιο έμπειρους επαγγελματίες του είδους.

Εξαιτίας του γεγονότος ότι ένα φορτωμένο δικτυακό περιβάλλον μπορεί να δημιουργήσει ψεύτικους συναγερμούς το NetRanger μπορεί να ρυθμιστεί διάταξη προς διάταξη. Για παράδειγμα, εάν ένα σύστημα διαχείρισης δικτύου προκαλεί συνεχείς συναγερμούς κατά τη διαδικασία του pinging στο δίκτυο, το NetRanger μπορεί να ρυθμιστεί κατά τρόπο που να αγνοεί το συγκεκριμένο συναγερμό από τη συγκεκριμένη διεύθυνση. Αυτή η δυνατότητα δεν υποβαθμίζει την ασφάλεια του δικτύου διότι το NetRanger δεν παύει να αναγνωρίζει οποιοδήποτε άλλο συναγερμό από την ίδια διεύθυνση.

***Συνήθεις Υπογραφές***

Οι χρήστες μπορούν να δημιουργήσουν τις δικές τους υπογραφές επιθέσεων από το διευθυντή. Αυτές οι υπογραφές σύγκρισης χαρακτήρων μπορούν να χρησιμοποιηθούν για τη δημιουργία άμυνας απέναντι σε συγκεκριμένες επιθέσεις νέου τύπου ή για την ανίχνευση πληροφοριών μοναδικών για το περιβάλλον του χρήστη. Για παράδειγμα ο διαχειριστής του συστήματος μπορεί να "φοβάται" ότι οι χρήστες στέλνουν ανασφαλή "ιδιόκτητα" έγγραφα στο Internet. Μία υπογραφή μπορεί να δημιουργηθεί για να ανιχνεύει όλα τα περιστατικά που περιέχουν τη λέξη "ιδιόκτητα".

***Απάντηση σε Επίθεση***

- Αφού ανιχνευθεί μια εισβολή ο αισθητήρας μπορεί να απαντήσει με έναν από τους ακόλουθους –ρυθμιζόμενους από το χρήστη – τρόπους
- Χτυπάει συναγερμό. Οι συναγερμοί ξεκινούν από τον αισθητήρα και δρομολογούνται προς έναν ή περισσότερους διευθυντές.
- Κρατάει ημερολόγιο των συναγερμών που χτυπάει. Όλα τα δεδομένα από τον αισθητήρα γράφονται σε επίπεδα αρχεία τα οποία είναι είτε ημερολόγια γεγονότων, είτε ημερολόγια IP συνόδων.
- Καταγράφει τη σύνοδο σε ένα ημερολόγιο IP συνόδων για να συλλέξει αποδείξεις παράνομης δραστηριότητας ή για να καταγράψει τη γνώση του hacker για το δίκτυο. Αυτή η δυνατότητα χρησιμοποιείται σε συνδυασμό με μία "fishbowl" ή "honeypot" τεχνική όπου ένας εισβολέας κατευθύνεται σε ένα "ασφαλές" δίκτυο ή server που υποδύεται ότι έχει ή τρέχει σημαντικές πληροφορίες και εφαρμογές αντίστοιχα.

Πρέπει να σημειώσουμε ότι τα ημερολόγια των IP συνόδων γράφονται μόνο όταν κάποιο συγκεκριμένο συμβάν λαμβάνει χώρα (π. χ. μία αίτηση σύνδεσης από συγκεκριμένη IP διεύθυνση ή ανίχνευση κάποιας συγκεκριμένης ακολουθίας χαρακτήρων όπως "εμπιστευτικό")Όταν οι παραπάνω όροι ικανοποιούνται, ο αισθητήρας μπορεί να ρυθμιστεί για να καταγράφει κάθε εισερχόμενο ή εξερχόμενο πακέτο σε ένα ημερολόγιο IP συνόδου για ένα προκαθορισμένο χρονικό διάστημα.

- Τα ημερολόγια γεγονότων είναι συνεχώς ενεργά και περιέχουν πληροφορίες συναγερμών, εντολών και σφαλμάτων

Πρέπει να σημειώσουμε ότι τα ημερολόγια των IP συνόδων γράφονται τοπικά σε κάποιον αισθητήρα ή και σε κάποιον απομακρυσμένο διευθυντή—το ποία ακριβώς πληροφορία στέλνεται και πού άπτεται των ρυθμίσεων του αισθητήρα.

