ΤΕΙ ΚΑΛΑΜΑΤΑΣ (ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ)

Τμήμα Πληροφορικής και Τηλεπικοινωνιών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ

ΑΣΦΑΛΕΙΑ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

WINDOWS VISTA

Επιβλέπων Καθηγητής: Μακροδημήτρης Γεώργιος

Φοιτητής : Μπλέκος Χρήστος

Εαρινό Εξάμηνο 2010-2011

Σπάρτη - Λακωνίας

ΤΕΙ ΚΑΛΑΜΑΤΑΣ (ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ)

Τμήμα Πληροφορικής και Τηλεπικοινωνιών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ

ΑΣΦΑΛΕΙΑ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ WINDOWS VISTA

Επιβλέπων Καθηγητής: Μακροδημήτρης Γεώργιος

Φοιτητής : Μπλέκος Χρήστος

Εαρινό Εξάμηνο 2010-2011

Σπάρτη - Λακωνίας

ΠΕΡΙΛΗΨΗ

Η Microsoft με την κυκλοφορία των Windows κατάφερε κάτι που άλλες εταιρίες δεν είχαν καταφέρει στο παρελθόν, να κάνει τους προσωπικούς υπολογιστές φιλικούς σε όλα τα είδη χρηστών και όχι μόνο στους εξειδικευμένους πληροφορικάριους. Το Λειτουργικό Σύστημα αυτό όμως, όντας τόσο δημοφιλές, έχει γίνει ο βασικός στόχος των πειρατών, γνωστοι και ως hackers, και δέχεται μια πληθώρα από επιθέσεις καθημερινά οι οποίες αποσκοπούν στην εξαπάτηση του χρήστη για υποκλοπή των στοιχείων του, τη χρησιμοποίηση του υπολογιστή σαν bot για την εκτόξευση επιθέσεων μεγάλου βεληνηκούς ή για την καταστροφή του υπολογιστικού μας συστήματος. Έτσι η Microsoft βρίσκεται σε συνεχή μάχη με τους πειρατές/εισβολείς με αναβαθμίσεις λογισμικού και κυκλοφορίες νέων Λειτουργικών Συστημάτων ώστε να διασφαλίζει την ασφαλή χρήση του υπολογιστή από τους καθημερινούς χρήστες.

Σε αυτή την εργασία αναλύουμε το Λειτουργικό Σύστημα Microsoft Windows Vista και τις καινοτομίες που έφερε στο κόσμο της πληροφορικής και πώς άλλαξε τα δεδομένα στη μάχη με τους hackers. Αναλύουμε τους μηχανισμούς ασφαλείας του και πώς αυτοί προστατεύουν τον χρήστη από καθημερινές απειλές. Έπειτα αναφέρουμε πέντε επιθέσεις ενάντια στα Windows πώς αυτές υλοποιούνται και πώς προστατευόμαστε από αυτές αλλά και τι ζημιές προκαλούνε στον υπολογιστικό μας σύστημα. Τέλος, υλοποιήσαμε μια από αυτές τις επιθέσεις για να δείξουμε πώς οι πειρατές εισβάλλουν στο σύστημά μας και αποσπούν δεδομένα.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τη βαθειά μου ευγνωμοσύνη στον επιβλέπων καθηγητή μου Γεώργιο Μακροδημήτρη για την καθοδήγηση του στην εκπόνηση αυτής της πτυχιακής εργασίας.

Επίσης θα ήθελα να ευχαριστήσω του υπόλοιπους καθηγητές του τμήμας Τεχνολογίας Πληροφορικής Και Τηλεπικοινωνιών για την προσφορά τους όλα αυτά τα χρόνια στην αναβάθμιση του γνωσιακού μου επιπέδου

Ειδικές ευχαριστίες στην οικογένεια μου για την διαρκή στήριξη τους σε όλα τα φοιτητικά μου και μη χρόνια

Και τέλος , θα ήθελα να εκφράσω το πιο ζεστό ευχαριστώ σε όλους εκείνους τους φίλους και συναδέλφους που μου μετέδωσαν ένα κομμάτι από τη γνώση τους και με διευκόλυναν στο να πετύχω τους σκοπούς μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1 Εισαγωγή

1.1 Πρόλογος

Από τότε που οι υπολογιστές κατέκλυσαν την αγορά είτε για επαγγελματικούς, είτε για στρατιωτικούς, είτε για προσωπικούς λόγους η ανάγκη για έναν τρόπο λειτουργίας που θα ήταν φιλικός προς το χρήστη και θα εκμεταλλευόταν τις δυνατότητες του συστήματος, ήταν εμφανής. Στους πρώιμους υπολογιστές ένας άνθρωπος χειριστής (operator) φόρτωνε τα προγράμματα στη μνήμη του υπολογιστή και φρόντιζε για την εκτέλεσή τους. Όμως, με τη ραγδαία ανάπτυξη στον τομέα της πληροφορικής και των υπολογιστών και συγκεκριμένα με την εισαγωγή των μικροϋπολογιστών κάτι τέτοιο δε μπορούσε να γίνει πλέον και η ανάγκη για κάτι νέο ήταν εμφανή. Έτσι το 1974 ο Dr. Gary A. Kildall δημιούργησε το CP/M το πρώτο λειτουργικό σύστημα για τους μικροϋπολογιστές, το οποίο αποτέλεσε βάση του MS DOS που είναι το πρότυπο των σημερινών Λειτουργικών Συστημάτων. Έκτοτε πολλά θέματα που αφορούν την ασφάλεια, την χρησιμότητα ,την εκμετάλλευση των ΛΣ έχουν ανεπτύχθει καθώς έχουν γίνει πλέον το μέσο που συνδέει τον άνθρωπο με τον υπολογιστή.

Στην πράξη πρόκειται για ένα επίπεδο λογισμικού που μεσολαβεί μεταξύ του υλικού και των εκτελούμενων προγραμμάτων σε έναν ηλεκτρονικό υπολογιστή. Αποτελείται από ένα σύνολο μηχανισμών μέσω των οποίων επιτυγχάνεται αυτόματη διαχείριση των πόρων ενός υπολογιστή και ελεγχόμενη κατανομή τους στις εκτελούμενες εφαρμογές. Οι εφαρμογές αυτές να είναι σε θέση να προσπελάσουν εύκολα τους πόρους και τις συσκευές του συστήματος χωρίς να χρειάζεται να γνωρίζουν με ακρίβεια τη δομή του υποκείμενου υλικού, έτσι ώστε να μπορούν να εκτελούνται ταυτόχρονα χωρίς να έρχονται σε διένεξη μεταξύ τους ή με τον υπολογιστή.

Χρόνο με το χρόνο οι επιθέσεις από εισβολείς, ενάντια στους απλούς και καθημερινούς χρήστες αυξάνονται με ραγδαίους ρυθμούς με αποτέλεσμα να έχει παρουσιαστεί η ανάγκη για όλο και πιο σύγχρονα λειτουργικά συστήματα τα οποία θα μας παρέχουν μεγαλύτερη προστασία έτσι ώστε οι χρήστες να μην πέφτουν θύματα εκμετάλλευσης από εισβολείς. Ως Λειτουργικό Σύστημα (ΛΣ) χαρακτηρίζεται μία συλλογή βασικών προγραμμάτων , η οποία ελέγχει τη λειτουργία του υπολογιστή συνολικά και χρησιμοποιείται ως υπόβαθρο για την εκτέλεση όλων των υπόλοιπων προγραμμάτων, τη διαχείριση των περιφερειακών συσκευών και την εξασφάλιση της επικοινωνίας μεταξύ χρήστη και υπολογιστή. [1]

Η ασφάλεια του λειτουργικού συστήματος έχει γίνει μια απαραίτητη επένδυση για τις επιχειρήσεις στα πλαίσια της προσπάθειας να καλύψουν τις αυξανόμενες ανάγκες των χρηστών για περισσότερη ασφάλεια. Με τον όρο ασφάλεια εννοούμε τη χρήση του λογισμικού, hardware, και διαδικαστικών μεθόδων για την προστασία των εφαρμογών από εξωτερικές απειλές, καθώς η ανταλλαγή δεδομένων γίνετε κατά κόρον από το διαδίκτυο ή από απόσταση με αποτέλεσμα να βρίσκονται σε συνεχή κίνδυνο από διαφόρους εισβολείς. κάθε χρόνο, οι εταιρίες για να ασφαλίσουν τα λειτουργικά τους συστήματα, και κατά συνέπεια και τα προσωπικά δεδομένα των πελατών τους, ξοδεύουν υπέρογκα ποσά για την έρευνα και πρόληψη των επιθέσεων κάθε μορφής.

1.2 Συνεισφορά της εργασίας

Σε αυτή την εργασία, θα αναλύσουμε την ασφάλεια των Windows Vista και θα αναφερθούμε πως προστατευόμαστε από εξωτερικές εισβολείς (hackers). Αρχικά, θα επικεντρωθούμε στους μηχανισμούς ασφαλείας και στις βασικές αρχές που χρησιμοποιούνται από το λειτουργικό σύστημα, και ποιες είναι οι διαφορές τους με προηγούμενες εκδόσεις των Windows.

Περαιτέρω, θα αναφερθούμε στις επιθέσεις που δέχονται οι χρήστες από εισβολείς και θα επικεντρωθούμε στις πέντε πιο βασικές. Θα αναλύσουμε τον τρόπο υλοποίησης τους, πώς παραβιάζουν το σύστημά μας, και ποια μέτρα μπορούμε να πάρουμε έτσι ώστε να τις αντιμετωπίσουμε. Επιπροσθέτως, θα υλοποιήσουμε μια επίθεση που έχουμε αναλύσει ώστε να κατανοηθεί ο τρόπος με τον οποίο οι εισβολείς λειτουργούν, τους μηχανισμούς ασφαλείας που παρακάμπτουν προτείνοντας τρόπους αντιμετώπισης τους. Τέλος, θα επισημάνουμε τρόπους με τους οποίους θα μπορέσουμε να ασφαλίσουμε το σύστημα μας καλύτερα σε τέτοιου είδους επιθέσεις.

1.3 Τι χρειαστήκαμε για αυτή την πτυχιακή

Για αυτή την εκπόνηση αυτής της πτυχιακής εργασίας χρειαστήκαμε ένα σύγχρονο φορητό υπολογιστή με Λειτουργικό Σύστημα Windows Vista Ultimate Edition. Επίσης, χρειαστήκαμε σύνδεση στο διαδίκτυο για την εύρεση του υλικού καθώς και αρκετά βιβλία. Επιπλέον, χρειαστήκαμε δύο φορητούς υπολογιστές επιπλέον, τρία καλώδια τύπου RJ-45, ένα router/switch και το πρόγραμμα Cain and Abel για την υλοποίηση μιας επίθεσης.

1.4 Οργάνωση της αναφοράς

Η οργάνωση της πτυχιακής εργασίας γίνετε ως εξής :

- Στο κεφάλαιο 2 αναφέρουμε διεξοδικά όλους τους μηχανισμούς ασφαλείας που η Microsoft εισήγαγε με τα Windows Vista, πώς ασφαλίζουν τα δεδομένα μας από κακόβουλους εισβολείς και τέλος θα συγκρίνουμε την υπάρχουσα τεχνολογία ασφαλείας του λειτουργικού συστήματος με αυτή των παλαιοτέρων λειτουργικών συστημάτων της Microsoft.
- Στο κεφάλαιο 3 θα αναφέρουμε πέντε βασικές επιθέσεις ενάντια των windows τις οποίες θα αναλύσουμε σε τέσσερα ξεχωριστά μέρη :

  (α) Ποιές διαφοροποιήσεις υπάρχουν αυτής της επίθεσης,

  (β) Με ποιούς τρόπους υλοποιείται αυτή,

  (γ) Ποιοι είναι οι μηχανισμοί ασφαλείας των Microsoft Windows Vista που παρακάμπτει, τους τρόπους αντιμετώπισης αυτών των επιθέσεων από πλευρά του λειτουργικού μας συστήματος

  (δ) Ένα παράδειγμα της συγκεκριμένης επίθεσης για την κατανόηση των προβλημάτων που δημιουργεί η κάθε επίθεση.
- Στο κεφάλαιο 4 θα υλοποιήσουμε μια από τις επιθέσεις που αναλύσαμε στο κεφάλαιο 3 έτσι ώστε να εμβαθύνουμε στο τρόπο σκέψης του εισβολέα και στο πως υλοποιείται μια επίθεση βήμα προς βήμα. Επίσης, θα δείξουμε με πλήρη εικονογράφηση τα βήματα αυτά και τον τρόπο με τον οποίο καταφέραμε να απομονώσουμε την επίθεση.
- Τέλος, στο κεφάλαιο 5, θα αναπτύξουμε τα συμπεράσματά μας προκειμένου να επαναδιατυπωθεί εν συντομία το έργο της εργασίας, και να συνοψίσει τις συστάσεις μας για περαιτέρω εργασία.

