τμήμα μηχανικών πληροφορικής τ.ε.
Τ.Ε.Ι. Δυτικής Ελλάδας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Συγκριτική μελέτη ενσύρματων δικτύων για την αξιολόγηση της επίδρασης της ασφάλειας IPSec (VPN) στην λειτουργία των δικτύων.

Ρίστα Άλντα & Γαβαλά Ιωάννα

Α.Μ.:

1091

0945

Επιβλέπων : Τσακανίκας Βασίλειος

Αντίρριο , Οκτώβριος 2017

ΠΕΡΙΛΗΨΗ

Τις τελευταίες δεκαετίες τα δίκτυα υπολογιστών είναι ένας δίαυλος επικοινωνίας για εκατομμύρια κόσμο από απλούς πολίτες με την ανάγκη της επικοινωνίας εξ αποστάσεως μέχρι και εταιρείες και επαγγελματίες με σκοπούς όπως εμπόριο, ανταλλαγή δεδομένων.

Στην παρούσα εργασία σκοπός μας είναι να οικειοποιηθούμε τα δίκτυα των υπολογιστών, καθώς και τις βασικές αρχές λειτουργίας τους. Θα μιλήσουμε για την ασφάλεια και την ακεραιότητα των δεδομένων, θα δούμε τρόπους επιθέσεων σε ένα δίκτυο υπολογιστών και τρόπους προστασίας σε κάθε επίπεδο καθώς και τι είναι κρυπτογράφηση και ποια κρυπτοσυστηματα χρησιμοποιούνται.

Επισημαίνουμε τι είναι ασφάλεια από άκρο σε άκρο, που βασίζεται, τι μηχανισμούς χρησιμοποιεί για να επιτευχτεί, αλλά και τις πρακτικές αδυναμίες που συναντάμε.

Στο τέταρτο κεφάλαιο αναλύουμε αλγορίθμους που χρησιμοποιούνται στην κρυπτογράφηση από άκρο σε άκρο όπως το πρότυπο AES , TWOFISH και τα πρότυπο IDEA , και μέσα από παραδείγματα και εικόνες βλέπουμε τον τρόπο λειτουργίας του κάθε πρότυπου.

Τι είναι όμως εικονικό δίκτυο και τι ασφάλεια παρέχει;

Φτάνουμε λοιπόν στο σημείο να μιλήσουμε για τα εικονικά δίκτυα (VPN), και τις εφαρμογές τους. Θα αναπτύξουμε την αρχιτεκτονική των VPN και θα δούμε ειδικότερα και το IPsec, τι ασφάλεια παρέχει αλλά και τα πρωτόκολλα που ορίζει.

Τέλος παρουσιάζονται ευρέως διαδεδομένες τεχνολογίες VPN L2TP και PPTP και στη συνέχεια συγκρίνονται σε πρακτικό επίπεδο. Αυτές οι τεχνολογίες, όπως και η IPSec, είναι ευρέως χρησιμοποιούμενες και έχουν αναλυθεί εκτενώς.

Abstract

Over the last decades, computer networks have been a communication means for millions of people varying from ordinary citizens with the need to communicate remotely, to companies and professionals for purposes such as commerce, data exchange.

In this paper, we aim to familiarize with computer networks, as well as their basic principles of operation. We will talk about the security and integrity of the data, we will look at ways of attacking a computer network and ways of protecting it at each level, as well as what is encryption and what cryptosystems are being used in the latter.

We highlight what is point-to-point security, what kind of mechanisms it uses to be achieved, and the practical weaknesses that we encounter.

In the fourth chapter we analyze algorithms that are used in point-to point encryption such as AES, TWOFISH, and IDEA, and through examples and images, we attempt to understand the way each model works.

At this point rises an crucial question. “What exactly is a Virtual Private Network, and what kind of security does it provide”?

So we get to talk about virtual networks (VPNs), and their applications. We will develop the architecture of VPNs and we will look in particular at IPsec, what kind ofsecurity it provides, and the protocols it defines.

Finally, widespread L2TP and PPTP VPN technologies are presented and then compared to a practical level. These technologies, like IPSec, are widely used and extensively analyzed.

ΕΥΧΑΡΙΣΤΙΕΣ

Νιώθουμε την ανάγκη να ευχαριστήσουμε εκ βαθέων όλους όσους συνέβαλλαν στην επιτυχή ολοκλήρωση της παρούσας πτυχιακής.

Θα θέλαμε να εκφράσουμε τις θερμές μας ευχαριστίες στον επιβλέποντα καθηγητή μας, κύριο Βασίλειο Τσακανίκα για την υποστήριξη του καθ'όλη την διάρκεια της πτυχιακής εργασίας . Ήταν πάντα διαθέσιμος και πλήρως υποστηρικτικός στις όποιες δυσκολίες προέκυψαν κατά την εκπόνηση αυτής της πτυχιακής.

Τέλος δεν θα τολμούσαμε να ξεχάσουμε την στήριξη από τις οικογένειες μας και τους αγαπημένους μας, και να τους ευχαριστήσουμε που πίστεψαν τόσο πολύ σε εμάς.

Άλντα Ρίστα

Ιωάννα Γαβαλά

Οκτώβριος 2017

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1ο – Δίκτυα υπολογιστών

Κεφάλαιο 2ο - Ασφάλεια και ακεραιότητα δεδομένων

Κεφάλαιο 6ο – Ανάλυση VPN τεχνολογιών

ΕΙΚΟΝΕΣ

Εισαγωγή

Κεφάλαιο 1ο

Δίκτυα υπολογιστών

1.1 Δίκτυα υπολογισμών

Δίκτυο υπολογιστών είναι ένα σύνολο αυτόνομων υπολογιστών που είναι διασυνδεδεμένοι με μια κοινή τεχνολογία. Δυο υπολογιστές λέμε ότι είναι διασυνδεδεμένοι αν είναι σε θέση να ανταλλάσουν πληροφορίες. Η σύνδεση δεν είναι απαραίτητο να γίνεται με χάλκινο σύρμα μπορεί επίσης να χρησιμοποιούνται οπτικές ίνες, μικροκύματα, υπέρυθρες ακτίνες, και τηλεπικοινωνιακοί δορυφόροι. Όπως θα δούμε στην συνεχεία , υπάρχουν δίκτυα με διάφορα μεγέθη, σχήματα και μορφές.

Επίσης υπάρχει σύγχυση στην βιβλιογραφία ανάμεσα σε ένα δίκτυο υπολογιστών και σε ένα κατανεμημένο σύστημα. Η βασική τους διάφορα είναι ότι σε ένα κατανεμημένο σύστημα έχουμε ένα σύνολο από ανεξαρτήτους υπολογιστές το όποιο εμφανίζεται στους χρηστές του σαν να ήταν ένα μοναδικό συνεκτικό σύστημα. Ένα ευρέως γνωστό μοντέλο παράδειγμα κατανεμημένου συστήματος είναι ο παγκόσμιος ιστός, όπου τα πάντα εμφανίζονται ως έγγραφα (ιστοσελίδες).

Στα δίκτυα υπολογιστών απουσιάζει η συνεκτικότητα, το μοντέλο και το λογισμικό που υπάρχει στα κατανεμημένα συστήματα. Ουσιαστικά το κατανεμημένο σύστημα είναι ένα σύστημα λογισμικού κτισμένο πάνω σε ένα δίκτυο.

1.2 Χρήσεις των δικτύων υπολογιστών

1.2.1 Επιχειρηματικές εφαρμογές

Μια εταιρία για παράδειγμα μπορεί να έχει ξεχωριστούς υπολογιστές για την παρακολούθηση της παράγωγης, τη διαχείριση αποθηκών, και την έκδοση μισθοδοσίας. Αρχικά κάθε ένας από αυτούς τους υπολογιστές μπορεί να λειτουργούσε απομονωμένος από τους άλλους , αλλά σε κάποιο σημείο η διοίκηση μπορεί να αποφάσισε να τους συνδέσει μεταξύ τους έτσι ώστε να είναι σε θέση να συλλέγει και να συσχετίζει πληροφορίες για ολόκληρη την εταιρία. Το ζητούμενο σε αυτήν την περίπτωση είναι η κοινοχρησία πόρων ή μερισμός πόρων και ο στόχος είναι όλα τα προγράμματα, ο εξοπλισμός, και ιδιαίτερα τα δεδομένα να είναι διαθέσιμα σε οποιοδήποτε δίκτυο, χωρίς να έχει σημασία η φυσική θέση του πόρου και του χρηστή. Στο μοντέλο αυτό τα δεδομένα αποθηκεύονται σε ισχυρούς υπολογιστές που ονομάζονται διακομιστές (servers) , ενώ οι υπάλληλοι έχουν στα γραφεία τους απλούστερες μηχανές που ονομάζονται πελάτες (clients).

1.2.2 Οικιακές εφαρμογές

Σήμερα σε κάθε σπίτι υπάρχει και ένας προσωπικός υπολογιστής, παλαιοτέρα αυτό συνέβαινε με στόχο την επεξεργασία κειμένου και τα παιχνίδια, αλλά τα τελευταία χρόνια η κατάσταση έχει αλλάξει ριζικά. Σήμερα ο σημαντικότερος λόγος είναι η πρόσβαση στο internet. Μερικές από τις ποιο δημοφιλείς χρήσεις του internet για τους οικιακούς χρηστές είναι πρόσβαση

σε απομακρυσμένες πληροφορίες , διαπροσωπική επικοινωνία, αλληλεπιδραστική διασκέδαση και το ηλεκτρονικό εμπόριο.

1.2.3 Μετακινούμενοι χρηστές

Οι φορητοί υπολογιστές, όπως οι υπολογιστές – σημειωματάρια (notebooks) και οι προσωπικοί ψηφιακοί βοηθοί (personal digital assistants). Οι χρηστές τέτοιων υπολογιστών θέλουν να είναι συνδεδεμένοι με την βάση τους ακόμα και όταν είναι στο δρόμο και γενικά όταν είναι μακριά από την βάση τους. Επειδή η καλωδιακή σύνδεση είναι αδύνατη όταν βρισκόμαστε μέσα σε ένα αυτοκίνητο ή ένα αεροπλάνο χρησιμοποιούνται τα ασύρματα δίκτυα .

1.3 Υλικό δικτύων

Σε γενικές γραμμές υπάρχουν δυο ειδή τεχνολογιών μετάδοσης που χρησιμοποιούνται ευρέως. Οι τεχνολογίες αυτές είναι οι ακόλουθες:

- **Δίκτυα εκπομπής.**
- **Δίκτυα από σημείο σε σημείο.**

1.3.1 Δίκτυα εκπομπής

Τα **δίκτυα εκπομπής** (broadcast networks) έχουν ένα μόνο κανάλι επικοινωνίας το όποιο είναι κοινόχρηστο από όλες τις μηχανές του δικτύου. Τα σύντομα μηνύματα που στέλνονται από κάθε μηχάνημα , τα οποία ονομάζονται πακέτα, λαμβάνονται από όλες τις άλλες μηχανές. Ένα πεδίο διεύθυνσης μέσα στο πακέτο προσδιορίζει τον επιθυμητό παραλήπτη.

1.3.2 Δίκτυα από σημείο σε σημείο

Τα **δίκτυα από σημείο σε σημείο** (point - to - point) αποτελούνται από πολλές συνδέσεις ανάμεσα σε ζεύγη μηχανών. Για να φτάσει ένα πακέτο από την προέλευση στον προορισμό του σε αυτόν τον τύπο διχτυού, μπορεί να χρειαστεί να επισκεφτεί πρώτα μια ή περιστέρες ενδιάμεσες μηχανές. Συχνά υπάρχουν πολλά πιθανά δρομολόγια, με διαφορετικά μήκη, άρα η ανεύρεση καλών δρομολογίων είναι ένα σημαντικό ζήτημα στα δίκτυα από σημείο σε σημείο. Ένας γενικός κανόνας είναι ότι μικρότερα, γεωγραφικά περιορισμένα, δίκτυα συνήθως χρησιμοποιούν εκπομπή, ενώ τα μεγαλύτερα δίκτυα συνήθως είναι δίκτυα από σημείο σε σημείο. Η μετάδοση από σημείο σε σημείο με έναν αποστολέα και έναν παραλήπτη μερικές φορές ονομάζεται και αποκλειστική διανομή (unicasting).

1.4 Δίκτυα ανά γεωγραφική κάλυψη

1.4.1 Τοπικά δίκτυα

Τα τοπικά δίκτυα (local area networks), που συνήθως αποκαλούνται δίκτυα LAN, είναι ιδιωτικά δίκτυα τα όποια βρίσκονται μέσα σε ένα κτίριο ή κτιριακό συγκρότημα, ή σε μια έκταση με μέγεθος μέχρι λίγα χιλιόμετρα. Χρησιμοποιούνται ευρέως για τη διασύνδεση προσωπικών υπολογιστών και σταθμών εργασίας σε γραφεία και εργοστάσια εταιριών, με στόχο την κοινοχρησία πόρων και την ανταλλαγή πληροφοριών. Τα δίκτυα LAN διακρίνονται από τα αλλά ειδή δικτύων με βάση τρία χαρακτηριστικά:

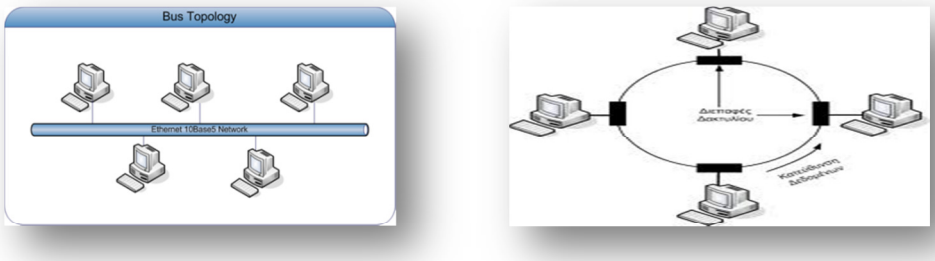
- **Το μέγεθος τους**
- **Την τεχνολογία μετάδοσης τους**
- **Την τοπολογία τους**

Τα δίκτυα LAN έχουν περιορισμένο μέγεθος, γεγονός που σημαίνει ότι ο χρόνος μετάδοσης στην χειρότερη περίπτωση βρίσκεται εντός συγκριμένων ορίων και είναι γνωστός εκ των πρότερων.

Υπάρχουν διαφορές πιθανές τοπολογίες για τα δίκτυα LAN εκπομπής. Όπως ένα **δίκτυο διαύλου** (δηλαδή, ενός ευθύγραμμου καλωδίου), ανά πάσα στιγμή το πολύ μια μηχανή είναι ο κύριος (master) και της επιτρέπεται να μεταδίδει δεδομένα. Όλες οι άλλες μηχανές πρέπει να αποφεύγουν την μετάδοση. Για να επιλύονται τυχόν σύγκρουσης όταν δυο η περισσότερες

μηχανές θέλουν να μεταδώσουν ταυτόχρονα, υπάρχει ένας μηχανισμός διαιτησίας, ο όποιος μπορεί να είναι είτε συγκεντρωτικός η αποκεντρωτικός.

Ένας δεύτερος τύπος συστήματος εκπομπής είναι ο δακτύλιος. Στα **δίκτυα δακτυλίου** το κάθε bit διαδίδεται μόνο του, χωρίς να περιμένει για το υπόλοιπο πακέτο στο όποιο ανήκει. Συνήθως το κάθε bit μπορεί να καλύψει ολόκληρο το δακτύλιο στο διάστημα που απαιτείται για την μετάδοση λίγων μόνο bit, συχνά πριν καν μεταδοθεί ολόκληρο το πακέτο. Όπως σε όλα τα συστήματα εκπομπής, απαιτούνται κάποιοι κανόνες διαιτησίας ώστε να αποφεύγονται οι ταυτόχρονες μετάδοσης στο δακτύλιο. Χρησιμοποιούνται διαφορές μέθοδοι όπως το να βάζουμε τις μηχανές να μεταδίδουν με την σειρά.



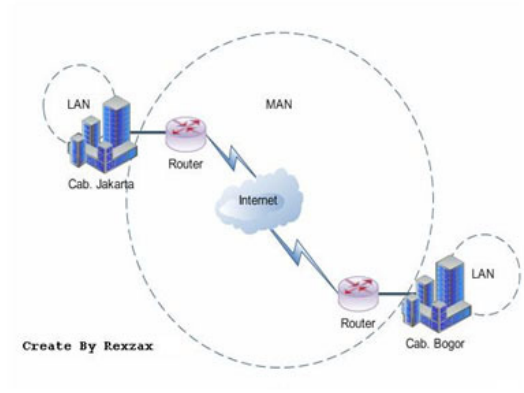
Εικονα 1-1: Δύο δίκτυα εκπομπής 1) *δίαυλος* , 2) *δακτυλιος*

1.4.2 Μητροπολιτικά δίκτυα

Το μητροπολιτικό δίκτυο (metropolitan area network), ή δίκτυο MAN, καλύπτει μια πόλη. Το ποιο γνωστό παράδειγμα δικτυού MAN είναι το δίκτυο καλωδιακής τηλεόρασης που υπάρχει σε πολλές πόλεις. Αυτό το σύστημα

είναι η εξέλιξη των παλαιοτέρων συστημάτων κοινοτικών κεραιών που χρησιμοποιούνται σε περιοχές με κακή τηλεοπτική λήψη από αέρος. Σε αυτά τα πρώιμα συστήματα, μια μεγάλη κεραία ήταν τοποθετημένη στην κορυφή ενός κοντινού λόφου και στην συνεχεία το σήμα στελνόταν στα σπίτια των συνδρομητών.

Από τότε που το internet άρχισε να προσελκύει το ενδιαφέρον του κόσμου, οι επιχειρήσεις δικτύου καλωδιακής τηλεόρασης άρχισαν να αντιλαμβάνονται ότι με ορισμένες αλλαγές στο σύστημα θα μπορούσαν να παρέχουν αμφίδρομες υπηρεσίες internet σε μη χρησιμοποιούμενα τμήματα του φάσματος. Σε αυτό το σημείο, το σύστημα καλωδιακής τηλεόρασης άρχισε να μεταλλάσσεται από έναν τρόπο διανομής τηλεόρασης σε ένα μητροπολιτικό δίκτυο.



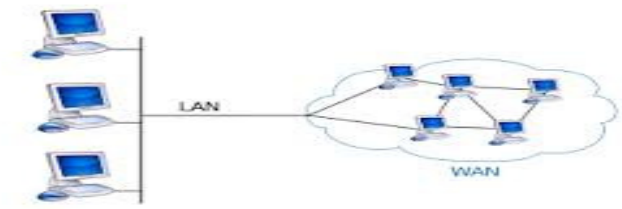
Εικόνα 1-2: Τοπικό δίκτυο LAN συνδεδεμένο σε μητροπολιτικό δίκτυο .

1.4.3 Δίκτυα ευρείας διανομής

Το δίκτυο ευρείας περιοχής (wide area network), ή δίκτυο WAN, εκτείνεται σε μια μεγάλη γεωγραφική περιοχή, όπως μια χωρά ή μια ήπειρο. Το δίκτυο WAN περιέχει ένα σύνολο μηχανών που προορίζονται για την εκτέλεση των προγραμμάτων των χρηστών. Θα ονομάσουμε αυτές τις μηχανές υπολογιστές υπηρεσίας (hosts) , οι όποιοι διασυνδέονται με ένα υπό-δίκτυο επικοινωνίας. Η δουλεία του υποδικτύου είναι να μεταφέρει μηνύματα ανάμεσα στους υπολογιστές υπηρεσίας.

Στα περισσότερα δίκτυα ευρείας περιοχής, το υποδίκτυο αποτελείται από δυο διακριτά συστατικά : τις γραμμές μετάδοσης και τα στοιχειά μεταγωγής. Οι γραμμές μετάδοσης μετακινούν bit ανάμεσα στις μηχανές. Μπορεί να υλοποιούνται με χάλκινα σύρματα, οπτικές ίνες, ή ακόμη και με ασύρματες συνδέσεις. Τα στοιχειά μεταγωγής είναι εξειδικευμένοι υπολογιστές που συνδέουν τρεις ή περισσότερες γραμμές μετάδοσης. Οι υπολογιστές μεταγωγής, ή αλλιώς δρομολογητές (router), όταν φτάνουν δεδομένα σε μια εισερχόμενη γραμμή επιλεγεί την εξερχομένη γραμμή στην όποια θα τα προωθήσει.

Στα περισσότερα WAN το δίκτυο περιέχει πολλές γραμμές μετάδοσης, με κάθε γραμμή να συνδέει ένα ζεύγος δρομολογητών. Όταν ένα πακέτο στέλνεται από ένα δρομολογητή σε κάποιον άλλο μέσω ενός ή περισσότερων ενδιάμεσων δρομολογητών, το πακέτο παραλαμβάνεται “αυτούσιο” σε κάθε ενδιάμεσο δρομολογητή, αποθηκεύεται εκεί μέχρι να απελευθερωθεί η απαιτουμένη γραμμή εξόδου, και μετά προωθείται. Τα υποδίκτυα που λειτουργούν με αυτόν τον τρόπο ονομάζονται δίκτυα αποθήκευσης και προώθησης ή υποδίκτυα μεταγωγής πακέτων.



Εικόνα 1-3: Τοπικό δίκτυο LAN συνδεδεμένο σε δίκτυο ευρείας γεωγραφικής περιοχής WAN.

1.5 Ασύρματα δίκτυα

Ένα **ασύρματο δίκτυο** είναι ένα τηλεφωνικό ή υπολογιστικό δίκτυο, το οποίο χρησιμοποιεί ραδιοκύματα ως φορείς ή ως το φυσικό επίπεδο. Στα δίκτυα αυτά η πληροφορία μεταφέρεται μέσω ηλεκτρομαγνητικών κυμάτων, με συχνότητα που εξαρτάται κάθε φορά από το ρυθμό μετάδοσης που απαιτείται να έχει το δίκτυο. Η ασύρματη επικοινωνία έχει ως μέσο μετάδοσης την γήινη ατμόσφαιρα ή το διάστημα.

1.5.1 Κατηγορίες ασύρματων δικτύων

Τα ασύρματα δίκτυα μπορούν να διαιρεθούν σε τρεις κύριες κατηγορίες:

- **Διασύνδεση συστήματος**

- **Ασύρματα LAN**

- **Ασύρματα WAN**

Τα ασύρματα τοπικά δίκτυα ή WLAN παρέχουν σύνδεση χωρίς καλώδια μεταξύ φορητών υπολογιστών, επιτραπέζιων υπολογιστών, εκτυπωτών, PDA και του δικτύου του γραφείου σας μέσω ασύρματων σημείων πρόσβασης. Όπως βλέπουμε παρακάτω στην εικόνα 1-4.

Τα στοιχεία τα οποία χρειάζεται ένα WLAN για να λειτουργήσει, καθώς και για να συνδεθεί στο ευρύτερο δίκτυο, είναι:

- **Προσαρμογείς : που λειτουργούν ως συνδετικά στοιχεία μεταξύ του τελικού εξοπλισμού του χρήστη και του σημείου ασύρματης πρόσβασης του δικτύου.**

- **Σημεία πρόσβασης: που είναι πομποδέκτες με μία ή δύο κεραίες. Συνδέονται με το ενσύρματο τοπικό δίκτυο. Μέσω αυτών, επικοινωνεί ο προσαρμογέας του τελικού χρήστη με το υπόλοιπο δίκτυο.**

- **Γέφυρες: Παρέχουν την από σημείο σε σημείο ασύρματη σύνδεση μεταξύ δύο WLANs, όπως μεταξύ δύο ορόφων.**

- **Κόμβοι Διανομής: Συγκεντρώνουν και συνδέουν πολλαπλά σημεία ασύρματης πρόσβασης με το ενσύρματο ή ασύρματο δίκτυο κορμού.**

- **Κόμβοι κορμού: Διασύνδεουν τους κόμβους διανομής. Καλύπτουν πολλούς χρήστες, λόγω του μεγάλου αριθμού των σημείων πρόσβασης που είναι συνδεδεμένα μέσω των κόμβων διανομής με αυτά. Σχεδόν πάντα επικοινωνούν μεταξύ τους, με περισσότερες από μία συνδέσεις, για να μειωθούν περιπτώσεις απώλειας επαφής.**

Εικόνα 1-4: Ασύρματο τοπικό δίκτυο ή WLAN

Ένα **ασύρματο WAN** (Wide Area Network) είναι ένα δίκτυο ασύρματων υπηρεσιών που λειτουργεί πέρα από ένα κτίριο και παρέχεται από κάποιον φορέα, όπως το φορέα κινητής τηλεφωνίας που χρησιμοποιείτε. Σε ένα ασύρματο WAN, μπορείτε να μεταβείτε ασύρματα στο δίκτυο φωνητικών υπηρεσιών ή δεδομένων αντί να συνδέσετε το notebook σε μια τηλεφωνική υποδοχή και να καλέσετε τον αριθμό σύνδεσης στο Internet ή να συνδεθείτε σε ένα δημόσιο hot spot. Σε ένα WAN, κάθε φορητή συσκευή επικοινωνεί με το σταθμό βάσης της υπηρεσίες παροχής.

1.6 Διαδίκτυα

Υπάρχουν πολλά δίκτυα στον κόσμο, συχνά με διαφορετικό υλικό και λογισμικό. Οι άνθρωποι που συνδέονται σε ένα δίκτυο θέλουν συχνά να επικοινωνούν με ανθρώπους που είναι συνδεδεμένοι σε κάποιο άλλο δίκτυο. Μερικές φορές αυτό επιτυγχάνεται μέσω μηχανών που ονομάζονται πύλες δικτύου (gateways), οι οποίες υλοποιούν την σύνδεση και παρέχουν τις απαιτούμενες μετατροπές τόσο από πλευράς υλικού, όσο και πλευράς λογισμικού. Ένα σύνολο διασυνδεδεμένων δικτύων ονομάζεται διαδίκτυο (internet). Μια συνηθισμένη μορφή διαδικτύου είναι ένα σύνολο LAN τα όποια είναι συνδεδεμένα μέσω ενός WAN.

Κεφάλαιο 2ο

Ασφάλεια και ακεραιότητα δεδομένων

2.1 Ασφάλεια

Κατά τις πρώτες δεκαετίες της ύπαρξης τους, τα δίκτυα υπολογιστών χρησιμοποιούνταν κυρίως από τους πανεπιστημιακούς ερευνητές για αποστολή ηλεκτρονικού ταχυδρομείου και από τους υπάλληλους των εταιριών για κοινή χρήση εκτυπωτών. Υπό αυτές τις συνθήκες, δεν δινόταν και πολλή σημασία στην ασφάλεια. Στις μέρες μας, όμως που εκατομμύρια άνθρωποι χρησιμοποιούν τα δίκτυα για τραπεζικές συναλλαγές, αγορές, και υποβολή φορολογικών δηλώσεων, η ασφάλεια των δικτύων είναι τεράστιο πρόβλημα. Η ασφάλεια ασχολείται με όσους προσπαθούν να προσπελάσουν απομακρυσμένες υπηρεσίες τις οποίες δεν είναι εξουσιοδοτημένοι να χρησιμοποιούν. Τα περισσότερα προβλήματα ασφάλειας προκαλούνται σκόπιμα από κακόβουλα άτομα τα όποια προσπαθούν να αποκομίσουν κάποιο κέρδος, να προσελκύσουν την προσοχή, η να βλάψουν κάποιο.

Η έννοια της **ασφάλειας Δικτύου Υπολογιστών** σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων τους. Εκτός αυτού, θεωρείται ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την

τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί μέσω των δικτύων και συστημάτων αυτών

2.2 Προβλήματα σαφάλειας διαδικτύου

Τα **προβλήματα ασφάλειας δικτύου** μπορούν να υποδιαιρεθούν σε τέσσερις στενά αλληλένδετους τομείς:

- **Μυστικότητα**
- **Πιστοποίηση ταυτότητας**
- **Μη αποκήρυξη**
- **Έλεγχος ακεραιότητας**

Η **μυστικότητα** (secrecy), η όποια ονομάζεται και εμπιστευτικότητα (confidentiality), προσπαθεί να διατηρήσει τις πληροφορίες μακριά από τα χεριά των μη εξουσιοδοτημένων χρηστών.

Η **πιστοποίηση ταυτότητας** (authentication) ασχολείται με τον προσδιορισμό του συνομιλητής μας πριν αποκαλύψουμε προσωπικά δεδομένα ή στοιχειά λογαριασμού για συναλλαγή σε μια αγορά.

Η **μη αποκήρυξη** (nonrepudiation) ασχολείται με τις υπόγραφες.

Τέλος ο **έλεγχος ακεραιότητας** ασχολείται με το εάν το μήνυμα που έλαβε κάποιος ήταν αυτό που στάλθηκε, και όχι κάτι που τροποποιήθηκε στην διαδρομή.

Όλα αυτά τα ζητήματα (μυστικότητα, πιστοποίηση ταυτότητας, μη αποκήρυξη , και έλεγχος ακεραιότητας) εμφανίζονται και στα παραδοσιακά συστήματα, αλλά με ορισμένες σημαντικές διαφορές. Η ακεραιότητα και η μυστικότητα επιτυγχάνονται με χρήση συστημένου ταχυδρόμου και με κλείδωμα των εγγράφων. Οι άνθρωποι πιστοποιούν την ταυτότητα των άλλων αναγνωρίζοντας τα πρόσωπα, τις φωνές, και το γραφικό χαρακτήρα τους. Καμία όμως από τις επιλογές αυτές δεν είναι διαθέσιμη ηλεκτρονικά.