- "Σκοτώνει" τις συνόδους ξαναρχίζοντας τις IP συνδέσεις. Ο αισθητήρας μπορεί να ξαναρχίσει συνδέσεις TCP μετά από μια επίθεση για να ελαχιστοποιήσει την απειλή. Η επικοινωνία μεταξύ όλων των άλλων συνδέσεων συνεχίζεται μειώνοντας έτσι την πιθανότητα προβλημάτων άρνησης υπηρεσιών (denial-of-service) που μπορούν να παρουσιαστούν μετά από την αποφυγή επιθέσεων με βάση το TCP.
- Αποφυγή της επίθεσης και άρνηση πρόσβασης στο δίκτυο. Αυτή η επιλογή περιλαμβάνει τη χρήση του χαρακτηριστικού: "Διαχείρισης Συσκευών" (Device Management) το οποίο περιγράφεται παρακάτω. Η διαδικασία αποφυγής της επίθεσης περιλαμβάνει επαναρύθμιση και επαναφόρτωμα των φίλτρων ασφάλειας ή των όποιων λιστών ελέγχου πρόσβασης(Access Lists--ACL) του router. Αυτός ο τύπος αυτόματης απάντησης του αισθητήρα πρέπει να ρυθμίζεται μόνο για υπογραφές επιθέσεων με μειωμένη πιθανότητα λανθασμένης ανίχνευσης, όπως μία σαφής SATAN επίθεση. Μία αποτροπή μπορεί να επιτευχθεί και "χειροκίνητα" από κάποιο διευθυντικό σύστημα σε απάντηση επίθεσης ή ύποπτης δραστηριότητας.

Πρέπει να σημειωθεί ότι η αποτροπή απαιτεί προσεκτική εφαρμογή και ενημέρωση του προσωπικού του δικτύου διότι η δημιουργία συναγερμού σε συγκεκριμένο host ή δίκτυο μπορεί να οδηγήσει στην άρνηση υπηρεσιών. Το NetRanger μπορεί να ρυθμιστεί για το λόγο αυτό κατά τέτοιο τρόπο που να μην κλείνει ποτέ host ή δίκτυο.

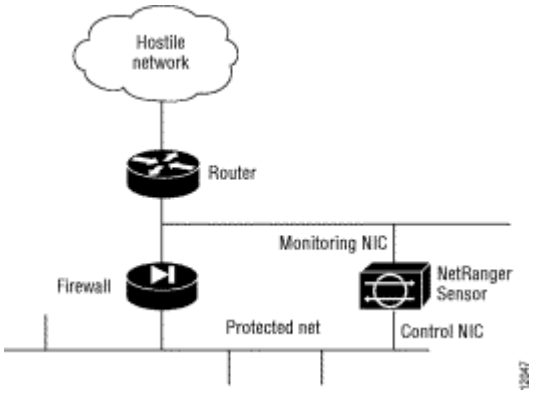
### *Διαχείριση Συσκευών*

Η διαχείριση συσκευών είναι ένα χαρακτηριστικό του προϊόντος που επιτρέπει στον αισθητήρα να επαναρυθμίζει δυναμικά τις λίστες πρόσβασης στους routers για να χτυπήσει την επίθεση στη πηγή της σε πραγματικό χρόνο. Αυτή η δυνατότητα αυξάνει σημαντικά την ικανότητα του αισθητήρα να προστατέψει το δίκτυο από εσωτερικές και εξωτερικές απειλές, δίνοντας ταυτόχρονα τη δυνατότητα στο χρήστη να ελέγξει τη κατάχρηση του δικτύου σε όλη την έκτασή του.

Ο αισθητήρας (σχήματα 1 & 2) χρησιμοποιεί το ένα interface –κάρτα του, για να παρακολουθεί τη κίνηση των πακέτων και την άλλη για να εκτελεί εντολές και να επικοινωνεί με τον router. Αυτή η τακτική επιτρέπει στον αισθητήρα να ανανεώνει δυναμικά τις λίστες πρόσβασης των router σε απάντηση των απαιτήσεων της κίνησης στο δίκτυο.