1.5 Επίλογος

Στο επόμενο κεφάλαιο θα εξετάσουμε τις βασικές αρχές και τους μηχανισμούς ασφαλείας του λειτουργικού συστήματος Windows Vista. Στη συνέχεια, θα αναλύσουμε διεξοδικά τα νέα χαρακτηριστικά ασφάλειας που εισάγουν για πρώτη φορά τα Windows Vista, τον τρόπο λειτουργίας τους, καθώς και την αποτελεσματικότητα αυτών.

ΚΕΦΑΛΑΙΟ 2:
ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΤΩΝ WINDOWS

2 Εισαγωγή

Στο προηγούμενο κεφάλαιο αναφερθήκαμε γενικά στο τι θα αναφερθούμε σε αύτη την εργασία. Σε αυτό το κεφάλαιο θα περιγράψουμε τους βασικότερους μηχανισμούς ασφαλείας των Windows Vista. Θα δούμε γιατί το νέο Λειτουργικό Σύστημα της Microsoft είναι ανώτερο από άποψη ασφαλείας σε σύγκριση με τα προηγούμενα και ποιές είναι οι βελτιώσεις αλλά και οι καινοτομίες στο καινούριο Λειτουργικό Σύστημα. Τέλος, θα συνοψίσουμε αυτά που αναφέραμε και θα γράψουμε τις απόψεις μας πάνω στους μηχανισμούς ασφαλείας.

2.1 Τι είναι οι μηχανισμοί ασφαλείας;

Μηχανισμοί ασφαλείας είναι όλες εκείνα τα προγράμματα, οι διεργασίες και οι υπηρεσίες του λειτουργικού συστήματος που συμβάλλουν στην ασφάλεια του υπολογιστή μας και κάνουν τη συνολική εμπειρία του χρήστη πιο φιλική καθώς η ασφάλεια των προσωπικών του δεδομένων αλλά και του συστήματος διασφαλίζεται.

2.1.1 Win Logon

Στην πληροφορική, το Winlogon είναι το συστατικό των λειτουργικών συστημάτων Microsoft Windows που είναι υπεύθυνο για το χειρισμό της ασφαλούς ακολουθίας προσοχή, τη φόρτωση των προφίλ των χρηστών κατά τη σύνδεση, και, προαιρετικά, το κλείδωμα του υπολογιστή, όταν ένα screensaver τρέχει. Το Winlogon είναι ένα κοινό στόχο για αρκετές απειλές που θα μπορούσαν να τροποποιήσουν τη λειτουργία του και τη χρήση μνήμης. Η αυξημένη χρήση μνήμης για τη διαδικασία αυτή θα μπορούσε να υποδηλώσει ότι κάποιος έχει διαπράξει κάποιοι είδους ηλεκτρονικού εγκλήματος στο σύστημα μας. Στα Windows Vista και σε νεότερα λειτουργικά συστήματα οι ρόλοι και οι ευθύνες του Winlogon έχουν αλλάξει σημαντικά και η ασφάλεια του έχει βελτιωθεί κατά πολύ. [2]

2.1.1.1 Improved Logon Architecture

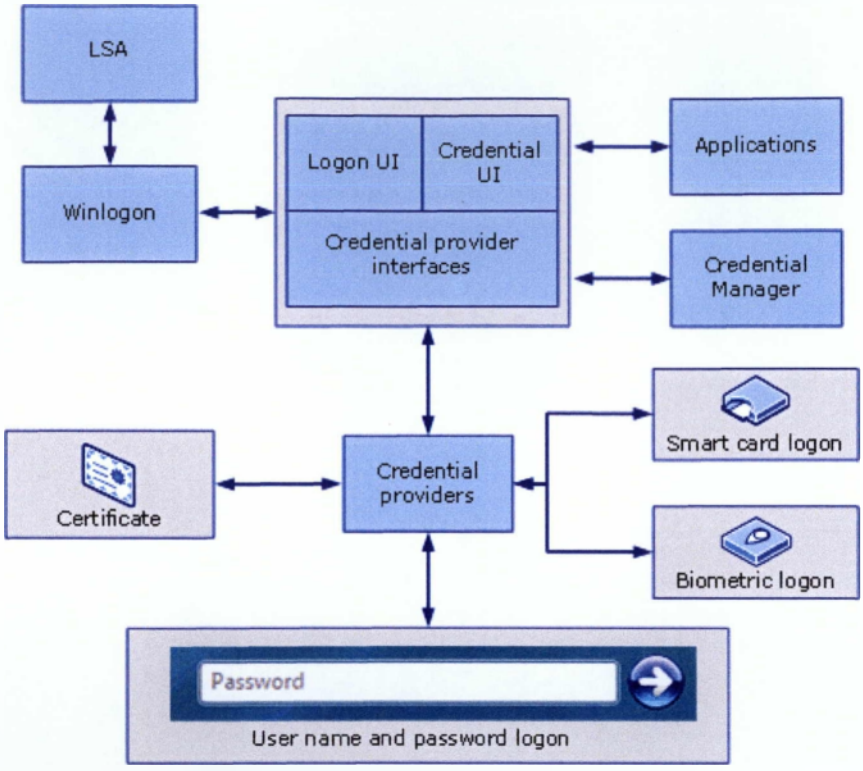
Η Microsoft έχει επίσης κάνει ευκολότερη την ενσωμάτωση των μεθόδων πρόσβασης χωρίς κωδικό, υποστηρίζοντας πολλαπλές ταυτόχρονες μεθόδους ελέγχου ταυτότητας, κατά τη διαδικασία πρόσβασης στο Λειτουργικό Σύστημα. Από τα Windows 2000, μπορούμε να χρησιμοποιήσουμε έξυπνες κάρτες για τον έλεγχο ταυτότητας και, πιο πρόσφατα, μπορούμε να αντικαταστήσουμε το περιβάλλον σύνδεσης με ένα άλλο από τρίτους παροχείς για να συνδεθείτε με ένα. Ωστόσο, μπορούμε να χρησιμοποιήσουμε μόνο μία μέθοδο ελέγχου ταυτότητας κάθε φορά που συνδεόμαστε. Τα Windows Vista διαθέτουν μια εντελώς νέα Winlogon Αρχιτεκτονική και ένα νέο API διαπιστευτηρίων (Credential Providers API) που

παρέχει βελτιωμένη ενσωματωμένη υποστήριξη για έξυπνες κάρτες, USB tokens, και επιτρέπει πολλαπλές πιστοποιήσεις που μπορούν να χρησιμοποιηθούν την ίδια στιγμή. (WVS pg.14-15)

Σε προηγούμενες εκδόσεις των Windows οι χρήστες αλληλεπιδρούσαν με τη επιφάνια εργασίας της Microsoft Graphical Interface for Network Authentication (GINA) , προηγούμενη διεπαφή του logon, η οποία χρησιμοποιούσε το Msgina.dll για να συνδεθεί. Το εκτελέσιμο αρχείο Winlogon.exe χειρίζεται τη διαδικασία σύνδεσης, αλλά η Microsoft GINA εμφανίζει το παράθυρο διαλόγου σύνδεσης, όπου ο χρήστης πληκτρολογεί το όνομα λογαριασμού χρήστη και τον κωδικό πρόσβασής. Όταν ο διαχειριστής ήθελε να προσθέσει ένα άλλο τρόπο για τον έλεγχο ταυτότητας, αναγκαζόταν τις περισσότερες φορές να αντικαταστήσει το Microsoft GINA με ένα αντίστοιχο πρόγραμμα. Δυστυχώς, το λογισμικό της άλλης εταιρίας, είχε τον πλήρη έλεγχο της ασφάλειας σύνδεσης του χρήστη. (WVS pg.14-15)

Η αντικατάσταση του αρχικού GINA συχνά δημιουργούσε προβλήματα ή εμπόδιζε τη χρήση άλλων λειτουργιών των Windows (Διακομιστής Τερματικών, Απομακρυσμένη Επιφάνια Εργασίας, κλπ). Επιπλέον, τα εναλλακτικά GINA ήταν πρόχειρα προγραμματιστικά σχεδιασμένα με αποτέλεσμα να δημιουργούν μεγάλα κενά ασφαλείας, θέτοντας την συνολική ασφάλεια του συστήματος σε υψηλά επίπεδα ρίσκου. (WVS pg 15)

Στα Windows Vista, μια νέα Διασύνδεση Προγράμματος Εφαρμογής (Credential Providers API) αντικαθιστά το GINA και όλες οι συνδέσεις χρηστών επιτυγχάνονται μέσω ενός νέου περιβάλλοντος εργασίας (Logonui.exe) . Οι προμηθευτές πρέπει να γράφουν το περιβάλλον πιστοποίησης και τα προγραμμάτων τους έτσι ώστε να συμπίπτουν με το νέο Credential Providers API. Το περιβάλλον εργασίας των παρόχων διαπιστευτηρίων API μαζί με το περιβάλλον εργασίας χρήστη και το LogonUI μπορεί να χειριστεί πολλαπλές εφαρμογές ταυτόχρονα.

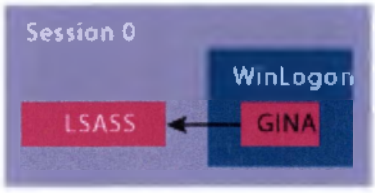


Εικόνα 1 : Νέα αρχιτεκτονική Logon στα Windows Vista

Επιπροσθέτως, σε συνδυασμό με την υποστήριξη υλικού, οι πάροχοι διαπιστευτηρίων μπορούν να επεκτείνουν το λειτουργικό σύστημα για να μπορούν οι χρήστες να συνδεθούν μέσω βιομετρικών συστημάτων (δακτυλικά αποτυπώματα, αναγνώριση αμφιβληστροειδούς ή αναγνώριση φωνής), κωδικών πρόσβασης, πιστοποιητικά έξυπνων καρτών και PIN, ή μέσω οποιοδήποτε προσαρμοσμένου πακέτου ελέγχου ταυτότητας επιθυμούν να δημιουργήσουν οι προγραμματιστές. Επίσης, οι πάροχοι διαπιστευτηρίων μπορούν να σχεδιάσουν προγράμματα τα οποία υποστηρίζουν το Single Sign On (SSO), για την επικύρωση των χρηστών σε ένα ασφαλές σημείο πρόσβασης του δικτύου καθώς και για τη σύνδεση σε ένα μηχάνημα. Επιπλεον, μπορεί να χρησιμοποιηθεί για τον έλεγχο ταυτότητας στους πόρους του δικτύου, που ενώνει μηχανές σε έναν τομέα, ή για την παροχή συναίνεσης του διαχειριστή για το User Account Control. Η πιστοποίηση υποστηρίζεται επίσης χρησιμοποιώντας το IPv6 ή κάποιες υπηρεσίες του διαδικτύου. Μια καινούρια παροχή ασφάλειας υπηρεσιών το CredSSP είναι διαθέσιμη μέσω του Security Support Provider Interface που επιτρέπει μια εφαρμογή να μεταβιβάζει τα διαπιστευτήρια του χρήστη από τον πελάτη (με τη χρήση του υπολογιστή-πελάτη SSP) στο διακομιστή προορισμού (μέσω του διακομιστή SSP). Η CredSSP χρησιμοποιείται επίσης από τις υπηρεσίες Terminal Services για την παροχή single-sign On

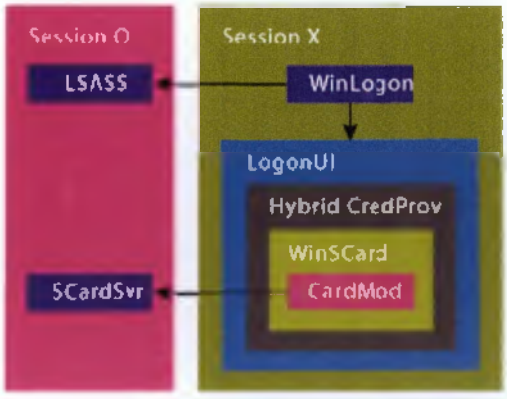
2.1.1.2 Session Isolation

Μια επίσης μεγάλη βελτίωση έγινε στην ασφάλεια της σύνδεσης του υπολογιστή. Πολλαπλές συνεδρίες(sessions) μπορούν να εκτελεστούν στα Windows κάθε φορά. Μια συνεδρια αρχίζει πάντα όταν ξεκινούν τα Windows και οι διεργασίες φορτώνονται. Μια άλλη όταν ο πρώτος χρήστης συνδέεται στο σύστημα και τέλος επιπρόσθετες συνεδρίες μπορούν να επίσης αρχίσουν (RunAs, Remote Desktop, Terminal Services).[3]



Εικόνα 2 : GINA Logon Architecture [3]

Το πρώτο Session αριθμείτε ως session 0 και τα υπόλοιπα σε αυξανόμενα νούμερα (Session 1, Session 2 κλπ). Σε προηγούμενες εκδόσεις των Windows όλα τα προγράμματα ξεκινούσαν όταν ο πρώτος χρήστης έτρεχε το Session 0 , μαζί με τα υπόλοιπα που είχαν ήδη ξεκινήσει. Επίσης, και άλλες συνεδρίες μπορούσαν να ξεκινήσουν, αλλά μπορούσαν εύκολα να αλληλεπιδράσουν και να επικοινωνήσουν με άλλα Sessions. Αυτό είχε σαν αποτέλεσμα εφαρμογές και διεργασίες να μπορούν να επικοινωνούν με χρήστες και προγράμματα τα οποία εκτελόντουσαν σε διαφορετικές συνεδρίες, το οποίο οδηγούσε το σύστημα μας στο να έχει μεγάλες αδυναμίες καθώς όχι μόνο ο χρήστης λειτουργούσε στο ίδιο Session με τις διεργασίες συστήματος, αλλά και μπορούσαν άλλα Sessions να επικοινωνήσουν με το Session 0 που αυτό είχε σαν αποτέλεσμα το σύστημα μας να είναι ευάλωτο καθώς πολλοί εισβολείς χρησιμοποιούσαν "shatter-attacks" για να αποκτούν πρόσβαση στα πιο προνομιούχα Sessions εκμεταλλευόμενοι τα λιγότερο προνομιούχα.