2.3 Το μοντέλο αναφοράς OSI και τρόποι αποφυγής επιθέσεων σε κάθε επίπεδο

Το μοντέλο αναφοράς OSI (Open Systems Interconnection Διασύνδεση Ανοιχτών Συστημάτων) αναφέρεται σε συνδέσεις ανοιχτών συστημάτων δηλαδή αυτά τα οποία είναι ανοιχτά για επικοινωνία με άλλα συστήματα . Το μοντέλο OSI έχει εφτά επίπεδα.

2.3.1 Φυσικό Επίπεδο

Το **φυσικό επίπεδο** καλύπτει τη φυσική διεπαφή ανάμεσα σε συσκευές και τους κανόνες με τους οποίους τα bit μεταδίδονται από τη μια στην άλλη. Το φυσικό επίπεδο έχει τέσσερα σημαντικά χαρακτηρίστηκα:

- **Μηχανικό : Σχετίζεται με τις φυσικές ιδιότητες της διεπαφής σε ένα μέσο μετάδοσης. Τυπικά η προδιαγραφή είναι η υποδοχή που ενώνει έναν ή περισσότερους αγωγούς σημάτων, που ονομάζονται κυκλώματα.**

- **Ηλεκτρονικό : Σχετίζεται με την αναπαράσταση των bit και τον ρυθμό μετάδοσης τους.**
- **Λειτουργικό : Καθορίζει τις λειτουργιές που εκτελούνται από ανεξάρτητα κυκλώματα της φυσικής διεπαφής ανάμεσα σε ένα σύστημα και στο μέσο μετάδοσης .**

- **Διαδικαστικό : Καθορίζει την ακολουθία γεγονότων κατά τα όποια σειρές από bit ανταλλάσσονται μέσω ενός φυσικού μέσου.**

Στο φυσικό επίπεδο, οι υποκλοπές μπορούν να αποφευχθούν τοποθετώντας τις γραμμές μετάδοσης σε σφραγισμένους σωλήνες που περιέχουν κάποιο αέριο σε υψηλή πίεση. Κάθε προσπάθεια τρυπήματος του σωλήνα απελευθερώνει μια ποσότητα από το αέριο με αποτέλεσμα να μειώνεται η πίεση του και να ενεργοποιείται κάποιος πιθανός συναγερμός.

2.3.2 Επίπεδο Συνδέσμου

Ενώ στο φυσικό επίπεδο παρέχει μόνο υπηρεσίες σε μια ακατέργαστη σειρά από bit, στο **επίπεδο συνδέσμου** επιχειρεί να κάνει τη φυσική ζεύξη αξιόπιστη και να παρέχει τα μέσα για την ενεργοποίηση, επισκευή και απενεργοποίηση της ζεύξης. Η κυρία υπηρεσία που παρέχεται από το στρώμα ζεύξης δεδομένων σε υψηλοτέρα στρώματα είναι η ανίχνευση και ο έλεγχος σφαλμάτων. Έτσι με ένα πλήρως λειτουργικό πρωτόκολλο στρώματος ζεύξης δεδομένων όπως HDLC, LAPB, LLC και LAPD, το

αμέσως υψηλότερο στρώμα μπορεί υποθέτει ότι η μετάδοση στη ζεύξη είναι απαλλαγμένη από σφάλματα. Παρόλα αυτά, αν η επικοινωνία εκτελείται ανάμεσα σε δυο συστήματα που δεν είναι άμεσα συνδεδεμένα η σύνδεση θα αποτελείται από έναν αριθμό ζεύξεις δεδομένων στη σειρά, που η καθεμία λειτούργει ανεξάρτητα.

Επίσης στο επίπεδο ζεύξεις , τα πακέτα σε μια γραμμή από σημείο σε σημείο μπορούν να κρυπτογραφούνται καθώς αφήνουν τη μια μηχανή και να αποκρυπτογραφούνται καθώς εισέρχονται σε μια άλλη. Όμως αυτός ο μηχανισμός αποτυγχάνει, όταν τα πακέτα πρέπει να διέλθουν από πολλούς δρομολογητές, επειδή τα πακέτα πρέπει να αποκρυπτογραφούνται σε κάθε δρομολογητή, γεγονός που τα κάνει ευάλωτα σε επιθέσεις στο εσωτερικό του δρομολογητή. Πάντως η κρυπτογράφηση συνδέσμου , όπως ονομάζεται αυτή η μέθοδος, μπορεί να προστεθεί εύκολα σε οποιοδήποτε δίκτυο και συχνά είναι χρήσιμη. Τέλος τα υψηλοτέρα στρώματα δεν απαλλάσσονται από την ευθηνή για έλεγχο σφαλμάτων.

2.3.3 Επίπεδο Δικτύου

Το **επίπεδο δικτύου** παρέχει υπηρεσίες για τη μεταφορά πληροφορίας ανάμεσα σε τερματικά συστήματα ενός τηλεπικοινωνιακού δικτύου. Απαλλάσσει τα υψηλότερα στρώματα από την ανάγκη να γνωρίζουν οτιδήποτε σχετικά με την υποκείμενη μετάδοση δεδομένων και τις τεχνολογίες μεταγωγής που χρησιμοποιούνται για να συνδέουν συστήματα. Σε αυτό το στρώμα ο υπολογιστής εμπλέκεται σε ένα διάλογο με το δίκτυο για να καθορίσει τη διεύθυνση προορισμού και να ζητήσει συγκεκριμένες υπηρεσίες δικτύου, όπως προτεραιότητα.

Υπάρχει ένα φάσμα από ενδιάμεσες υπηρεσίες επικοινωνιών που μπορεί να διαχειριστεί το στρώμα δικτύου. Στην ακραία περίπτωση, όπου υπάρχει άμεση point- to - point ζεύξη ανάμεσα σε σταθμούς, μπορεί να μην υπάρχει η

ανάγκη για στρώμα δικτύου επειδή το στρώμα ζεύξης δεδομένων μπορεί να εκτελέσει την αναγκαία λειτούργει της διαχείρισης της ζεύξης. Έπειτα, τα συστήματα μπορεί να είναι συνδεδεμένα σε ένα απλό δίκτυο, όπως ένα δίκτυο μεταγωγής κυκλώματος ή ένα δίκτυο μεταγωγής πακέτου. Στην άλλη ακραία περίπτωση δυο τερματικά συστήματα που να επιθυμούν να επικοινωνήσουν μπορεί να μην είναι καν συνδεδεμένα στο ίδιο δίκτυο. Αντί αυτού, είναι συνδεδεμένα σε δίκτυα έτσι ώστε άμεσα ή έμμεσα είναι συνδεδεμένα το ένα με το άλλο. Αυτή η περίπτωση απαιτεί τη χρήση κάποιου είδους τεχνικής διαδικτυακής.

Στο **επίπεδο δικτύου** μπορούν να εγκατασταθούν ζώνες (firewalls), οι οποίες θα διατηρούν τα καλά πακέτα εντός του δικτύου και τα κακά πακέτα εκτός. Η ασφάλεια IP λειτούργει επίσης στο επίπεδο αυτό. Ένα βασικό θέμα στη σχεδίαση του δικτύου είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την αφετηρία στον προορισμό τους. Οι διαδρομές θα μπορούσαν να βασιστούν σε στατικούς πίνακες οι οποίοι είναι «καλωδιωμένοι» στο δίκτυο και σπάνια τροποποιούνται. Ακόμη θα μπορούσαν να οριστούν στην αρχή κάθε συνομιλίας , για παράδειγμα μιας συνόδου τερματικών. Τέλος θα μπορούσαν να είναι δυναμικές και να καθορίζονται εκ νέου για κάθε πακέτο για να απεικονίζουν το τρέχων φορτίο του δικτύου. Εάν στο υποδίκτυο είναι παρόντα πολλά πακέτα την ίδια χρονική στιγμή, θα εμπλακεί το ένα στην διαδρομή του άλλου, δημιουργώντας συμφόρηση (bottleneck) . Ο έλεγχος μιας τέτοιας συμφόρησης επίσης ανήκει στις αρμοδιότητες του επιπέδου δικτύου.

2.3.4 Επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς παρέχει ένα μηχανισμό για την ανταλλαγή δεδομένων ανάμεσα σε τερματικά συστήματα. Η υπηρεσία μεταφοράς με σύνδεση εξασφαλίζει ότι τα δεδομένα παραδίδονται απαλλαγμένα από σφάλματα, στη σωστή σειρά, χωρίς απώλειες ή πολλαπλά αντίγραφα. Το στρώμα μεταφοράς μπορεί επίσης να σχετιστεί με την βελτιστοποίηση της χρήσης των υπηρεσιών δικτύου όπως επίσης και για να παρέχει μια ζητούμενη ποιότητα υπηρεσίας στις οντότητες συνόδου. Για παράδειγμα, η οντότητα συνόδου μπορεί να καθορίσει αποδεκτούς ρυθμούς σφαλμάτων, μεγίστη καθυστέρηση, προτεραιότητα και ασφάλεια.

Το μέγεθος και η πολυπλοκότητα ενός πρωτοκόλλου μεταφοράς εξαρτάται από το ποσό αξιόπιστα ή αναξιόπιστα είναι το υποκείμενο δίκτυο και οι υπηρεσίες του στρώματος δικτύου. Ως επακόλουθο, ο ISO έχει αναπτύξει μια οικογένεια από πέντε πρότυπα πρωτόκολλων μεταφοράς, το καθένα για διαφορετικές υποκείμενες υπηρεσίες. Στη στοίβα πρωτόκολλων TCP/IP υπάρχουν δυο συνηθισμένα πρωτοκολλά στρώματος μεταφοράς : το TCP Πρωτόκολλο Έλεγχου Μετάδοσης που προσφέρει υπηρεσίες με σύνδεση και το UDP Πρωτόκολλο Αυτόνομων Πακέτων Χρηστή που προσφέρει υπηρεσίες χωρίς σύνδεση.

Σε **επίπεδο μεταφοράς** μπορούν να κρυπτογραφούνται ολόκληρες συνδέσεις απ' άκρου εις άκρο, δηλαδή από διεργασία σε διεργασία. Για μεγίστη ασφάλεια, απαιτείται ασφάλεια από άκρο σε άκρο. Η βασική λειτουργιά του επίπεδου μεταφοράς είναι η αποδοχή δεδομένων, η διάσπαση αυτών σε μικρότερες μονάδες αν χρειαστεί , η μεταφορά τους στο επίπεδο δικτύου και η διασφάλιση ότι όλα τα τμήματα φτάνουν σωστά στην άλλη πλευρό. Τέλος, ζητήματα όπως η πιστοποίηση ταυτότητας των χρηστών και η μη αποκήρυξη μπορούν να αντιμετωπίσουν μόνο σε επίπεδο εφαρμογών.

2.3.5 Επίπεδο Συνόδου

Τα τέσσερα χαμηλότερα στρώματα του μοντέλου OSI παρέχουν τα μέσα για την αξιόπιστη ανταλλαγή των δεδομένων και μπορεί να παρέχουν διαφορές επιλογές ποιότητας υπηρεσίας. Για πολλές εφαρμογές η βασική υπηρεσία είναι ανεπαρκής. Για παράδειγμα, μια εφαρμογή απομακρυσμένης πρόσβασης τερματικού μπορεί να απαιτεί ημιαμφίδρομο (half –duplex) διάλογο. Μια εφαρμογή επεξεργασίας συναλλαγών μπορεί να απαιτεί σημεία έλεγχου στη ροη μεταφοράς δεδομένων που να επιτρέπουν τη δημιουργία αντίγραφων και ανάκτηση της πληροφορίας. Μια εφαρμογή επεξεργασίας μηνυμάτων μπορεί να απαιτεί την ικανότητα να διακόπτεται ένας διάλογος για να προετοιμαστεί ένα νέο μέρος ενός μηνύματος και αργότερα να συνεχιστεί ο διάλογος από το σημείο που διακόπηκε.

Το στρώμα συνόδου παρέχει το μηχανισμό για τον έλεγχο του διαλόγου ανάμεσα σε εφαρμογές και τερματικά συστήματα. Σε πολλές περιπτώσεις θα υπάρχει μικρή ή καθόλου ανάγκη για υπηρεσίες στρώματος συνόδου, όμως σε μερικές εφαρμογές χρησιμοποιούνται τέτοιες υπηρεσίες. Οι κυριότερες υπηρεσίες που παρέχονται από το στρώμα συνόδου περιλαμβάνουν τα παρακάτω:

- **Τρόπος διαλόγου: Μπορεί να είναι δύο κατευθύνσεων ταυτόχρονα (full- duplex) ή δυο κατευθύνσεων εναλλάξ (half – duplex).**

- **Ομαδοποίηση: Η ροη των δεδομένων μπορεί να σημειωθεί έτσι ώστε να καθορίζονται ομάδες δεδομένων.**

- **Ανάκτηση: Το στρώμα συνόδου μπορεί να παρέχει έναν μηχανισμό με σημεία έλεγχου έτσι ώστε, αν συμβεί κάποιου είδους βλάβη ανάμεσα στα σημεία έλεγχου η οντότητα συνόδου να**

μπορεί να επαναμεταδώσει όλα τα δεδομένα από το τελευταίο σημείο OSI

2.3.6 Επίπεδο Παρουσίασης

Το στρώμα παρουσίασης καθορίζει τη μορφή των δεδομένων που πρόκειται να ανταλλαγούν ανάμεσα στις εφαρμογές και προσφέρει στα προγράμματα εφαρμογών ένα σύνολο υπηρεσιών μετασχηματισμού δεδομένων. Το στρώμα παρουσίασης καθορίζει τη σύνταξη που χρησιμοποιείται ανάμεσα στις οντότητες εφαρμογών και προνοεί για την επιλογή και ακολούθως την μετατροπή της αναπαράστασης που χρησιμοποιείται. Παράδειγμα συγκεκριμένων υπηρεσιών που μπορούν να εκτελεστούν σε αυτό το στρώμα περιλαμβάνουν τη συμπίεση και την κρυπτογράφηση δεδομένων.

2.3.7 Επίπεδο Εφαρμογής

Το στρώμα εφαρμογής παρέχει το μέσο ώστε τα προγράμματα εφαρμογών να έχουν πρόσβαση στο περιβάλλον OSI. Αυτό το στρώμα περιλαμβάνει διαχειριστικές λειτουργιές και γενικά χρησίμους μηχανισμούς για την υποστήριξη κατανεμημένων εφαρμογών. Επιπλέον, εφαρμογές γενικού σκοπού όπως η μεταφορά αρχείων, το ηλεκτρονικό ταχυδρομείο και η πρόσβαση τερματικού σε απομακρυσμένους υπολογιστές βρίσκονται σε αυτό το στρώμα.

Το επίπεδο εφαρμογής περιέχει μια ποικιλία πρωτοκόλλων που χρειάζονται συχνά. Για παράδειγμα μπορούμε να αναφέρουμε το λογισμικό των νοητών

τερματικών δικτύων (network virtual terminals) ή την εφαρμογή της μεταφοράς αρχείων. Στην τελευταία περίπτωση διαφορετικά συστήματα αρχείων έχουν διαφορετικούς μεθόδους καθορισμού ονομασίας , διαφορετικούς τρόπους αναπαράστασης των γραμμών κειμένου και ούτω καθεξής. Η μεταφορά ενός αρχείου μεταξύ δύο διαφορετικών συστημάτων απαιτεί αντιμετώπιση αυτών και άλλων μη συμβατών καταστάσεων. Η εργασία αυτή επίσης ανήκει στο επίπεδο εφαρμογής, όπως η εμφάνιση καταλόγων αρχείων και διάφορες άλλες ειδικού και γενικού σκοπού ευκολίες.

2.4 Μέθοδοι επίθεσης

2.4.1 Daniel – of – services (DoS)

Μια από τις πλέον διάσημες και αποτελεσματικές μεθόδους επίθεσης που χρησιμοποιούν οι crackers για να θέτουν εκτός λειτουργιάς δικτυωμένους υπολογιστές είναι οι επίθεσης **DoS.** Το όνομα της τεχνικής (άρνηση εξυπηρέτησης) οφείλεται στο γεγονός ότι ο υπολογιστής – θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων – πελατών (clients) εξαιτίας του τεράστιου πλήθους εικονικών αιτήσεων που δέχεται από τον επιτιθέμενο. Υπάρχουν διάφορα ειδή επιθέσεων **DoS,** πολλά από τα όποια εκμεταλλεύονται εγγενείς αδυναμίες του TCP/IP. Για τα περισσότερα από αυτά, είναι ήδη γνωστά τα αντίστοιχα μετρά προστασίας. Συγκεκριμένα οι διαχειριστές συστημάτων μπορούν να εγκαθιστούν patches σε λειτουργικά συστήματα και προγράμματα – διακομιστές,

ώστε να αποτρέπουν επίθεσης **DoS** ή να ελαχιστοποιούν τις συνέπειες τους. Όπως όμως, συμβαίνει και με τους ιούς υπολογιστών, κατά καιρούς

εφευρίσκονται νέα ειδή ή παραλλαγές επιθέσεων **DoS** . Παρακάτω θα δούμε εν συντομία τέσσερις από τις διασημότερες παραλλαγές .

2.4.2 Ping of Death

Αίτηση PING ή αλλιώς, αίτηση ICMP (Internet Control Message Protocol) προς τον υπολογιστή – στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή (header) πάνω από 64Kb. Αυτού του είδους πακέτα μπορούν να καταστρέψουν υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα διαχειριστούν.

2.4.3 Smurf Attack

Επίθεση που επιτυγχάνεται αποστέλλοντας αιτήσεις ICMP σε μια διεύθυνση εκπομπής στο υπό επίθεση δίκτυο ή σε κάποιο άλλο ενδιάμεσο. Η διεύθυνση επιστροφής (return address) των πακέτων ICMP παραποιείται, ώστε να είναι ιδία με τον υπολογιστή – στόχου. Από την στιγμή που μια διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου , λειτούργει ενισχυτικά, δημιουργώντας με μια μόνο αίτηση ICMP δεκάδες ή και εκατοντάδες απαντήσεις, προκαλώντας με τον τρόπο αυτό πληροφοριακό “μποτιλιάρισμα.

2.4.4 SYN Flood Attack

Πριν εγκαθιδρυθεί μια σύνοδος (session) μεταξύ ενός πελάτη και ενός διακομιστεί, λαμβάνει χώρα μια ακολουθία τριών βημάτων, γνωστή και ως "ακολουθία χειραψίας" (handshaking sequence). Εάν ο πελάτης αγνοήσει την τελευταία απάντηση SYN – ACK (SYNchronize –ACKnowledge) του διακομιστεί, ο τελευταίος θα επιμένει για ένα προκαθορισμένο χρονικό διάστημα. Ένας εισβολέας μπορεί να εκμεταλλευτεί τη συγκεκριμένη συμπεριφορά για να υπερφορτώσει το διακομιστεί – θύμα ή ακόμα και για να τον οδηγήσει σε καταρρεύσει. Κατά τη διάρκεια μιας τέτοιας επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση (IP address), κρύβοντας με τον τρόπο αυτό τα ίχνη του.

2.4.5 Teardrop Attack

Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων IP. Όταν ένα τέτοιο πακέτο αποστέλλεται στο διαδίκτυο, ενδέχεται να ταξιδεύει τεμαχισμένο σε επιμέρους μικρότερα τμήματα. Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο, όπου περιγράφεται η θέση του στο αρχικό, πακέτο IP. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, ονόματι " Teardrop", το οποίο τεμαχίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στο πεδίο αυτό. Όταν ο υπολογιστής – στόχος προσπαθήσει να συναρμολογήσει τα "παραπλανητικά" αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσεις, εκτός και αν ο διαχειριστής συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο patch που διορθώνει το πρόβλημα.

Όταν σε μια επίθεση DoS συμμετέχουν περισσότερα του ενός μηχανήματα, έχουμε τις λεγόμενες κατανεμημένες επιθέσεις ή DDoS (Distributed Daniel of Services). Στις επιθέσεις αυτού του είδους, είναι δυνατό να συμμετέχουν και

προσωπικοί υπολογιστές, ακόμα και οικιακοί προσωπικοί υπολογιστές, χωρίς να το γνωρίζουν οι χρηστές τους. Ο επιτιθέμενος κατορθώνει με κάποιον τρόπο να τοποθετήσει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα που θα συμμετάσχουν, εν αγνοία τους, στην επίθεση. Τη στιγμή που αποφασίζει να εξαπολύσει την επίθεση στέλνει μια ειδοποίηση σε ένα από αυτά (διακομιστείς DDoS). Τότε, εκείνο ειδοποιεί σε μια συγκεκριμένη χρονική στιγμή καθέναν από τους υπόλοιπους υπολογιστές (πελάτες DDoS) και όλοι μαζί αρχίζουν να βάλλουν κατά του στόχου με πλαστές αιτήσεις. Το αποτέλεσμα είναι εκείνος να “πλημμυρίσει ” και να μη μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών. Ένας καλός τρόπος για να προστατεύσουμε τους υπολογιστές μας, ώστε να μη χρησιμοποιούνται εν αγνοία μας, είναι να χρησιμοποιούμε κάποιο προσωπικό πρόγραμμα φράγματος ασφάλειας (firewall).

2.4.6 sniffers

Από τα παλαιότερα εργαλεία που χρησιμοποιούνται και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά δικτύων και να εντοπίζουν πιθανά προβλήματα είναι τα λεγόμενα “sniffer”. Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να “υποκλέπτει ” δεδομένα που ταξιδεύουν σε ένα δίκτυο. Ωστόσο, όπως έχει ήδη γίνει προφανές, τις υπηρεσίες τους μπορούν να εκμεταλλευτούν και οι crackers για την υλοποίηση των παράνομων δραστηριοτήτων τους. Για παράδειγμα, ο cracker μπορεί να χρησιμοποιεί ένα sniffer για να υποκλέπτει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών και διάφορα αλλά προσωπικά στοιχειά χρηστών.

Ο προφανής τρόπος για να προστατευτεί ένα δίκτυο από την επιβλαβή χρήση των sniffer είναι να υπάρχει αυστηρή επίβλεψη στα προγράμματα που εγκαθιστούν οι χρηστές στους υπολογιστές. Εάν ένας cracker δε μπορεί να

αποκτήσει φυσική πρόσβαση σε κάποιον υπολογιστή, τότε αδυνατεί να εγκαταστήσει ένα sniffer. Άλλος ένας τρόπος προστασίας από τους sniffers είναι η αποστολή δεδομένων σε κρυπτογραφημένη μορφή.

2.4.7 Σάρωση Θυρών (Port Scanning)

Μια άλλη τεχνική που χρησιμοποιούν διαχειριστές και crackers, καθένας για διαφορετικούς σκοπούς , είναι η σάρωση θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομίστες, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφάλειας. Από την στιγμή που εισβολέας γνωρίζει ποιες υπηρεσίες προσφέρει το μηχάνημα - στόχος , μπορεί στη συνεχεία να σχεδιάσει την επίθεση του βασιζόμενος σε γνώστες αδυναμίες των προσφερόμενων υπηρεσιών. Υπάρχουν διάφορα εργαλεία για την αποτροπή της σάρωσης θυρών (port scanning). Όπως η χρήση κάποιου προσωπικού προγράμματος "φράγματος ασφάλειας " (firewall).

2.4.8 Μη Εξουσιοδοτημένη Πρόσβαση

Όσα μετρά ασφάλειας και αν ληφθούν, πάντοτε τα χρησιμοποιούμενα προγράμματα θα είναι ατελή υπό την έννοια ότι θα παρουσιάζουν αδυναμίες τις οποίες ενίοτε θα εκμεταλλεύονται οι crackers. Πρόκειται για τα λεγόμενα "exploits", δηλαδή προγραμματιστικές αδυναμίες σε γνώστες και ευρέως χρησιμοποιούμενες εφαρμογές, τις οποίες να αξιοποιούν οι crackers για να αποκτούν μη εξουσιοδοτημένη πρόσβαση. Όπως η τεχνική IP spoofing

χρησιμοποιείται για την αποκτήσει μη εξουσιοδοτημένης πρόσβασης σε δικτυωμένα μηχανήματα. Ο εισβολέας αποστέλλει μηνύματα με διεύθυνσης IP που υποδεικνύουν ότι αυτά προέρχονται από ένα έμπιστο port. Ο cracker αρχικά καταφεύγει σε ένα πλήθος τεχνικών για να βρει μια διεύθυνση IP που αντιστοιχεί σε μια τέτοια θύρα. Στην συνεχεία, τροποποιεί τα περιεχόμενα της κεφαλής των πακέτων που θα αποστείλει, ώστε να φαίνεται ότι προέρχονται από μια έμπιστη θύρα. Οι εταιρείες υπολογιστών προσπαθούν να αντιμετωπίσουν τα προβλήματα ασφάλειας παρέχοντας στους χρηστές αναβαθμίσεις ή διορθώσεις .

2.4.9 Ιοί και bugs

2.4.9.1 Ιοί

Οι “ιοί” είναι προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκριση μας και να μολύνουν αλλά αρχεία. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι από μηδαμινές έως και καταστροφικές σε έναν υπολογιστή. Ο ιός θα προσπαθήσει να αναπαραχθεί και να πολλαπλασιαστεί έτσι έστω να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία αλλά και άλλους υπολογιστές που είναι συνδεδεμένη σε τοπικό επίπεδο ή μέσω διαδικτύου.

Υπάρχουν αρκετά ειδή ιών, όπως:

- **Οι ιοί που προσβάλλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου (boot sector viruses) αν και είναι σχετικά σπάνιοι σήμερα.**

- **Αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program/ file viruses)**

- **Αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών (Macro viruses), όπως του Word και του Excel.**

- **Οι πολυμορφικοί, οι όποιοι μπορεί να ανήκουν σε μερικές ή και σε όλες τις προαναφερόμενες κατηγορίες.**

Υπάρχει και μια ειδική κατηγορία ιών, η όποια εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως , για παράδειγμα, το Outlook Express, με αποτέλεσμα ένα απλό κείμενο ηλεκτρονικού ταχυδρομείου να προκαλέσει ζημία. Βεβαία, οι ιοί αυτοί είναι σπάνιοι και εξουδετερώνονται με την εγκατάσταση νεοτέρων εκδόσεων των εφαρμογών που στο παρελθόν παρουσίασαν προβλήματα.

2.4.9.2 Bugs

Τα bugs κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Η μέθοδος επίθεσης τους είναι ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καλυμμένα / παραλλαγμένα μηνυμάτων ηλεκτρονικού ταχυδρομείου σε όλη την λίστα επαφών. Με αποτέλεσμα ανυποψίαστη χρήστες να λαμβάνουν μηνύματα από γνωστούς, και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο με καταστροφικές συνέπειες για τον υπολογιστή του. Η μαζική αποστολή μηνυμάτων e-mail, εκτός από την κατασπατάληση του εύρους ζώνης, ιδίως των συνδέσεων με modem ανεξαρτήτων χρηστώ, επιβαρύνει

δραματικά τους κεντρικούς εξυπηρετητές αλληλογραφίας του διαδικτύου, με αποτέλεσμα να τίθενται συχνά εκτός λειτουργιάς.

2.4.10 Trojan horses

Δεν θα ήταν υπερβολή αν λέγαμε ότι μετά τους ιούς ο μεγαλύτερος κίνδυνος για τους χρηστές του Διαδικτύου είναι οι **"Δούρειοι Ίπποι" (Trojan horses)**. Πρόκειται για προγράμματα που αποτελούνται από δυο μέρη τον πελάτη|(client) και τον εξυπηρετητή (server). Ο "Εξυπηρετητής Δούρειος Ίππος" (Trojan – server) "φωλιάζει" στον υπολογιστή του θύματος και ο "πελάτης" (Trojan – client) τρέχει στο μηχάνημα του θύτη. Από την στιγμή που ο cracker αποκτά πρόσβαση στον υπολογιστή στόχο, μπορεί αναλόγως το είδος του "Δούρειου Ίππου" να διαγράψει αρχεία ή ακόμα και να προκαλέσει ζημίες στο υλικό του υπολογιστή, όπως να του διαγράψει τα BIOS ή να χτυπήσει τις κεφάλες του σκληρού δίσκου. Μια ακόμη λειτουργιά των Δούρειων Ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα, με αποτέλεσμα αν το θύμα πληκτρολογεί κωδικούς πρόσβασης, το πρόγραμμα τα καταγράφει και τα στέλνει αργότερα στον εισβολέα.

Ένας Δούρειος Ίππος μπορεί να "εισαχθεί" στον υπολογιστή μας από ένα μήνυμα με επισυναπτόμενο αρχείο στο ηλεκτρονικό ταχυδρομείο ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ. ένα παιχνίδι με ευρεία διάδοση. Υπάρχουν δυο τρόποι να αποφύγουμε τους "Δούρειους Ίππους". Ο πρώτος είναι να χρησιμοποιήσουμε ένα πρόγραμμα "Antivirus" ή "AntiTrojan". Πολλά προγράμματα της κατηγορίας αυτής μπορούν να ανιχνεύουν ιούς και να διαγράφουν μολυσμένα αρχεία. Ο άλλος τρόπος είναι να χρησιμοποιήσουμε ένα προσωπικό φράγμα ασφάλειας. Κάθε φορά που ένας "Εξυπηρετητής Δούρειος ίππος " θα προσπαθεί να βγει στο Διαδίκτυο, το φράγμα ασφάλειας θα μας ειδοποιοί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει την μεγίστη προστασία.