Προς το παρών ο αισθητήρας υποστηρίζει Ethernet, Fast Ethernet, Token Ring και FDDI interfaces. Είναι σημαντικό ο αισθητήρας να χρησιμοποιείται σε "αδιάκριτης" κατάστασης και όχι σε switched hub . Εάν χρησιμοποιείται σε switched, τότε θα μπορεί να "βλέπει" τη κίνηση μόνο εάν ο διακόπτης υποστηρίζει δυνατότητα παρακολούθησης ή το SPAN (Switched port Analyzer ). Το interface εντολών είναι πάντα Ethernet.

## 5.9.7 Παρακολούθηση του Ημερολογίου των Δρομολογητών




Οι Cisco Routers που είναι εγκατεστημένοι ανά τον κόσμο ξεπερνούν τα δύο εκατομμύρια και οι λίστες πρόσβασης (ACL-Access Control Lists) είναι ο πιο διαδεδομένος μηχανισμός ασφάλειας που χρησιμοποιείται στα δίκτυα. Επειδή χρησιμοποιούνται για αυτό το λόγο, ο αισθητήρας του NetRanger έχει φτιαχτεί να παρακολουθεί και να αναλύει τα ημερολόγια που κρατάνε και να προειδοποιεί, αν χρειαστεί, το διευθυντή.

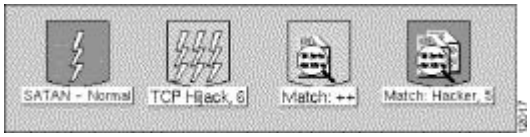
## 5.9.8 Δυνατότητες Director-Διευθυντή

Ο διευθυντής παρέχει κεντρικό έλεγχο πάνω στους αισθητήρες ενός δικτύου. Ο διευθυντής που είναι βασισμένος σε software, περιλαμβάνει wizards (μάγους) εγκατάστασης για γρήγορη εγκατάσταση και χωρίς την ανάγκη compilation. Η δουλεία του είναι να ελέγχει και να διαχειρίζεται τους αισθητήρες, να συλλέγει και να αναλύει τα δεδομένα ασφάλειας, να "κατεβάζει" νέες υπογραφές επιθέσεων και να διευκολύνει τους χρήστες στη δουλειά τους. Δεν παρέχει υπηρεσία δημιουργίας αναφορών διότι αυτό θα λειτουργούσε ανασταλτικά ως προς την ικανότητά του επεξεργασίας κρίσιμων πληροφοριών. Κατά συνέπεια τα δεδομένα διοχετεύονται σε βάσεις δεδομένων και συγγραφής αναφορών τρίτων συστημάτων.

**Βάση Δεδομένων Ασφάλειας Δικτύου**

Ο διευθυντής κάνει χρήση μιας χαρτογραφημένης με χρωματιστά εικονίδια μεθόδου παρουσίασης συναγερμών που επιτρέπουν στο χρήστη να επιλέξει συγκεκριμένο είδος συναγερμού και να αναλύσει την απειλή που ο τελευταίος αποτελεί για το σύστημα. Η βασισμένη στο HTML Δικτυακή άρση Δεδομένων παρέχει περιγραφή επίθεσης, πιθανά αντίμετρα και μπορεί να ρυθμιστεί για να περιλαμβάνει και άλλες εξειδικευμένες πληροφορίες για συγκεκριμένα συστήματα. Αυτή η πολιτική διασφαλίζει συνεχή και σταθερή πολιτική άμυνας ανεξάρτητη από το ανθρώπινο δυναμικό και τις τυχόν αλλαγές του.

**Παρακολούθηση Αισθητήρων**




Ο διευθυντής παρουσιάζει πληροφορίες ασφάλειας πραγματικού χρόνου οι οποίες του έρχονται από τους αισθητήρες μέσω εικονιδίων που βρίσκονται σε χάρτες ασφαλείας του δικτύου. Αυτά ταξινομούνται με ιεραρχικά σε χάρτες βασισμένους στη Διαχείριση Δικτυακών Κόμβων(Network Node Management-NNM) από την HP Open View. Ο χρήστης μπορεί να επιλέξει με διπλό click του mouse να πάει σε έναν χάρτη που βρίσκεται πιο κάτω στην ιεραρχική δομή. Το τελευταίο επίπεδό της περιέχει εικονίδια "Συναγερμού" και "Λάθους" όπως φαίνεται στο σχήμα 3.