Εικόνα 3 : New Logon Architecture[3]

Όμως με την κυκλοφορία των Windows Vista το session 0 χρησιμοποιείται αποκλειστικά και μόνο από τον πυρήνα του συστήματος και ο χρήστης ποτέ του δεν έχει καμία επαφή με αυτό. Αυτή και μόνο η αλλαγή εμποδίζει μια πολύ μεγάλη γκάμα από "shatter-attacks".

2.1.2 Bitlocker Drive Encryption

Τα δεδομένα σε ένα κλεμμένο υπολογιστή είναι ευάλωτα σε μια μη-εξουσιοδοτημένη πρόσβαση από κάποιον εισβολέα, είτε εκτελώντας ένα λογισμικό για να επιτεθεί στα δεδομένα είτε μεταφέροντας το σκληρό δίσκο σε ένα άλλο υπολογιστή. Η Κρυπτογράφηση Μονάδων Δίσκου (Bitlocker Drive Encryption) παρέχει μια βελτιωμένη προστασία κατά της κλοπής σε περίπτωση που ο υπολογιστής χαθεί ή κλαπεί, και είναι μια δυνατότητα προστασίας των δεδομένων διαθέσιμη στα Windows Vista Enterprise , Windows Vista Ultimate και Windows Server 2008 .

Το Bitlocker βοηθά στον περιορισμό της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα από κλεμμένους υπολογιστές, συνδυάζοντας τις ακόλουθες διαδικασίες προστασίας δεδομένων:

- Κρυπτογραφεί ολόκληρο τον τόμο των Windows στο σκληρό δίσκο. Το Bitlocker κρυπτογραφεί όλα τα αρχεία χρήστη και τα αρχεία συστήματος του λειτουργικού συστήματος, συμπεριλαμβάνοντας τα αρχεία ανταλλαγής και τα αρχεία αδρανοποίησης.

- Το Bitlocker κρυπτογραφεί πολλαπλούς καθορισμένους όγκους. Μόλις ο όγκος του λειτουργικού συστήματος έχει κρυπτογραφηθεί, το Bitlocker μπορεί να κρυπτογραφήσει άλλους όγκους.

- Ελέγχει την ακεραιότητα των πρώτων στοιχείων εκκίνησης του υπολογιστή και τις παραμέτρους των δεδομένων εκκίνησης. Σε υπολογιστές που έχουν Trusted Platform Module (TPM), το Bitlocker χρησιμοποιεί τις βελτιωμένες δυνατότητες ασφαλείας του TPM για να διασφαλίσει ότι τα δεδομένα είναι προσβάσιμα μόνο από εξαρτήματα εκκίνησης του υπολογιστή που δεν έχουν αλλαχτεί και ο κρυπτογραφημένος δίσκος βρίσκεται στον αρχικό υπολογιστή.[4]

- Απαιτεί από το χρήστη να παρέχει κάποια πιστοποίηση πριν μπει σε περιβάλλον εκκίνησης ο υπολογιστής ζητώντας ένα PIN. (ευάλωτο σε μία επίθεση rootkit).

- Ο χρήστης πρέπει να εισάγει στον υπολογιστή μια συσκευή USB που περιέχει ένα κλειδί εκκίνησης έτσι ώστε να είναι σε θέση ο χρήστης να εκκινήσει το προστατευόμενο Λειτουργικό Σύστημα. Αυτή η λειτουργία είναι επίσης ευάλωτη σε μια επίθεση rootkit.
- Ένα αριθμητικό κλειδί προστάτης για τους σκοπούς της αποκατάστασης
- Ένα εξωτερικό κλειδί για σκοπούς αποκατάστασης.
- Προσθέτει ένα πιστοποιητικό με βάση το δημόσιο κλειδί προστασίας για σκοπούς αποκατάστασης.[5]

2.1.2.1 Λειτουργία του BitLocker Drive Encryption

Τα δεδομένα μας προστατεύονται κρυπτογραφώντας ολόκληρο τον τόμο των Windows. Εάν το λειτουργικό μας σύστημα με ένα συμβατό TPM (Trusted Platform Module) τότε το BitLocker χρησιμοποιεί το TPM για να ασφαλίσει τα κλειδιά τα οποία προστατεύουν τα δεδομένα μας. Σαν αποτέλεσμα κανείς δεν μπορεί να έχει πρόσβαση στα κλειδιά αν το TPM δεν έχει μια επιβεβαιωμένη κατάσταση του συστήματος. Αξιοσημείωτο είναι, ότι κρυπτογράφηση ολόκληρου του τόμου προστατεύει όλα τα δεδομένα, συμπεριλαμβανομένου και του λειτουργικού συστήματος, το μητρώο των Windows, προσωρινά αρχεία, και το αρχείο αδρανοποίησης. Επίσης, τα κλειδιά που απαιτούνται για την αποκρυπτογράφηση δεδομένων παραμένουν κλειδωμένα από το TPM, ένας εισβολέας δεν μπορεί να διαβάσει τα δεδομένα απλά αφαιρώντας τον σκληρό σας δίσκο και να το εγκαταστήσετε σε έναν άλλο υπολογιστή.

Κατά τη διάρκεια της διαδικασίας εκκίνησης, το TPM ελευθερώνει το κλειδί που ξεκλειδώνει την κρυπτογραφημένη κατάτμηση μόνο μετά από σύγκριση με ένα hash σημαντικές τιμές παραμέτρων του λειτουργικού συστήματος με ένα στιγμιότυπο που ελήφθη νωρίτερα. Αυτό επαληθεύει την ακεραιότητα της διαδικασίας εκκίνησης των Windows. Το κλειδί δεν ελευθερώνεται αν η TPM εντοπίσει ότι η εγκατάσταση των Windows έχει αλλοιωθεί.

Ποιό αναλυτικά, το Bitlocker Drive Encryption απαιτεί τουλάχιστον δύο NTFS διαμορφωμένους τόμους: ένα για το ΛΣ (συνήθως C:) και ένα άλλο με ελάχιστο μέγεθος τα 100MB από το οποίο το λειτουργικό σύστημα κάνει εκκίνηση. Το bitLocker απαιτεί κατά την εκκίνηση των Windows να παραμένουν χωρίς κρυπτογράφηση. Σε αντίθεση με προηγούμενες εκδόσεις των Windows, τα Vista είναι "diskpart" εργαλείο της γραμμής

εντολών καθώς περιλαμβάνει τη δυνατότητα να συρρικνωθεί το μέγεθος ενός τόμου NTFS, έτσι ώστε ο όγκος του συστήματος για το BitLocker να μπορεί να δημιουργηθεί από τον ήδη κατανεμημένο χώρο. Ένα εργαλείο που ονομάζεται BitLocker εργαλείο προετοιμασίας (BitLocker Drive Preparation Tool) είναι επίσης διαθέσιμο από τη Microsoft που επιτρέπει σε έναν υπάρχοντα τόμο στα Windows Vista να συρρικνωθεί για να δημιουργηθεί χώρος για ένα νέο τόμο εκκίνησης, καθώς και για τα απαραίτητα bootstrapping αρχεία που πρόκειται να μεταφερθούν σε αυτό.

Μόλις ένα εναλλακτικό διαμέρισμα εκκίνησης έχει δημιουργηθεί, η μονάδα TPM πρέπει να προετοιμαστεί (με την προϋπόθεση ότι αυτό το χαρακτηριστικό χρησιμοποιείται), αφότου το απαιτούμενο κρυπτογραφημένο κλειδί του δίσκου, όπως TPM, PIN ή κλειδί USB. έχει ρυθμιστεί. Ο όγκος του σκληρού δίσκου κρυπτογραφείτε ως εργασία, παράλληλα με τις βασικές εργασίες του συστήματος, κάτι που απαιτεί χρόνο σε ένα δίσκο μεγάλης χωρητικότητας καθώς κάθε λογικό τομέας διαβάζεται, κρυπτογραφείται και ξαναγράφεται πίσω στον δίσκο. Μόνο όταν ολόκληρος ο όγκος έχει κρυπτογραφηθεί τότε τα κλειδιά είναι προστατευμένα, και ο όγκος θεωρείται ασφαλής. Το Bitlocker χρησιμοποιεί ένα οδηγό συσκευής χαμηλού επιπέδου για την κρυπτογράφηση και αποκρυπτογράφηση όλων των αρχείων της πλατφόρμας, καθιστώντας την αλληλεπίδραση με το κρυπτογραφημένο όγκο διαφανής για εφαρμογές που τρέχουν στην πλατφόρμα [5] [6]

2.1.3 Cryptographic Application Programming Interface

Η Κρυπτογραφική Διασύνδεση Προγραμματισμού Εφαρμογών είναι μια διασύνδεση προγραμματισμού εφαρμογών η οποία περιλαμβάνεται σε όλες τις εκδόσεις των Windows NT και επιτρέπει στους προγραμματιστές να ασφαλίσουν τις Windows-based εφαρμογές χρησιμοποιώντας κρυπτογραφία. Πρόκειται για μια σειρά από δυναμικά συνδεδεμένες βιβλιοθήκες οι οποίες παρέχουν ένα επίπεδο αφαίρεσης που απομονώνει τους προγραμματιστές από τον κώδικα που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Επίσης, το Cryptographic API χρησιμοποιεί δημόσια και συμμετρικά κλειδιά κρυπτογράφησης. Τέλος, περιλαμβάνει τη λειτουργία για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων, καθώς και τον έλεγχο ταυτότητας με χρήση ψηφιακών πιστοποιητικών.

2.1.3.1 Νέα γενιά Cryptographic API

Τα Windows Vista διαθέτουν μια ενημέρωση για το Cryptographic API η οποία είναι γνωστή και ως Cryptography API: Next Generation (CNG). Έχει καλύτερο API συντελεστή επιτρέποντας να λειτουργούν οι ίδιες εργασίες χρησιμοποιώντας ένα ευρύ φάσμα

κρυπτογραφικών αλγορίθμων, συμπεριλαμβανομένου και ενός αριθμού νεωτέρων αλγόριθμων. Το νέο κρυπτογραφικό API περιλαμβάνει την υποστήριξη για την σύνδεση προσαρμοσμένων κρυπτογραφικών APIs σε πραγματικό χρόνο λειτουργίας καθιστώντας το ευέλικτο. Επίσης, το CNG λειτουργεί και στις δύο καταστάσεις (χρήστη, πυρήνα) αλλά και υποστηρίζει το σύνολο των αλγορίθμων από το Cryptographic API. Ο πάροχος της Microsoft που υλοποιεί CNG στεγάζεται σε Bcrypt.dll. Το CNG υποστηρίζει επίσης κρυπτογραφία ελλειπτικής καμπύλης η οποία είναι εξίσου ασφαλής και χρησιμοποιεί μικρότερα κλειδιά απ' ότι ο RSA. Επιπροσθέτως, το API CNG ενσωματώνεται με το υποσύστημα των έξυπνων καρτών με την προσθήκη μιας βάσης κρυπτογράφησης έξυπνων καρτών (Base CSP) η οποία ενθυλακώνει την έξυπνη κάρτα API.[7]

2.1.4 Windows Defender

Με την εισαγωγή των Windows Vista η Microsoft πρόσθεσε στο ήδη αναβαθμισμένο σύστημα ασφαλείας των Windows Vista και ένα αντί-κατασκοπευτικό πρόγραμμα (antispyware) λογισμικού το Windows Defender. Αρχικά κατασκευασμένο από την Giant Company Software, το Windows Defender μας παρέχει προστασία από κατασκοπευτικά προγράμματα, τα γνωστά spyware, καθώς και από ανεπιθύμητα προγράμματα όπως ψεύτικα anti-virus.