2.5 Τρόποι αποφυγής επιθέσεων

Παρά την ύπαρξη πολλών κακόβουλων λογισμικών ο κίνδυνος “μόλυνσης ” μπορεί να ελαχιστοποιηθεί αν τηρηθούν μερικοί βασικοί κανόνες. Εκτός από την αναβαθμίσει των εφαρμογών που σχετίζονται με το Διαδίκτυο, είναι πλέον επιβεβλημένη η εγκατάσταση κάποιας εφαρμογής προστασίας από ιούς, η όποια χρειάζεται καθημερινή ενημέρωση , ώστε να υπάρχει αυξημένο επίπεδο προστασίας απέναντι και στους νεότερους ιούς. Τα μέτρα προστασίας ή *αντίμετρα* είναι όλες εκείνες οι διαδικασίες, τεχνικές, ενέργειες ή και συσκευές που περιορίζουν τις ευπάθειες του συστήματος. Οι διαφορετικοί τύποι αντίμετρων έχουν σαν αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας πληροφοριακών στις ακόλουθες συνιστώσες:

- ***Φυσική ασφάλεια συστήματος* (*physical security*). Αναφέρεται στη προστασία ολόκληρου του σχετικού εξοπλισμού του υπολογιστή από φυσικές καταστροφές.**

- ***Ασφάλεια υπολογιστικού συστήματος* (*computer security*). Αναφέρεται στη προστασία των πληροφοριών εκείνων του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (προγράμματα εφαρμογών, αρχεία δεδομένων κλπ.). Επικεντρώνεται κυρίως στις συγκεκριμένες υπηρεσίες των λειτουργικών συστημάτων που καθορίζουν το ποιος και πως θα δικαιούται να προσπελάσει τα δεδομένα και τις εφαρμογές που φιλοξενεί ο υπολογιστής.**

- ***Ασφάλεια βάσεων δεδομένων* (*database security*). Αναφέρεται στην ικανότητα του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, μια πολιτική που διευκρινίζει ποιοι**

εξουσιοδοτούνται να δουν ή και να τροποποιήσουν τα προστατευμένα δεδομένα.

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

2.6 Κρυπτογράφηση

Στην σημερινή κοινωνία της πληροφορίας η κρυπτογράφηση είναι ένα από τα βασικά εργαλεία διατήρησης του απορρήτου των μηνυμάτων. Στην ορολογία της κρυπτογραφίας, το αρχικό μήνυμα που προορίζεται για κρυπτογράφηση ονομάζεται *απλό κείμενο (plaintext)*. Η διαδικασία μετατροπής του περιεχομένου του μηνύματος σε μορφή τέτοια που να είναι μη κατανοητή για μη εξουσιοδοτημένους χρηστές ονομάζεται *κρυπτογράφηση*, ενώ το κρυπτογραφημένο μήνυμα ονομάζεται *κρυπτογράφημα(ciphertext)* . Η κρυπτογράφηση ενός μηνύματος πραγματοποιείται με την χρήση μιας μαθηματικής συνάρτησης η όποια ονομάζεται *κλειδί (key).* Ως *αποκρυπτογράφηση(decryption)* ορίζεται η αντίστροφη διαδικασία όπου το κρυπτογραφημένο μήνυμα με την βοήθεια του κλειδιού μετατρέπεται στο αρχικό μήνυμα.

Ως αποτέλεσμα, η σύγχρονη κρυπτογραφία αποτελεί κάτι παραπάνω από κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Για παράδειγμα η πιστοποίηση αποτελεί μια εξίσου θεμελιώδη έννοια που συνδέεται άμεσα με την κρυπτογραφία. Για παράδειγμα όταν υπογράφεται ένα έγγραφο , είναι απαραίτητο να υπάρχουν μηχανισμοί με τους οποίους μπορούμε να

πιστοποιήσουμε τον κάτοχο του έγγραφου. Η κρυπτογραφία μας παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή “συνδέει” ένα έγγραφο με τον κάτοχο ενός συγκεκριμένου κλειδιού, ενώ η ψηφιακή χρονοσφραγίδα “συνδέει” ένα έγγραφο με τον χρόνο τις δημιουργίας του.

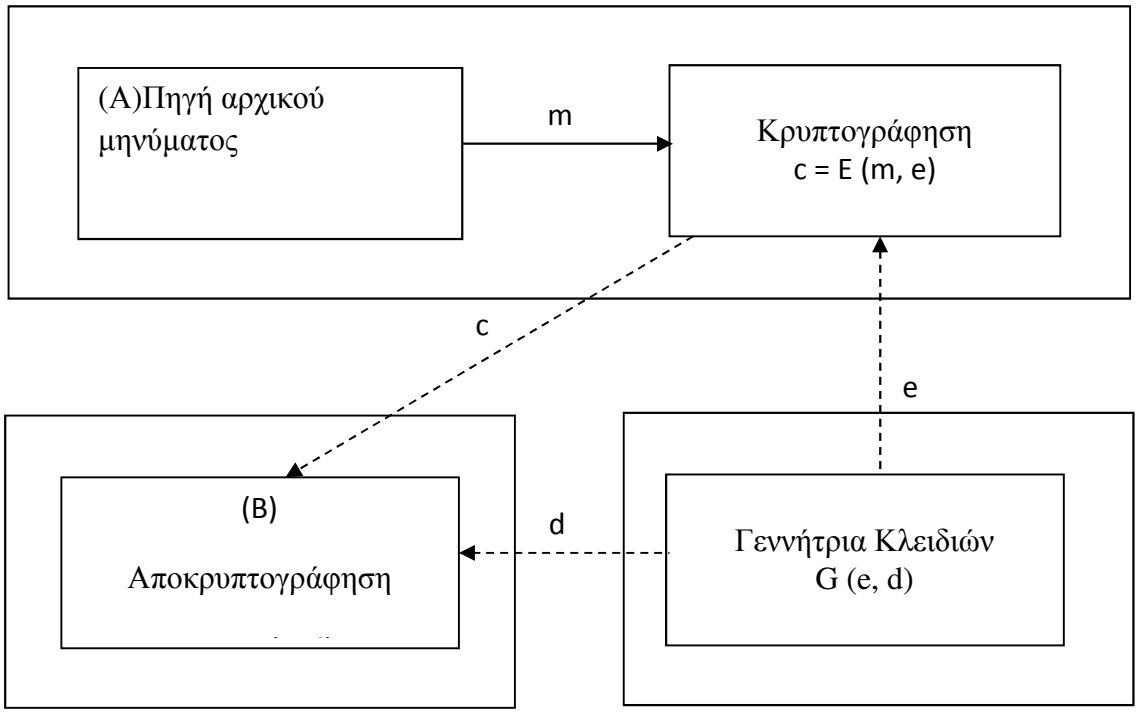
Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί στις παρακάτω εφαρμογές :

- **Προστασία δεδομένων, αποθηκευμένων σε υπολογιστή, από μη εξουσιοδοτημένη πρόσβαση.**
- **Προστασία δεδομένων κατά την μεταφορά τους ανάμεσα σε δυο υπολογιστικά συστήματα.**
- **Ανίχνευση τυχαίας ή εσκεμμένης αλλαγής σε δεδομένα.**
- **Πιστοποίηση της ταυτότητας του συντάκτη ενός κειμένου η μηνύματος.**

2.6.1 Μερικά από τα δημοφιλή κρυπτοσυστήματα

- **RSA: Πηρέ το όνομα του από τα αρχικά των επιστημόνων που το ανακάλυψαν (Rivest, Shamir, Adleman).**
- **DSA: Εξίσου γνωστή μέθοδος που χρησιμοποιείται στις ψηφιακές υπόγραφες.**
- **Diffie –Hellman: Δημοφιλής τεχνική δημόσιου κλειδιού για την εγκατάσταση ιδιωτικών κλειδιών πάνω από μη ασφαλή κανάλια επικοινωνίας.**

- **ECC (Elliptic Curve Cryptosystems): Είναι κρυπτοσυστήματα τα όποια βασίζονται σε μαθηματικά αντικείμενα γνωστά ως ελλειπτικές καμπύλες.**



Εικόνα 2-1: Γενική Μορφή Κρυπτογραφικού Συστήματος

Το σχήμα 3.1 αποτυπώνει τη γενική μορφή ενός σύγχρονου κρυπτογραφικού συστήματος. Υποθέτουμε ότι ένας χρήστης *A* και ένας χρήστης *B* θέλουν να έχουν μια ασφαλή επικοινωνία. Αρχικά, πρέπει να διαλέξουν ή να ανταλλάξουν ένα ζεύγος κλειδιών (*e,d*). Στη συνέχεια, όταν ο Α (αποστολέας) θελήσει να στείλει μυστικά δεδομένα *m* στον Β (παραλήπτη), εφαρμόζεται μια μαθηματική

2.7 Ψηφιακές Υπογραφές

Για την απόδειξη της γνησιότητας ενός εγγράφου, χρησιμοποιούνται οι συμβατικές υπογραφές. Ειδικότερα, η υπογραφή αποτελεί μαρτυρία της εγκυρότητας του υπογεγραμμένου εγγράφου έτσι ώστε ο υπογράφων να μη μπορεί να το απαρνηθεί. Στο ανοικτό περιβάλλον του Διαδικτύου, καθίσταται αναγκαία η χρησιμοποίηση ενός ηλεκτρονικού ισοδύναμου της συμβατικής υπογραφής, δηλαδή μιας ηλεκτρονικής υπογραφής. Ο μηχανισμός της ηλεκτρονικής υπογραφής θα πρέπει να παρέχει απόδειξη της προέλευσης, της γνησιότητας και της ακεραιότητας των ανταλλασσόμενων μηνυμάτων. Επιπλέον, η ηλεκτρονική υπογραφή πρέπει να δημιουργείται και να αναγνωρίζεται εύκολα, ενώ δύσκολα να πλαστογραφείται συνάρτηση Ε, η οποία χρησιμοποιεί ως παράμετρο το κλειδί *e*, με σκοπό τον υπολογισμό του κρυπτογραφήματος $c = E(m, e)$. Το κρυπτογράφημα *c* αποστέλλεται στον Β. Μόλις αυτός το λάβει, εφαρμόζεται μια αντίστροφη μαθηματική συνάρτηση D, η οποία χρησιμοποιεί το άλλο κλειδί d, με σκοπό τον υπολογισμό του $m = D(c, d)$. Οπότε ανακτώνται τα αρχικά δεδομένα *m*.

Οι ηλεκτρονικές υπογραφές που βασίζονται στη κρυπτογραφία δημοσίου κλειδιού, ονομάζονται ψηφιακές υπογραφές (*digital signatures*). Υπάρχουν δύο γενικές κατηγορίες αλγορίθμων δημόσιου κλειδιού που μπορούν να χρησιμοποιηθούν για τη δημιουργία ψηφιακών υπογραφών. Η μία κατηγορία χρησιμοποιεί αλγορίθμους κρυπτογράφησης όπως ο RSA, ενώ η άλλη χρησιμοποιεί ιδιάζοντες αλγορίθμους υπογραφής χωρίς κρυπτογράφηση. Αντιπροσωπευτικός αλγόριθμος της δεύτερης κατηγορίας είναι ο DSA, ο οποίος προτάθηκε από το NIST και βασίζεται στο σύστημα ψηφιακής υπογραφής El Gamal. Βασικό του χαρακτηριστικό είναι ότι το μήκος της υπογραφής ενός μηνύματος είναι διπλάσιο του μήκους του μηνύματος, σε αντίθεση με τον αλγόριθμο RSA όπου τα μήκη είναι ίσα.

2.8 Firewall

Ένα σύστημα firewall ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο Διαδίκτυο και στο υπό προστασία δίκτυο, επιτρέπει τη προσπέλαση των εξωτερικών χρηστών στο προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά. Έτσι ένα τυπικό σύστημα firewall μπορεί να επιτρέπει επιλεκτικά τη πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε *ονόματα επικρατειών (domain names).* Αυτός είναι ο κύριος σκοπός του: να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το προστατευμένο περιβάλλον. Επιπλέον, είναι σε θέση να ρυθμίσει και τις παρεχόμενες Διαδικτυακές υπηρεσίες για τους εσωτερικούς χρήστες. Για τη λειτουργία του αυτή δεν εξετάζει μόνο χαρακτηριστικά των χρηστών, αλλά και στοιχεία σχετικά με το προορισμό των αιτήσεων προσπέλασής τους. Ένα σύστημα λοιπόν firewall έχει σαν στόχο να ελέγχει και να καταγράφει τη πρόσβαση σε προστατευμένες υπηρεσίες, που προέρχονται και από το εσωτερικό και από το εξωτερικό του δικτύου ενός οργανισμού, με το να επιτρέπει, να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του.

Ένα firewall μπορεί να θεωρηθεί σαν ένα ζευγάρι μηχανισμών που ο ένας μπλοκάρει τη κυκλοφορία των δεδομένων και ο άλλος επιτρέπει τη ροή τους. Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της *πολιτικής* (*policy*) ελέγχου που αυτό υποστηρίζει και εξαρτάται από τη διαμόρφωσή του (*firewall configuration*). Πραγματικά, ένα σύστημα firewall δεν είναι απλά ένας *δρομολογητής* (*router*), ένας *διανομέας* ή *διακομιστής* ή εξυπηρετητής (*server*), ένας *οικοδεσπότης* (*host*) ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα. Οι αληθινές δυνατότητές του γίνονται εμφανείς αν τον θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας που καθορίζει τις παρεχόμενες υπηρεσίες και τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη-έμπιστες επικράτειες. Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων *(network access control policy)* γίνεται με την υποχρεωτική κατεύθυνση όλων των

επικοινωνιών μέσω του firewall, όπου αποτελούν αντικείμενο εξέτασης και καταγραφής.

Η τοποθέτηση ενός firewall συστήματος ανάμεσα στο τοπικό δίκτυο ενός οργανισμού και το Διαδίκτυο, εγκαθιστά δυνατότητες ελέγχου στη ροή των πληροφοριών και διασφαλίζει τη διαδικτυακή σύνδεση (*internet link*) προστατεύοντας στον οργανισμό:

- **Τους πόρους του (υλικό, λογισμικό, δεδομένα) από φθορά, κατάχρηση, κλοπή και κατάχρηση.**

- **Την υπόληψή του από τη δημοσιοποίηση αδυναμιών στην ασφάλεια του δικτύου του.**

- **Την επικρατούσα πολιτική ορθής χρήσης των υπηρεσιών του Διαδικτύου από τους εργαζομένους του.**

Όμως σπουδαίες είναι και οι υπόλοιπες επιμέρους ωφέλειες που παρέχει ένα σύστημα firewall. Αναλυτικά:

- **Επιτρέπει αποτελεσματικά την *υλοποίηση* και *διαχείριση* μέρους της *πολιτικής ασφάλειας* (*policy enforcement*) που θέλουμε να εφαρμόσουμε στο σύστημά μας.**

- ***Προστατεύει από ευπαθείς υπηρεσίες δικτύων (protecting from vulnerable services).* Είναι γνωστό ότι τα πρωτόκολλα επικοινωνίας του Διαδικτύου παρουσιάζουν εγγενή προβλήματα ασφάλειας. Η εγκαθίδρυση ενός συστήματος firewall προσφέρει δυνατότητες φιλτραρίσματος που ελαχιστοποιούν τους κινδύνους. Ακόμη μπορεί και καλύπτει γνωστές ρωγμές ασφαλείας στο**

κατώτερο επίπεδο των λειτουργικών συστημάτων. Έτσι, κάποια αδύνατα σημεία για την ασφάλεια του δικτύου, που έχουν ήδη εκμεταλλευτεί διάφοροι βάνδαλοι, έρχεται να προστατέψει και να οχυρώσει το firewall.

- **Αποτελεί μέσο *καταγραφής* και *δημιουργίας στατιστικών στοιχείων* για τη *χρήση και κατάχρηση του δικτύου (logging-alarming & statistics of network use/misuse)*. Η χρησιμότητά τους είναι μεγάλη. Τεκμηριώνουν την ικανότητα ή όχι του ίδιου του firewall για αποτροπή των επιθέσεων που συνέβησαν και κρίνουν την καταλληλότητα της πολιτικής ασφάλειας που εφαρμόζεται. Επιπλέον, τα στατιστικά χρήσης του δικτύου είναι χρήσιμα και στις διαδικασίες *ανάλυσης επικινδυνότητας (risk analysis)* και *ανάλυσης απαιτήσεων δικτύου (network requirement analysis)*. Ένα firewall μπορεί ακόμη με τις δυνατότητες επεξεργασίας των πληροφοριών αυτών που διαθέτει, να εντοπίσει ύποπτες δραστηριότητες και να αντιδράσει με προαποφασισμένες ενέργειες όπως το κλείσιμο της σύνδεσης ή η ενημέρωση του διαχειριστή ασφάλειας με e-mail.**

- **Επιβάλλει *ελεγχόμενη προσπέλαση (controlled access)* στους πόρους ενός εσωτερικού δικτύου. Για παράδειγμα, κάποιοι διακομιστές ενδέχεται να προσφέρονται για επικοινωνία με το Internet, ενώ άλλοι όχι.**

- **Προσφέρει *διευρυμένη ιδιωτικότητα* (*enhanced privacy*). Για παράδειγμα αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου. Έτσι, οι εξωτερικοί εισβολείς (*intruders*) δυσκολεύονται στις ενδεχόμενες προσπάθειές τους να «ξεφύγουν»**

από τα όρια χρήσης του δικτύου που εμείς τους ορίσαμε. Έτσι, μέσω του firewall, πολλοί οργανισμοί σταματούν υπηρεσίες όπως η *Finger* και η *DNS* (*Domain Name Service*). Η πρώτη δίνει πληροφορίες σχετικά με τους χρήστες ενός δικτύου, όπως το πότε συνδέθηκαν για τελευταία φορά, αν διαβάσανε το ηλεκτρονικό τους ταχυδρομείο κλπ. Η υπηρεσία DNS από την άλλη, παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος, όπως τα ονόματα των τόπων και οι IP διευθύνσεις του. Η μη δημοσιοποίησή τους στο Διαδίκτυο, αφαιρεί σίγουρα χρήσιμα στοιχεία από όσους τα επιβουλεύονται.

- ***Συγκεντρώνει υπηρεσίες ασφάλειας*** **σε μια καλά ορισμένη και οχυρωμένη περιοχή *(concentrated security).* Ελαχιστοποιεί τη ζώνη κινδύνου (*zone risk*) ενός οργανισμού εφόσον η ευρεία περιοχή των μηχανημάτων του παύει να απειλείται άμεσα. Ουσιαστικά το ίδιο το firewall αποτελεί τη μοναδική ζώνη κινδύνου για τον οργανισμό**

- **Αρκετά σύγχρονα συστήματα firewall προσφέρουν ως μια επιπλέον λειτουργία τους και τις υπηρεσίες τους ως *πύλες κρυπτογράφησης (encrypting gateways).* Δηλαδή έχουν ταυτόχρονα δυνατότητες *κρυπτογράφησης* στις επικοινωνίες μεταξύ των διακομιστών που προστατεύουν. Ένας τέτοιος λογικός διαχωρισμός των δικτύων μέσω firewalls και τεχνικών κρυπτογράφησης δημιουργεί τα λεγόμενα *εικονικά ιδιωτικά δίκτυα (VPN – Virtual Private Networks).***

Κεφάλαιο 3ο

Ασφαλεια από ακρο σε ακρο

3.1 Ασφάλεια από άκρο σε άκρο

Η ασφάλεια από άκρο σε άκρο βασίζεται σε πρωτόκολλα και μηχανισμούς που εφαρμόζονται αποκλειστικά στις παραμέτρους μιας σύνδεσης. Το πιο χαρακτηριστικό παράδειγμα είναι η HTTPS σύνδεση (για παράδειγμα σχετικά με το Transport Layer Security (TLS)) σε έναν web server. Το IP Security (IPSec) μπορεί επίσης να χρησιμοποιηθεί για end-to-end ασφάλεια, όπως είχε προταθεί αρχικά ως προεπιλεγμένο μηχανισμό σύνδεσης για το IPv6.

Υπάρχει μια αντίληψη που η end-to-end ασφάλεια είναι επαρκής ως λύση σε ένα πρόβλημα ασφάλειας, και ότι η ασφάλεια των δικτύων που βασίζονται είναι παρωχημένη. Στη συνέχεια θα περιγράψουμε γιατί στην πράξη η end-to-end ασφάλεια από μόνη της δεν είναι επαρκής, και γιατί απαιτείται επίσης η ασφάλεια των δικτύων που βασίζονται.

3.1.1 Ο ορισμός "Άκρου"

Ο παραδοσιακός ορισμός ενός άκρου είναι ένας πελάτης ή ενας διακομιστής. Σε αυτόν τον ορισμό εννοούμε ότι η από άκρο σε άκρο ασφάλεια ξεκινά από τον πελάτη και καταλήγει στο διακομιστή. Με δεδομένη την πληθώρα των εφαρμογών που εκτελούνται παράλληλα σε ένα λειτουργικό σύστημα, και με δεδομένη την αυξανόμενη εικονικότητα, ο ορισμός αυτός δεν είναι συνήθως

αρκετά ακριβής. Το λειτουργικό σύστημα μπορεί να δημιουργήσει μια ένωση ασφάλειας είτε στη σύνοδο ή στο επίπεδο εφαρμογής. Μπορεί επίσης να τερματιστεί σε ένα εμπρόσθιο άκρο, εξαιτίας πολλών διακομιστών, όπως συμβαίνει σε πολλές περιπτώσεις TLS αναπτύξων.

Επειδή ο κύριος στόχος αυτού του άρθρου είναι να καταλάβουμε γιατί το δίκτυο παίζει σημαντικό ρόλο στον τομέα της ασφάλειας; Ο ακριβής ορισμός της παραμέτρου δεν έχει σημασία εδώ. Αφηρημένα ένα τελικό σημείο, είναι ένα αντικείμενο που επικοινωνεί μέσω ενός δικτύου με άλλο αντικείμενο.

3.2 Θεμελιώδης ασφάλεια από άκρο σε άκρο

Η ασφάλεια στα άκρα (client-server ή client-client για peer-to-peer) είναι απαραίτητη προϋπόθεση για ασφαλείς επικοινωνίες. Μια τέτοια λύση περιέχει τα ακόλουθα στοιχεία:

Ταυτότητα: Αυτό το στοιχείο είναι υπεύθυνο για την εξακρίβωση της ταυτότητας των αντικειμένων και στα δύο άκρα. Σημειώστε ότι η ταυτότητα μπορεί να είναι προσωρινή για μια σύνδεση. Για παράδειγμα, ένας χρήστης συχνά ταυτίζεται με το όνομα χρήστη και τον κωδικό πρόσβασης, ενώ ένας διακομιστής μπορεί να προσδιοριστεί μέσω πιστοποιητικού του διακομιστή.

Πρωτόκολλα (για παράδειγμα, TLS και του IPSec): πρωτόκολλα χρησιμοποιούνται για την διαχείρηση κλειδιών συνόδου, και να παράσχουν τις απαιτούμενες λειτουργίες ασφαλείας (για παράδειγμα, κρυπτογράφηση και επαλήθευση της ακεραιότητας) σε μια σύνδεση. Τα πρωτόκολλα χρησιμοποιούν αλγόριθμους για να εφαρμόσουν αυτές τις λειτουργίες.

Αλγόριθμοι (για παράδειγμα, Advanced Encryption Standard [AES], τριπλό σύστημα ψηφιακής Encryption Standard [3DES], και αλγόριθμου

κατακερματισμού ασφαλείς [SHA-1]): Αυτοί οι αλγόριθμοι χρησιμοποιούν τα προαναφερθέντα κλειδιά συνόδου για την προστασία δεδομένων κατά τη μεταφορά, για παράδειγμα μέσω κρυπτογράφησης ή τον έλεγχο της ακεραιότητας.

Ασφαλής εφαρμογή: Το τελικό σημείο (client ή server) που τρέχει ένα από αυτά τα πρωτόκολλα που αναφέρθηκαν προηγουμένως πρέπει να είναι απαλλαγμένο από σφάλματα που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια. Η ασφάλεια του προγράμματος περιήγησης στο Web είναι σχετική εδώ. Επίσης, ενα κακόβουλο λογισμικό μπορεί να θέσει σε κίνδυνο την ασφάλεια.

Ασφαλής λειτουργία: Οι χρήστες και οι διαχειριστές πρέπει να κατανοήσουν τους μηχανισμούς ασφάλειας, και πώς να αντιμετωπίσουν τυχόν παρεκκλίσεις. Για παράδειγμα, όταν το προγράμματα περιήγησης στο Web προειδοποιούν για πιστοποιητικά διακομιστή τα οποια είναι μη έγκυρη, αλλά οι χρήστες παρακάμτουν την προειδοποίηση και συνεχιζουν κανονικα τη σύνδεση.

Για πλήρη από άκρο σε άκρο ασφάλεια, όλα αυτά τα στοιχεία πρέπει να είναι ασφαλής. Σε δίκτυα με end-to-end ασφάλεια, και τα δύο άκρα μπορεί τυπικά (ανάλογα με τα πρωτόκολλα και τους αλγόριθμους που χρησιμοποιούνται) να στηρίζονται στο γεγονός ότι η επικοινωνία τους δεν είναι ορατή σε κανέναν άλλο, και ότι κανένας άλλος δεν μπορεί να τροποποιήσει τα δεδομένα κατά τη μεταφορά. Η End-to-end ασφάλεια χρησιμοποιείται επιτυχώς σήμερα, για παράδειγμα, σε απευθείας online τραπεζικές εφαρμογές. Απαιτείται η σωστή και πλήρη ο άκρο σε άκρο ασφάλεια χωρίς αυτό πολλές εφαρμογές όπως online τραπεζικές συναλλαγές δεν θα ήταν δυνατές.

Ωστόσο, ένα μόνο πρόβλημα ασφαλείας σε οποιοδήποτε από τα προαναφερθέντα στοιχεία μπορεί να θέσει σε κίνδυνο την συνολική ασφάλεια μιας σύνδεσης. Σήμερα, τα περισσότερα κρίσιμα προβλήματα είναι τα προβλήματα εφαρμογής στα τελικά σημεία, καθώς και τα ανθρώπινα λάθη, ειδικά στη διεκπεραίωση των υποθέσεων εξαίρεσης.

3.3 Πρακτικές αδυναμίες της ασφάλειας από άκρο σε άκρο

Λύσεις που βασίζονται αποκλειστικά σε end-to-end ασφάλεια έχουν πολλά πιθανά προβλήματα, τα οποία εμπίπτουν σε δύο γενικές κατηγορίες: αυτές που επηρεάζουν τον **τελικό χρήστη** και σε αυτές που επηρεάζουν τον **διαχειριστή δικτύου** (για παράδειγμα τον φορέα παροχής υπηρεσιών ή το διαχειριστή εταιρικών δικτύων) .

3.3.1 Ο τελικός χρήστης

Οι αναφορές σχετικά με διαδυκτιακά εγκλήματα και της απάτες αποδεικνύουν ξεκάθαρα, ακόμη και με την χρήση end-to-end ασφάλειας είναι δύσκολο να εξασφαλιστεί ότι κανένα από τα στοιχεία που αναφέρθηκαν προηγουμένως δεν είναι "σπασμένα". Παρά το γεγονός ότι τα πρωτόκολλα και οι αλγόριθμοι που χρησιμοποιούνται τείνουν να είναι ασφαλή και αξιόπιστα, τα κυριότερα προβλήματα εντοπίζονται στους δύο κύριους τομείς της ασφάλειας των τελικών σημείων (ασφαλές στοιχείο υλοποίησης) και η έλλειψη εκπαίδευσης των χρηστών (ασφαλές στοιχείο λειτουργίας).

Τα ζητήματα για την ασφάλεια στα τελικά σημεία περιλαμβάνουν την παρουσία κακόβουλου λογισμικού, καθώς και σφάλματα στο λογισμικό. Ακόμα και οι επαγγελματίες έχουν δυσκολία στο να καθορίσουν αν ένα PC περιέχει κακόβουλο λογισμικό. Τέτοιου είδους κακόβουλο λογισμικό μπορεί να ελέγξει τη σύνδεση πριν να είναι ασφαλισμένο, επιτυγχάνοντας έτσι τη δυνατότητα τα δεδομένα να είναι ορατά, καθώς και το ενδεχόμενο να τα αλλάξουν σε πραγματικό χρόνο. Αν και στα τελικά σημεία υπάρχουν λογισμικά ασφάλειας, όπως είναι τα antivirus, καθώς και λύσεις πρόληψης zero-day τα οποια παρέχουν καλή ασφάλεια, δεν είναι πάντα εγκατεστημένα, και το λογισμικό προστασίας από ιούς δεν είναι συχνά up-to-date. Οι χρήστες

μπορούν επίσης να απενεργοποιήσοουν προσωρινά τις λύσεις. Ως εκ τούτου, η παρουσία του κακόβουλου λογισμικού εξακολουθεί να αποτελεί πρόβλημα ασφάλειας. Σφάλματα στο λογισμικό μπορούμε να εχουμε επισης και στα προγράμματα περιήγησης ή και σε λειτουργικά συστήματα.