Κάθε εικονίδιο ανεξάρτητα με το αν αναπαριστά έναν Μηχανισμό μια Εφαρμογή ή έναν Συναγερμό, βρίσκεται σε κάποια κατάσταση η οποία παρουσιάζεται υπό τη μορφή γραφικών και προσδιορισμών κειμένου διαφορετικών για κάθε κατηγορία. Η πιο ορατή ένδειξη της κατάστασης ενός εικονιδίου είναι το χρώμα του. Τα χρώματα αναπαριστούν καταστάσεις και επίπεδα συναγερμού όπως καθορίζονται στον πίνακα 2.

Πίνακας 2:

Χρώμα εικονιδίου, Κατάσταση και Επίπεδο Συναγερμού

| Χρωμα εικονιδιου | κατασταση εικονιδιου | επιπεδο συναγερμου |
|---|---|---|
| Πράσινο | Κανονική | 1 |
| Κίτρινο | Οριακή | 2-3 |
| Κόκκινο | Κρίσιμη | 4-5 |

Το χρώμα ενός εικονιδίου μεταδίδεται προς τα πάνω μέσα στην ιεραρχία. Για παράδειγμα ένα εικονίδιο συναγερμού που βρίσκεται σε κρίσιμη κατάσταση είναι κόκκινο. Η εφαρμογή που δημιουργεί αυτό το κόκκινο συναγερμό θα γίνει και αυτή

κόκκινη για να ταιριάξει το χρώμα της – και φυσικά η κατάστασή της – με το χρώμα του εικονιδίου. Σε αποτέλεσμα αυτής της διαδικασίας έχουμε την αλλαγή του χρώματος, σε κόκκινο, ακόμα και της μηχανής στην οποία τρέχει η εφαρμογή.

### *Διαχείριση Αισθητήρων*

Ο διευθυντής μπορεί να ρυθμίζει εξ αποστάσεως τις ρυθμίσεις των αισθητήρων. Η εφαρμογή που είναι υπεύθυνη για αυτή τη λειτουργία είναι η nrConfigure. Η ρύθμιση των υπογραφών του nrConfigure φαίνεται στο σχήμα 1-4. Η ρύθμιση αυτή για έναν αισθητήρα είναι διαδικασία – κλειδί στην ασφάλιση ενός δικτύου με το σύστημα NetRanger.

### *Εγκατάσταση Αισθητήρων*

Ο αισθητήρας μπορεί να εγκατασταθεί εύκολα και γρήγορα από έναν τεχνικό χωρίς να είναι απαραίτητη καμιά ειδική εκπαίδευση. Ο αισθητήρας απλώς εφαρμόζεται στο δίκτυο και αυτό που πρέπει να κάνει ο τεχνικός είναι να του δώσει κάποια βασική πληροφόρηση για τη Διευθυνσιοδότηση στο δίκτυο μέσω ενός laptop υπολογιστή. Κατόπιν ο διευθυντής προγραμματίζεται να αναζητήσει το νέο αισθητήρα. Όταν αποκατασταθεί η επικοινωνία ο αισθητήρας πρώτα από όλα "κατεβάζει" τις ρυθμίσεις του οι οποίες είναι αποθηκευμένες στη Βιβλιοθήκη Ρυθμίσεων του διευθυντή (Director's Configuration librarian) ως SENSOR X, VERSION 1. Ο αισθητήρας τότε ξεκινά να τη λειτουργία του με την αποστολή συναγερμών και την αποδοχή εντολών από τον διευθυντή. Όποτε ο αισθητήρας επαναρυθμίζεται κάθε νέα ρύθμιση παίρνει έναν νέο αριθμό έκδοσης.