Επίσης, το Windows Defender εγκαθίσταται σαν υπηρεσία και εκτελείται συνεχώς στη μνήμη χωρίς να παρενοχλεί τον χρήστη παρά μόνο όταν εντοπίσει κάποιο spyware, δηλαδή είναι πρόγραμμα που εκτελείται σε πραγματικό χρόνο. Επιπροσθέτως, επιβλέπει συνεχώς πάνω από εκατό τοποθεσίες του υπολογιστή περιλαμβάνοντας φακέλους εκκίνησης, κλειδιά του μητρώου (registry keys) χρησιμοποιώντας δύο διεργασίες την Msmpeng.exe ή την Msacui.exe. Επιπλέον, πριν κάνει μια σάρωση (την προγραμματισμένη καθημερινή σάρωση) ελέγχει για ενημερώσεις για νέα spyware χρησιμοποιώντας τις Ενημερώσεις Windows.

Ακόμη, περιλαμβάνει ένα εργαλείο που ονομάζετε software explorer (εξερευνητής λογισμικού) το όποιο μπορεί να αποκαλύψει προγράμματα τα όποια εκτελούνται εκείνη τη στιγμή, που συνδέονται στο διαδίκτυο και προγράμματα αυτόματης εκκίνησης. Όμως το πιο σημαντικό που μας προσφέρει είναι η δυνατότητα να δούμε ποιες διεργασίες εκτελούνται μέσω του εκτελέσιμου αρχείου Svchost.exe. Το Svchost.exe (Service Host Process) είναι μια γενική διεργασία που μέσω αυτής εκτελούνται άλλες διεργασίες και πιο συγκεκριμένα την χρησιμοποιούν τα DLLs για να εκτελούνται σαν διεργασίες και να επικοινωνούν μέσω του

υπολογιστή. Αυτό βοηθάει στις εργασίες να επικοινωνούν μεταξύ τους πολύ πιο εύκολα και γρήγορα, καθώς χρησιμοποιούν μια διεργασία αντί για ξεχωριστές διεργασίες για κάθε DLL.

Τέλος, το Windows Defender έχει ενσωματωθεί με μια διαδικτυακή κοινότητα γνωστή και ως SpyNet. Το Microsoft SpyNet είναι το δίκτυο των χρηστών του Windows Defender και του Microsoft Security Essentials όπου βοηθούν να καθορίσουν ποια προγράμματα έχουν ταξινομηθεί ως spyware. Και με αυτό το τρόπο το Λειτουργικό Σύστημα μας παραμένει συνεχώς προστατευμένο από spyware με τη βοήθεια του Windows Defender . [8] [9]

2.1.5 Hardened Services

Η Microsoft θεωρεί τα Windows Vista ως το πιο ασφαλές Λειτουργικό Σύστημα που έχει εκδώσει ποτέ καθώς περιλαμβάνει πολλά νέα χαρακτηριστικά τα οποία εξασφαλίζουν την ασφάλεια του συστήματος μας από πολλές πλευρές, σε σύγκριση με προηγούμενα Windows.Ένα από αυτά τα νέα χαρακτηριστικά είναι και το Windows Hardened Services.

Σε παλαιότερες εκδόσεις των Windows, οι υπηρεσίες δεν ήταν αναγκαίο να εκτελούνται με το ελάχιστο δυνατό προνόμιο. Στην πραγματικότητα, οι υπηρεσίες των Windows έτρεχαν κάτω από λογαριασμούς που είχαν μεγάλο βαθμό πρόσβασης, όπως ο λογαριασμός τοπικού συστήματος. Επιπλέον, οι χρήστες συχνά δεν έχουν τη γνώση των υπηρεσιών που λειτουργούν στο σύστημά τους, και δεν συνειδητοποιούν ότι υπάρχουν υπηρεσίες που είναι ασφαλή για να απενεργοποιήσουν. Τελικά, οι υπηρεσίες και οι εφαρμογές του χρήστη εκτελούνταν στον ίδιο χώρο, κάτι το οποίο θα μπορούσε να οδηγήσει σε ακατάλληλη πρόσβαση. Ως αποτέλεσμα οι υπηρεσίες εκτελούνταν με προνόμια, τα οποία δεν ταίριαζαν στην αναγκαιότητα της διεργασίας, με αποτέλεσμα η επιφάνεια εργασίας των Windows να είναι πιο ευάλωτη σε επιθέσεις.

Το Windows Vista Hardening έχει σχεδιαστεί για να μετριάσει ορισμένες από αυτές τις ελλείψεις και χρησιμοποιεί τέσσερις μεθόδους γι' αυτό :

- Υπηρεσία απομόνωση (Service Isolation)
- Λιγότερο προνόμιο (Least Privilege)
- Περιορισμένη πρόσβαση στο δίκτυο (Restricted Network Access)
- Απομόνωση Περιόδου λειτουργίας 0 (Session 0 Isolation)

2.1.5.1 Service Isolation

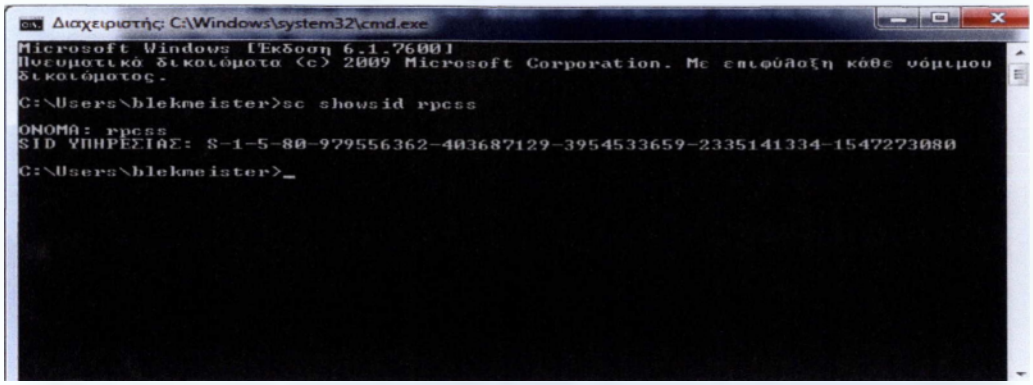
Πριν από τα Windows Vista, όταν μια υπηρεσία χρειάζονταν πρόσβαση σε ένα αντικείμενο το οποίο χρειαζόταν ένα μεγάλο επίπεδο ασφαλείας μία από τις δύο παρακάτω προσεγγίσεις μπορούσε να γίνει :

- Η υπηρεσία μπορούσε να εκτελεστεί χρησιμοποιώντας ένα λογαριασμό ο οποίος θα έδινε το απαραίτητο υψηλό επίπεδο δικαιωμάτων, όπως για παράδειγμα ο λογαριασμός τοπικού συστήματος (Local System Account) . Αυτή είναι προσέγγιση η οποία ήταν πιο συχνά λαμβάνονται χωρίς λόγο, καθώς άνοιγε το σύστημα σε πιθανές επιθέσεις.

- Η ρύθμιση παραμέτρων ασφαλείας, για το αντικείμενο το οποίο απαιτούσε πρόσβαση, ήταν υποχρεωμένη να μπορούσε να μεταρρυθμιστεί ώστε να επιτρέπει την πρόσβαση από έναν ειδικό λογαριασμό με λιγότερα δικαιώματα.

Γι' αυτό η Microsoft εισήγαγε την απομόνωση υπηρεσιών(Service Isolation).Η απομόνωση υπηρεσιών είναι μια μέθοδος μέσω της οποίας μια υπηρεσία των Windows Vista μπορεί να αποκτήσει πρόσβαση σε ένα αντικείμενο χωρίς να χρησιμοποιήσει κάποιους λογαριασμούς διαχειριστή όπως το Local System Account. Αποτρέπει τις υπηρεσίες των Windows από το να κάνουν εργασίες σε συστήματα αρχείων, μητρώο ή δικτύων στα οποία δεν πρέπει να κάνουν, μειώνοντας έτσι τη συνολική επιφάνεια των επιθέσεων κατά του συστήματος και σαν αποτέλεσμα την παρεμποδίζουν την είσοδο του κακόβουλου λογισμικού. Στις υπηρεσίες έχει πλέον ανατεθεί ανά υπηρεσία αναγνώρισης τίτλου (SID), το οποίο επιτρέπει τον έλεγχο της πρόσβασης στην υπηρεσία σύμφωνα με την πρόσβαση που καθορίζεται από το αναγνωριστικό ασφαλείας. Η απομόνωση υπηρεσιών ασφαλίζει το επιθυμητό αντικείμενο-όπως ένα κλειδί μητρώου(registry key)-με μια καταχώρηση ελέγχου πρόσβασης χρησιμοποιώντας ένα αναγνωριστικό ασφαλείας (pre-service security ID).

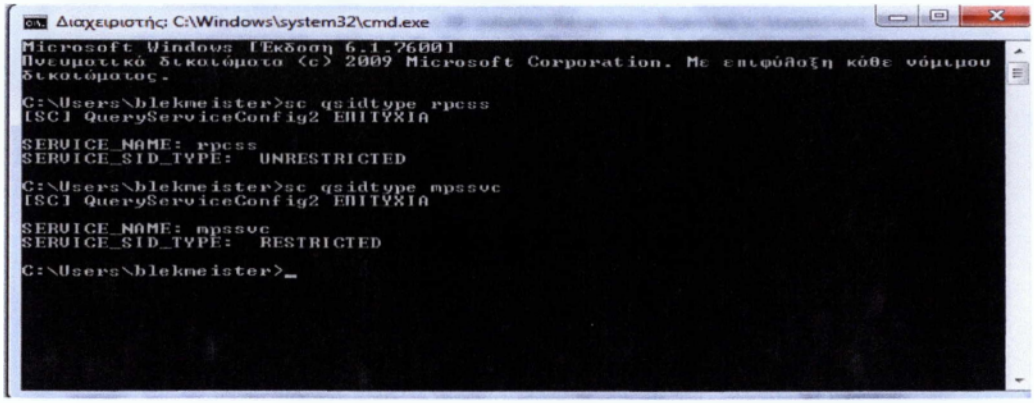
Το per-service-SID δημιουργεί, στην ουσία, μια ταυτότητα για κάθε υπηρεσία η οποία επιτρέπει τον έλεγχο πρόσβασης χρησιμοποιώντας την υπάρχουσα δυνατότητα πρόσβασης στο μοντέλο ελέγχου των Windows.Τώρα, οι υπηρεσίες μπορούν να εφαρμόσουν τις λίστες έλεγχου πρόσβασης (Access Control Lists)σε πόρους που είναι ιδιωτικοί ως προς την υπηρεσία, εμποδίζοντας άλλες υπηρεσίες καθώς και τον χρήστη να έχει πρόσβαση σε αυτό τον πόρο. Μια ανά-υπηρεσία SID μπορεί να αποδοθεί, κατά τη διάρκεια της εγκατάστασης της υπηρεσίας μέσω του ChangeServiceConfig2 API ή χρησιμοποιώντας την Sc.exe εντολή με το ρήμα sidtype



Εικόνα 4 : Το SID μιας υπηρεσίας

Υπάρχουν τρεις πιθανές τιμές:

- None (0x0) - η υπηρεσία δεν θα έχει ανά-υπηρεσία SID. Αυτή είναι η προεπιλεγμένη ρύθμιση παραμέτρων για μια υπηρεσία
- Unrestricted (0x1) - η υπηρεσία έχει ανά υπηρεσία SID
- Restricted (0x3) - η υπηρεσία έχει ανά υπηρεσία SID και ένα περιορισμένης εγγραφής συμβολικό(write restricted token).