Η έλλειψη εκπαίδευσης των χρηστών είναι ένα άλλο σημαντικό ζήτημα για την end to end ασφάλεια. Οι χρήστες πρέπει να γνωρίζουν πώς να προσδιορίσουν μια ασφαλή σύνδεση. Θα πρέπει επίσης να γνωρίζουν πώς να ασχοληθούν με ζητήματα όπως πιστοποιητικά έχουν λήξει ή μη έγκυρα πιστοποιητικά. Οι περισσότεροι χρήστες δεν καταλαβαίνουν πλήρως όλες αυτές τις λεπτομέρειες, το οποιο πρόβλημα οδηγεί σε παραβιάσεις της ασφάλειας.

3.3.2 Ο Διαχειριστής του Δικτύου

Κατά τις πρώτες μέρες του IPv6 πρωτοκόλλου, είχε διατυπωθεί η άποψη ότι το πρωτόκολλο IPv6 θα μπορούσε να ενθυλακώνεται σε πακέτα IPsec για ασφάλεια από άκρο σε άκρο , εξαλείφοντας έτσι όλα τα προβλήματα ασφαλείας. Αυτή η υπόθεση αποδείχθηκε ότι ήταν λάθος, επειδή πολλά προβλήματα παραμένουν από την πλευρά τυο δίκτυο, για παράδειγμα γενικά προβλήματα με end-to-end ασφάλεια τα οποια εφαρμόζονται σε όλες τις παραλλαγές, όπως IPsec, TLS, ή Secure Sockets Layer (SSL) .

Σήμερα οι περισσότεροι διαχειριστές εταιρικών δικτύων καθώς και οι πάροχοι υπηρεσιών είναι επιφυλακτικοί σχετικά με την συνεχή χρήση της end-to-end ασφαλείας. Η βασική ανησυχία είναι ότι τα τελικά σημεία σε γενικές γραμμές δεν είναι αξιόπιστα. Ο διαχειριστής του δικτύου, είτε μιας επιχείρησης, πανεπιστήμιου, ή παροχής υπηρεσιών έχει την υποχρέωση να εφαρμόσει συγκεκριμένες πολιτικές για την εξασφαλίσει την ορθή επικοινωνία μεταξύ των άκρων, για παράδειγμα, για να διασφαλίσει ότι δεν θα εξαπλωθούν τα

παρασιτα ή θα επιτεθούν στους servers. Αν, ωστόσο, οι διαχειριστές του δικτύου δεν μπορούν να «δουν» την κυκλοφορία ενός τελικού σημείου, διότι είναι end-to-end ασφάλεια, τότε δεν μπορούν να πληρούν τις προυποθέσεις ώστε να μπορούν να ελέγχουν τις παραμέτρους. Από την πλευρά του διαχειριστή δικτύου, επομένως, δεν είναι γενικά επιθυμητή η χρήση end-to-end ασφάλειας για όλες τις επικοινωνίες, αλλά όταν πραγματικά χρειάζεται.

3.4 Γιατί η ασφάλεια δικτυου είναι ζωτικής σημασίας

Υπάρχουν πολλά παραδείγματα όπου η ασφάλεια του δικτύου είναι απαραίτητη, και όπου η end-to-end ασφάλεια, όχι μόνο δεν βοηθάει, αλλά μπορεί να παρουσιάσει πραγματικά ένα πρόσθετο πρόβλημα. Σε όλες αυτές τις περιπτώσεις είναι απαραίτητο να υπάρχει ισχυρή ασφάλεια που βασίζεται σε ασφάλεια δικτύου.

3.5 Ο Πάροχος Υπηρεσιών με DSL Πελάτες

Ένας φορέας παροχής υπηρεσιών DSL πρέπει να έχει τον έλεγχο της κυκλοφορίας των χρηστών του με διάφορους τρόπους. Ωστόσο, ο πάροχος δεν έχει κανένα έλεγχο επί των τελικών άκρων, επειδή αυτά είναι ιδιοκτησία των πελατών. Επειδή, επίσης, δεν μπορεί να αναγκάσει τους πελάτες τους να χρησιμοποιούν το κατάλληλο λογισμικό ασφαλείας, υπάρχει πάντα ένα ορισμένο ποσοστό των μολυσμένων υπολογιστών σε οποιονδήποτε πάροχο υπηρεσιών. Κρίσιμα ζητήματα παροχής υπηρεσιών είναι τα ακόλουθα:

Έλεγχος των υπολογιστών που έχουν μολυνθεί με κακόβουλο λογισμικό: Αυτοί οι υπολογιστές (αναφέρονται επίσης ως "bots" ή "zombies") μπορεί να μολύνουν άλλους υπολογιστές και να συμμετέχουν σε παράνομες

δραστηριότητες, όπως το spam mail, click fraud, Denial-of-Service (DoS) επιθέσεις, κ.λπ. Υπάρχει μια ισχυρή, συχνά νομική υποχρέωση για τους παρόχους να εντοπίζουν υπολογιστές που έχουν μολυνθεί με κακόβουλο υλικό, να τους απομονώσουν, να προειδοποιήσουν τους ιδιοκτήτες τους και να τους βοηθήσουν να «απολυμάνουν» το PC. Απαιτούνται οι μηχανισμοί ασφαλείας δικτύου, κατ 'ουσίαν, επειδή η ασφάλεια στα άκρα δεν είναι αποτελεσματική.

Επιθέσεις από τους χρήστες: Ακόμη και στην απουσία του κακόβουλου λογισμικού, οι χρήστες ενός παρόχου υπηρεσιών μπορούν να συμμετέχουν σε παράνομες δραστηριότητες, όπως οι επιθέσεις DoS, και εισβολές στους web servers ή στους δρομολογητές. Απαιτούνται μέθοδοι που βασίζονται σε δίκτυο για την ανίχνευση τέτοιων προσπαθειών, αρχίζοντας με απλές μορφές, όπως IP spoofing και για να τους αποτρέψουν ή να τους εμποδίσουν. Ένα παράδειγμα είναι αντιμετώπιση προβλημάτων με βάση το δίκτυο κατά των επιθέσεων DoS.

Έλεγχος εύρους ζώνης: Πολλοί πάροχοι υπηρεσιών πρέπει να επιβάλουν όρια εύρους ζώνης σε ορισμένες εφαρμογές ή χρήστες, διότι παραβιάζουν τις συμφωνίες παροχής υπηρεσιών. Επίσης εδώ, οι εφαρμογές είναι απαραίτητες για τον έλεγχο των υπολογιστών, και να περιορίσουν τη χρήση τους από την υπηρεσία για να παραμείνουν εντός των ορίων σύμβαση. Οι πάροχοι υπηρεσιών σήμερα απασχολούν μεγάλο αριθμό των μηχανισμών ασφάλειας που βασίζονται σε δίκτυο. Η ασφάλεια στα άκρα δεν λύνει αυτά τα προβλήματα, επειδή ο υπολογιστής δεν είναι υπό τον έλεγχο του πάροχου υπηρεσιών, και συνήθως είναι μη αξιόπιστη.

Υπηρεσίες: Οι πάροχοι υπηρεσιών στην προσπαθειά τους να διαφοροποιηθούν από τους ανταγωνιστές τους προσφέρουν υπηρεσίες διαχείρισης, όπως για παράδειγμα η διαχείριση των υπηρεσιών ασφαλείας. Οι εν λόγω υπηρεσίες παρέχονται επίσης με βάση το δίκτυο, και συμπληρώνουν την ασφάλεια στα άκρα την οποια χρησιμοποιούν οι πελάτες τους.

3.6 Συμπεράσματα για δίκτυα end to end

Η ασφάλεια από άκρο σε άκρο αποτελούν τον ακρογωνιαίο λίθο για την ασφάλεια του δικτύου. Είναι απαραίτητα. Ωστόσο, δεν είναι ρεαλιστικό σήμερα να υποθέσουμε ότι οι λύσεις ασφάλειας end-to-end και μόνο θα αρκούσαν. Το θεμελιώδες πρόβλημα είναι ότι συνήθως ο διαχειριστής του δικτύου, όπου ένας υπολογιστής είναι συνδεδεμένος, έχει μια ανάγκη και συχνά μια υποχρέωση, να παρακολουθεί τη συμπεριφορά του τελικού σημείου, και να ελέγχει κακόβουλες δραστηριότητες που προκύπτουν από τον υπολογιστή του. Όλες οι λύσεις για τον έλεγχο στα τελικά σημεία, όμως, είναι εξ ορισμού με βάση το δίκτυο. Ως εκ τούτου, οι μηχανισμοί ασφάλειας που βασίζονται στο δίκτυο είναι επίσης ένα σημαντικό στοιχείο της συνολικής ασφάλειας του δικτύου: Γενικά η ασφάλειας βασίζεται τόσο την endpoint ασφάλεια οσο και την network-based ασφάλεια.

Κεφάλαιο 4ο

Αλγόριθμοι κρυπτογράφησης για κρυτογράφηση από άκρο σε άκρο

4.1 Το Πρότυπο AES

Το πρότυπο AES (Advanced Encryption Standard) περιγράφει μια συμμετρική μπλοκ διαδικασία κρυπτογράφησης μυστικού κλειδιού. Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος επενεργεί πάνω σε μπλοκ δεδομένων μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε μπλοκ δεδομένων γίνεται μια επεξεργασία η οποία επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round). Στον πρώτο γύρο επεξεργασίας ως είσοδος είναι ένα plaintext μπλοκ και το αρχικό κλειδί, ενώ στους γύρους που ακολουθούν ως είσοδος είναι το μπλοκ που έχει προκύψει από τον προηγούμενο γύρο καθώς και ένα κλειδί που έχει παραχθεί από το αρχικό με βάση κάποια διαδικασία που ορίζει ο αλγόριθμος. Το τελικό προϊόν της επεξεργασίας είναι το κρυπτογραφημένο μπλοκ (ciphertext). Το μπλοκ αυτό πρέπει να σημειωθεί ότι έχει ακριβώς το ίδιο μέγεθος (128 bits) με το plaintext μπλοκ.

4.2 Είσοδοι, Έξοδοι και Εσωτερική Κατάσταση

Όπως ήδη αναφέρθηκε, ο AES τροφοδοτείται με ακολουθίες από bits των 128 bits (μπλοκ) καθώς και από κλειδιά, που μπορεί να έχουν μέγεθος 128, 192 ή 256 bits. Τα κλειδιά αυτά ονομάζονται κλειδιά κρυπτογράφησης (cipher keys) για να διαχωριστούν από τα κλειδιά που παράγονται κατά την λειτουργία του αλγορίθμου. Η βασική μονάδα επεξεργασίας στον AES είναι το byte. Έτσι τα bits ενός μπλοκ ή ενός κλειδιού χωρίζονται σε ομάδες των 8 για να σχηματιστούν τα bytes. Κάθε byte στον AES αντιστοιχεί σε ένα πολυώνυμο (αριθμητική πεπερασμένων πεδίων - finite field arithmetic). Αν υποθέσουμε ότι τα bits που αποτελούν ένα byte είναι τα {b7, b6, b5, b4, b3, b2, b1, b0}, τότε το byte αυτό αναπαριστά το πολυώνυμο :

$$\mathbf{b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0 = \sum_{i=0}^{7} b_ix^i}$$

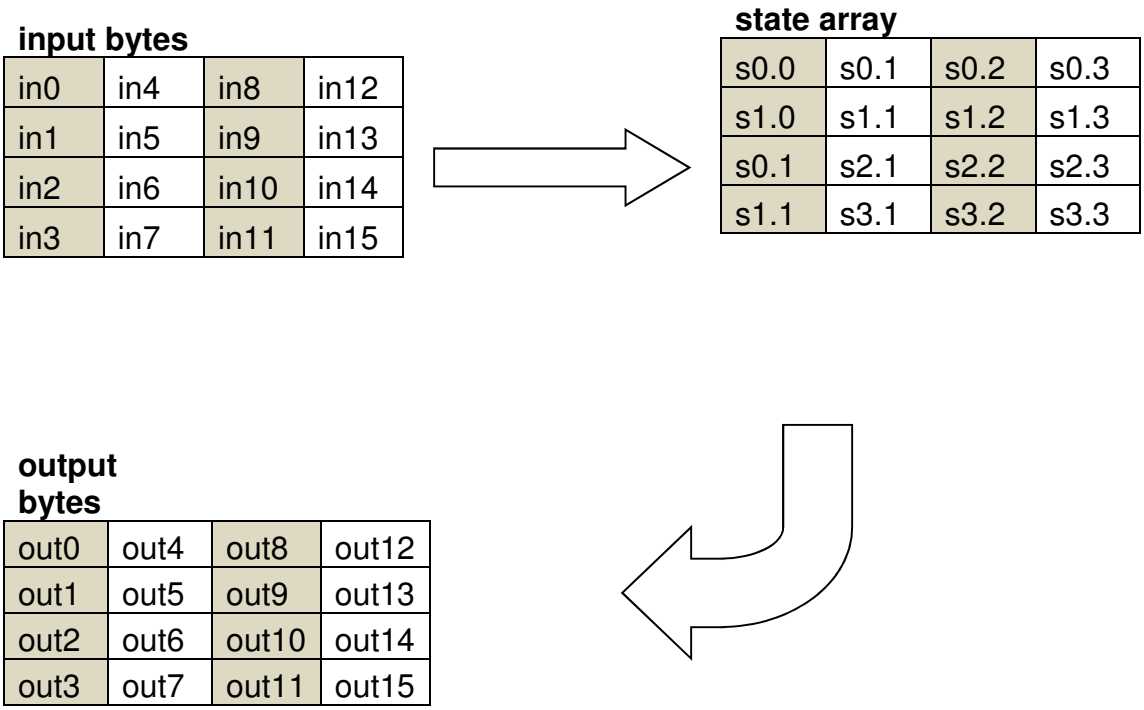
Έτσι για παράδειγμα το byte {11001101} αντιστοιχεί στο πολυώνυμο $x^7+x^6+x^3+x^2+1$. Κλείνοντας την αναφορά στις μονάδες των δεδομένων που διαχειρίζεται ο AES, πρέπει να αναφερθεί το πώς γίνεται η δεικτοδότηση των bits και των bytes στα μπλοκ και στα κλειδιά. Στο σχήμα που ακολουθεί φαίνεται την αντιστοιχία.

input bit sequence	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**……**
byte number	**0**								**1**								
bit number in byte	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**	**….**

Εικόνα 4-1: Δεικτυοδότηση των bits και bytes.

Όλες οι λειτουργίες που επιτελεί ο αλγόριθμος γίνονται πάνω σε ένα δισδιάστατο πίνακα που αποκαλείται Κατάσταση (State). Ο πίνακας αυτός περιλαμβάνει τέσσερις γραμμές από bytes, με κάθε μία γραμμή να αποτελείται από Nb bytes. Ο αριθμός που αντιστοιχεί στην ποσότητα Nb υπολογίζεται αν διαιρεθεί το μήκος του μπλοκ με το 32. Εφόσον στον AES υποστηρίζονται μπλοκ μεγέθους μόνο 128 bits, το Nb θα έχει τιμή 4.

Το μπλοκ εισόδου περιλαμβάνει 16 bytes, τα οποία δεικτοδοτούνται in0 έως in15. Το κρυπτογραφημένο μπλοκ εξόδου περιλαμβάνει επίσης 16 bytes που δεικτοδοτούνται ως out0 έως out15. Η State χρησιμοποιεί την μεταβλητή s με δύο δείκτες που δηλώνουν την θέση κάθε byte στον πίνακα. Η πρώτη λοιπόν και τελευταία λειτουργία που μπορεί να υποτεθεί ότι γίνεται στον AES είναι να αντιστοιχηθούν τα bytes εισόδου σε κάποια θέση του πίνακα της State και το αντίστροφο στην έξοδο. Στο παρακάτω σχήμα φαίνεται πώς γίνεται αυτό.



Εικόνα 4-2: Αντιστοίχιση των bytes εισόδου σε κάποια θέση του πίνακα της State και το αντίστροφο στην έξοδο.

Η αντιστοίχηση που περιγράφηκε παραπάνω μπορεί να περιγραφεί μαθηματικά. Η αντιστοίχηση εισόδου στην State περιγράφεται από την σχέση :

s[r,c] = in[r+4c] για 0 ≤ r < 4 και 0 ≤ c < Nb

ενώ η αντιγραφή της State στην έξοδο από την σχέση :

out[r+4c] = s[r,c] για 0 ≤ r < 4 και 0 ≤ c < Nb

Ένας άλλος τρόπος να δει κάποιος τα περιεχόμενα της State είναι σαν 32-bit λέξεις (words) αντί για byte. Μια 32-bit word περιλαμβάνει τα 4 bytes μιας στήλης, οπότε τα 4 words που αποτελούν την State είναι τα ακόλουθα :

w(0) = s(0,0) s(1,0) s(2,0) s(3,0)
w(1) = s(0,1) s(1,1) s(2,1) s(3,1)
w(2) = s(0,2) s(1,2) s(2,2) s(3,2)
w(3) = s(0,3) s(1,3) s(2,3) s(3,3)

Περιγραφή Αλγορίθμου: Το πρότυπο AES ορίζει ότι τα μπλοκ που επεξεργάζεται ο αλγόριθμος έχουν μέγεθος 128 bits και αυτό ορίζεται από την ποσότητα Nb = 4, που συμβολίζει τον αριθμό των 32-bit λέξεων στο μπλοκ. Από την άλλη, τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση, μπορούν να έχουν μήκος 128, 192 ή 256 bits. Η μεταβλητή Nk συμβολίζει τον αριθμό των 32-bit λέξεων που μπορεί να περιλαμβάνει ένα κλειδί και
κατά συνέπεια μπορεί να πάρει τις τιμές 4, 6 και 8. Ανάλογα με το μήκος κλειδιού που θα επιλεχθεί για την κρυπτογράφηση, ο αλγόριθμος ορίζει έναν αριθμό από γύρους επεξεργασίας που απαιτούνται για την ολοκλήρωση της. Η μεταβλητή Nr χρησιμοποιείται για να δηλώσει το πλήθος των γύρων. Αν

χρησιμοποιηθεί μήκος κλειδιού 128 bits τότε απαιτούνται 10 γύροι επεξεργασίας. Για μήκη κλειδιού ίσα με 192 και 256 bits απαιτούνται αντίστοιχα 12 και 14 γύροι.

	Key Length (Nk words)	**Blosk Size (Nb words)**	**Number Of Rounds (Nr)**
AES - 128	4	4	10
AES - 192	6	4	12
AES - 256	8	4	14

Εικόνα 4-3: Μέγεθος των μεταβλητών του αλγορίθμου.

Nr = Αριθμός των γύρων
Nb = Αριθμός των byte
Nk = Μέγεθος κλειδιού

Να σημειωθεί ότι οι παραπάνω συνδυασμοί μήκους μπλοκ, μήκους κλειδιού και γύρων επεξεργασίας είναι αυτοί που ορίζονται αυστηρά στο πρότυπο AES. Ο αλγόριθμος κρυπτογράφησης Rijndael στον οποίο βασίζεται ο AES δίνει την δυνατότητα πραγματοποίησης περισσότερων συνδυασμών. Έτσι, καταλαβαίνει κανείς ότι ο AES ουσιαστικά ορίζει ένα υποσύνολο του αλγορίθμου Rijndael. Τόσο κατά την διάρκεια της διαδικασίας κρυπτογράφησης όσο και αποκρυπτογράφησης, κάθε γύρος επεξεργασίας αποτελείται από μια σειρά μετασχηματισμών σε επίπεδο byte. Για την ακρίβεια, χρησιμοποιούνται 4 τύποι μετασχηματισμών :

- **ένας μετασχηματισμός αντικατάστασης bytes χρησιμοποιώντας κάποιον σχετικό πίνακα αντικατάστασης**

- **ένας μηχανισμός ολίσθησης των bytes της State κατά διαφορετικά offsets**

- **μια διαδικασία ανάμειξης των bytes της State**

- **μια πρόσθεση ενός κλειδιού στην State**

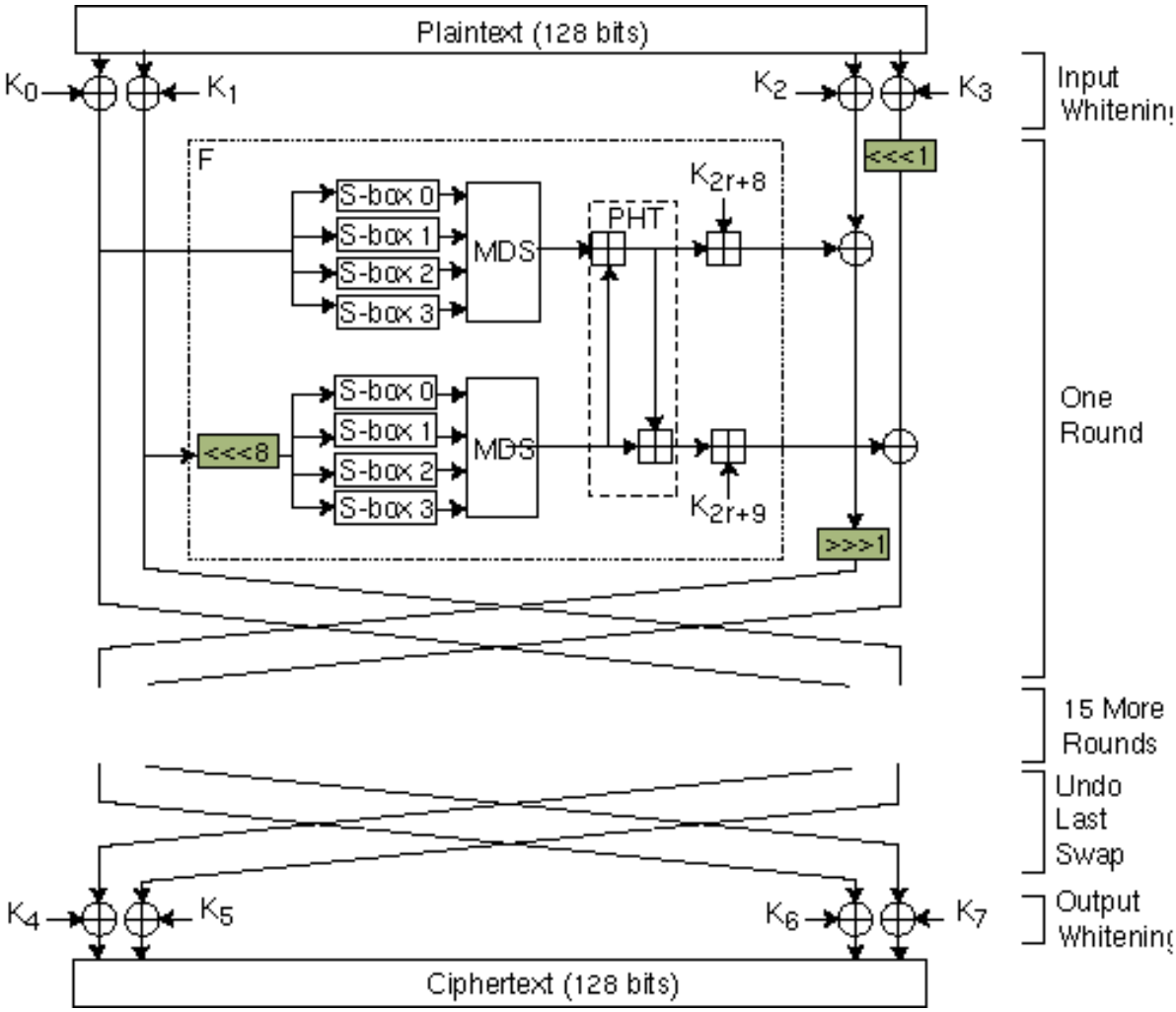
4.3 Το πρότυπο TWOFISH

Twofish είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης. Ένα μόνο κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αλγόριθμος Twofish έχει μέγεθος 128 bits, και δέχεται κλειδί οποιουδήποτε μήκους μέχρι 256 bits (NIST απαιτείται ο αλγόριθμος να δέχεται μέγεθος κλειδιών 128-, 192- και 256-bit). Ο αλγόριθμος Twofish είναι εξίσου γρήγορος σε επεξεργαστές 32-bit και 8-bit (όπως έξυπνες κάρτες, ενσωματωμένο τσιπ, και τα παρόμοια), και σε hardware. Είναι ευέλικτο, μπορεί να χρησιμοποιηθεί σε εφαρμογές δικτύου όπου τα κλειδιά αλλάζονται συχνά και σε εφαρμογές όπου υπάρχει μικρή ή καθόλου RAM και ROM διαθέσιμα.

Ο αλγόριθμος Twofish περιλαμβάνει 16 κύκλους, σε καθέναν από τους οποίους εφαρμόζονται 4 S-boxes τα οποία εξαρτώνται από το μυστικό κλειδί. Τα επόμενα στάδια περιλαμβάνουν την αξιοποίηση σταθερών S-boxes, τη διενέργεια μετασχηματισμού pseudo-Hadamard, καθώς και την πρόσθεση του υποκλειδιού.
Twofish είναι ένα δίκτυο Feistel. Αυτό σημαίνει ότι σε κάθε γύρο, το ήμισυ του text block στέλνεται μέσω μιας συνάρτηση F, και στη συνέχεια γίνεται πράξη XOR με το άλλο ήμισυ του text block.

Ο 256-bit Twofish, σχεδιασμένος από τα Counterpane Labs. Ήταν επίσης ένας εκ των πέντε φιναλίστ Advanced Encryption Standard που επιλέχθηκαν από το National Institute of Standard and Technology (NIST). Αναθεωρείται και αναβαθμίζεται συχνά και δεν έχουν καταγραφεί έως και σήμερα επιθέσεις εναντίον του αλγορίθμου αυτού.

4.3.1 Παράδειγμα Twofish αλγόριθμου



Εικόνα 4-4: Twofish αλγόριθμος

Σε κάθε γύρο Twofish, δύο λέξεις 32- bit χρησιμεύουν ως εισροές στη συνάρτηση F. Κάθε λέξη χωρίζεται σε τέσσερα byte. Αυτά τα τέσσερα bytes που αποστέλλονται μέσω τεσσάρων διαφορετικών εξαρτημένων κλειδιών S-boxes. Τα τέσσερα byte εξόδου (τα S-boxes έχουν εισόδο και έξοδο 8-bit) συνδυάζονται χρησιμοποιώντας μια Μέγιστη Διαχωρίσιμη Απόσταση (MDS) και συνδυάζονται σε μια λέξη 32-bit. Στη συνέχεια, οι δύο λέξεις 32-bit συνδυάζονται χρησιμοποιώντας έναν Ψευδο-Μετασχηματισμός Hadamard (PHT), προστίθεται στο δεύτερο γύρο δευτερεύοντα κλειδιά, τότε πραγματοποιείται πράξη XOR με το μισό δεξί του κειμένου. Υπάρχουν επίσης δύο περιστροφές 1-bit σε εξέλιξη, μία πριν και μία μετά την XOR. Ο Twofish έχει επίσης κάτι που ονομάζεται «prewhitening» και «postwhitening " Τα πρόσθετα δευτερεύοντα κλειδιά XORed στο text block πριν από τον πρώτο γύρο και μετά τον τελευταίο γύρο.

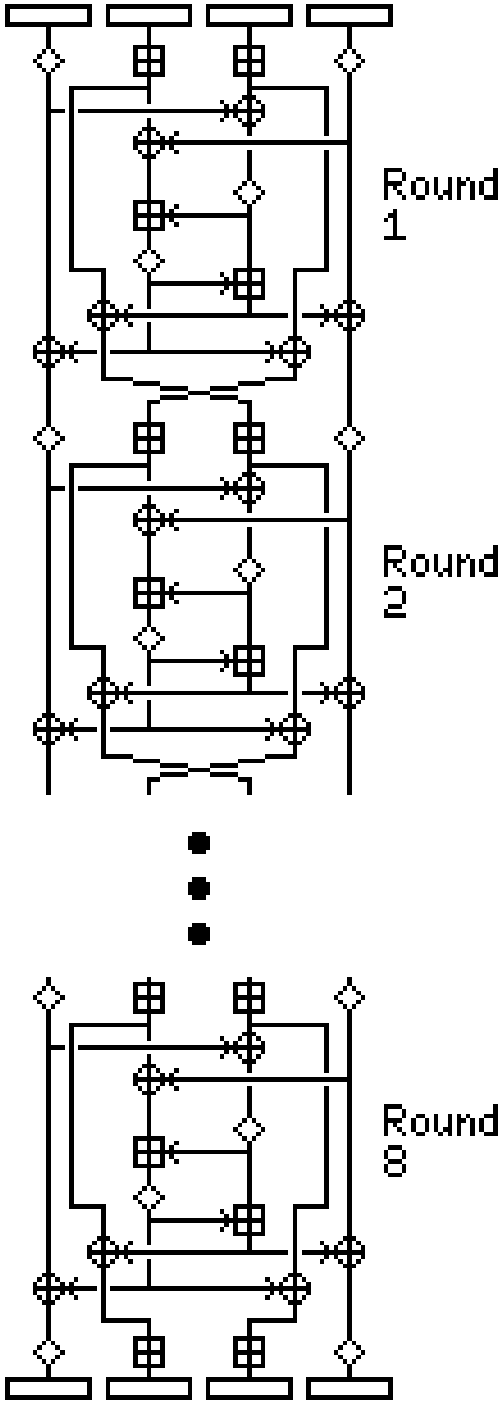
4.4 Το πρότυπο IDEA

Ο αλγόριθμος International Data Encryption Algorithm – IDEA αποτελεί συμμετρικό κωδικοποιητή τμημάτων, που αναπτύχθηκε από τους X. Lai Και J. Massey, στο Swiss Federal Institute of Technology, το 1991. Ο IDEA Χρησιμοποιεί κλειδί μήκους 128- bit και διαφέρει από τον DES τόσο στη συνάρτηση F, οσο και στη συνάρτηση παραγωγής των υποκλειδιών. Για τη συνάρτηση F, ο IDEA Δε χρησιμοποιεί S-boxes, Αλλά στηρίζεται σε τρεις διαφορετικές μαθηματικές λειτουργίες: τη δυαδική πράξη XOR, Τη δυαδική πρόσθεση ακεραίων των 16-bit και το δυαδικό πολλαπλασιασμό ακεραίων των 16-bit.