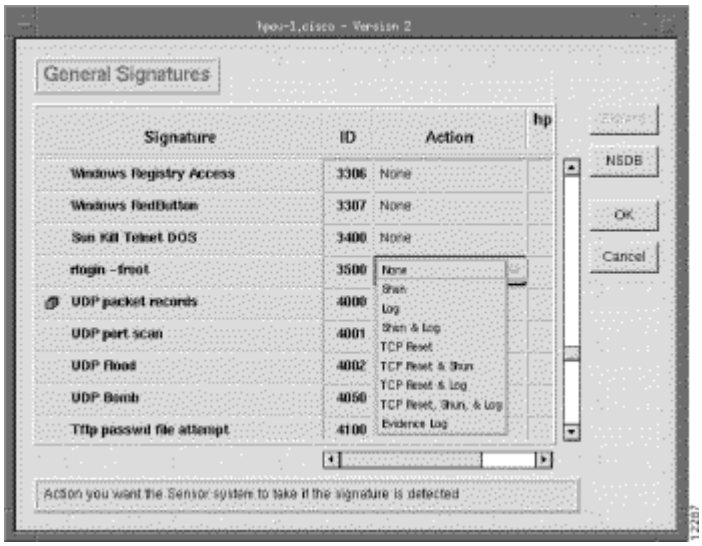
Ο αισθητήρας δεν χρειάζεται ειδική άδεια προϊόντος και μπορεί να εγκατασταθεί όπου χρειάζεται στο δίκτυο.

### *Επαναφορά Αισθητήρα*

Εάν κάποιος αισθητήρας βγει εκτός υπηρεσίας, χτυπάει αμέσως ένας συναγερμός στον διευθυντή. Εάν διαπιστωθεί ότι ο αισθητήρας έχει πρόβλημα μπορεί να εγκατασταθεί κάποιος άλλος στη θέση του. Η ρύθμιση του νέου θα γίνει με την ίδια διαδικασία που ακολουθήθηκε και με τον παλιό—με το nrConfigure.

### *NrConfigure*

Το nrConfigure είναι ένα εργαλείο βασισμένο σε Java και χρησιμοποιείται για ρύθμιση αισθητήρων από απόσταση και διαχείριση των αρχείων ρυθμίσεων. Με το εργαλείο αυτό ο χρήστης μπορεί να αλλάξει τα αρχεία ρυθμίσεων κάποιου αισθητήρα και να διαχειριστεί αρχεία ρυθμίσεων διαφορετικών εκδόσεων. Αυτή η λειτουργία επιτρέπει στο χρήστη να κρατάει τόσο τις ενεργές όσο και τις παλιές ρυθμίσεις. Με το τρόπο αυτό έχουμε τη δυνατότητα σαν χρήστες να επαναφέρουμε σε ενέργεια παλιότερες ρυθμίσεις ή να αναπαράγουμε τις ήδη υπάρχουσες και σε άλλους αισθητήρες αντί να τις ξαναδημιουργήσουμε για καθέναν από αυτούς.

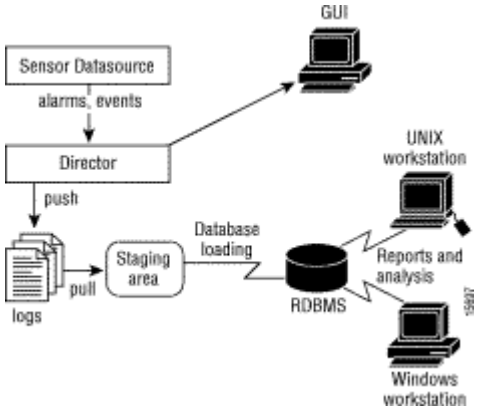



Το nrConfigure δίνει τη δυνατότητα ρύθμισης των παρακάτω παραμέτρων σε οποιαδήποτε έκδοση των αρχείων ρυθμίσεων:

- Επικοινωνίες
- Διαχείριση Δεδομένων
- Διαχείριση Συσκευών
- Προώθηση Διευθυντή
- Επεξεργασία Γεγονότων
- Ανίχνευση Εισβολών
- Αρχεία Συστήματος
- Συλλογή Δεδομένων Προερχομένων από Αισθητήρες

Ο Διευθυντής μπορεί να συλλέξει και να κατατάξει δεδομένα από αισθητήρες χρησιμοποιώντας έναν απλό μηχανισμό της μορφής: σπρώξιμο-τράβηγμα (push-pull). Το σύστημα NetRanger γράφει (σπρώχνει) δεδομένα "οριζόντια" αρχεία και μετά τα κατατάσσει (τραβάει) σε μια βάση δεδομένων. Η όλη διαδικασία φαίνεται στο σχήμα 5.