Εικόνα 5 : Τύποι SID

2.1.5.2 Least Privilege (Λιγότερο προνόμιο)

Ο λογαριασμός τοπικού συστήματος παρέχει τα κλειδιά για κάθε πτυχή του συστήματος. Αυτός είναι και ο λογαριασμός σύμφωνα με τον οποίο λειτουργούν πολλές υπηρεσίες των Windows. Ως εκ τούτου, οι υπηρεσίες αυτές είναι τα αγαπημένα μεταξύ των χάκερ δεδομένου ότι μια επιτυχημένη εκμετάλλευση εναντίον μιας από αυτές τις υπηρεσίες μπορεί να παρέχει ευρεία και βαθιά πρόσβαση σε ένα σύστημα.

Προκειμένου να προστατευθεί καλύτερα το σύστημα, μια βέλτιστη πρακτική είναι να εκτελεστεί κάθε υπηρεσία, χρησιμοποιώντας ένα λογαριασμό με τα λιγότερα αναγκαία προνόμια για την υλοποίηση των στόχων της υπηρεσίας. Αν και τα Windows παρέχουν άλλους λογαριασμούς που έχουν πολύ λιγότερα δικαιώματα, ορισμένες υπηρεσίες απαιτούν προνόμια που παρέχονται μόνο από τον λογαριασμό τοπικού συστήματος.

Σύμφωνα με παλαιότερες εκδόσεις των Windows, ο λογαριασμό τοπικού συστήματος παρείχε εν λευκώ πρόσβαση. Στα Windows Vista, οι υπηρεσίες που απαιτούν μόνο δικαιώματα του τοπικού συστήματος μπορούν να χρησιμοποιούν ακόμα το λογαριασμό τοπικού συστήματος, αλλά μπορεί να ρυθμιστεί ώστε να χορηγεί μόνο αυτά τα δικαιώματα που απαιτούνται για την υπηρεσία να λειτουργεί, και όχι περισσότερα. Το τοπικό σύστημα δεν είναι ο μόνος λογαριασμός που μπορεί να χρησιμοποιήσει αυτό το νέο χαρακτηριστικό. Οι παρακάτω λογαριασμοί ή τα είδη των λογαριασμών μπορούν επίσης να χρησιμοποιήσουν αυτό το μηχανισμό λιγότερο προνομίου :

- **Λογαριασμός Τοπικών Υπηρεσιών**: Ο λογαριασμός τοπικής Υπηρεσίας έχει ελάχιστα δικαιώματα στον τοπικό υπολογιστή και χρησιμοποιεί ανώνυμα διαπιστευτήρια στο δίκτυο. Αυτός ο λογαριασμός έχει μειώσει τα προνόμια και τις πράξεις με παρόμοιο τρόπο με επικυρωμένο τοπικό λογαριασμό χρήστη. Η χρήση αυτού του λογαριασμού είναι χρήσιμη όταν ο λογαριασμός τοπικού συστήματος παρέχει υπερβολική πρόσβαση για τις υπηρεσίες που δεν χρειάζονται βαθιά πρόσβαση σε ένα σύστημα.

- **Λογαριασμός Δικτυακών Υπηρεσιών** : Ο Λογαριασμός Δικτυακών Υπηρεσιών είναι παρόμοιος με το λογαριασμό τοπικών υπηρεσιών η βασική διαφορά είναι ότι ο λογαριασμός αυτός παρέχει λιγότερα δικαιώματα σε σχέση με το τοπικό σύστημα. Εκεί που η Υπηρεσία του Δικτύου διαφέρει από την Τοπική Υπηρεσία είναι σε περιπτώσεις κατά τις οποίες η υπηρεσία πρέπει να έχει πρόσβαση σε απομακρυσμένους πόρους. Εκεί η Τοπική Υπηρεσία παρέχει ανώνυμα διαπιστευτήρια για την πρόσβαση σε απομακρυσμένους πόρους, ενώ η υπηρεσία δικτύου έχει πρόσβαση σε απομακρυσμένους πόρους χρησιμοποιώντας τα διαπιστευτήρια του λογαριασμού του υπολογιστή.

- **Domain accounts**: User accounts created in the Active Directory domain.

- **Τοπικοί Λογαριασμοί** : Λογαριασμοί που δημιουργήθηκαν στον τοπικό υπολογιστή.

2.1.5.3 Service Network Access Restriction

Με τα χρόνια, οι υπηρεσίες που τρέχουν στα Windows έχουν γίνει όλο και περισσότερο εξαρτώμενες από τη πρόσβαση στο δίκτυο ή την πρόσβαση από άλλους υπολογιστές δικτύου. Υπηρεσίες που αντιμετωπίζουν το δίκτυο με αυτό τον τρόπο είναι πιο ευάλωτες σε επιθέσεις γιατί οι υπηρεσίες αυτές είναι ακριβώς που περιμένουν για απομακρυσμένες συνδέσεις, που τους καθιστά πιο επιρρεπείς σε κακόβουλη δραστηριότητα.

Στα Windows Vista, ένας προγραμματιστής μπορεί να περιορίσει την πρόσβαση μιαςυπηρεσίας από το TCP / UDP πρωτόκολλο ή ακόμη και από την κατεύθυνση που κίνηση στο δίκτυο ρέει. Όταν οι περιορισμοί όπως αυτοί τεθούν σε εφαρμογή, οι προσπάθειες για πρόσβαση μιας υπηρεσίας χρησιμοποιώντας άλλες μεθόδους θα μπλοκαριστούν προστατεύοντας την εν λόγω υπηρεσία από ορισμένους φορείς της επίθεσης.

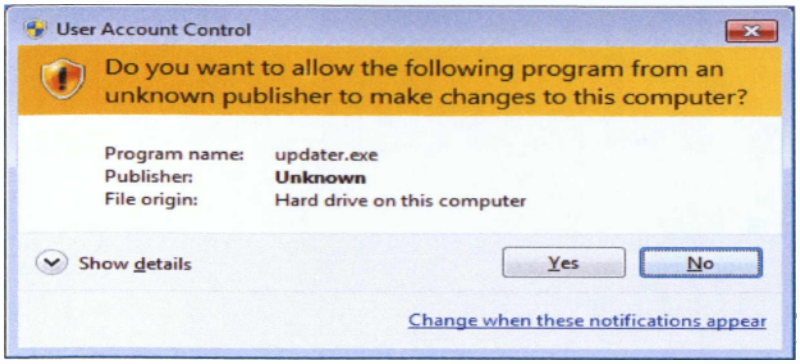
Οι υπηρεσίες των Windows Vista μπορούν να παραμετροποιηθούν έτσι ώστε να μην επιτρέπετε η πρόσβαση από το δίκτυο. Σε αυτή την περίπτωση η υπηρεσία δε μπορεί να εκμεταλλευτεί από απόσταση και ούτε μπορεί να κάνει συνδέσεις με απομακρυσμένες υπηρεσίες.

2.1.5.4 Session 0 Isolation

Τα Windows Vista δεν επιτρέπουν σε καμία εφαρμογή να εκτελεστεί στο Session 0. Όλες οι εφαρμογές πρέπει να εκτελεστούν σε Session 1 ή υψηλότερο. Μόνο οι υπηρεσίες και άλλες εφαρμογές που ο χρήστης δεν έχει καμία επαφή με αυτές εκτελούνται στο Session 0 , διατηρώντας έτσι την απομόνωση μεταξύ των υπηρεσιών και εφαρμογών χρήστη.

2.1.6 User Account Control

Το UAC είναι σίγουρα το πιο πολυσυζητημένο από τις βελτιώσεις των windows vista.Το UAC δημιουργήθηκε για να μειώσει στο ελάχιστο τον κίνδυνο ενός χρήστη να συνδεθεί στο λειτουργικό σαν διαχειριστής ενώ δεν κάνει κάποιες εργασίες διαχειριστή. Στο παρελθόν η πλειοψηφία των χρηστών παγκοσμίως συνδεόταν στο λειτουργικό τους σύστημα σαν διαχειριστές και με αυτό τον τρόπο τα περισσότερα κακόβουλα προγράμματα έπαιρναν τον έλεγχο του υπολογιστή στις περισσότερες των περιπτώσεων των επιθέσεων που δέχεται το λειτουργικό σύστημα.



Εικόνα 6 : User Account Control Dialog Box

Το UAC είναι μέρος από μια μακροχρόνια στρατηγική για να αλλάξει τον τρόπο με το οποίο είναι προγραμματιστές εφαρμογών γράφουν κώδικα και τον τρόπο με τον οποίο οι χρήστες χρησιμοποιούν το λογισμικό των προγραμματιστών αυτών. Η ιδέα είναι να μειωθεί η έμφυτη έκθεση, δηλαδή να εκτιθέμεθα στους εισβολείς χωρίς να το ξέρουμε διότι έτσι είναι ο τρόπος που λειτουργεί το λειτουργικό, σαν διαχειριστές όλη την ώρα.

Τα συστήματα UNIX είχαν μια «εργαλειοθήκη» και μια βασική αρχιτεκτονική σχεδιασμεένη γύρω από τη ιδέα του ελάχιστου δικαιώματος. Τα Windows είχαν μια παρόμοια αρχιτεκτονική αλλά το λειτουργικό δεν είχε σχεδιαστεί έτσι γιατί πολλές εφαρμογές των Windows είχαν γραφτεί υπο το μοντέλο windows 9x και windows 3x οπού όλοι ήταν συνδεδεμένοι σαν διαχειριστές έτσι ο κώδικας που έγραψαν δεν ήταν ποτέ σχεδιασμένος να τρέχει με χαμηλά δικαιώματα. Αφήνοντας ουσιαστικά το σύστημα συνεχώς εκτεθειμένο καθώς όλες οι διεργασίες έτρεχαν με δικαιώματα διαχειριστή.

Έτσι η ιδέα για το UAC ξεκίνησε και η Microsoft προσπάθησε να κάνει τους χρήστες να εργάζονται με χαμηλά δικαιώματα. Ένας από τους βασικούς στόχους ήταν να εξαλειφθούν οι «φτωχές» εφαρμογές έτσι ώστε οι χρήστες να δουλεύουν σαν κανονικοί χρηστες(standard users)και όχι σαν διαχειριστές, έτσι οι προγραμματιστές και οι υπεύθυνοι για την ανάπτυξη εφαρμογών θα έγραφαν εφαρμογές για κανονικούς χρήστες.

Όμως εάν οι χρήστες έβγαζαν το UAC εκτός λειτουργίες τότε αυτός ο σκοπός δεν θα μπορούσε πότε να επιτευχθεί. Έτσι χρειάστηκαν διαρθρωτικές αλλαγές στις λειτουργίες του λειτουργικού συστήματος.

2.1.6.1 Αναγνωριστικό ασφάλειας (SID)

Οι περισσότεροι χρηστές που χρησιμοποιούν ένα λειτουργικό με βάση τα Windows NT (Windows 98, 2000, Vista, 7, server κλπ) γνωρίζουν ότι οι χρηστές συσχετίζονται με τα

ονόματα χρηστή που έχουν στο λειτουργικό τους σύστημα. Αυτό που στην πραγματικότητα συμβαίνει η χρήση ενός SID που χρησιμοποιεί το λειτουργικό μας σύστημα. Το SID είναι μια παγκόσμια μοναδική τιμή η όποια αναγνωρίζει έναν χρηστή ή αλλιώς ένα αντικείμενο στη γλωσσά της ασφάλειας των ηλεκτρονικών υπολογιστών. Σαν αντικείμενο εννοούμε *όχι μόνο τους χρηστές αλλά* και τις ομάδες χρηστών, τα domains, τους υπολογιστές και στα windows vista ακόμα και κάποιες διεργασίες. Το SID είναι κάπως έτσι:

S-1-5-21-57989841-1336602894-682003330-500

Όλο αυτό από το S μέχρι το -500 είναι το αναγνωριστικό ασφάλειας του υπολογιστή. Το τελευταίο κομμάτι, δηλαδη το 500, προσδιορίζει την παραπάνω SID ως την SID ενός χρηστή. Αναλυωντας τα κομμάτια του SID ξεχωριστά ξεκινάμε με το :

S - Το όποιο σημαίνει SID.

1 – Είναι το νούμερο της έκδοσης του SID.

5 - Είναι η αρχή αναγνώρισης από την οποία προήρθε το αναγνωριστικό ασφαλείας. Είναι μια αριθμητική αναπαράσταση του SECURITY_NT_AUTHORITY ή ποιο απλά αναφέρεται ότι είναι μια έκδοση ενός Windows NT συστήματος.

21 – Είναι η πρώτη υπό αυθενπία SECURITY_NT_NON_UNIQUE

και σημαίνει ότι το συγκεκριμένο αναγνωριστικό ασφαλείας μπορεί να μην είναι παγκοσμίως μοναδικό. Δηλαδή, ότι μπορεί να υπάρχουν και άλλοι ηλεκτρονικοί υπολογιστές στον πλανήτη οι οποίοι μπορούν να έχουν ακριβώς το ίδιο αναγνωριστικό ασφαλείας.