Αλγόριθμος	Μήκος κλειδιού	Αριθμός κύκλων	Μαθηματικές πράξεις	Εφαρμογές
DES	56 bits	16	XOR, σταθερά S-boxes	SET, Kerveros
Triple DES	112 ή 168 bits	48	XOR, σταθερά S-boxes	Financial Key management, PGP, S/MINE
IDEA	128 bits	8	XOR, πρόσθεση, πολ/σμός	PGP
Blowfish	Μεταβλητό μέχρι 448 bits	16	XOR, μεταβλητά S-boxes, πρόσθεση	
RS5	Μεταβλητό μέχρι 2048 bits	μεταβλητό μέχρι 255	πρόσθεση, αφαίρεση, XOR, περιστροφή	
CAST-128	40 μέχρι 128 bits	16	πρόσθεση, αφαίρεση, XOR, περιστροφή, σταθερά S-boxes	PGP

Εικόνα 4-5 : Συμβατικοί Αλγόριθμοι κρυπτογράφησης

Οι συναρτήσεις συνδυάζονται με τρόπον ώστε να αναπτυχθεί ένας πολύπλοκος μετασχηματισμός που αναλύεται δύσκολα, ώστε να καθίσταται πολύ δύσκολη η διαδικασία κρυπτανάλυσης. Ο αλγόριθμος παραγωγής δευτερευόντων κλειδιών βασίζεται στη χρήση κυκλικών μετατοπίσεων, οι οποίες χρησιμοποιούνται με πολύπλοκο τρόπο για να παραχθούν συνολικά έξι δευτερεύοντα κλειδιά, για καθέναν από τους οκτώ γύρους του IDEA. Ο IDEA ήταν ένας από τους προτεινόμενους 128-bit αντικαταστάτες του DES, έχει υποβληθεί σε αξιοσημείωτη διερεύνηση και εμφανίζεται ανθεκτικός σε κρυπταναλυτικές επιθέσεις. Ο IDEA χρησιμοποιείται στο προϊόν λογισμικού PGP, ως μία από τις εναλλακτικές επιλογές, καθώς και σε διάφορα εμπορικά προϊόντα.



Εικόνα 4-6 : Αλγόριθμος IDEA

Κεφάλαιο 5ο

Εικονικά ειδιωτικα δίκτυα (VPN)

5.1 Ιδιωτικά δίκτυα

Τα ιδιώτικα δίκτυα έχουν σχεδιαστεί για να μπορούν να χρησιμοποιηθούν μόνο μέσα σε μια εταιρεία. Παρέχει ιδιωτικότητα επιτρέποντας την πρόσβαση σε κοινά αρχεία. Τα πιο διαδεδομένα ιδιωτικά δίκτυα ειναι το **intranet** και το **extranet.**

5.1.1 INTRANET

Το intranet είναι ένα ιδιωτικό δίκτυο (LAN) που χρησιμοποιεί τα πρωτόκολλα TCP/IP. Η πρόσβαση όμως στο δίκτυο περιορίζεται μόνο στους χρήστες μέσα στον οργανισμό. Το δίκτυο χρησιμοποιεί προγράμματα εφαρμογής που ορίζονται για το παγκόσμιο internet, όπως το HTTP, και μπορει να εχει Web server, server εκτύπωσης, server αρχεία και άλλα στοιχεία.

5.1.2 EXTRANET

Το extranet είναι παρόμοιο με το intranet με μια διαφοροποίηση. Κάποια στοιχεία μπορούν και είναι ορατά από συγκεκριμένες ομάδες χρηστών εκτός του δικτύου, υπό την εποπτεία του διαχειριστή του δικτύου. Για παράδειγμα μια εταιρεία μπορεί να δώσει την δυνατότητα σε πελάτες που έχουν εξουσιοδοτηθεί να μπορούν να δουν την διαθεσιμότητα και την online παραγγελία προϊόντων. Ένα αλλο παράδειγμα ειναι οι εξ αποστάσεως σπουδαστές, με έναν κωδικό πρόσβασης να έχουν την δυνατότητα να προσπελαύνουν τα εργαστήρια υπολογιστών.

5.1.3 Διευθυνσιοδότηση

Τα ιδιωτικά δίκτυα τα οποία χρησιμοποιούν TCP/IP πρωτόκολα, εξ ορισμού πρέπει να χρησιμοποιού και IP διευθυνσιοδότηση. Έχουμε τις κάτωθι επιλογές:

- **Το δίκτυο μπορεί να ζητήσει διευθύνσεις απο την διοίκηση του διαδικτύου, τις οποίες χωρίς να είναι συνδεδεμέμη στο διαδίκτυο θα μπορει να χρησιμοποιήσει. Το πλεονέκτημα της μεθόδου αυτης είναι η σχετική ευκολία του οργανισμού να έχει πρόσβαση στο διαδίκτυο . ενώ το μειονέκτημα της μεθόδου ειναι οτι ο χώρος των διευθύνσεων θα χαθεί.**

- **Το δίκτυο μπορεί και χρησιμοποιεί όποιες διευθύνσεις αυτο χρειάζεται, χωρίς να υπάρχει η ανάγκη να εγγραφεί στις αρχές του διαδικτύου. Δεν υπάρχει η ανάγκη της μοναδικότητας των διευθύνσεων διοτι το δίκτυο ειναι απομονωμένο. Υπάρχει ομως**

ένα μειωνέκτημα αυτης της μεθόδου. Υπάρχει ο κίνδυνος οι χρήστες να μπερδέψουν αυτές τις διεθύνσεις με τις διευθυνσεις του διαδικτύου.

- **Για την αντιμετώπιση των προβλημάτων που δημιουργούνται με τις δυο πάνω μεθόδου, οι αρχές του διαδικτύου έχουν δεσμεύσει τρεία σύνολα διευθύνσεων**

Εύρος	Σύνολο
10.0.0.0 ως 10.255.255.255	2^{24}
172.16.0.0 ως 172.31.255.255	2^{20}
192.168.0.0 ως 192.168.255.255	2^{16}

Εικόνα 5-1: Διευθύνσεις για ιδιωτικά δίκτυα

Μια εταιρεία μπορεί να χρησιμοποιήσει μια διεύθυνση εκτός αυτού του συνολού διευθύνσεων χωρις την έγκριση απο τις αρχές του διαδικτύου. Είναι ευρέως γνωστό οτι αυτές οι δεσμευμένες διευθύνσεις αφορούν ιδιωτικά δίκτυα. Μπορεί οι δεσμευμένες διευθύμσεις να είναι μοναδικές σε μια εταιρεια αλλα οχι παγκοσμίως. Κανένας δρομολογητής δεν θα προωθήσει ένα πακέτο που έχει μια από αυτές τις διευθύνσεις ως διεύθυνση προορισμού.

5.2 Εικονικά ιδιωτικά δίκτυα (VPN)

Το εικονικό ιδιωτικό δίκτυο (vpn) είναι μια τεχνολογία που κερδίζει συνεχώς έδαφος σε μεγάλους οργανισμούς, που χρησιμοποιούν το διαδίκτυο για επικοινωνία εντός και εκτός του οργανισμού, επίσης επιθυμούν ιδιωτικότητα στην επικοινωνία εντός του οργανισμού.

5.2.1 Επίτευξη ιδιωτικότητας

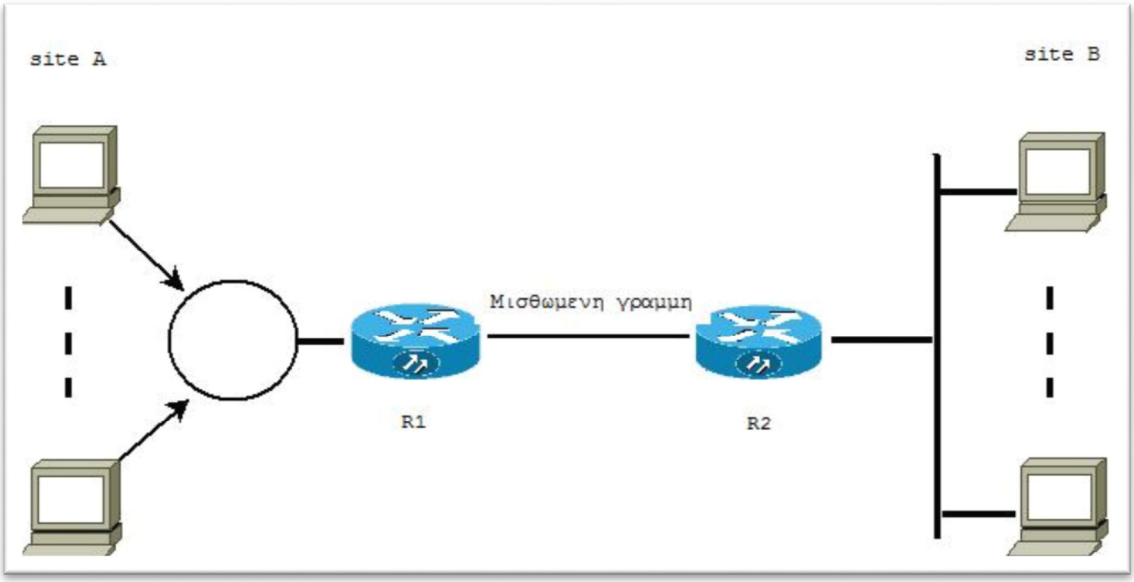
Για να μπορούν να πετύχουν την ιδιωτικότητα οι εταιρείες πρέπει να χρησιμοποιήσουν μια απο τις εξής μεθόδους : ιδιωτικά δίκτυα, υβριδικά δίκτυα και εικονικά ιδιωτικά δίκτυα.

5.2.2 Ιδιωτικά δίκτυα

Για να επιτευχθεί η ιδιωτικότητα σε μια εταιρεία , θα πρέπει όταν δρομολογούνται πληροφορίες μέσα στην εταιρεία να χρησιμοποιείται ένα ιδιωτικό δίκτυο. Μια εταιρεία μικρού μεγέθους με ένα μόνο site θα μπορούσε να χρησιμοποιήσει ένα απομονωμένο LAN. Τα άτομα μιας εταιρείας μπορούν να στέλνουν πληροφορίες μεταξύ τους, οι οποίες πληροφορίες παραμένουν μέσα στην εταιρεία, ασφαλής από εξωτερκούς παράγωντες. Μία μεγάλη εταιρεία με πολλά sites μπορεί να δημιουργήσει ένα ιδιωτικό διαδίκτυο. Τα τοπικά δίκτυα σε διαφορετικά site μπορούν να συνδέονται μεταξύ τους χρησιμοποιώντας δρομολογητές και μισθωμένες γραμμές. Δηλαδή ενα διαδίκτυο μπορεί να υλοποιηθεί από ιδιωτικά LAN και ιδιωτικά WAN. Στην

περίπτωση αυτή έχει δημιουργηθεί από την εταιρεία ένα ιδιωτικό internet το οποίο είναι τελείως απομονωμένο από το παγκόσμιο διαδίκτυο. Η εταιρεία χρησιμοποιεει τα πρωτόκολλα TCP/IP για επικοινωνία μεταξύ σταθμών σε διαφορετικά sites. Στην περίπτωση αυτή έχει δημιουργηθεί από την εταιρεία, ένα ιδιωτικό internet το οποίο είναι τελείως απομονωμένο από το παγκόσμιο διαδίκτυο.

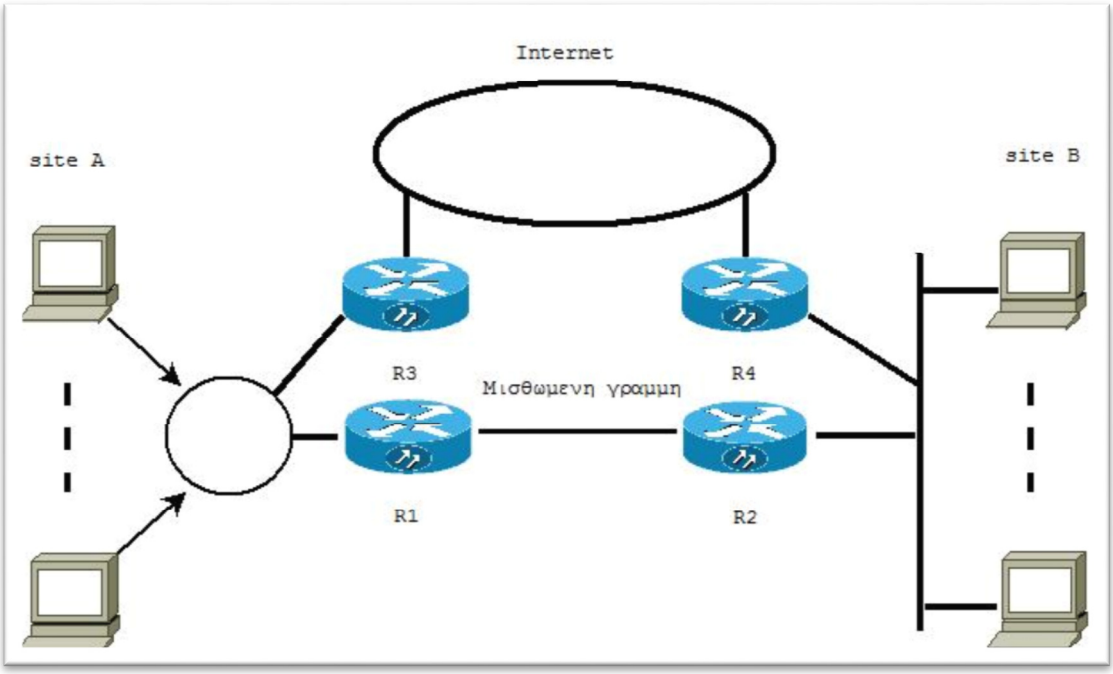
Η εταιρεία, μπορεί να χρησιμοποιεί τα πρωτοκολλά TCP/IP για επικοινωνία μεταξύ σταθμών σε διαφορετικά sites. Η εταιρεία, χρησιμοποιεί συνήθως ιδιωτικές διευθύνσεις IP με αποτέλεσμα να μην χρειάζεται να ζητήσει διευθύνσεις IP από την διοίκηση του διαδικτύου. Η εταιρεία είναι σε θέση να χρησιμοποιήσει οποιαδήποτε τάξη IP και να εισάγει τις διευθύνσεις στο δίκτυο και τους κεντρικούς υπολογιστές εσωτερικά. Δεν υφίσταται το πρόβλημα της επανάληψης διευθύνσεων από άλλη εταιρεία στο παγκόσμιο διαδίκτυο, διότι το δίκτυο είναι ιδιωτικό.



Εικόνα 5-2 : Ιδιωτικό δίκτυο

5.3 Υβριδικά δίκτυα

Η χρήση των υβριδικών δικτύων είναι αναγκαία, διότι στις μέρες μας όλο και περισσότερες εταιρείες επιθυμούν ιδιωτικότητα στην ανταλλαγή πληροφοριών μέσα στην εταιρεία, ζητούν όμως ταυτόχρονα να συνδέονται με το παγκόσμιο διαδίκτυο για ανταλλαγή πληροφοριών με άλλες εταιρείες. Με το υβριδικό δίκτυο, μια εταιρεία έχει το δικό της ιδιωτικό διαδίκτυο και ταυτόχρονα να προσπελαύνει το παγκόσμιο διαδίκτυο. Τα δεδομένα μέσα στην εταιρεία δρομολογούνται μεσώ του ιδιωτικού διαδικτύου, ενώ τα δεδομένα εκτός της εταιρείας δρομολογούνται μεσώ του παγκοσμίου διαδικτύου. Μια εταιρεία έχει 2 sites. Η εταιρεία επιτυγχάνει ιδιωτικά σύνδεση των 2 sites, χρησιμοποιώντας τους δρομολογητές R1 και R2, τα οποία συνδέονται μεσώ μιας μισθωμένης γραμμής, και επιτυγχάνει σύνδεση των 2 sites με το παγκόσμιο διαδίκτυο χρησιμοποιώντας τους δρομολογητές R3 και R4. Η εταιρεία χρησιμοποιεί παγκόσμιες διευθύνσεις IP και για το ιδιωτικό διαδίκτυο και για το παγκόσμιο. Τα δεδομένα όμως που προορίζονται για εσωτερική επικοινωνία (δηλαδή εντός της εταιρείας), δρομολογούνται μόνο μεσώ των δρομολογητών R1 και R2. Για επικοινωνία με το παγκόσμιο διαδίκτυο, τα δεδομένα δρομολογούνται μεσώ των δρομολογητών R3 και R4.



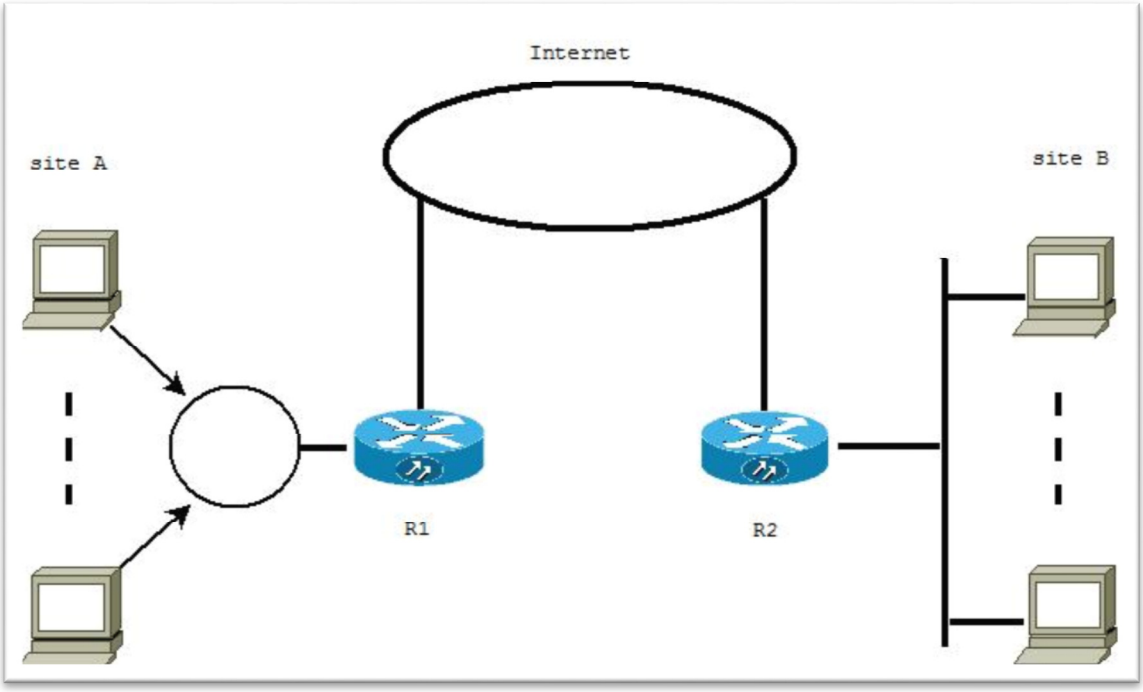
Εικόνα 5-3 : Υβριδικό δίκτυο

5.4 Παράδειγμα εικονικού ιδιωτικού δικτυού

Ένα σοβαρό μειονέκτημα που έχουν τα ιδιωτικά και υβριδικά δίκτυα, είναι το κόστος. Τα ιδιωτικά WAN έχουν υψηλό κόστος. Μια εταιρεία για να συνδέσει πολλά sites χρειάζεται να έχει πολλές μισθωμένες γραμμές, κάτι που συνεπάγεται με μεγάλο κόστος μηνιαίως. Η εταιρεία για την λύση του σοβαρού αυτού προβλήματος, χρησιμοποιεί το παγκόσμιο διαδίκτυο και για την ιδιωτική και για την δημοσιά επικοινωνία.

Κάτι τέτοιο επιτυγχάνεται μεσώ μιας τεχνολογίας, που ονομάζεται εικονικό ιδιωτικό δίκτυο (VPN), η οποία τεχνολογία επιτρέπει στην εταιρεία να χρησιμοποιεί το παγκόσμιο διαδίκτυο και για την ιδιωτική και για την δημοσιά επικοινωνία.

Το VPN είναι ένα ιδιωτικό δίκτυο, όμως εικονικό. Εξασφαλίζει την ιδιωτικότητα μέσα σε μια εταιρεία για αυτό είναι ιδιωτικό. Επειδή δεν χρησιμοποιεί πραγματικά ιδιωτικά WAN, είναι εικονικό δίκτυο. Είναι συνεπώς, φυσικά δημόσιο και εικονικά ιδιωτικό δίκτυο.
Στην παρακάτω εικόνα παρουσιάζεται ένα εικονικό ιδιωτικό δίκτυο. Οι δρομολογητές R1 και R2 χρησιμοποιούν VPN τεχνολογία και με αυτόν τον τρόπο, εξασφαλίζεται η ιδιωτικότητα για την εταιρεία.



Εικόνα 5-4 : εικονικό ιδιωτικό δίκτυο

Το VPN είναι ένα δίκτυο εικονικών ζεύξεων ανεπτυγμένο σε μια υπάρχουσα δικτυακή υποδομή, με την ιδιότητα ότι έχει την ιδία ασφάλεια, διαχείριση και την ιδία πολιτική σε όλο το μήκος του σαν να επρόκειτο για ιδιωτικό δίκτυο. Οι απαιτήσεις των VPN δεν είναι άλλες από αυτές των WAN:

- **Υποστήριξη πολλαπλών πρωτόκολλων**
- **Υψηλή αξιοπιστία**
- **Εκτεταμένη διαβάθμιση**

5.5 Αρχιτεκτονικές των VPNs

Ένα Εικονικό Ιδιωτικό Δίκτυο είναι ένα ιδιωτικό δίκτυο που κατασκευάζεται χρησιμοποιώντας την υπάρχουσα υποδομή ενός δημόσιου δικτύου, όπως για παράδειγμα το Internet ή το υπάρχον δίκτυο του παρόχου. Ο ορός εικονικό δίκτυο σημαίνει ότι οι δικτυακές συνδέσεις είναι ιδεατές , δηλαδή τα δεδομένα που αποστέλλονται μεταξύ δυο χρηστών μπορεί να ακολουθούν κάθε φορά διαφορετική διαδρομή μέχρι να φτάσουν στον προορισμό τους.

Η δημιουργία ενός VPN είναι δυνατόν να βασίζεται στο πρωτόκολλο IP, όπου η προς μετάδοση πληροφορία διαμορφώνεται σε πακέτα IP και μεταδίδεται στο δίκτυο IP. Ένα IP VPN είναι μια δικτυακή σύνδεση η όποια χρησιμοποιεί κοινή διαμοιρασμένη δικτυακή υποδομή για την πραγματοποίηση της σύνδεσης, όμως από την πλευρά των χρηστών συμπεριφέρεται σαν να είναι μια ιδιωτική σύνδεση, παρόλο που χρησιμοποιείται κοινή διαμοιρασμένη δικτυακή υποδομή. Επιπλέον η υλοποίηση ενός εικονικού ιδιωτικού δικτύου

μπορεί να βασίζεται στις τεχνολογίες ATM (Asynchronous Transfer Mode), Frame Relay ή MPLS (Multiprotocol Lapel Switching).

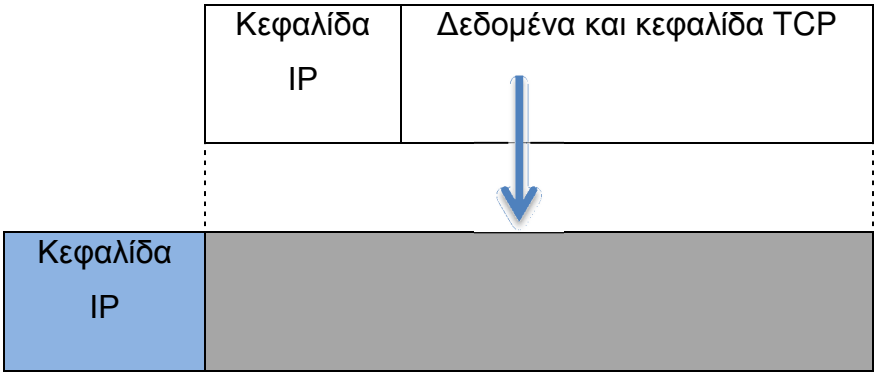
Μια συνηθισμένη σχεδίαση είναι να εξοπλίσουμε κάθε γραφείο μιας εταιρίας με αντιπυρική ζώνη και να δημιουργήσουμε σήραγγες μέσω του internet ανάμεσα σε όλα τα ζεύγη των γραφείων. Αν χρησιμοποιείται το IPSec για τις σήραγγες , τότε είναι εφικτή η συνάθροιση όλης της κίνησης ανάμεσα σε δυο ζεύγη γραφείων σε μια μόνο κρυπτογραφημένη και πιστοποιημένη SA, ώστε να μπορούμε να παρέχουμε έλεγχο ακεραιότητας, μυστικότητα, και σημαντική ανοσία στην ανάλυση της κίνησης. Όταν ξεκινά το σύστημα, κάθε ζεύγος αντιπυρικών ζωνών πρέπει να διαπραγματευτεί τις παραμέτρους την σύνδεσης SA, δηλαδή τις υπηρεσίες , την κατάσταση λειτουργιάς, τους αλγορίθμους και τα κλειδιά. Έτσι οι αντιπυρικές ζώνες , τα VPN και το IPSec με το ESP σε κατάσταση σήραγγας είναι ένας φυσικός συνδυασμός που χρησιμοποιείται ευρέως.

Για να επιτευχθεί η ιδιωτικότητα μέσα σε μια εταιρεία, χρησιμοποιούνται ταυτόχρονα 2 τεχνικές από την τεχνολογία VPN. Δίαυλος και ασφάλεια IP (IPsec).

5.5.1 Δίαυλος

Για να εξασφαλισθεί η ιδιωτικότητα για μια εταιρεία, η τεχνολογία VPN καθορίζει ότι κάθε διάγραμμα δεδομένων IP που προορίζεται για ιδιωτική χρήση σε μια εταιρεία, πρέπει να ενσωματώνεται σε άλλο διάγραμμα δεδομένων

Εσωτερικό διάγραμμα δεδομένων (κρυπτογραφημένο)

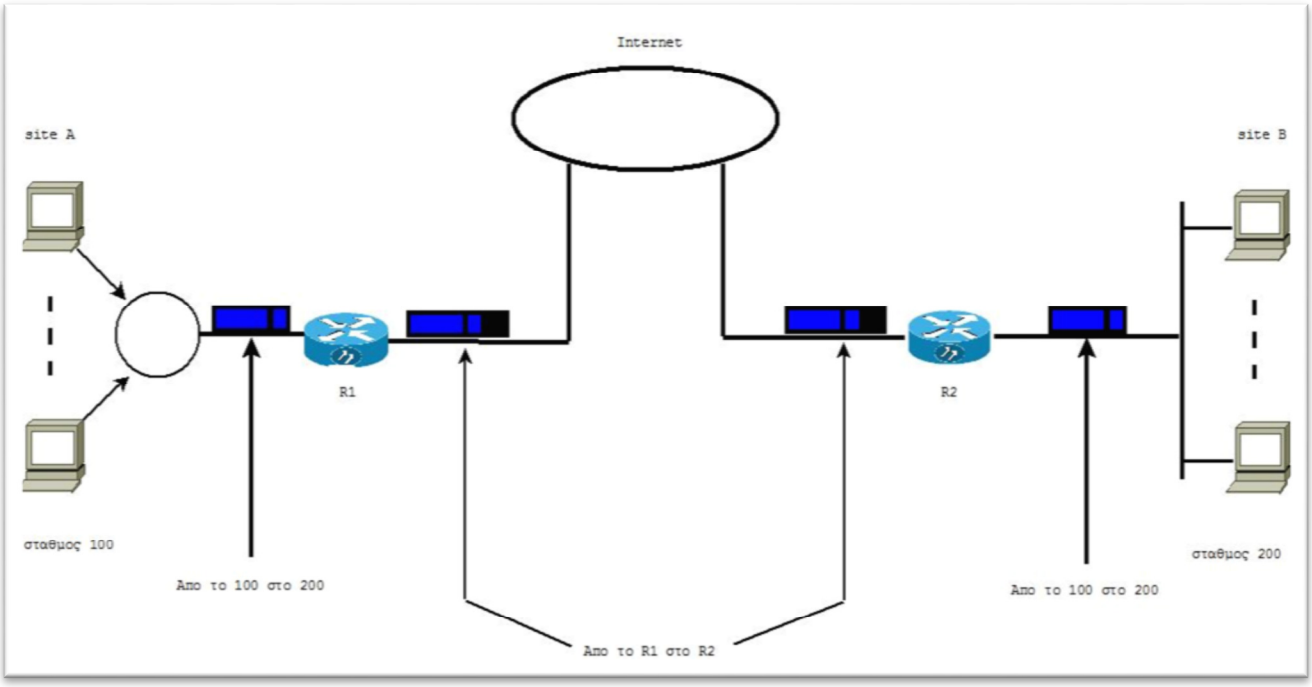


Εξωτερικό διάγραμμα δεδομένων (κρυπτογραφημένο)

Εικόνα 5-5 : Δίαυλος

Αυτό λέγεται δίαυλος, διότι το αρχικό διάγραμμα δεδομένων, κρύβεται στο εξωτερικό διάγραμμα δεδομένων αφού εξέλθει από τον δρομολογητή R1 και είναι ορατό μέχρι να φτάσει στον δρομολογητή R2.