Με το να γράφονται τα δεδομένα σε "οριζόντια" αρχεία παρέχονται από το σύστημα επίπεδα ανοχής σφαλμάτων και απόδοσης που δεν θα μπορούσε να επιτευχθεί γράφοντας απευθείας στη βάση δεδομένων. Η ροή δεδομένων σε ένα διαμοιρασμένο σύστημα όπως το NetRanger περιορίζεται μόνο από το πιο αδύναμη διασύνδεση του συστήματος. Με τη διαδικασία συλλογής πληροφοριών του NetRanger η συλλογή πληροφοριών δεν εξαρτάται ή κατά οποιοδήποτε τρόπο επηρεάζεται από τη βάση δεδομένων ή την αυξομείωση της απόδοσης.




Ο Διευθυντής δίνεται, προς το παρόν, με οδηγούς από την Oracle και τη Remedy. Ωστόσο, αυτοί οι οδηγοί μπορούν να ρυθμιστούν για να γράφουν και σε άλλες βάσεις δεδομένων όπως η Sybase και η Informix. Παραδείγματα scripts που έρχονται μαζί με τον διευθυντή δείχνουν πώς τα υπάρχων κύρια μέρη της βάσης δεδομένων μπορούν να εισαχθούν στο NetRanger.

Ο Διευθυντής περιέχει επιπλέον μία ρυθμιζόμενη δυνατότητα διαχείρισης αρχείων η οποία αρχειοθετεί αυτόματα γεγονότα και ημερολόγια IP είτε σε έναν αισθητήρα είτε σε κάποιο διευθυντή. Πρότυπα αρχεία με διάφορα προφίλ ρυθμίσεων παρέχονται και για τους αισθητήρες και για τους διευθυντές.

***Ανάλυση Δεδομένων Αισθητήρων***

Ο διευθυντής μπορεί επίσης να αναλύει δεδομένα από τον αισθητήρα χρησιμοποιώντας εργαλεία άλλων συστημάτων που παρέχουν διαχείριση βάσεων δεδομένων και δημιουργία αναφορών.

Ως δημιουργός αναφορών, ο διευθυντής περιλαμβάνει ένα σύνολο της Sequenced Query Language (SQL) που μπορεί εύκολα προσαρμοστεί σε οποιοδήποτε εργαλείο άλλου συστήματος.

Τα εργαλεία αυτά μπορούν να ρυθμιστούν για την υποστήριξη μεμονωμένων ερευνών ή προκαθορισμένων αναφορών. Για παράδειγμα αυτά τα εργαλεία μπορούν να συντάξουν αναφορές που να περιλαμβάνουν τα ακόλουθα:

- Όλους τους συναγερμούς επιπέδου 4 και 5 που έλαβαν χώρα τις τελευταίες 30 ημέρες
- Ένα γράφημα της δραστηριότητας του Web Server των περασμένων 24 ωρών
- Ένα πίνακα όλων των γεγονότων των περασμένων 30 ημερών κατά σειρά επιπέδου συναγερμού

**Υποστήριξη Ενεργειών Καθορισμένων από το Χρήστη**

Ο διευθυντής μπορεί να πραγματοποιήσει ενέργειες καθορισμένες από το χρήστη. Μία κοινή ενέργεια είναι η ειδοποίηση του προσωπικού με e-mail και η προώθηση δεδομένων σε άλλα προγράμματα. Υποστήριξη παρέχεται και σε scripts πολλαπλών λειτουργιών.

**Δυνατότητες Post Office**

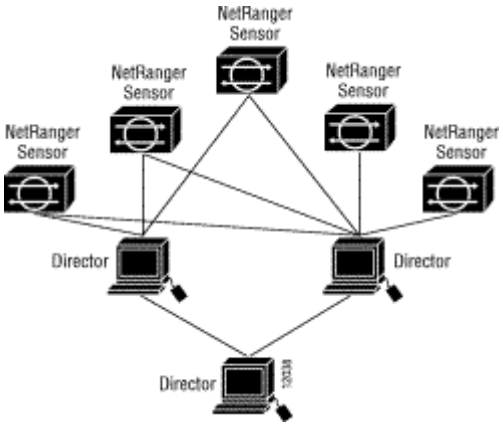
Οι υπηρεσίες και οι υπολογιστές του NetRanger επικοινωνούν μεταξύ τους κάνοντας χρήση του Post Office, συμπεριλαμβανομένων υπηρεσιών στον ίδιο υπολογιστή και στο ίδιο δίκτυο. Όλες οι επικοινωνίες βασίζονται σε ένα σχήμα τριών μερών με επικεφαλίδες του Οργανισμού, του Υπολογιστή και της Εφαρμογής που δίνουν ταυτότητα σε κάθε κόμβο του NetRanger.