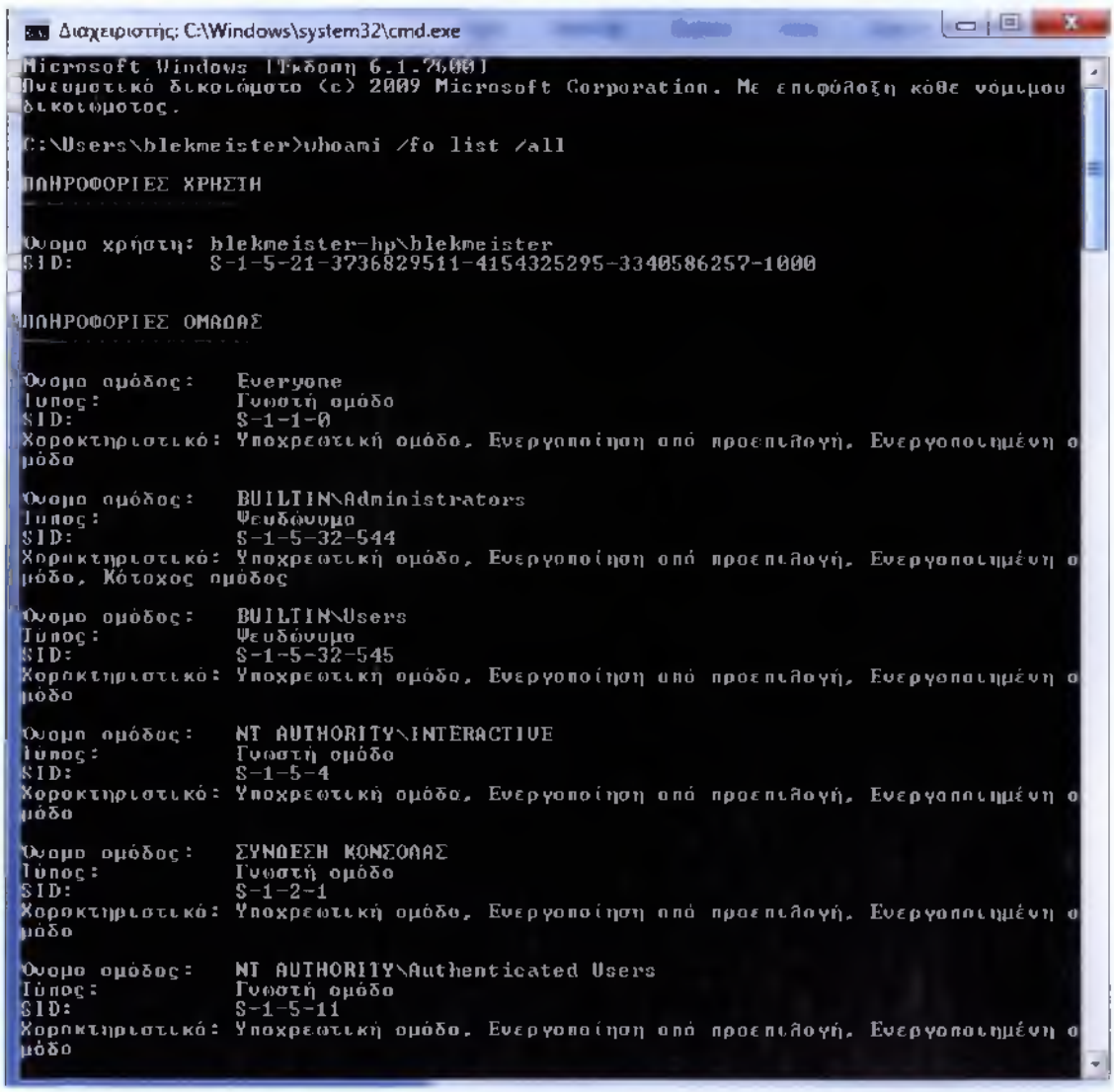
57989841-1336602894-682003330 – είναι sub-authorities που αναγνωρίζουν τον ηλεκτρονικό μας Υπολογιστή.

500 – Τέλος έχουμε το Relative Identifier(RID ή συγκριτικός αναγνωριστής)

Ενα RID του 500 πάντα αναγνωρίζει το λογαριασμό BUILT-IN\Administrator ο οποίος υπάρχει σε όλους τους ηλεκτρονικούς υπολογιστές που χρησιμοποιούν Windows. Ενα RID 501 μας δειχνει ενα λογαριασμο BUILT-IN\Guest. Οι πραγματικες RIDs των χρηστών που δημιουργούμε σαν διαχειριστές ξεκινάμε από το 1000 ή από το 1100 αναλόγως το λειτουργικό σύστημα που χρησιμοποιούμε. Τα RID δεν φεύγουν πότε από τον υπολογιστή μας ακόμα και να διαγράψουμε τον χρηστή τον όποιο δημιουργήσαμε.

2.1.6.2 Security Tokens (ενδεικτικά ασφαλείας)

Όταν ένα αντικείμενο εισέρχεται στο λειτουργικό μας σύστημα δημιουργεί ένα ενδεικτικό ασφαλείας, ή αλλιώς ενδεικτικό πρόσβασης, για το αντικείμενο αυτό. Το ενδεικτικό ασφαλείας περιέχει ουσιαστικές πληροφορίες για το αντικείμενο. Επιπροσθέτως, στον προσωπικό SID του αντικειμένου το ενδεικτικό περιέχει όλα τα SIDs από όλες τις ομάδες όπου το αντικείμενο είναι μέλος, όλων των δικαιωμάτων και προνομίων που έχει. Όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 7 : Ενδεικτικό ασφαλείας, πληροφορίες ομάδας

Κάθε διεργασία που «τρέχει» για λογαριασμό του χρήστη παίρνει ένα αντίγραφο από το ενδεικτικό ασφαλείας. Αυτό το ενδεικτικό της διεργασίας περιέχει περίπου τις ίδιες πληροφορίες όπως και το ενδεικτικό ασφαλείας, θα έχει επίσης επιπρόσθετες πληροφορίες οι

οποίες συσχετίζονται για το πως μπορεί να χρησιμοποιηθεί και αν έχουν αφαιρεθεί κάποια πράγματα.

2.1.6.3 Στόχοι User Account Control

Το User Account Control σχεδιάστηκε με σκοπό να βελτιώσει κατά πολύ την εμπειρία του χρήστη στο Λειτουργικό σύστημα καθώς και την ασφάλεια του. Δηλαδή πέτυχε τους παρακάτω στόχους :

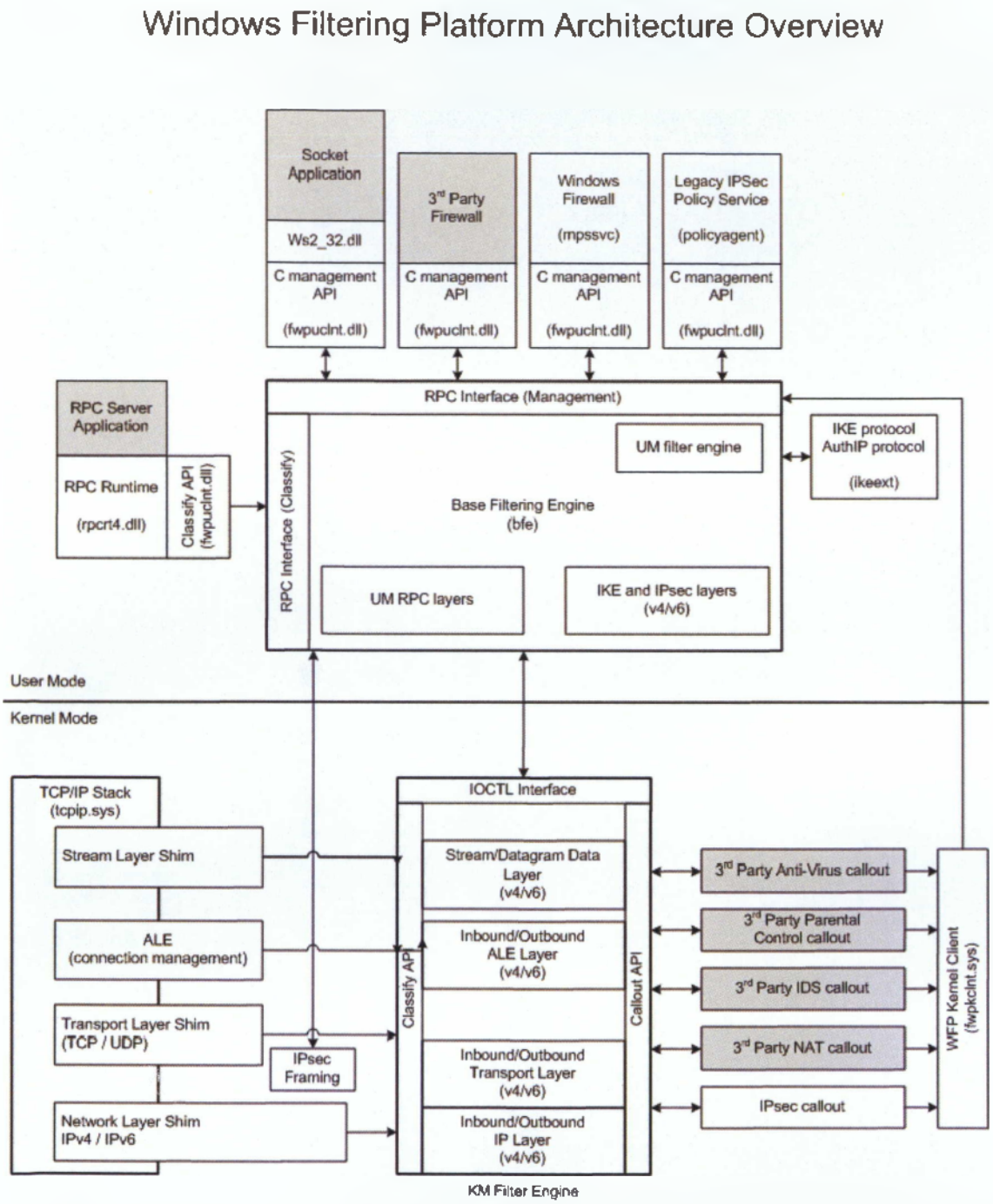
- Αύξηση του αριθμού των χρηστών που μπορούν να δουλεύουν σαν μη διαχειριστές στην πλειονότητα του χρόνου που είναι στον ηλεκτρονικό τους υπολογιστή
- Μείωση του αριθμού των σεναρίων τα οποία απαιτούν την προαγωγή του χρήστη σε διαχειριστή
- Αν χρειάζεται να κάνουμε την προαγωγή (elevation) πιο εύκολη - αυτόματα αν είναι πιθανό - από τα τωρινά kluges* που χρησιμοποιούν το runas .exe
- Να παρέχει κάποια προστασία από τις εφαρμογές που εκτελούνται σαν διαχειριστής από ότι αυτές που δεν εκτελούνται σαν διαχειριστές.
- Να ενεργοποιήσει μερικές πολύ εκτεθειμένες εφαρμογές με λιγότερα δικαιώματα όταν χρειάζεται.

2.1.7 Windows Firewall

Η εισαγωγή του τείχους προστασίας windows με την έκδοση του service pack 2 για τα windows XP έφερε τρομερές αλλαγές στην προστασία των υπολογιστών ,καθώς μειώθηκε δραματικά η εξάπλωση των ιών και των κακόβουλων προγραμμάτων καθώς και των επιθέσεων από εισβολείς. Στα Windows Vista το τείχος προστασίας αναπρογραμματίστηκε από την αρχή και περιλαμβάνει και το εξερχόμενο φιλτράρισμα(outbound filtering). Επίσης περιλαμβάνει πολλές εξαιρέσεις για πολλές κοινές εφαρμογές. Για το τείχος προστασίας των windows vista η Microsoft έκανε ένα τεράστιο πρόγραμμα με πολλούς ανθρώπους να εξετάζουν λεπτομερώς τι νέα χαρακτηριστικά θα έπρεπε να προστεθούν στο τείχος προστασίας των Windows και τι αδυναμίες είχε η προηγούμενη έκδοση του. Και έτσι αυτό που δημιούργησαν ήταν ουσιαστικά μια εκτενή πλατφόρμα φιλτραρίσματος με πολλά νέα χαρακτηριστικά.

2.1.7.1 Windows Filtering Platform

Το Windows Filtering Platform είναι η πλατφόρμα φιλτραρίσματος που χρησιμοποιείται από το τείχος προστασίας. Στην εικόνα δείχνουμε την λειτουργιά του.