Όπως φαίνεται και στην παρακάτω εικόνα, ολόκληρο το διάγραμμα δεδομένων IP (και η κεφαλίδα), πρώτα κρυπτογραφείται και μετά ενσωματώνεται σε άλλο διάγραμμα δεδομένων με μια νέα κεφαλίδα. Το ενσωματωμένο διάγραμμα δεδομένων φέρει την διεύθυνση πηγής και διεύθυνση προορισμού της πληροφορίας. Η κεφαλίδα του εξωτερικού διαγράμματος δεδομένων, φέρει την πηγή και τον προορισμό των 2 δρομολογητών στα όρια του ιδιωτικού και δημοσίου δικτύου. Το δημόσιο δίκτυο (internet) είναι υπεύθυνο για την μεταφορά της πληροφορίας από το R1 στο R2. Είναι αδύνατη η αποκρυπτογράφηση των περιεχόμενων του πακέτου από εξωτερικούς χρήστες ή διευθύνσεις πηγής και προορισμού. Η αποκρυπτογράφηση πραγματοποιείται στο R2 που βρίσκει την διεύθυνση προορισμού του πακέτου και το παραδίδει.



Εικόνα 5-6 : Διευθυνσιοδότηση σε ένα VPN

5.5.2 IPSec ασφάλεια στο internet

Για την παροχή ασφάλειας σε ένα πακέτο στο επίπεδο IP, το IETF (Internet Engineering Task Force), σχεδίασε μια συλλογή πρωτοκόλλων, την ασφάλεια IP (IPSec). Δεν εφαρμόζεται συγκεκριμένη μέθοδος αυθεντικοποίησης από το IPSec. Το IPSec αφήνει την επιλογή των μεθόδων κρυπτογράφησης, αυθεντικοποίησης και κατακερματισμού στην οντότητα, παρέχοντας ένα περιβάλλον εργασίας και έναν μηχανισμό.

Τα μετρά που λαμβάνονται για την ασφάλεια εφαρμόζονται στο επίπεδο μεταφοράς, το επίπεδο εφαρμογής και το επίπεδο δικτύου.

Στο επίπεδο IP πρέπει κάθε συσκευή να ενεργοποιηθεί. Για αυτόν τον λόγο, η υλοποίηση των στοιχείων ασφάλειας είναι πολύ πολύπλοκη.Το IP πέρα από τις υπηρεσίες που παρέχει σε εφαρμογές χρηστών, παρέχει υπηρεσίες και σε πρωτόκολλα όπως ICMP, IGMP ΚΑΙ OSPF. Για τον λόγο αυτό, δεν είναι ιδιαίτερα αποτελεσματική η ασφάλεια σε αυτό το επίπεδο, με εξαίρεση τις συσκευές που έχουν εξοπλιστεί έτσι, ώστε να την χρησιμοποιούν. Θα δούμε το IPsec πρωτόκολλο, το οποίο παρέχει ασφάλεια στο επίπεδο IP.

5.6 Εφαρμογές του IPSec

Το IPSec παρέχει τη δυνατότητα να ασφαλίζει τις επικοινωνίες κατά μήκος ενός τοπικού δικτύου(LAN), κατά μήκος ιδιωτικών και δημοσίων δικτύων ευρείας περιοχής(WAN) και κατά μήκος του Διαδικτύου. Παραδείγματα της χρήσης του:

- **Ασφάλεια στην συνδεσιμότητας υποκαταστημάτων μέσω του Διαδικτυου: Μια εταιρεία μπορεί να δημιουργήσει ασφαλή εικονικά ιδιωτικά δίκτυα (Virtual Private Networks, VPN) μέσω του Διαδικτύου ή μέσω ενός δημοσίου WAN. Αυτό επιτρέπει σε μια επιχείρηση να βασίζεται στο διαδίκτυο μειώνοντας την ανάγκη της για ιδιωτικά δίκτυα, εξοικονομώντας χρήματα και μειώνοντας το διαχειριστικό κόστος.**

- **Ασφάλεια στην τηλεπρόσβαση μέσω του Διαδικτύου: Ένας τερματικός χρήστης του οποίου το σύστημα είναι εφοδιασμένο με πρωτοκολλά ασφάλειας IP μπορεί να κάνει μια τοπική κλήση σε έναν παροχέα υπηρεσιών Διαδικτύου (ISP) και να επιτύχει ασφαλή πρόσβαση σε ένα εταιρικό δίκτυο. Με τον τρόπο αυτό μειώνεται το κόστος για την μετακίνηση ή τη σύνδεση των εργαζομένων.**

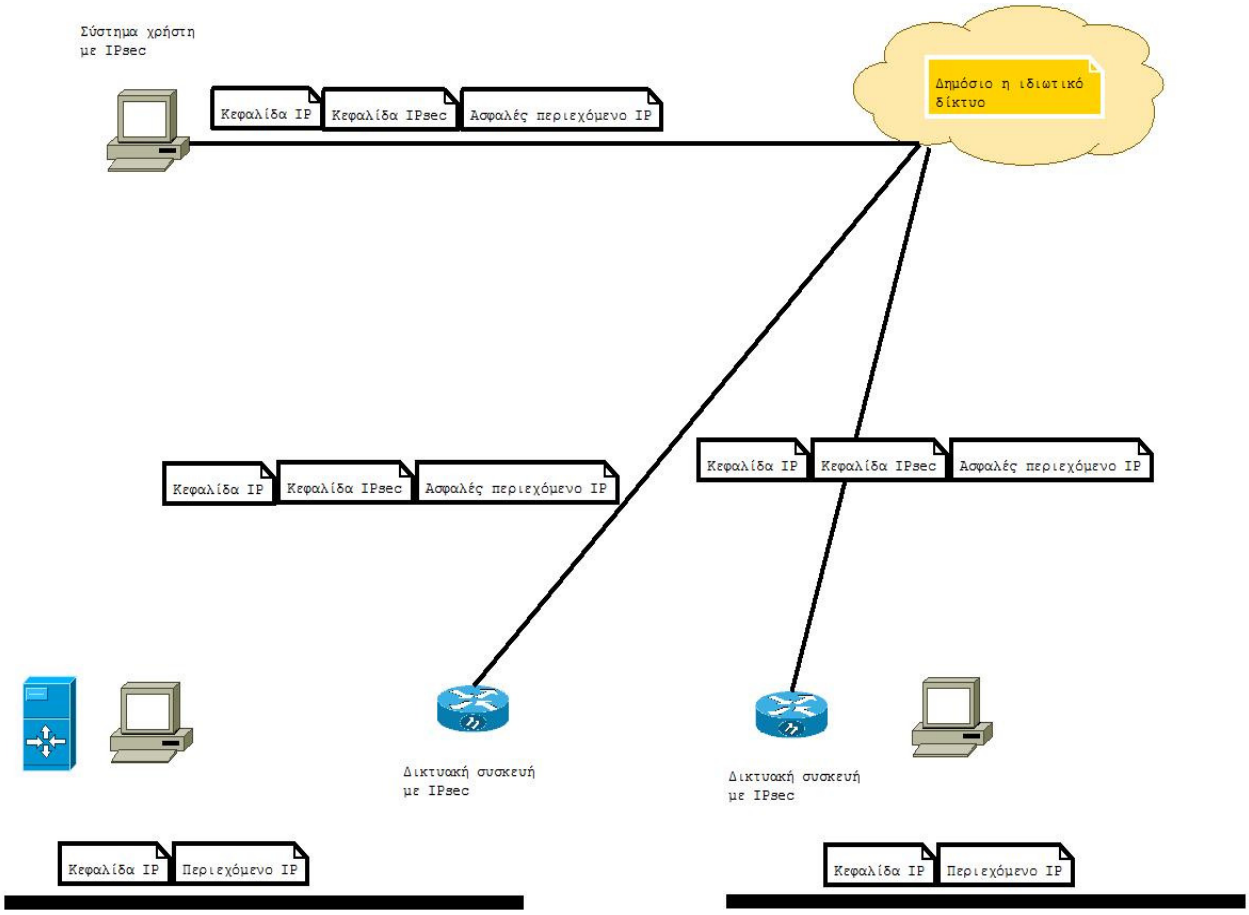
- **Εγκατάσταση συνδεσιμότητας υπερενδοδικτύου (extranet) και ενδοδικτύου (intranet) με συνεταίρους: Το IPSec μπορεί να χρησιμοποιηθεί για να ασφαλίσει την επικοινωνία με άλλους οργανισμούς, εξασφαλίζοντας πιστοποίηση αυθεντικότητας και την εμπιστευτικότητα και παρέχοντας μηχανισμούς ανταλλάγης κλειδιού.**

- **βελτίωση ασφάλειας ηλεκτρονικού εμπορίου : Έστω και αν κάποιες εφαρμογές του ηλεκτρονικού εμπορίου και συναλλαγών μέσω του Διαδικτύου έχουν ενσωματωμένα πρωτόκολλα ασφάλειας , η χρήση του IPSec αυξάνει την υπάρχουσα ασφάλεια**.

Το βασικό χαρακτηριστικό του IPSec που του επιτρέπει να υποστηρίζει αυτές τις ποικίλες εφαρμογές είναι ότι μπορεί να κρυπτογραφήσει και να πιστοποίηση όλη την κίνηση δεδομένων στο επίπεδο IP. Με τον τρόπο αυτό μπορούν να χρησιμοποιούν κρυπτογραφία όλες οι κατανεμημένες εφαρμογές, όπως η τηλεσύνδεση, οι εφαρμογές πελάτη διακομιστή, το ηλεκτρονικό ταχυδρομείο, η μεταφορά αρχείων, η πρόσβαση στον Παγκοσμιο ιστό, κ.λπ.

Στην παρακάτω εικόνα βλέπουμε μια τυπική εφαρμογή της χρήσης του IPSec. Μια εταιρεία εχεις τοπικά δίκτυα LAN σε διασκορπισμένα σημεία . Στο

κάθε τοπικό δίκτυο έχουμε κίνηση IP χωρίς τις λειτουργίες ασφάλειας. Για την κίνηση μέσω ιδιωτικού ή δημόσιου WAN , εφαρμόζουμε τα πρωτόκολλα IPsec. Τα πρωτόκολλα αυτά διαχειρίζονται συσκεύες δικτύου, όπως δρομολογητές ή αντιπυρικές ζώνες (firewalls), τα οποία συνδέουν κάθε LAN με τον εξωτερικό κόσμο. Οι συσκευές δικτύων IPSec συννήθως κρυπτογραφούν και συμπιέζουν την εξερχόμενη κίνηση προς το δίκτυο WAN, και αποκρυπτογραφούν και αποσυμπιέζουν την εισερχόμενη κίνηση άπο το δίκτυο WAN. Οι λειτουργίες αυτές δεν είναι ορατές στους σταθμούς εργασίας και τους διακομιστές του LAN. Είναι επίσης εφικτή και η ασφαλής μετάδοση σε μεμονωμένους χρήστες που συνδέονται με το δίκτυο WAN. Αυτοί οι σταθμοί εργασίας θα πρέπει να υλοποιούν τα πρωτόκολλα IPSec για την παροχή ασφάλειας.



Εικόνα 5-7 : Ένα σενάριο πρωτοκκόλου IPSec

5.7 Πλεονεκτήματα του IPsec

Τα πλεονεκτήματα του ipsec είναι τα εξής:

- **Όταν το IPsec υλοποιείται σε μια αντιπυρική ζώνη ή ένα δρομολογητή, παρέχει υψηλή ασφάλεια η οποία εφαρμόζεται σε όλη την κίνηση που διέρχεται από την περίμετρο του δικτύου. Η κίνηση στο εσωτερικό του δικτύου ή της ομάδας εργασίας δεν υφίσταται το πρόσθετο φορτίο της σχετικής με την ασφάλεια επεξεργασίας.**

- **Το IPsec βρίσκεται κάτω απο το επίπεδο μεταφοράς (TCP, UDP), επομένως είναι διαφανές (αόρατο) για τις εφαρμογές. Δεν χρειάζται να γίνει καμία αλλαγή στο λογισμικό του χρήστη του διακομιστή του συστήματος όταν το Ipsec υλοποιείται σε αντιπυρική ζώνη ή στο δρομολογητή. Ακόμα και αν το IPsec υλοποιείται σε τελικά συστήματα, το λογισμικό των υψηλότερων επιπέδων (όπως οι εφαρμογές) δεν επηρεάζεται.**

- **Το IPsec σε μια αντιπυρική ζώνη αποτρέπει την παράκαμψη όταν όλη η εξωτερική κίνηση χρησιμοποιεί το πρωτόκολλο IP και η αντιπυρική ζώνη είναι το μόνο σημείο εισόδου απο το διαδίκτυο στην εταιρεία.**

- **Το IPsec είναι αόρατο για τους τελικούς χρήστες. Δεν απαιτείται εκπαίδευση των χρηστών φια την εκμάθηση των μηχανισμών που έχουν σχέση με την ασφάλεια, ούτε και διανομή κλειδιών ή ανάκλησή τους αν οι χρήστες αποχωρήσουν απο την εταιρεία.**

- **Το IPsec μπρεί να παρέχει ασφάλεια για μεμονομένους χρήστες, αν υπάρχει τέτοια ανάγκη. Αυτό είναι χρήσιμο για εξωτερικούς χρήστες και για τη διαμόρφωση ενός εικονικού υποδικτύουευαίσθητων εφαρμογών στο εσωτερικό του οραγανισμού.**

5.8 Εφαρμογές δρομολόγησης

Έκτος από την υποστήριξη των τελικών χρηστών και την προστασία των αντίστοιχων συστημάτων και δικτύων, το IPSec παίζει ζωτικό ρόλο στην αρχιτεκτονική δρομολόγησης που απαιτείται για την διαδικτύωση (σύνδεση δικτύων). Το IPSec εξασφαλίζει ότι:

- **Μια γνωστοποίηση νέου δρομολογητή (ο νέος δρομολογητής δηλώνει την παρουσία του) προέρχεται από έναν πιστοποιημένο δρομολογητή.**

- **Μια γνωστοποίηση γειτονικού δρομολογητή προέρχεται από έναν πιστοποιημένο δρομολογητή (ένας δρομολογητής επιζητά τη δημιουργία ή την διατήρηση μιας σχέσης γειτονιάς με κάποιον δρομολογητή από άλλη περιοχή δρομολόγησης).**

- **Ένα μήνυμα ανακατεύθυνσης προέρχεται από τον δρομολογητή στον οποίο είχε αποσταλεί το αρχικό πακέτο.**

- **Η ενημέρωση μιας δρομολόγησης δεν έχει πλαστογραφηθεί.**

Χωρίς τέτοια μέτρα ασφάλειας, ένας αντίπαλος μπορεί να αναστατώσει την επικοινωνία ή να εκτρέψει την κίνηση δεδομένων. Τα πρωτόκολλα δρομολόγησης, όπως το OSPF, πρέπει να εκτελούνται πάνω από συσχετίσεις ασφάλειας μεταξύ των δρομολογητών που καθορίζονται από το IPSec.

5.9 Αρχιτεκτονική IPSec

οι προδιαγραφές του IPSec έχουν γίνει αρκετά σύνθετες. Για να πάρουμε μια εικόνα της γενικής αρχιτεκτονικής, πρέπει να εξετάσουμε την τεκμηρίωση του IPSec. Στην συνέχεια θα μελετήσουμε τις υπηρεσίες του και θα εισάγουμε την έννοια της συσχέτισης ασφάλειας (securuty association).

5.9.1 Τεκμηρίωση IPSec

Οι προδιαγραφές του αποτελούνται από αρκετά έγγραφα. τα πιο σημαντικά από αυτά είναι τα RFC 2401, 24202, 2406, και 2408.

- **RFC 2401: Γενική περιγραφή για την αρχιτεκτονική της ασφάλειας.**
- **RFC 2402: Περιγραφή της επέκτασης πιστοποίησης πακέτων για IPv4 και IPv6.**
- **RFC 2406: Περιγραφή της επέκτασης κρυπτογράφησης πακέτων για IPv4 και IPv6.**

- **RFC 2408: Προδιαγραφές λειτουργιών διαχείρισης κλειδιών.**

Η υποστήριξη αυτών των χαρακτηριστικών είναι υποχρεωτική στο IPv6 και προαιρετική στο IPv4. Και στις δυο περιπτώσεις, τα χαρακτηριστικά ασφάλειας υλοποιούνται ως επεκτάσεις της κύριας κεφαλιδας του IP. Η κεφαλίδα επέκτασης που αφορά την πιστοποίηση ονομάζεται κεφαλίδα πιστοποίησης (Authentication Header, AH), και η κεφαλίδα επέκτασης που αφορά την κρυπτογράφηση ενθυλάκωση φορτίου ασφάλειας (Encapsulating Security Payload, ESP).

Εκτός από τα παραπάνω έγγραφα, έχουν εκδοθεί πολυάριθμα προσχέδια από το IP Security Protocol Working Group του IETF. Αυτά χωρίζονται σε επτά ομάδες, όπως φαίνεται στην παρακάτω εικόνα.

- **Αρχιτεκτονική: Καλύπτει γενικές έννοιες, απαιτήσεις ως προς την ασφάλεια, ορισμούς, και μηχανισμούς που προσδιορίζουν την τεχνολογία IPSec.**

- **Ενθυλάκωση φορτίου ασφάλειας (ESP): καλύπτει την διαμόρφωση των πακέτων και γενικά θέματα για την χρήση του ESP στην κρυπτογράφηση, και προαιρετικά στην πιστοποίηση.**

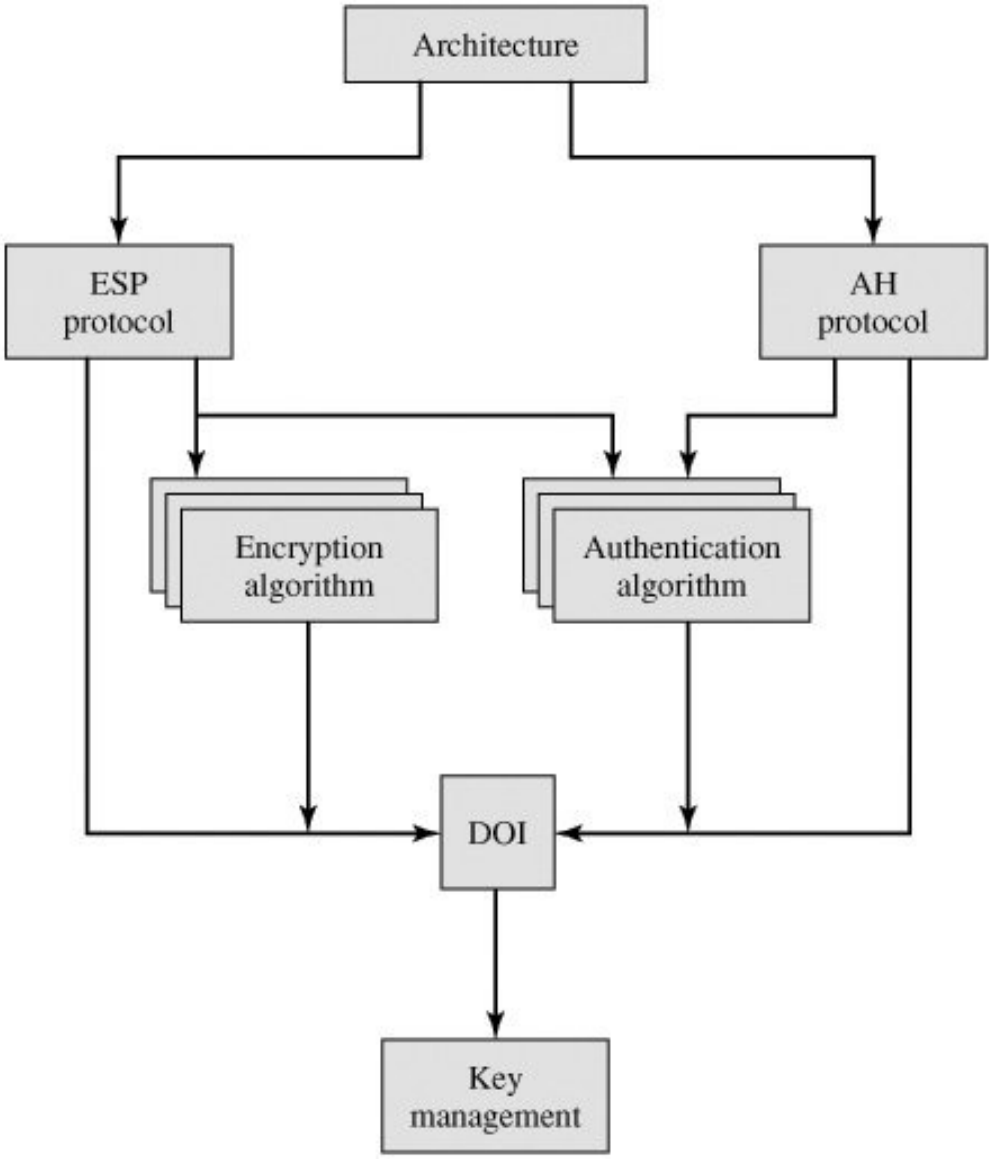
- **Κεφαλίδα πιστοποίησης αυθεντικότητας (AH): Καλύπτει την διαμόρφωση των πακέτων και γενικά θέματα για την χρήση της κεφαλιδας AH στην πιστοποίηση των πακέτων.**

- **Αλγόριθμος κρυπτογράφησης: Ένα σύνολο από έγγραφα που περιγράφουν πως χρησιμοποιούνται οι κρυπτογραφικοί αλγόριθμοι στο ESP.**

- **Αλγόριθμος πιστοποίησης: Ένα σύνολο από έγγραφα που περιγράφουν πως χρησιμοποιούνται οι αλγόριθμοι πιστοποίησης για τη κεφαλίδα AH και για τις επιλογές πιστοποίησης του ESP.**

- **Διαχείριση κλειδιών: Έγγραφα που περιγράφουν θέματα σχετικά με την διαχείριση κλειδιών.**

- **Τομέας ερμηνείας (Domain of Interpretation, DOI): Περιεχέι τιμές που απαιτούνται για την συσχέτιση των υπολοίπων εγγράφων. Σε αυτές τις τιμές περιλαμβάνονται αναγνωριστικά για τους εγκεκριμένους αλγορίθμους κρυπτογράφησης και πιστοποίησης, καθώς και λειτουργικές παράμετροι όπως η διάρκεια ζωής των κλειδιών.**



Εικόνα 5-8 : Επισκόπηση των εγγράφων IPSec

5.10 Υπηρεσίες IPSec

Το IPSec παρέχει υπηρεσίες ασφάλειας στο επίπεδο IP ενεργοποιώντας ένα σύστημα το οποίο δίνει την δυνατότητα επιλογής του απαιτούμενου πρωτοκόλλου ασφάλειας, προσδιορισμού των αλγορίθμων που θα χρησιμοποιηθούν, και εγκαθίδρυσης των κλειδιών κρυπτογραφίας που είναι απαραίτητα για την παροχή των υπηρεσιών. Χρησιμοποιώντας δυο πρωτοκολλά για την παροχή της ασφάλειας: η κεφαλίδα πιστοποίησης (AH) και ένας συνδιασμος πρωτοκόλλων κρυπτογράφησης και πιστοποίησης για την διαμόρφωση πακέτων -η ενθυλάκωση φορτίου ασφάλειας (ESP). Οι υπηρεσίες είναι οι ακόλουθες:

- **Έλεγχος πρόσβασης**
- **Ασυνδεσμική (connectionless) ακεραιότητα**
- **Πιστοποίηση προέλευσης δεδομένων**
- **Απόρριψη επαναλαμβανόμενων πακέτων (μια μορφή μερικής ακεραιότητας ακολουθίας)**
- **Εμπιστευτικότητα (κρυπτογράφηση)**
- **Περιοριμένη εμπιστευτικότητα ροής.**

Στον παρακάτω πινάκα φαίνονται οι υπηρεσίες που παρέχονται από τα πρωτοκολλά AH και ESP. Για το ESP υπάρχουν δυο εκδοχές: με ή χωρίς πιστοποίηση αυθεντικότητας. Και τα δυο πρωτοκολλά παρέχουν έλεγχο πρόσβασης, ο οποίος βασίζεται στην διανομή κρυπτογραφικών κλειδιών και τη διαχείριση της κυκλοφορίας ως προς τα πρωτοκολλά αυτά.

	AH	**ESP(μόνο κρυπτογράφηση)**	**ESP(κρυπτογράφηση και πιστοποίηση)**
Έλεγχος πρόσβασης	✓	✓	✓
Ασυνδεσμική ακεραιότητα	✓		✓
Πιστοποίηση δεδομένων	✓		✓
Απόρριψη επαναλαμβανόμενων πακέτων	✓	✓	✓
Εμπιστευτηκότητα		✓	✓
Περιορισμένη εμπιστευτηκότητα		✓	✓

Εικόνα 5-9 : Υπηρεσίες IPSec

5.11 Συσχέτιση ασφάλειας

Συσχέτιση ασφάλειας (SA), λέγεται η λογική σύνδεση μεταξύ 2 κεντρικών υπολογιστών οι οποίοι χρησιμοποιούν ένα πρωτόκολλο σηματοδότησης, το οποίο χρειάζεται το IPsec. Για να καταστεί εφικτή η εφαρμογή της ασφάλειας, το IPsec θα χρειαστεί το χωρίς σύνδεση πρωτόκολλο IP αλλαγμένο, όμως σε ένα βασισμένο σε σύνδεση πρωτόκολλο. Μια SA σύνδεση είναι μια μονόδρομη σύνδεση μεταξύ μιας πηγής και ενός προορισμού. Για μια αμφίδρομη σύνδεση, χρειάζονται 2 SA συνδέσεις, μια κάθε κατεύθυνση. Τα τρία στοιχειά που ορίζουν μια SA σύνδεση είναι:

- **Ένας δείκτης παραμέτρου ασφάλειας (SPI) μεγέθους 32 bits, ο οποίος ενεργεί ως ένα αναγνωριστικό εικονικού κυκλώματος το οποίο βασίζεται σε πρωτοκολλά με σύνδεση όπως το Package Relay ή το ATM.**

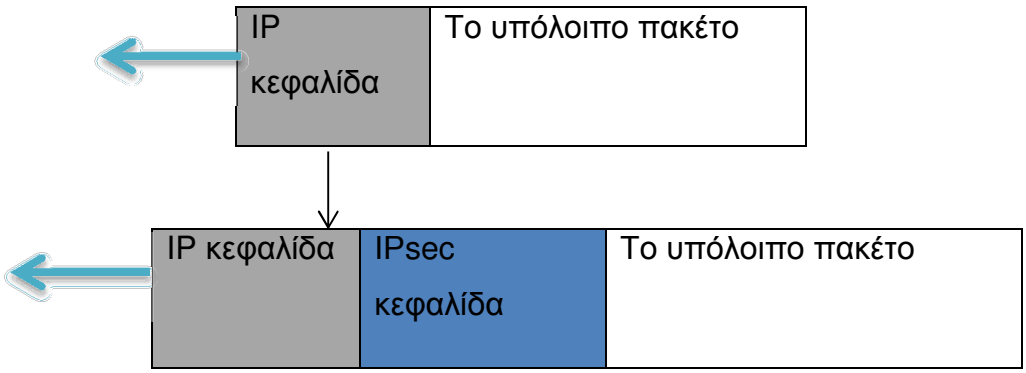
- **Η διεύθυνση IP της πηγής.**

- **Ο τύπος του πρωτοκόλλου που ορίζεται για ασφάλεια. Το IPsec ορίζει 2 εναλλακτικά πρωτοκολλά, το AH και το ESP.**

5.12 Δύο καταστάσεις

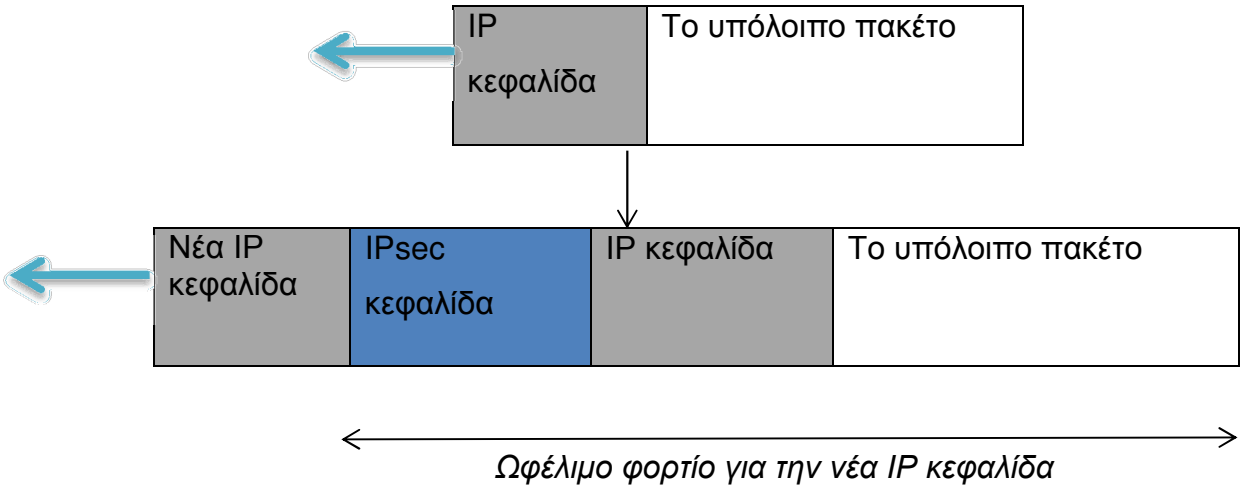
Το IPSec λειτουργεί σε δυο διαφορετικές καταστάσεις, την κατάσταση μεταφοράς και την κατάσταση διαύλου. Η κατάσταση μας δείχνει σε ποιο σημείο του IP πακέτου προστίθεται η κεφαλίδα IPsec.