Το ιδιαίτερο σχήμα διευθυνσιοδότησης του NetRanger έχει τα ακόλουθα χαρακτηριστικά:

- Μπορεί να τοποθετηθεί σε επίπεδο πάνω από αυτό των υπαρχόντων δικτυακών πρωτοκόλλων
- Επιτρέπει επικοινωνία ανάμεσα σε ετερογενή δίκτυα με ανοχή στα σφάλματα
- Διευθυνσιοδοτεί μια πολύ μεγαλύτερη περιοχή από το υπάρχον 32-bit πρωτόκολλο

Το σχήμα αυτό διευθυνσιοδότησης του NetRanger λειτουργεί επιπλέον ως η βάση για κάποιο point-to-point πρωτόκολλο που επιτρέπει έως 255 εναλλακτικές οδούς-δρομολόγια μεταξύ δύο δικτυωμένων υπολογιστών. Αυτό το εναλλακτικό πρωτόκολλο δρομολόγησης μεταπηδά αυτόματα στην επόμενη διαδρομή οποτεδήποτε η χρησιμοποιούμενη αποτυγχάνει. Χρησιμοποιεί, επίσης, ένα παλμό συστήματος για να ανιχνεύσει πότε μία σύνδεση μέσω της προτιμούμενης διαδρομής μπορεί να επανεγκαθιδρυθεί. Ένα μήνυμα λάθους του συστήματος δημιουργείται και καταγράφεται όποτε μία σύνδεση πέφτει και τα πακέτα που χάθηκαν κατά τη διάρκεια της μετάβασης από τη μία διαδρομή στην άλλη επανεκπέμπονται.

Ακόμα ένα χαρακτηριστικό που συμπληρώνει την εναλλακτική δρομολόγηση είναι η ικανότητα του χτισίματος ιεραρχημένες δομές αισθητήρων και διευθυντών μέσω της χρήσης αναπαραγόμενων μηνυμάτων. Αντί να στέλνουμε στοιχεία από έναν αισθητήρα σε πολλούς υπολογιστές, η πληροφορία μπορεί να στέλνεται σε έναν διευθυντή ο οποίος με τη σειρά του μπορεί να αναπαράγει τα πακέτα και προς άλλες πλατφόρμες οι οποίες βρίσκονται στα τοπικά αρχεία ρυθμίσεών του. Οι αισθητήρες μπορούν να αναπαράγουν πακέτα προς περισσότερους από έναν διευθυντές διασφαλίζοντας έτσι επικοινωνία με ανοχές σφαλμάτων.




Το σχήμα 6 δείχνει το σκεπτικό μέσω μιας απλής ιεραρχημένης δομής διευθυντών.

Σε συμπλήρωμα της παροχής πλεονεκτημάτων στην απόδοση και ανοχή σφαλμάτων, οι διανεμημένες ιεραρχικές δομές μπορούν να απλουστεύσουν τη διαχείριση του συστήματος. Για παράδειγμα, οι τοπικές μηχανές που "τρέχουν" διευθυντές μπορεί να είναι υπεύθυνες για την παρακολούθηση του συστήματος από τις 09: 00 έως τις 17: 00 και μετά να περνούν τον έλεγχο σε ένα κεντρικό διευθυντή κάθε βράδυ.

## 5.9.9 Αρχιτεκτονική του NetRanger

Οι Αισθητήρες, οι Διευθυντές και το Post Office έχουν το καθένα ξεχωριστά λειτουργικά κομμάτια που ονομάζονται δαίμονες ή υπηρεσίες. Επειδή κάθε κύρια λειτουργία του NetRanger επιτυγχάνεται μέσω μιας ξεχωριστής υπηρεσίας, το αποτέλεσμα είναι ένα σύστημα ασφάλειας που είναι γρήγορο, ανθεκτικό και κλιμακωτό. Οι υπηρεσίες, που φαίνονται στο σχήμα 7, ορίζονται ως εξής:

- ***Sensord/packetd*:** Και οι δύο αυτές υπηρεσίες παρέχουν ανίχνευση εισβολών. Η sensord χρησιμοποιείται όταν ένας αισθητήρας συνεργάζεται με μια δικτυακή συσκευή που υποστηρίζει copy_to/log_to (αντιγραφή_σε/καταγραφή_σε) λειτουργίες (που στέλνουν αντίγραφα αιχμαλωτισμένων πακέτων στον αισθητήρα). Η packetd χρησιμοποιείται όταν ο αισθητήρας ο ίδιος αιχμαλωτίζει πακέτα απευθείας από το δίκτυο.
- ***Loggerd*:** Αυτή η υπηρεσία είναι η καταγραφική υπηρεσία του NetRanger. Είναι υπεύθυνη για να καταγράφει σφάλματα, εντολές και συναγερμούς στα αρχεία-ημερολόγια του αισθητήρα.
- ***Sapd*:** Αυτή η υπηρεσία παρέχει διαχείριση δεδομένων και αρχείων. Είναι υπεύθυνη για τη μετακίνηση αρχείων ημερολογίου σε χώρους των βάσεων δεδομένων, ανενεργών αρχείων, και να εκτελέσει και άλλες διαδικασίες ρουτίνας για να αποτρέψει την υπερχείλιση του file system.
- ***Postofficed*:** Αυτή η υπηρεσία χειρίζεται τις επικοινωνίες μεταξύ των υπηρεσιών και των κόμβων του NetRanger. Όπως φαίνεται στο σχήμα 7 όταν το sensord ανιχνεύσει παράνομη δραστηριότητα ειδοποιεί το postofficed. Από εκεί και πέρα το τελευταίο είναι υπεύθυνο να πει στο loggerd να αρχίσει την καταγραφή, θέτοντας σε συναγερμό το smid στο διευθυντή και μεταβιβάζοντας εντολές προς τους routers ώστε να αποτραπεί η επίθεση.

- ***Smid*****:** Αυτή η υπηρεσία τρέχει στον διευθυντή μόνο και είναι υπεύθυνη για την μετάφραση των δεδομένων που προέρχονται από τους αισθητήρες σε δεδομένα που να έχουν νόημα για το nrdirmap.
- ***Nrdirmap*****:** Αυτή η υπηρεσία είναι υπεύθυνη για να παρουσιάζει διάφορα σύμβολα που αναπαριστούν μηχανισμούς, εφαρμογές, συναγερμούς και σφάλματα στο γραφικό interface του διευθυντή.
- ***Eventd*****:** Αυτή η υπηρεσία είναι υπεύθυνη για να κρατάει διαδικασίες ενημέρωσης που έχουν καθοριστεί από το χρήστη. Ο χρήστης μπορεί να καθορίσει τι είδους συναγερμών ή άλλου είδους γεγονότων μπορούν να ξεκινούν κάποια αντίδραση, συνήθως κάποιο e-mail ή ειδοποίηση σελίδας
- ***Configd*****:** Αυτή η υπηρεσία παρέχει ένα μηχανισμό μέσω του οποίου το nrdirmap μπορεί να αλληλεπιδράσει με άλλες υπηρεσίες όπως το postofficed, sensord και το managed. Με άλλα λόγια οι εντολές του γραφικού περιβάλλοντος μπορούν να εκτελεστούν μέσω της υφιστάμενης υπηρεσίας configd.

# *Βιβλιογραφία*

*“Internetworking With TCP/IP“*

Douglas E. Comer

Prentice-Hall International, Inc.

*“THE INTERNET MESSAGE, Closing The Book With Electronic Mail”*

Marshall T. Rose

Prentice-Hall International, Inc.

*“THE SIMPLE BOOK, An Introduction To Management of TCP/IP-based Internets”*

Marshall T. Rose

Prentice-Hall International, Inc.

*“UNIX “*

Paul W. Abrahams, Bruce R. Larson

Εκδόσεις NUBIS

*"ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ"*

Άρης Αλεξόπουλος, Γιώργος Λαγογιάννης

*“Practical Unix & Internet Security”*

Garfinkel & Spafford

O' REILLY™

*“Practical Internetworking With TCP/IP and UNIX”*

Smoot Carl-Mitchell, John S. Quarteman

Addison Wesley

*“JAVA Networking Programming”*

Elliotte Rusty Harold

O’ Reilly