Εικόνα 8 : Windows Filtering Platform [10]

Όπως δείχνει η εικόνα η πλατφόρμα φιλτραρίσματος (Windows Filtering Platform) περιλαμβάνει και φιλτράρισμα πυρήνα και φιλτράρισμα για τον χρήστη και αυτό διευκολύνει την προστασία του υπολογιστή καθώς προηγούμενες εκδόσεις του τείχους προστασίας των Windows χρησιμοποιούσαν αναποτελεσματικούς τρόπους για την παρακολούθηση της κίνησης που είχε το δίκτυο του υπολογιστή πριν αυτή εισχωρήσει στο σύστημα μας και

μολυνθεί με κάποιο κακόβουλο πρόγραμμα. Στο πάνω μέρος τις εικόνας βλέπουμε το UI του τείχους προστασίας (explorer.exe). Από κάτω βλέπουμε τη βασική μηχανή φιλτραρίσματος που χρησιμοποιεί το τείχος προστασίας και τα δεδομένα που παραμετροποιητή τα αποθηκεύει στη registry. Επίσης, στο σχήμα παρατηρούμε πολλά φίλτρα όταν βρισκόμαστε σε κατάσταση χρήστη τα οποία χρησιμοποιούνται για να φιλτράρουν την κίνηση των εφαρμογών στο δίκτυο μας όπως το RPC.

Επιπλέον, παρατηρούμε μια μηχανή φιλτραρίσματος και στον πυρήνα στην οποία και τα δυο τοπικά χαρακτηριστικα (δηλαδή τα χαρακτηριστικά του τείχους προστασίας) αλλά και εργαλεία από άλλες εφαρμογές άλλων εταιριών (δηλαδή antivirus από άλλες εταιρίες), συνεργάζονται για κάποιες λειτουργίες με την μηχανή φιλτραρίσματος.

Αυτες οι λειτουργίες καλούνται μόνο όταν κάποια συγκεκριμένα γεγονότα συμβαίνουν στο σύστημά μας, στα οποία σε κάποιο σημείο ανιχνεύουν κάποια περίεργη δραστηριότητα και αποφασίζουν τι ενέργεια να κάνουν,δηλαδά να το αποτρέψουν ή να το αποτρέψουν μερικώς ή να το επιτρέψουν ή να τροποποιήσουν την κίνηση στο δίκτυο.

Η μηχανή φιλτραρίσματος λειτουργεί σε πολλά διαφορετικά επίπεδα. Όπως για παράδειγμα, ένα συγκεκριμένο φίλτρο θα μπορούσε να ζητήσει για πακέτα μόνο στο επίπεδο δικτυού ή μόνο στο επίπεδο μεταφοράς. Ένα φίλτρο επίσης θα μπορούσε να ζητήσει μόνο για το πρώτο πακέτο σε μια σύνδεση ή για όλα τα πακέτα στο επίπεδο εφαρμογών, χρησιμοποιώντας τα νέα Application Layer Enforcement (ALE, Εκτέλεση επίπεδου εφαρμογών) φίλτρα που αναφέρθηκαν προηγουμένως.

2.1.7.2 Boot Time Filtering

Ένα πρόβλημα το οποίο αντιμετώπιζαν οι παλαιότερες εκδόσεις των Windows ήταν ότι όταν ξεκινούσε το σύστημά μας δεν υπήρχε καμία προστασία. Και αυτός ήταν ο λόγος που ξέσπασε το σκουλήκι worm blaster το 2003.

Στα Windows Vista τα φίλτρα για την ώρα που ξεκινάει το σύστημά μας ενσωματώθηκαν στο Windows File Protection .Έτσι όταν ξεκινάει ο ηλεκτρονικός υπολογιστής μας συμβαίνουν οι ακόλουθες ενέργειες :

1. Ο υπολογιστής μας ξεκινάει, χωρίς ενεργοποιημένο το δίκτυο
2. Η στοίβα του δικτύου ξεκινάει και μαζί της το βοηθητικό πρόγραμμα οδήγησης της Προστασίας Φακέλων Windows.

3. Το δίκτυο λειτουργεί και τα φίλτρα Προστασίας Φακέλων Windows είναι ενεργά.

4. Η υπηρεσία, μηχανή φιλτραρίσματος βάσης (Base filtering engine) ξεκινά και αντικαθιστά τα φίλτρα χρόνου εκκίνησης(boot-time filters), με συνεχόμενα και σταθερά φίλτρα(persistent filters).

5. Η υπηρεσία του τείχους προστασίας ξεκινά και διαβάζει την τρέχουσα πολιτική που καθορίζει το τρέχων προφίλ και επιτρέπει επιπρόσθετη κίνηση στο δίκτυο

Τα φίλτρα χρόνου εκκίνησης (boot-time filters) και τα συνεχόμενα φίλτρα (persistent filters) είναι ακριβώς τα ίδια φίλτρα. Ο κύριος λόγος που χρησιμοποιούνται δύο ειδών φίλτρα είναι για να μπορεί η Μηχανή Φιλτραρίσματος Βάσης να ανακτεί τα φίλτρα του από ένα σημείο μόνο. Και τα δυο μαζί κάνουν τα έξης :

- Αποκλείουν όλη την εσωτερική κίνηση που δεν έχει ζητηθεί
- Επιτρέπουν εσωτερική κίνηση από κάθε loopback διεύθυνση
- Επιτρέπουν την εισερχόμενη ICMPv6 "γειτονική ανακάλυψη"(Neighbor Discovery). Αυτή χρησιμοποιείται για να χαρτογραφήσει τις διευθύνσεις IPv6 σε μέτριο έλεγχο πρόσβασης (Medium Access Control) ή σε διευθύνσεις τοπικού δικτύου, που λειτουργεί το ίδιο με το πρωτόκολλο ARP στην IPv4.

Επίσης όταν το τείχος προστασίας λειτουργεί, τα persistent filters λειτουργούν ακόμα. Μόνο εάν το τείχος προστασίας απενεργοποιηθεί τα φίλτρα αυτά απενεργοποιούνται. Αυτό σημαίνει ότι αν για κάποιο λόγο η υπηρεσία του τείχους προστασίας τερματιστεί, τα φίλτρα αυτά είναι ακόμα ενεργά και αποκλείουν όλη την εσωτερική κίνηση.

2.1.7.3 Stealth

Το Τείχος προστασίας των Windows έχει ένα χαρακτηριστικό stealth που είναι ενεργό κάθε στιγμή που το τείχος προστασίας είναι ενεργό. Το χαρακτηριστικό stealth χρησιμοποιείται για την καταπολέμηση από επιθέσεις εισβολέων που χρησιμοποιούν τη μέθοδο portscan μέσω του τείχους προστασίας. Εάν μια θύρα TCP σε έναν κεντρικό υπολογιστή ακούει έναν απομακρυσμένο υπολογιστή και προσπαθεί να συνδεθεί με αυτό, η σύνδεση θα οδηγήσει σε μια τυπική χειραψία TCP, και η portscanner θα αναφέρει μια ανοιχτή θύρα. Ωστόσο , εάν ο host δεν κάνει ακρόαση στη θύρα, τότε επιστρέφει ένα TCP RST (reset) μήνυμα στον υπολογιστή που προσπάθησε να συνδεθεί με αυτόν. Σε περίπτωση που ένα τείχος προστασίας ,μπροστά από τον host, έχει ρυθμιστεί ώστε να αφήνει μια θύρα

ανοιχτή, αλλά ο host πίσω από το τείχος προστασίας δεν ακούει σε αυτό, τότε το reset μήνυμα λέει στον εισβολέα ότι το τείχος προστασίας έχει παραμετροποιηθεί έτσι ώστε να αφήνει μια πόρτα ανοιχτή.

Το τείχος προστασίας στα Windows Vista περιλαμβάνει ένα Stealth χαρακτηριστικό το οποίο δεν αφήνει να στέλνονται εξερχόμενα reset μηνύματα. Εάν ένα μήνυμα σταλθεί σε μια UDP πόρτα ή σε μία υποδοχή μη-TCP/UDP που δεν ακούει τότε δημιουργείτε ένα ανάλογο «Δεν είναι κανείς στο σπίτι» μήνυμα ,το οποίο το τείχος προστασίας το εμποδίζει και αυτό. Αυτό σημαίνει ότι αν το τείχος προστασίας των Windows επιτρέπει κάποια κίνηση μέσα στο δίκτυο και ένας εισβολέας προσπαθεί να κάνει portscan μέσω του τείχους προστασίας, ακόμα και αν το τείχος προστασίας έχει ρυθμιστεί έτσι ώστε να επιτρέπει την κυκλοφορία σε μια θύρα που δεν έχει ακρόαση υπηρεσίας, ο εισβολέας δεν θα δει καμία ένδειξη αυτής .

2.1.7.4 Outbound Filtering

Περισσότερο από οποιοδήποτε άλλο χαρακτηριστικό του τείχους προστασίας, η έλλειψη εξερχόμενου φιλτραρίσματος των Windows XP ήταν μία απόδειξη του γιατί ήταν ανεπαρκής για την ασφάλεια στην πάλαια έκδοση του τείχος προστασίας. Η βασική λειτουργία που μετατρέπει το εξερχόμενο φιλτράρισμα από ένα απλό speed bump σε ένα χρήσιμο χαρακτηριστικό ασφαλείας δεν υπήρχε σε προηγούμενες εκδόσεις του Λειτουργικού Συστήματος, υπάρχει όμως στα Windows Vista.

Χωρίς την «σκλήρυνση υπηρεσιών» το εξερχόμενο φιλτράρισμα είναι απλά σαν μια συμβουλή που ένας χρήστης θα την έπαιρνε εάν ήθελε να αποφύγει κάποιες καταστροφικές ενέργειες στο σύστημά του. Στα Windows XP κάθε εκτελέσιμο πρόγραμμα μπορεί να στείλει εξερχόμενη κίνηση σε οποιονδήποτε host και σε οποιαδήποτε θύρα. Όμως στα Windows Vista,η σκλήρυνση υπηρεσιών το αλλάζει αυτό, και επιτρέπει στο τείχος προστασίας να παρέχει ουσιώδες εξερχόμενο φιλτράρισμα. Από προεπιλογή, η περισσότερη εισερχόμενη κίνηση είναι αποκλεισμένη, και η περισσότερη εξερχόμενη κίνηση επιτρέπεται, αλλά πολλές υπηρεσίες έχουν εξερχόμενη κίνηση η οποία περιορίζεται από προεπιλογή. Το εξερχόμενο φιλτράρισμα έχει σχεδιαστεί για δύο λόγους :

- Φιλτράρισμα τον εξερχόμενων συνδέσεων που κάνουν οι υπηρεσίες
- Για εντοπισμό συγκεκριμένου, ανάλογα την περίσταση, φιλτραρίσματος από τους διαχειριστές του συστήματος όπως η παρεμπόδιση της εξερχόμενης κίνησης του

μηνύματος αποκλεισμού του διακομιστή (smb traffic) - μια εφαρμογή σε επίπεδο πρωτοκόλλου δικτύου που χρησιμοποιείται συνήθως για την κοινή χρήση αρχείων και εκτύπωσης- .

Αυτοί είναι οι δύο τύποι φιλτραρίσματος που προσδίδουν πραγματική ασφάλεια στο σύστημά μας, αν και όταν ένας χρήστης έχει συνδεθεί σαν διαχειριστής ή ένα πρόγραμμα τρέχει για λογαριασμό του χρήστη, μπορεί να απενεργοποιήσει τις δύο αυτές λειτουργίες.

2.1.7.5 Strict Source Mapping

Στα UDP, και portless πρωτόκολλα, δεν υπάρχει καμία σημασιολογία συνόδου, και ως εκ τούτου είναι δύσκολο να εμποδιστεί ένας τρίτος να συμμετάσχει σε μια σύνοδο. Για παράδειγμα, εάν συσκευή Α στείλει ένα αίτημα UDP στην συσκευή Β, η συσκευή Α θα δέχεται απαντήσεις από οποιοδήποτε κεντρικό υπολογιστή που μπορεί να ανταποκριθεί στην αιτούμενη θύρα και στο πρωτόκολλο, εντός μιας ορισμένης προθεσμίας. Αυτό ονομάζεται Χαλαρή Χαρτογράφηση Πηγής (loose source mapping).