- **Στην κατάσταση μεταφοράς η IPsec κεφαλίδα τοποθετείται ανάμεσα της IP κεφαλίδας και του υπολοίπου πακέτου, όπως φαίνεται στην παρακάτω.**



Εικόνα 5-10 : Κατάσταση μεταφοράς

- **Στην κατάσταση διαύλου η IPsec κεφαλίδα τοποθετείται μπροστά από την IP κεφαλίδα, ενώ μια νέα IP κεφαλίδα προστίθεται στην αρχή. Η IPsec κεφαλίδα, η αρχική IP κεφαλίδα καθώς και το υπόλοιπο πακέτο, αντιμετωπίζονται ως ωφέλιμο φορτίο. Στην παρακάτω εικόνα βλέπουμε το αρχικό και το νέο IP πακέτο.**



Εικόνα 5-11 : κατάσταση δίαυλου

5.13 Τα δύο πρωτόκολλα ασφαλείας

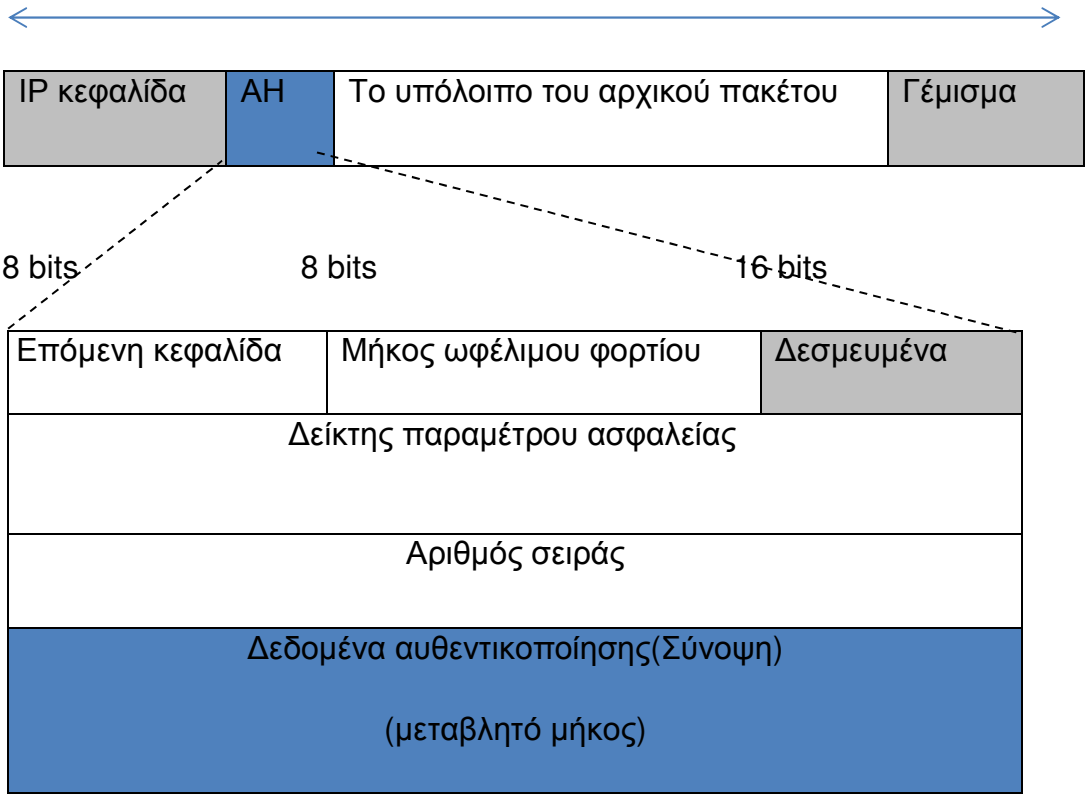
Το IPsec ορίζει 2 πρωτοκολλά:

Πρωτόκολλο Authentication Header (AH) και πρωτόκολλο Encapsulating Security Payload (ESP).

5.13.1 Authentication Header

Authentication Header (AH): Το πρωτόκολλο AH δημιουργήθηκε για να αυθεντικοποιεί την πηγή και να βεβαιώνει την ακεραιότητα του ωφελίμου φορτίου που υπάρχει στο IP πακέτο. Το πρωτόκολλο χρησιμοποιεί μια συνάρτηση κατακερμαστισμού και ένα συμμετρικό κλειδί, για να υπολογίσει μια σύνοψη μηνύματος. Στην συνεχεία εισάγει την σύνοψη στην κεφαλίδα αυθεντικοποιησης. Το AH, ανάλογα με την κατάσταση, θα τοποθετηθεί στην κατάλληλη θέση (μεταφοράς η διαύλου). Στην παρακάτω εικόνα φαίνεται η θέση καθώς και τα πεδία του πρωτοκόλλου Authentication Header στην κατάσταση μεταφοράς.

Δεδομένα που χρησιμοποιούνται στον υπολογισμό των δεδομένων αυθεντικοποίησης.



Εικόνα 5-12 : AH

Η αρχική τιμή του πεδίου πρωτοκόλλου της κεφαλιδας IP, σε ένα διάγραμμα δεδομένων IP που έχει ένα Authentication Header, θα αντικατασταθεί με την τιμή 51. Ένα πεδίο ενσωματωμένο στην κεφαλίδα αυθεντικοποίησης ορίζει την αρχική τιμή του πεδίου πρωτοκόλλου, δηλαδή ορίζει τον τύπο του ωφελίμου φορτίου το οποίο μεταφέρει το διάγραμμα δεδομένων IP. Η διαδικασία προσθήκης του Authentication Header είναι η εξής:

- **Ενα Authentication Header προστίθεται στο ωφέλιμο φορτίο με το πεδίο δεδομένων αυθεντικοποίησης να έχει τιμή μηδέν.**

- **Μπορεί να προστεθεί γέμισμα για να επιτευχθεί το συνολικό μήκος και στην περίπτωση ενός συγκεκριμένου αλγορίθμου κατακερματισμού.**

- **Ο κατακερματισμός βασίζεται στο συνολικό πακέτο. Μόνο όμως τα πεδία της κεφαλιδας IP που δεν αλλοιώνονται κατά την μεταφορά εμπεριέχονται στον υπολογισμό της σύναψης του μηνύματος (δεδομένα αυθεντικοποίησης).**

- **Τα δεδομένα της αυθεντικοποίησης περιλαμβάνονται στο Authentication Header.**

- **Η κεφαλίδα IP προστίθεται αφού έχει γίνει η αλλαγή του πεδίου πρωτοκόλλου 51.**

5.13.1.1 Περιγραφή πεδίων:

Επόμενη κεφαλίδα: Το πεδίο αυτό των 8 bits ορίζει τον τύπο του ωφελίμου φορτίου που μεταδίδεται από το διάγραμμα δεδομένων IP (TCP, UDP, ICMP, OSPF κ. ο. κ.). Η λειτουργία του είναι παρόμοια με το πεδίο πρωτοκόλλου στην κεφαλίδα IP πριν την πρόσθεση. Δηλαδή αντιγράφεται η τιμή του πεδίου πρωτοκόλλου στο διάγραμμα δεδομένων IP σε αυτό το πεδίο. Για να δείξουμε ότι ένα πακέτο φέρει ένα Authentication Header, η τιμή του πρωτοκόλλου στο διάγραμμα δεδομένων IP αλλάζει σε 51.

Ωφέλιμο φορτίο μήκους: Το πεδίο ωφέλιμο φορτίο μήκους των 8 bits έχει παραπλανητικό όνομα. Δεν ορίζει το μήκος του ωφελίμου φορτίου, αλλά ορίζει το μήκος του Authentication Header σε πολλαπλάσια των 4 bytes, χωρίς όμως να περιλαμβάνει τα πρώτα 8 bytes.

Δείκτης παραμέτρου ασφάλειας: Το πεδίο του SPI των 32 bits είναι αναγνωριστικό εικονικό κύκλωμα και είναι σταθερό για όλα τα πακέτα που αποστέλλονται κατά την διάρκεια μιας σύνδεσης συσχέτισης ασφάλειας.

Αριθμός σειράς: Η λειτουργία του συγκεκριμένου πεδίου των 32bits, είναι να τοποθετήσει τις πληροφορίες σε σειρά για τα διαγράμματα δεδομένων. Οι αριθμοί σειράς αποτρέπουν την επανάληψη, καθώς επίσης δεν επαναλαμβάνονται ακόμη και αν ένα πακέτο αναμεταδοθεί. Ο αριθμός σειράς όταν φτάσει το 2^{32} δεν αναδιπλώνεται και πρέπει να δημιουργηθεί μια νέα σύνδεση.

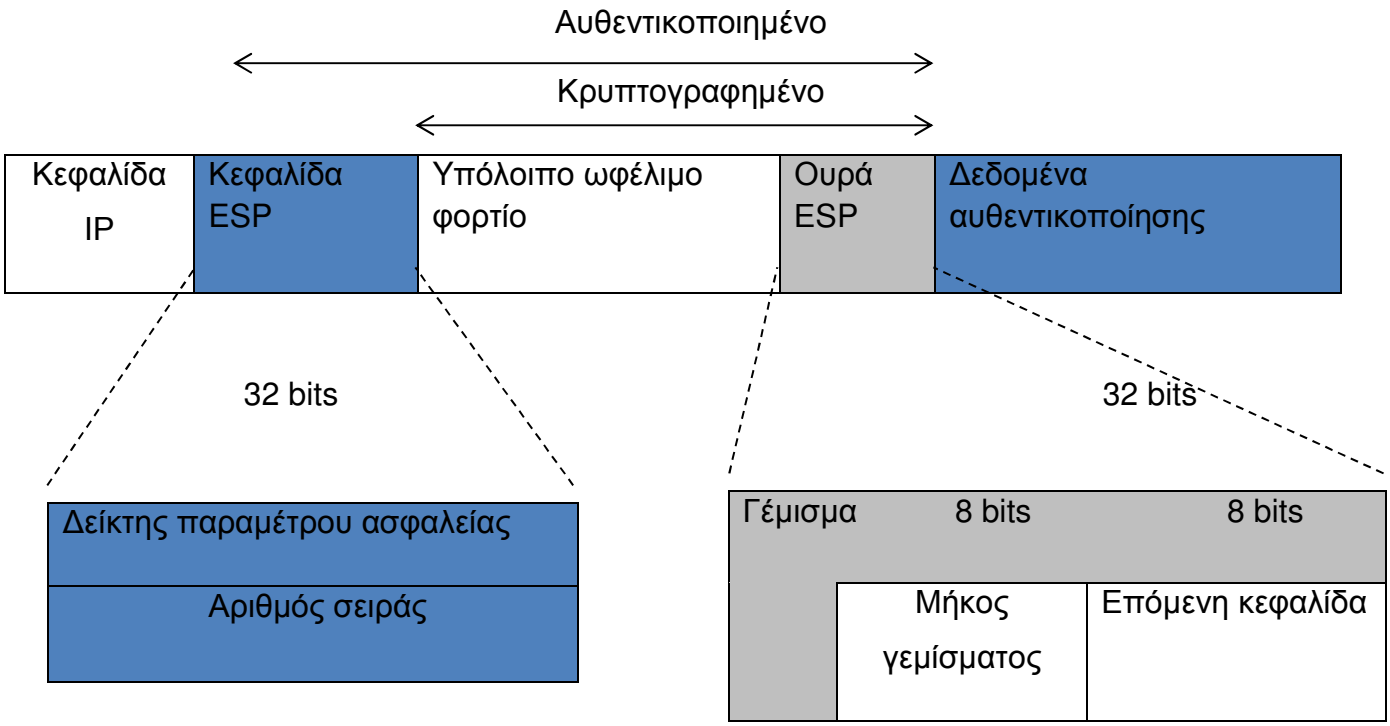
Δεδομένα αυθεντικοποίησης: Το πεδίο αυτό είναι το αποτέλεσμα της εφαρμογής μιας συνάρτησης κατακερματισμού σε όλο το διάγραμμα δεδομένων IP, εκτός από τα πεδία που αλλάζουν κατά την μεταφορά (π. χ. χρόνος ζωής).

Να σημειωθεί ότι το πρωτόκολλο Authentication Header εξασφαλίζει αυθεντικοποίηση και ακεραιότητα του μηνύματος, όχι όμως ιδιωτικότητα.

5.13.2 Ενσωματωμένο ωφέλιμο φορτίο δικτύου (ESP) :

Το πρωτόκολλο Authentication Header εξασφαλίζει την αυθεντικοποίηση και την ακεραιότητα του μηνύματος, αλλά δεν παρέχει και την ιδιωτικότητα.

Λόγω του συγκεκριμένου μειονεκτήματος το IPsecurity δημιούργησε αργότερα το εναλλακτικό πρωτόκολλο Encapsulating Security Payload (ESP), το οποίο εξασφαλίζει αυθεντικοποίηση, ακεραιότητα καθώς και ιδιωτικότητα. Το ESP ενσωματώνει μια κεφαλίδα και μια ουρά. Στο τέλος του πακέτου προστίθενται τα δεδομένα αυθεντικοποίησης του ESP, και με αυτόν τον τρόπο γίνεται πιο εύκολος ο υπολογισμός.



Εικόνα 5-13 : ESP

Όταν ένα διάγραμμα δεδομένων IP έχει μια κεφαλίδα και ουρά ESP, η τιμή του πεδίου πρωτοκόλλου στην κεφαλίδα IP αλλάζει σε 50. Το πεδίο επόμενης κεφαλίδας μέσα στην ουρά ESP, περιεχέι την αρχική τιμή του πεδίου πρωτοκόλλου (τον τύπο του ωφελίμου φορτίου που μεταδίδεται από το διάγραμμα δεδομένων IP, οπως το TCO ή το UDP). Η προσθήκη ενός Encapsulating Security Payload (ESP) ακολουθεί τα εξής βήματα:

- **Ενσωματωνεται μια ουρά ESP στο ωφέλιμο φορτίο.**

- **Γίνεται κρυπτογράφηση του ωφελίμου φορτίου και της ουράς.**

- **Ενσωματώνεται η κεφαλίδα ESP.**

- **Για να δημιουργηθούν τα δεδομένα αυθεντικοποίησης, θα χρησιμοποιηθούν η ουρά ESP, το ωφέλιμο φορτίο και η κεφαλίδα ESP.**

- **Στο τέλος της ουράς ESP, θα προστεθούν τα δεδομένα αυθεντικοποίησης.**

- **Η κεφαλίδα IP ενσωματώνεται μετά την αλλαγή της τιμής πρωτοκόλλου σε 50.**

Τα πεδία για την κεφαλίδα και την ουρά είναι τα ακόλουθα:

- ***Δείκτης παραμέτρου ασφάλειας*:** Το πεδίο αυτό των 32 bits, έχει την ίδια λειτουργία στο ESP όπως και στο AH.

- ***Αριθμός σειράς*:** Το πεδίο του αριθμού σειράς των 32 bits, έχει την ίδια λειτουργία στο ESP όπως και στο AH.

- ***Γέμισμα:*** Το συγκεκριμένο πεδίο είναι μεταβλητού μήκους (0 έως 255 bytes) με μηδενικά, και εξυπηρετεί ως γέμισμα.

- ***Μήκος γεμίσματος*****:** Το μήκος γεμίσματος είναι ένα πεδίο των 8bits, και στην ουσία αυτό που κάνει, είναι να ορίζει τον αριθμό των bytes γεμίσματος. Η τιμή ορίζεται μεταξύ 0 και 255 bytes. Να σημειωθεί ότι η μεγίστη τιμή ορίζεται σπάνια.

- ***Επόμενη κεφαλίδα*****:** Το πεδίο επόμενης κεφαλίδας των 8 bits, έχει την ίδια λειτουργία με αυτήν στο πρωτόκολλο AH. Έχει την ίδια λειτουργία με το πεδίο πρωτοκόλλου στην κεφαλίδα IP, πριν την ενσωμάτωση.

- ***Δεδομένα αυθεντικοποίησης*****:** Το συγκεκριμένο πεδίο είναι το αποτέλεσμα της εφαρμογής μιας μεθόδου αυθεντικοποίησης σε μέση του διαγράμματος δεδομένων. Υπαρχει μια διάφορα ανάμεσα στα δεδομένα αυθεντικοποίησης στο AH και στο ESP. Η διάφορα είναι ότι στο AH, μέρος της κεφαλιδας IP εμπεριέχεται στον υπολογισμό των δεδομένων αυθεντικοποίησης ενώ στο ESP, δεν περιλαμβάνεται.

5.14 IPv4 και IPv6

Το IPsec υποστηρίζει και τα δυο πρωτόκολλα. Υπάρχει μια διαφορά, στο IPv6 το AH και το ESP είναι μέρος της κεφαλίδας επέκτασης.

5.15 AH vs ESP

Η έλλειψη της ιδιωτικότητας μηνύματος είναι το μειονέκτημα του AH. Είναι επίσης, ο λόγος της δημιουργίας ενός βελτιωμένου πρωτοκόλλου, το οποίο περιέχει την ιδιωτικότητα μηνύματος, καθώς επίσης και όλες τις λειτουργίες του AH (αυθεντικοποίηση και ακεραιότητα μηνύματος). Λόγω του ότι το ESP είναι βελτιωμένη έκδοση του AH, γεννάται το ερώτημα: γιατί χρειαζόμαστε το AH; Η απάντηση είναι ότι δεν το χρειαζόμαστε. Η υλοποίηση του όμως, έχει συμπεριληφθεί στο παρελθόν σε μερικά εμπορικά προιοντα, πράγμα που σημαίνει ότι το Authentication Header θα παραμείνει στο διαδίκτυο έως ότου αποσυρθούν αυτά τα προιοντα.

Κεφάλαιο 6ο

Ανάλυση VPN τεχνολογιών

6.1 VPN τεχνολογίες

Τα πρωτόκολλα μετάδοσης δεδομένων που χρησιμοποιούνται στο διαδίκτυο, όπως το TCP/IP, δεν έχουν σχεδιαστεί για να προσφέρουν ασφάλεια δεδομένων. Σε αυτό το πλαίσιο, η έννοια ασφάλεια μπορεί να γίνει κατανοητή ως εξής; αν ο Bob και η Alice θέλουν να ανταλλάξουν προσωπικές πληροφορίες με ηλεκτρονικό τρόπο και η Mallory θέλει να τους παρακολουθήσει, τότε η μετάδοση θεωρείται ασφαλής αν η Mallory δεν έχει καμία πιθανότητα επιτυχίας. Με άλλα λόγια, ο εγκλωβισμός (encapsulation), η αυθεντικοποίηση και η κρυπτογράφηση δεν επιτρέπουν στη Mallory να αποκτήσει πρόσβαση στα δεδομένα. Αυτό επιτυγχάνεται με τη χρήση πρωτοκόλλων ασφαλείας όπως τα IPSec, L2TP και PPTP μαζί με τα υπάρχοντα πρωτόκολλα. Αυτές οι τεχνολογίες παρέχουν ασφαλείς διόδους (tunnels) μέσω ενός μη ασφαλούς δικτύου.

Όμως η προσθήκη τεχνολογιών ασφαλείας χαρακτηρίζεται και από κάποια μειονεκτήματα. Είτε οι συγκεκριμένες προδιαγραφές δεν είναι επαρκώς καλές για να προσφέρουν ασφαλείς, γρήγορες και σταθερές συνδέσεις δεδομένων, είτε η αλληλεπίδραση με πρωτόκολλα χαμηλότερων επιπέδων προκαλεί προβλήματα. Σε αυτή την ενότητα παρουσιάζονται οι ευρέως διαδεδομένες τεχνολογίες VPN L2TP και PPTP και στη συνέχεια συγκρίνονται σε πρακτικό επίπεδο. Αυτές οι τεχνολογίες, όπως και η IPSec, είναι ευρέως χρησιμοποιούμενες και έχουν αναλυθεί εκτενώς. Υπάρχουν τόσο για

εμπορικά προϊόντα και open-source υλοποιήσεις που στηρίζονται σε αυτές. Παρουσιάζεται επίσης και η λύση phion VPN.

6.1.1 L2TP (Layer Two Forwarding Protocol)

Το πρωτόκολλο Layer Two Tunneling βασίζεται στο πρωτόκολλο Layer Two Forwarding (L2F). Ενεργοποιεί τον εγκλωβισμό ενός ολόκληρου πλαισίου data-link-layer σε ένα πακέτο UDP σε επίπεδο μεταφοράς, για παράδειγμα ένα πλαίσιο Ethernet. Το πρωτόκολλο UDP (User Datagram Protocol) είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στην ανταλλαγή πληροφοριών στο διαδίκτυο, δεν εγγυάται αξιόπιστη επικοινωνία και χρησιμοποιείται όταν η γρήγορη παράδοση των πακέτων είναι πιο σημαντική από την "ακριβή" παράδοση.

Έτσι, ένα πακέτο δεδομένων με διεύθυνση τοπικού ή ιδιωτικού δικτύου μπορεί να σταλεί στο διαδίκτυο. Το πακέτο UDP, που μεταφέρει το πλαίσιο δύο επιπέδων, αποτελείται από τα παρακάτω πεδία δεδομένων: μετά την κεφαλίδα UDP (port 1701), αρκετά bits ελέγχου που αναπαριστούν διάφορες επιλογές, εκδόσεις και μήκη του πακέτου. Μετά από αυτά, ακολουθίες αριθμών και πεδία ταυτοποίησης διόδων διατηρούν στοιχεία για την τρέχουσα VPN σύνδεση έτσι ώστε να βεβαιώσουν τη σωστή επεξεργασία και προώθηση του πακέτου. Στη συνέχεια, ακολουθεί το πλαίσιο δύο επιπέδων, το οποίο περιέχει για παράδειγμα διευθύνσεις κωδικών media (Media Access Code – MAC) και πληρωμές. Είναι φανερό πως ο απλός εγκλωβισμός ενός πλαισίου δύο επιπέδων σε ένα πακέτο UDP δεν προσφέρει ταυτοποίηση δεδομένων και ιδιωτικότητα. Επομένως, το πρωτόκολλο L2T συνδυάζεται συχνά με IPSec προσθέτοντας την κεφαλίδα IPSec μπροστά από την κεφαλίδα του L2TP κάνοντας τις κατάλληλές προσαρμογές ώστε το overhead να μην ξεπεράσει το επιθυμητό όριο.

6.1.2 PPTP (point-to-point tunneling protocol)

Το πρωτόκολλο PTP της Microsoft αποτελεί επέκταση του Point-To-Point πρωτοκόλλου της εταιρείας. Χρησιμοποιεί δύο διαφορετικά είδη πακέτων για να καταστήσει τη σύνδεση VPN. Πρώτα, τα πακέτα generic routing encapsulation (GRE) μεταφέρουν το φορτίο του VPN προσθέτοντας την κεφαλίδα GRE στο αντίστοιχο πακέτο. Η κεφαλίδα αυτή μοιάζει αρκετά με την κεφαλίδα L2TP και περιέχει διάφορα bit ελέγχου, ακολουθίες διόδων και αριθμών. Ο δεύτερος τύπος πακέτων είναι το PPTP μήνυμα ελέγχου. Αυτό είναι απλώς ένα πακέτο TCP (port 1723) που περιέχει πληροφορίες ελέγχου, όπως αιτήματα σύνδεσης και απαντήσεις, παραμέτρους σύνδεσης και μηνύματα λάθους. Προκειμένου να υπάρχει και κρυπτογράφηση και αυθεντικοποίηση, το PPTP πρέπει να συνδυαστεί με επιπλέον μεθόδους ασφαλείας. Για αυτό το σκοπό η Microsoft χρησιμοποιεί το πρωτόκολλο αυθεντικοποίησης MS-CHAP για να αυθεντικοποιεί και τους δύο χρήστες των διόδων. Η κρυπτογράφηση γίνεται με το συμμετρικό κρυπτογράφημα RC4. Επειδή το πρωτόκολλο είναι αρκετά απλό, μπορεί να εφαρμοστεί για την εγκαθίδρυση συνδέσεων VPN μεταξύ των δικτύων των παρόχων διαδικτύου και των πελατών τους χωρίς επιπλέον λογισμικό.

6.1.3 Phion VPN

Η Αυστριακή εταιρεία phion Information Technologies αναπτύσσει και πουλάει ένα λογισμικό ασφαλείας που ονομάζεται netfence, που περιέχει μία λύση VPN. Το πρόγραμμα είναι μία ολοκληρωμένη εμπορική λύση για επαγγελματικά δίκτυα και προσφέρει ολοκληρωμένες λύσεις ασφαλείας, συμπεριλαμβανομένων firewalls, ασφάλεια στο mail και το διαδίκτυο και δυνατότητες καταγραφής συμβάντων.

Η εγκαθίδρυση συνδέσεων VPN γίνεται ως εξής: με τον όρο αρχικοποιητής θα ονομάζουμε τον Client που θέλει να εγκαθιδρύσει τη σύνδεση, ενώ με τον όρο απαντητή αυτόν που ενεργεί ως server και ελέγχει την ταυτότητα του αρχικοποιητή πριν εγκαθιδρυθεί η δίοδος σύνδεσης.

Τη στιγμή της ρύθμισης μία μοναδική συμβολοσειρά με την ταυτότητα της διόδου ανατίθεται σε κάθε σύνδεση VPN. Πρώτα, ο αρχικοποιητής στέλνει ένα αίτημα διόδου στον απαντητή, που περιέχει ένα κρυπτογραφημένο cookie. Ο server δε χρειάζεται να υπολογίσει το cookie κάθε φορά που ο αρχικοποιητής στέλνει ένα αίτημα. Μπορεί να χρησιμοποιήσει το αποθηκευμένο cookie, που παρέχει μία βασική προστασία DOS (denial of service TODO) για να τον αυθεντικοποιήσει. Μετά την αποκρυπτογράφηση το server cookie επιστρέφεται στο server μαζί με ένα κρυπτογραφημένο client-cookie. Ο απαντητής ελέγχει το αποκρυπτογραφημένο server cookie και αποκρυπτογραφεί το client-cookie που έλαβε από τον client. Το επόμενο βήμα είναι η ανταλλαγή των παραμέτρων της διόδου όπως κρυπτογραφήματα, διαδρομές στο δίκτυο και άλλες επιλογές. Μετά από αυτό η σύνδεση έχει εγκαθιδρυθεί.

Μετά από την εγκαθίδρυση της σύνδεσης, η VPN κίνηση μπορεί να ανταλλαχθεί μέσω τεσσάρων διαφορετικών εκδοχών των διόδων, που καθορίζονται κατά τη ρύθμιση. Οι δύο πρώτες, που ονομάζονται TCP και UDP δίοδοι, προσθέτουν μία επιπλέον TCP ή UDP κεφαλίδα στο εγκλωβισμένο πακέτο. Η τρίτη εκδοχή διόδου ονομάζεται υβριδική και αναπαριστά ένα συνδυασμό από διόδους TCP και UDP, καθώς στέλνει κίνηση TCP σε μία δίοδο UDP και το αντίστροφο. Η τελευταία εκδοχή είναι η ESP, η οποία έχει ήδη περιγραφεί σε προηγούμενη ενότητα.

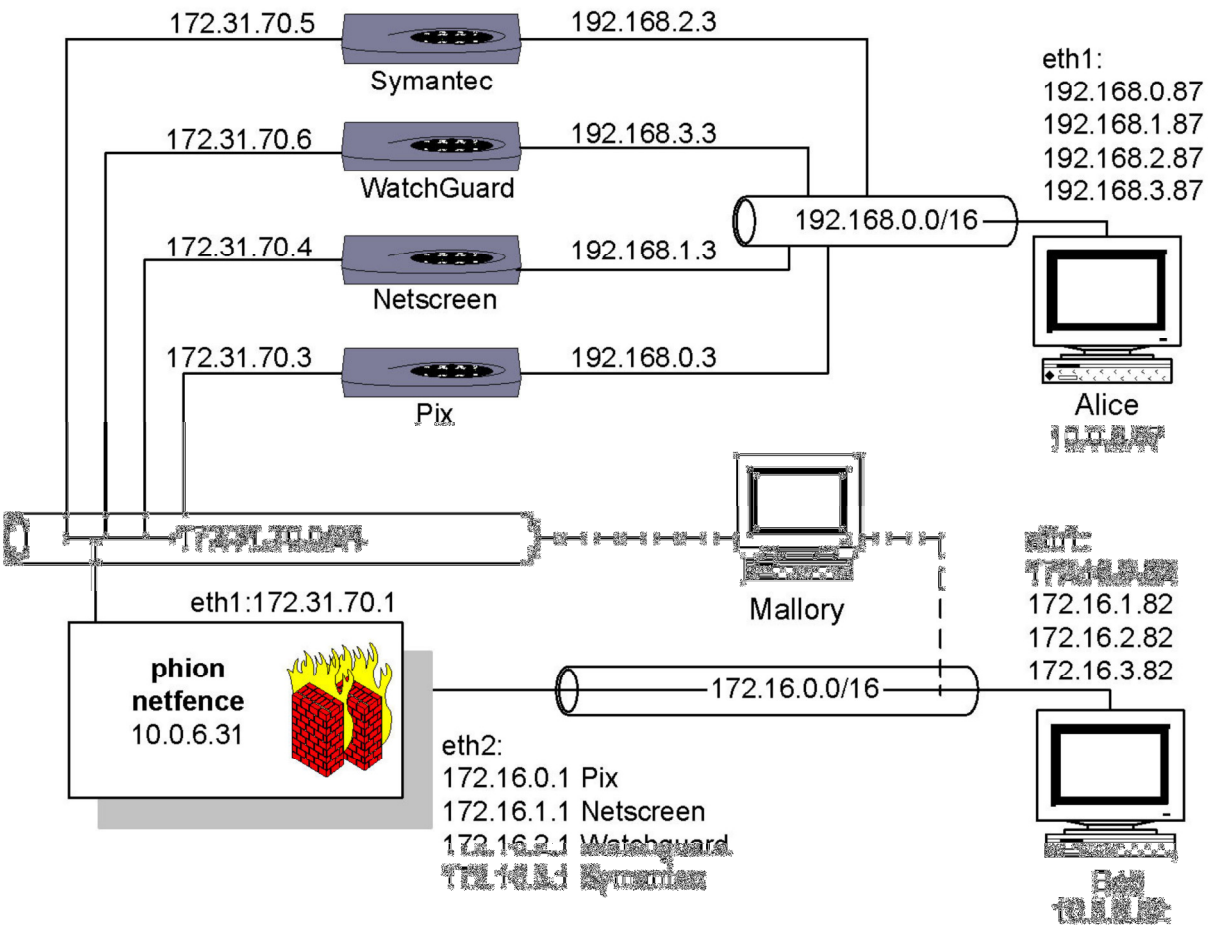
6.2 Πρακτική ανάλυση

Ακολουθεί η πρακτική ανάλυση όσων τεχνολογιών περιγράφηκαν παραπάνω. Κάθε σενάριο που τεστάρεται, περιγράφεται από το περιβάλλον ελέγχου, τη μέθοδο ελέγχου και έναν πίνακα σύγκρισης.

6.2.1 Περιβάλλοντα ελέγχου

Το περιβάλλον ελέγχου για το IPSec φαίνεται στο σχήμα. Τεσταρίστηκαν τέσσερις διαφορετικές συσκευές VPN και η αλληλεπίδρασή τους με το phion netfence IPSec:

- Cisco Systems Pix 501
- Netscreen 5XP
- Soho Watchguard WG2500
- Symantec FW/VPN 100

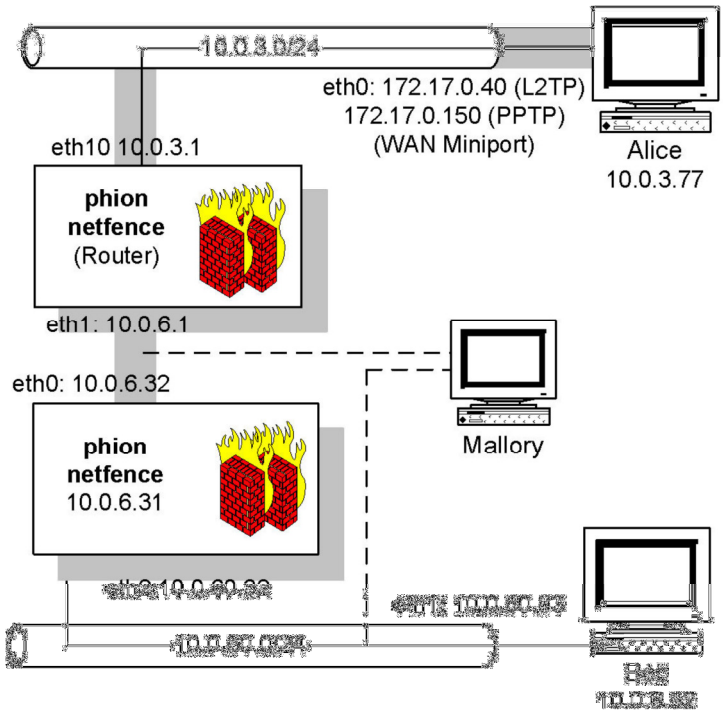


Εικόνα 6-1 : περιβάλλοντα ελέγχου IPSec

Οι σταθμοί εργασίας Linux με ονόματα Alice και Bob ανταλλάσσουν δεδομένα είτε απευθείας από το δίκτυο Ethernet (10.0.6.0/24, δε φαίνεται στην εικόνα) είτε των διόδων IPSec μεταξύ των συσκευών και της phion netfence gateway. Επομένως, οι Alice και Bob λαμβάνουν διευθύνσεις IP από το δίκτυο, 172.16.0.0/16 και 192.169.0.0/16 αντίστοιχα. Ο σταθμός εργασίας Mallory τοποθετήθηκε στο δίκτυο ως 172.31.70.0/24 (wiretap VPN traffic) και 172.16.0.0/16 (wiretap normal traffic).

Από τη στιγμή που τα phion VPN gateways υποστηρίζουν τόσο L2TP όσο και PPTP διόδους, η μία πλευρά της διόδου (Alice) στηρίχθηκε σε ένα Microsoft Windows XP σταθμό εργασίας, διότι και τα δύο πρωτόκολλα υποστηρίζονταν

(WAN miniport). Προκειμένου να διαχωρίσουμε τους δύο τύπους από VPN διόδους, χρησιμοποιήθηκαν διαφορετικές διευθύνσεις IP όπως φαίνεται στο επόμενο σχήμα. Το πρωτόκολλο χρησιμοποιήθηκε μαζί με το IPSec, όπως γίνεται και στην πράξη. Το phion router gateway μεταξύ του phion VPN gateway και της Alice εκτελούσε απλώς την προώθηση των πακέτων και τη μετάφραση των διευθύνσεων. Ο Bob ήταν ένας σταθμός εργασίας Linux και αντάλλασσε δεδομένα με την Alice είτε απευθείας είτε μέσω δύο διαφορετικών διόδων VPN. Η Mallory χρησιμοποιήθηκε για την παρακολούθηση και την ανάλυση της κίνησης.



Εικόνα 6-2 : περιβάλλοντα ελέγου L2TP/ PPTP

Για τις διάφορες ακολουθίες ελέγχων, εκτός των λειτουργικών συστημάτων και του λογισμικού για τις πύλες των VPN, χρησιμοποιήθηκαν ειδικά λογισμικά προκειμένου να παράγουν και να αναλύσουν την κίνηση IP.

Για την ανάλυση των πακέτων, χρησιμοποιήθηκε το δωρεάν πρόγραμμα Ethereal. Για τη δημιουργία κίνησης και τις μετρήσεις throughput και χρόνου για την ολοκλήρωση της μετάδοσης των πληροφορίων (και για τις δύο διαδρομές) χρησιμοποιήθηκε το Iperf. Πρόκειται για ένα εργαλείο που κάνει χρήση της γραμμής εντολών που παράγει δεδομένα UDP ή TCP. Για τη διαχείριση των πακέτων και τις επιθέσεις ασφαλείας εφαρμόστηκε το Hping έτσι ώστε να διεισδύει αυτοσχεδιαζόμενα πακέτο στο δίκτυο.

Προκειμένου να λάβουμε συγκρίσιμα πειραματικά αποτελέσματα, η ρύθμιση όλων των διαφορετικών τεχνολογιών VPN πρέπει να είναι όσο πιο παρεμφερής γίνεται. Παρόλα αυτά, αφού οι VPN τεχνολογίες χρησιμοποιούν διαφορετικές τεχνικές για να εγκαθιδρύσουν τις συνδέσεις, μία εντελώς ίδια ρύθμιση δεν ήταν εφικτή. Σε κάθε περίπτωση, οι ρυθμίσεις που χρησιμοποιήθηκαν για τους ελέγχους δίνουν συγκρίσιμα αποτελέσματα και αφού έχει χρησιμοποιηθεί και ακριβώς το ίδιο υλικό, οι διαφορές που προκύπτουν στις μετρήσεις αφορούν αμιγώς τις διαφορετικές τεχνολογίες VPN που χρησιμοποιήθηκαν, οι οποίες φαίνονται στον παρακάτω πίνακα:

VPN-Tech.	Tunnel-mode	Authen-tication	Key-length	Algo-rithmn	Hash-funct.
IPSec	ESP-Tunnel	Diffie-Hellman	Group 2 768	3DES-CBC	MD5
L2TP-IPSec	ESP Tunnel	Diffie-Hellman	Group 2 768	3DES-CBC	MD5
PPTP-ption	GRE-Tunnel ESP-Tunnel	MS-CHAP ener.	Hash-192 --	RC4 3DES-	- MD5
VPN	Tunnel	Cookies		CBC	

Εικόνα 6-3 : Διαμόρφωση VPN

6.3 Βασικές λειτουργίες

Τα πρώτα τεστ αφορούν τις βασικές λειτουργίες VPN, όπως ο χρόνος εγκαθίδρυσης διόδων VPN, η ποιότητα των συνδέσεων και ο χρόνος επαναρχικοποίησης των διόδων. Η εγκαθίδρυση των VPN διόδων μετρήθηκε μέσω του Ethereal. Η Alice και ο Bob αντάλλασσαν ping μηνύματα ICMP (Internet Control Message Protocol) κάθε 100 ms.

Μετά την επιτυχή εγκαθίδρυση διόδων, αυτά τα μηνύματα ICMP έφτασαν στον προορισμό τους. Το χρονικό διάστημα μεταξύ του πρώτου πακέτου της αρχικοποίησης της διόδου και της πρώτης μετάδοσης ICMP μηνύματος παρουσιάζεται στον επόμενο πίνακα.

Για τη μέτρηση της ποιότητας, η Alice και ο Bob αντάλλασσαν μηνύματα μεγέθους 1400-Byte. Οι μετρήσεις αφορούσαν το χρόνο αποστολής των μηνυμάτων και για τις δύο διαδρομές (round-trip time - RTT). Το ίδιο τεστ

έλαβε χώρα για την απευθείας σύνδεση χωρίς VPN έτσι ώστε να φανεί ο επιπλέον χρόνος που απαιτείται κατά τη χρήση τεχνολογιών VPN.

Η τρίτη σειρά ελέγχων σε αυτό το σενάριο αφορούσε το χρόνο επανεγκαθίδρυσης των διόδων, με λίγα λόγια, πόσο διαρκεί η επανασύνδεση μετά τη διακοπή της σύνδεσης. Για αυτό το σκοπό η Alice και ο Bob αντάλλασσαν μηνύματα ICMP κάθε 100 ms μέσω της διόδου ICMP. Τότε, η σύνδεση του δικτύου διακοπτόταν σκοπίμως. Μετά από 10 sec επιτρεπόταν η επανασύνδεση. Η μέτρηση αφορούσε το χρόνο από τη στιγμή της επανεγκαθίδρυσης της σύνδεσης μέχρι την εμφάνιση του πρώτου μηνύματος ICMP στη δίοδο. Οι μετρήσεις αυτές φαίνονται στον επόμενο πίνακα.

VPN-techn.	Vendor	Init. time [sec]	RTT [msec]	Re-init. time [sec]
no VPN	(ethernet)	-	0,18	-
IPSec	Cisco	0,72	18,00	33
	Netscreen	0,72	15,86	31
	Symantec	1,89	14,76	100
	Watchguard	1,96	22,01	33
L2TP	Microsoft	7,42	10,56	31
PPTP	Microsoft	7,84	4,15	-
netfence	phion	3,07	17,09	2

Εικόνα 6-4 : Αποτελέσματα βασικών δοκιμών λειτουργικότητας

Παρότι το IPSec χαρακτηρίζεται από μία περίπλοκη διαδικασία εγκαθίδρυσης σύνδεσης, όλες οι συσκευές IPSec παρουσίασαν αξιόλογα αποτελέσματα όσον αφορά το χρόνο αρχικοποίησης, ενώ την ίδια στιγμή και οι τρεις άλλες τεχνολογίες χρειάζονται περισσότερο χρόνο. Μελετώντας τα αποτελέσματα για το round-trip time, το πρωτόκολλο PPTP παρουσιάζει την καλύτερη επίδοση, και αυτό αφορά το μικρό GRE overhead. Όλες οι άλλες τεχνολογίες έχουν συγκριτικά κακά αποτελέσματα. Ο χρόνος RTT για τη σύνδεση χωρίς VPN είναι δραματικά μικρότερος, πράγμα που δείχνει ότι η χρήση VPN τεχνολογιών οδηγεί σε απώλεια επίδοσης. Τα αποτελέσματα της επανεγκαθίδρυσης της διόδου δείχνουν ότι το IPSec απαιτεί αρκετό χρόνο, ειδικά η υλοποίηση της Symantec. Αυτό δε σημαίνει απαραίτητα ότι η υλοποίηση της Symantec ήταν κακή, αλλά ίσως υπήρχε κακή αλληλεπίδραση μεταξύ των πυλών της Symantec και του IPSec. Αυτό υποδεικνύει ότι η διαλειτουργικότητα του IPSec δεν είναι πάντα εύκολη, πράγμα που οδηγεί πίσω στα μειονεκτήματα του IPSec. Οι δίοδοι L2TP και PPTP δεν επαναρχικοποιήθηκαν αυτόματα, αλλά χρειαζόταν χειροκίνητη ενεργοποίηση της αρχικοποίησης των διόδων στα Windows XP. Η καλύτερη επίδοση επιτεύχθηκε από την τεχνολογία phion netfence VPN.

6.4 Επίδοση

Για τη μέτρηση της επίδοσης, χρησιμοποιήθηκε το Iperf. Για όλες τις VPN τεχνολογίες ανταλλάχθηκε ο ίδιος αριθμός κίνησης (traffic): TCP traffic, μέγεθος παραθύρου 32 Kbytes, διάρκεια 10 sec. Η πρώτη σειρά ελέγχων έλαβε χώρα χρησιμοποιώντας μόνο ένα TCP session, για τη δεύτερη παράχθηκαν 100 ταυτόχρονων TCP sessions. Το Iperf εκτυπώνει το μέσο throughput. Οι τιμές φαίνονται στον παρακάτω πίνακα.

VPN-. Tech.	Vendor	Throughput 1 TCP session [MBits/sec]	Throughput 100 TCP sessions [MBits/sec]
no VPN	(ethernet)	94,0	92,2
IPSec	Cisco	2,71	-
	Netscreen	7,02	-
	Symantec	3,25	-
	Watchguard	1,45	-
L2TP	Microsoft	8,72	6,42
PPTP	Microsoft	29,80	8,25
netfence	phion	9,66	4,78

Εικόνα 6-5 : Αποτελέσματα μέτρησης επίδοσης

Χωρίς VPN, επιτεύχθηκε ρυθμός 94 Mbit/Sec, το οποίο αντιστοιχεί περίπου στο μέγιστο througput που μπορεί να επιτευχθεί με μέσα της τάξης των 100 Mbit, δηλαδή γρήγορες συνδέσεις Ethernet. Συγκρινόμενα με τα αποτελέσματα των διαφορετικών VPN τεχνολογιών, υπάρχει δραματική απώλεια απόδοσης, ειδικά όταν χρησιμοποιούνται IPSec συσκευές. Οι συσκευές αυτές, που δεν ήταν εξοπλισμένες με γρήγορους επεξεργαστές, δεν ήταν σε θέση να διαχειριστούν 100 ταυτόχρονα sessions. Όλα τα IPSec sessions κατέρρευσαν και έπρεπε να αρχικοποιηθούν ξανά, πράγμα που σημαίνει ότι τέτοιου είδους συσκευές δεν πρέπει να πιέζονται ιδιαίτερα. Τα καλύτερα αποτελέσματα επιτεύχθηκαν από το PPTP, αλλά αυτό προκύπτει λόγω του απλού RC4 κρυπτογραφήματος. Ο επιπλέον χρόνος επεξεργασίας που απαιτείται όταν χρησιμοποιούνται τεχνολογίες VPN οδηγεί σε σημαντική απώλεια επίδοσης.

6.5 Αλληλεπίδραση με TCP/IP

Τα επόμενα τεστ έλαβαν χώρα προκειμένου να αναλυθούν τα προβλήματα του συνδυασμού των τεχνολογιών VPN με το πρωτόκολλο TCP/IP. Αυτό εξετάστηκε μέσω μηνυμάτων ICMP διαφορετικών μεγεθών, επιπλέον κεφαλίδες VPN, τη συμπεριφορά του κατακερματισμού των IP πακέτων και τις NAT/NAPT (network address translation) δυνατότητες. Το πρώτο τεστ ελέγχει το επιπλέον overhead δεδομένων που προκαλείται από τις τεχνολογίες VPN. Για αυτό το σκοπό, ανταλλάχθηκαν ICMP μηνύματα μεγέθους 1000 bytes, έτσι ώστε να μετρηθούν το πραγματικό μέγεθος των μηνυμάτων που στάλθηκαν μέσω της διόδου VPN με τη χρήση του Ethereal. Τα αποτελέσματα φαίνονται στον παρακάτω πίνακα.

VPN-Tech.	Vendor	ICMP [bytes]	ICMP echo [bytes]
IPSec	all	1084	1094
L2TP	Microsoft	1110	1118
PPTP	Microsoft	1079	1083
netfence	phion	1094	1094
no VPN	(direct)	1042	1042

Εικόνα 6-6 : Πραγματικό μέγεθος πακέτου VPN

Χωρίς το VPN, μόνο 42 επιπλέον bytes overhead λόγω πρωτοκόλλου προστέθηκαν στο αρχικό μήνυμα των 1000 bytes. Τα IPSec και phion netfence VPN, που χρησιμοποιούν ESP πακέτα, προκαλούν overhead δεδομένων μεγέθους 94 bytes. Από τη στιγμή που το L2TP απαιτεί κεφαλίδες L2TP και IPSec, αυτή είναι η τεχνολογία με το μεγαλύτερο overhead δεδομένων. Αυτό είναι 110 bytes, και 118 bytes για το μήνυμα απάντησης. Το PPTP προσθέτει φυσικά λιγότερο overhead δεδομένων. Προκειμένου να αναλυθεί τη συμπεριφορά του κατακερματισμού των πακέτων, το μέγεθος των πακέτων ICMP αυξήθηκε στα 1600 bytes. Από τη στιγμή που το προεπιλεγμένο MTU (Maximum Transmission Unit) της σύνδεσης δεδομένων είναι 1500 bytes, αυτά τα πακέτα πρέπει να κατακερματιστούν σε επίπεδο IP. Οι διαφορές των τεχνολογιών VPN ως προς αυτή την παράμετρο φαίνονται στον ακόλουθο πίνακα.

VPN-Tech.	Vendor	ICMP-packets	ICMP echo packets	Don't fragment set	Dest. reach-able
IPSec	Cisco	3	3	yes	yes
	Netscreen	3	3	no	yes
	Symantec	3	0	no	no
	Watchguard	3	2	no	yes
L2TP	Microsoft	2	2	no	yes
PPTP	Microsoft	3	2	yes	yes
netfence	phion	3	3	no	yes

Εικόνα 6-7 : κατακερματισμός VPN πακέτων

Ο κατακερματισμός των πακέτων φαίνεται να μην αποτελεί πρόβλημα για καμία τεχνολογία VPN, πλην μίας, της υλοποίησης του IPSec από τη Symantec, όπου ο τερματικός σταθμός εργασίας δεν μπορούσε να αποκριθεί. Αυτό βέβαια παραπέμπει στην κακή διαλειτουργικότητα των διαφορετικών υλοποιήσεων του IPSec. Ένα πολύ ενδιαφέρον σημείο είναι ότι διαφέρει ο αριθμός των πακέτων των ICMP μηνυμάτων και των ICMP απαντήσεών τους. Τέλος, όταν χρησιμοποιήθηκαν το Cisco IPSec και το PPTP, τέθηκε η σημαία (flag) “Don't fragment” - “Μην κατακερματίσεις”.

Για το τεστάρισμα της συμπεριφοράς της μετάφρασης διευθύνσεων δικτύου (NAT/NAPT), ο δρομολογητής μεταξύ των πυλών ασφαλείας ρυθμίστηκαν για να κάνουν μετάφραση διευθύνσεων. Από τη στιγμή που όλες οι τεχνολογίες VPN, πλην της PPTP, αντάλλαξαν ESP πακέτα, όπου το κρυπτογραφημένο και το πακέτο αυθεντικοποίησης IP εγκλωβίστηκαν σε ένα άλλο πακέτο IP η κεφαλίδα του οποίου μπορεί να αλλαχθεί, η μετάφραση διευθύνσεων δικτύου ήταν εφικτή χωρίς προβλήματα. Με το PPTP, όπου μόνο το κύριο μέρος της μεταφοράς κρυπτογραφείται και αυθεντικοποιείται, και όχι όλο το πακέτο IP, ήταν εφικτό να αλλάξουν οι διευθύνσεις IP κατά τη μετάδοση.

6.6 Επιθέσεις ασφάλειας

Τα τελευταία τεστ έλαβαν χώρα προκειμένου να αναλύσουν τις τεχνολογίες VPN από την οπτική γωνία της Mallory. Μέσω των Ethereal και Hping, δοκιμάστηκαν διαφορετικές μέθοδοι για να ελεγχθεί αν η επικοινωνία μέσω VPN μπορεί να παρακολουθηθεί ή να διακοπεί. Παρόλα αυτά, οι εφαρμοζόμενες τεχνικές είναι θεμελιώδεις και χαμηλού επιπέδου και δεν αναπαριστούν όλες τις δυνατότητες κρυπτοανάλυσης, αλλά στην πράξη οι περισσότερες επιθέσεις ασφαλείας βασίζονται σε αυτές τις τεχνικές.

Η παρακολούθηση και η ανάλυση της κίνησης του VPN τόσο κατά την εγκαθίδρυση των συνδέσεων όσο και κατά την αποστολή δεδομένων δεν προσέφερε κάποια αξιόλογα αποτελέσματα. Κανένας κωδικός ασφαλείας ή οτιδήποτε σχετικό με την ασφάλεια δε μεταδόθηκε ως απλό κείμενο. Γι' αυτό το λόγο έπρεπε να εφαρμοστούν άλλες τεχνικές. Το πρώτο πακέτο που μεταδιδόταν κατά την αρχικοποίηση της σύνδεσης αποθηκευόταν. Στη συνέχεια, με χρήση του Hping, ένα νέο πακέτο δημιουργούταν χρησιμοποιώντας την διεύθυνση IP της πηγής μιας πύλης ενός VPN και την αντίστοιχη διεύθυνση προορισμού ενός άλλου VPN. Το μεταφερόμενο φορτίο αυτού του ψεύτικου πακέτου γέμιζε με το περιεχόμενο του αποθηκευμένου πακέτου. Έτσι, δημιουργούταν από τη Mallory ένα ακριβές αντίγραφο από το πακέτο αρχικοποίησης που χρησιμοποιήθηκε για τη σύνδεση. Οι πύλες όλων των VPN όλων των τεχνολογιών απάντησαν με ένα μήνυμα αυθεντικοποίησης, χωρίς αυτή να είναι εφικτή αν δε γίνει χρήση των κατάλληλων δεδομένων αυθεντικοποίησης.

Κατά την επόμενη προσπάθεια, το πακέτο γεμίστηκε με αυθαίρετες τιμές. Όλες οι πύλες των VPN ανταποκρίθηκαν με μηνύματα λάθους, χωρίς να υπάρχει κάποια αλλαγή στην επικοινωνία του Bob και της Alice.

Στο επόμενο τεστ δοκιμάστηκε να γίνει μία επίθεση DOS (denial of service) στις πύλες ασφαλείας. Για αυτό το σκοπό, το ψεύτικο μήνυμα αρχικοποίησης της διόδου στελνόταν στην πύλη ανά 10 ms. Καθένα από αυτά τα αιτήματα διόδων έπρεπε να απαντηθούν μέσω των πυλών VPN. Την ίδια στιγμή, η κίνηση ICMP λάμβανε χώρα μεταξύ της Alice και του Bob μέσω διόδων VPN. Ξανά, δεν υπήρχε καμία επιρροή στις πύλες VPN, εκτός της συσκευής Watchguard VPN. Σε αυτή, η όποια ανταλλαγή δεδομένων διακόπηκε αμέσως. Η συσκευή συνέχισε να αποκρίνεται στα ψεύτικα αιτήματα για διόδους, ενώ δε μεταδόθηκαν ESP πακέτα. Αυτό αποτελεί μία επιτυχημένη επίθεση DOS.

6.7 Συμπεράσματα

Τα αποτελέσματα των τεστ που παρουσιάστηκαν παραπάνω δείχνουν ότι οι τρέχουσες τεχνολογίες VPN προσφέρουν ασφαλείς και αρκετά σταθερές συνδέσεις δεδομένων. Ένα σημαντικό μειονέκτημα αποτελεί η δραματική απώλεια επίδοσης και throughput, που υποδεικνύει ως αίτια τις περίπλοκες τεχνικές αυθεντικοποίησης και εγκλωβισμού. Αυτό σημαίνει πως η προσθήκη των VPN τεχνολογιών στα υπάρχοντα πρωτόκολλα προσθέτει επίσης επιπλέον πολυπλοκότητα και κόστη επεξεργασίας δεδομένων. Το IPSec υφίσταται από μία περίπλοκη διαδικασία εγκαθίδρυσης διόδου, που προκαλεί προβλήματα διαλειτουργικότητας μεταξύ διαφορετικών υλοποιήσεων. Το L2TP προσφέρει ιδιωτικότητα και αυθεντικοποίηση αν και μόνο αν συνδυαστεί με το IPSec, πράγμα που οδηγεί σε μεγάλα overhead. Το PPTP είναι η πιο γρήγορη τεχνολογία μεταξύ αυτών που παρουσιάστηκαν, αλλά το επίπεδο ασφαλείας του δεν επαρκεί για ευαίσθητες εφαρμογές. Τέλος, το phion netfence VPN προσφέρει αποδεκτές λύσεις για τα προβλήματα που προκύπτουν όταν χρησιμοποιείται το IPSec, αλλά είναι διαθέσιμο μόνο σε συνδυασμό με τις αντίστοιχες εμπορικές εφαρμογές.

Βιβλιογραφία

1. *James F. Kurose, Keith W. Ross : Computer Netwirking, A Top-Down Approach, Εκδόσεις Μ.Γκιούρδας, Αθήνα 2011*
2. *Williams Stallings : Networking Security Essentials, Applications And Standards, Εκδόσεις Κλειδάριθμος, Αθήνα 2010*
3. *Berhrouz A. Forouzan : TCP/IP , Protocol Suite, Εκδόσεις Μ. Γκιούρδας, Αθήνα 2005*
4. *K. Schmeh, Cryptography and Public Key Infrastructure on the Internet, John Wiley & Sons Inc., New York, 2003*
5. *R. Yuan, W.T. Strayer, Virtual Private Networks: Technologies and Solutions, Addison-Wesley Professional, Boston, 2001*
6. *N. Doraswamy, D. Karkins, IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks, Prentice Hall PTR Internet Infrastructure Series, New York, 1999*
7. *E. Lewis, J. Davies, Deploying Virtual Private Networks with Microsoft Windows Server 2003, Microsoft Press, Redmond, 2003*
8. *PHION Information Technologies GmbH, Austria, A-6020 Innsbruck, Eduard-Bodem-Gasse 1, www.phion.com (2006-02-05)*
9. *M. Finlayson, J. Harrison, R. Sugarman, VPN Technologies - A Comparison, Data Connection Ltd., Enfield, UK, http://www.cse.iitb.ac.in/˜varsha/ allpapers/network-misc/vpntechwp.pdf (2006-02-05)*
10. *H. Hamed, E. Al-Shaer, W. Marrero, "Modeling and Verification of IPSec and VPN Security Policies", In Proceedings of the 13th IEEE International Conference on Network Protocols (ICNP'05), pp. 259-278, 2005*
11. *L. Jin-Cherng, C. Ching-Tien, C. Wei-Tao "Design, Implementation and Performance Evaluation of IP-VPN", In Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA'03), p. 206, 2003*
12. *B. Schneier, Mudge, Cryptanalysis of Microsoft's PPTP, Mountain View, CA, http://www.schneier.com/paper-pptp.pdf (2006-02-05)*
13. *T. Berger, Analyse aktueller VPN Technologien in Bezug auf kryptographische Methoden, Performance und Tunnelmanagement, Dipl. Thesis, University of Salzburg, 2005*
14. *C. Draschl, Querkopplung von kommerziellen und nichtkommerziellen IPsec-Systemen, Dipl. Thesis, Salzburg University of Applied Sciences and Technologies, 2004*

15. *R. Kämpfe, Analyse und Vergleich von VPN Protokollen, Dipl. Thesis, University of Mittweida, 2002*
16. *http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ipsec.htm*
17. *https://supportforums.cisco.com/t5/security-documents/crypto-map-based-ipsec-vpn-fundamentals-negotiation-and/ta-p/3153502*
18. *http://www.infocellar.com/networks/Security/encryption.htm*
19. *http://www.met.edu/Institutes/ICS/NCNHIT/papers/33.pdf*
20. *Analysis of Current VPN Technologies, T. Berger, University of Salzburg, 2006*