Στα Windows Vista, το τείχος προστασίας χρησιμοποιεί Αυστηρή Χαρτογράφηση Πηγής (strict source mapping).Αυτό σημαίνει ότι διατηρεί έναν πίνακα με UDP και portless αιτήματα, και προκειμένου να επιτρέψει μια απάντηση δεν πρέπει να ταιριάζει μόνο με το πρωτόκολλο και τη θύρα(για UDP), αλλά και με τη διεύθυνση IP που χρησιμοποιήθηκε στην αρχική αίτηση. Αυτό είναι αυτό που είναι γνωστό ως Αυστηρή Χαρτογράφηση Πηγής. Είναι μια προσπάθεια να φέρει την σημασιολογία συνόδου στα πρωτόκολλα που έχουν εγγενώς κανένα.

2.1.8 Mandatory Integrity Control

Όταν οι προγραμματιστές της Microsoft δημιούργησαν τα Windows Vista έθεσαν ως στόχο να διασφαλιστεί ότι ήταν η πιο ασφαλής έκδοση του Λειτουργικών Συστημάτων της Microsoft μέχρι στιγμής. Μια από τις λειτουργίες που εισάχθηκαν στα Windows Vista που συμβάλει στην ασφάλεια είναι ο έλεγχος της ακεραιότητας, ή Windows Integrity Control (WIC).

Ο σκοπός του έλεγχου ακεραιότητας είναι η προστασία των αντικειμένων, είτε πρόκειται για αρχεία, εκτυπωτές, τα κλειδιά μητρώου, από τις επιθέσεις των κακόβουλων λογισμικών ή ακόμα από τα αθώα σφάλματα του χρήστη. Η έννοια της WIC βασίζεται στον καθορισμό της αξιοπιστίας των διαφόρων αντικειμένων και του έλεγχο των

αλληλεπιδράσεων μεταξύ των αντικειμένων με βάση την ακεραιότητα τους, ή το επίπεδο της αξιοπιστίας τους.

Τα επίπεδα ακεραιότητας του WIC ελέγχονται υποχρεωτικά και έχουν υψηλή προτεραιότητα καθώς το λειτουργικό σύστημα παρακάμπτει άλλους ελέγχους, όπως αυτούς των αρχείων και των φακέλων NTFS, με τους οποίους οι περισσότεροι διαχειριστές είναι εξοικειωμένοι. Ο πρωταρχικός στόχος της WIC είναι να διασφαλίσει ότι μόνο τα αντικείμενα με ένα επίπεδο ακεραιότητας ίσο ή μεγαλύτερο από το αντικείμενο-στόχο να έχουν τη δυνατότητα να αλληλεπιδράσουν με αυτό. Ουσιαστικά, αν ένα αντικείμενο είναι λιγότερο αξιόπιστο, του απαγορεύεται να αλληλεπιδρά με πιο αξιόπιστα αντικείμενα.

Προκειμένου τα Windows να ιεραρχικοποιήσουν τις αλληλεπιδράσεις μεταξύ των αντικειμένων , ορίζουν πρώτα την αξιοπιστία καθενός ξεχωριστά. Ο έλεγχος ακεραιότητας θέτει ένα από τα παρακάτω επίπεδα ακεραιότητας για τα αντικείμενα :

- **Μη αξιόπιστο** - οι διεργασίες που καταγράφονται σε ανώνυμα αυτόματα χαρακτηρίζονται ως μη αξιόπιστες

- **Χαμηλή** - το χαμηλό επίπεδο ακεραιότητας είναι το επίπεδο που χρησιμοποιείται από προεπιλογή για την αλληλεπίδραση του χρήστη με το Internet. Εφ 'όσον ο Internet Explorer λειτουργεί στην προεπιλεγμένη κατάστασή του, Protected Mode, όλα τα αρχεία και οι διαδικασίες που σχετίζονται με τον Internet Explorer τους αποδίδεται χαμηλό επίπεδο ακεραιότητας. Μερικοί φάκελοι, όπως ο Temporary Internet Folder, του αποδίδεται επίσης το χαμηλό επίπεδο ακεραιότητας από προεπιλογή.

- **Μεσαίο** - Είναι στο επίπεδο στο οποίο τα περισσότερα αρχεία λειτουργούν. Οι χρήστες λαμβάνουν αυτόματα την ακεραιότητα αυτή, καθώς και κάθε αντικείμενο που δεν του έχει δοθεί υψηλό ή χαμηλό επίπεδο ορίζεται αυτόματα από το σύστημα στο μεσαίο.

- **Υψηλό** - Οι διαχειριστές χορηγούνται υψηλού επιπέδου ακεραιότητας. Αυτό εξασφαλίζει ότι οι διαχειριστές είναι σε θέση να αλληλεπιδρούν και να τροποποιούν όσα αντικείμενα τους έχει δοθεί χαμηλό ή μεσαίο επίπεδο ακεραιότητας.

- **Σύστημα** - Όπως υποδηλώνει το όνομα, το επίπεδο της ακεραιότητας του συστήματος είναι αποκλειστικά για το σύστημα. Ο πυρήνας των Windows και βασικών υπηρεσιών στα οποία χορηγείται το επίπεδο ακεραιότητας του συστήματος. Όντας ακόμη υψηλότερο από το υψηλό επίπεδο ακεραιότητας προστατεύει αυτές τις βασικές λειτουργίες του συστήματος ακόμα και από τους διαχειριστές του συστήματος.

Εικόνα 9: Ορισμός επιπέδων ακεραιότητας [11]

Υπάρχει και μια ειδική περίπτωση των επιπέδων ακεραιότητας το επίπεδο εγκατάστασης. Το επίπεδο αυτό είναι το ανώτερο απ όλα τα άλλα και όποιο αντικείμενο έχει ανατεθεί σε αυτό έχει τη δυνατότητα να απεγκαταστήσει άλλα προγράμματα ακόμα και αυτά του συστήματος.

Οι λίστες ελέγχου πρόσβασης (ACL) περιορίζονται στη χορήγηση δικαιωμάτων πρόσβασης (ανάγνωσης, εγγραφής και εκτέλεσης) και τα προνόμια για τους χρήστες ή για τις ομάδες. Ο έλεγχος της ακεραιότητας (MIC) επιτρέπει κατηγορίες εφαρμογών που θα απομονωθούν, επιτρέποντας σενάρια όπως Sandboxing πιθανώς ευάλωτες εφαρμογές (όπως το διαδίκτυο -που αντιμετωπίζει η εφαρμογή).

Ωστόσο, δεδομένου ότι δεν εμποδίζει μια διαδικασία με χαμηλότερο επίπεδο ακεραιότητας(IL) να κάνει κοινή χρήση αντικειμένων με μια διαδικασία με υψηλότερο IL, μπορεί να προκαλέσει ρωγμές στην διαδικασία με υψηλότερο IL και να δουλέψει για λογαριασμό της χαμηλής διαδικασία IL, με αποτέλεσμα να έχουμε κίνδυνο από squatting attack (ένα είδος DoS επίθεσης) . Μια «Shatter Attack» ωστόσο, μπορεί να προληφθεί με τη

χρήση ένα άλλο χαρακτηριστικό, την απομόνωση των δικαιωμάτων της επιφάνειας εργασίας του χρήστη(User Interface privilege Isolation) σε συνδυασμό με το MIC.

Ο υποχρεωτικός έλεγχος της ακεραιότητας προσδιορίζεται χρησιμοποιώντας ένα νέο τύπο καταχώρησης ελέγχου πρόσβασης (ACE), που εκπροσωπεί το IL του αντικειμένου, στην περιγραφή ασφαλείας του. Το επίπεδο ακεραιότητας ενός αντικειμένου ανατείθετε επίσης στο διακριτικό πρόσβασης όταν αυτό αρχικοποιείται.

Επιπλέον ,το επίπεδο ακεραιότητας στο διακριτικό πρόσβασης συγκρίνεται με το επίπεδο ακεραιότητας στην περιγραφή ασφαλείας όταν η οθόνη αναφοράς της ασφάλειας πραγματοποιεί αναγνώριση πριν από την παροχή πρόσβασης σε αντικείμενα. Τα Windows περιορίζουν τα επιτρεπόμενα δικαιώματα πρόσβασης ανάλογα με το αν το επίπεδο της ακεραιότητας του υποκειμένου είναι υψηλότερο ή χαμηλότερο από το αντί κείμενο, και ανάλογα με τις σημαίες της πολιτικής ακεραιότητας στη νέα ACE ελέγχου πρόσβασης. Το υποσύστημα της ασφάλειας θέτει σε εφαρμογή το επίπεδο ακεραιότητας ως υποχρεωτική σήμανση ώστε να διακρίνεται από τη διακριτική πρόσβαση υπό τον έλεγχο του χρήστη, το οποίο παρέχουν οι ACLs.

2.1.9 Other Security Features and Security Protocols

2.1.9.1 Secure Sockets Layers (SSL)

Το πρωτόκολλο SSL (Secure Sockets Layer) αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο ηλεκτρονικών υπολογιστών εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP πρωτόκολλο για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το telnet κοκ.

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (email). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από

τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

Εικόνα 10 : Το SSL λειτουργεί πρίν τα πρωτόκολλα

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής[13][14]

- DES - Data Encryption Standard,
- DSA - Digital Signature Algorithm,
- KEA - Key Exchange Algorithm,
- MD5 - Message Digest,
- RC2/RC4,
- RSA,
- SHA-1 - Secure Hash Algorithm,
- SKIPJACK,
- Triple-DES.

2.1.9.2 Προστασία Πόρων Windows (Windows Resource Protection)

Η Προστασία Πόρων του συστήματος είναι μια δυνατότητα των Windows Vista, η οποία αντικαθιστά την προστασία των αρχείων Windows(Windows File Protection). Εκτός από τα κρίσιμα αρχεία του συστήματος. προστατεύει επίσης και τα κλειδιά μητρώου και τους

φακέλους .Ο τρόπος που προστατεύει τους πόρους διαφέρει εξ ολοκλήρου από τη μέθοδο που χρησιμοποίησε η προστασία των αρχείων Windows.

Η Προστασία αρχείων των Windows λειτουργεί με την εγγραφή για την κοινοποίηση των αλλαγών στο αρχείο winlogon. Εάν εντοπιστούν αλλαγές σε ένα προστατευμένο αρχείο συστήματος, το τροποποιημένο αρχείο αντικαθίσταται από ένα προσωρινά αποθηκευμένο αντίγραφο που βρίσκεται σε ένα συμπιεσμένο φάκελο *στο* `% windir% \ system32 \ Dllcache`.

Η Προστασία Πόρων του συστήματος λειτουργεί θέτοντας διακριτικές λίστες ελέγχου πρόσβασης (DACL) και λίστες ελέγχου πρόσβασης (ACL) που ορίζονται για την προστασία των πόρων. Η άδεια για πλήρη πρόσβαση για την τροποποίηση των πόρων που είναι προστατευμένοι από την προστασία πόρων (WRP) περιορίζεται στις διαδικασίες που χρησιμοποιούν την *Windows Modules Installer υπηρεσίας* (TrustedInstaller.exe).Επιπλέον, οι διαχειριστές δεν έχουν πλήρη δικαιώματα στα αρχεία συστήματος οπότε οι προστατευόμενες πόροι μπορούν να τροποποιηθούν ή να αντικατασταθούν μόνο αν οι διαχειριστές αναλάβουν την κατοχή του πόρου και να προσθέσουν τις κατάλληλες καταχωρήσεις ελέγχου πρόσβασης (ACE). Ο "Installer Trusted" λογαριασμός χρησιμοποιείται για να ασφαλίζει βασικά αρχεία συστήματος λειτουργίας και κλειδιά μητρώου.

Windows Resource Προστασίας προστατεύει ένα μεγάλο αριθμό τύπων αρχείων κάποια από αυτά είναι τα εξής:

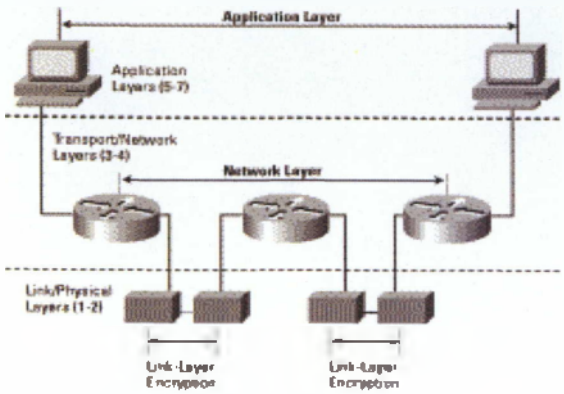
* .dll, *.exe, *.acm, *.app, *.aspx, *.bas, *.bat, *.bin,
*.cmd, *.com, *.cpl, *.h1s, *.lnk, *.mad *.tsp, *.url, *.wsf, *.xsl

Επίσης, το WRP προστατεύει επίσης πολλούς κρίσιμους φακέλους. Επιπροσθέτως , Τα σημαντικά κλειδιά μητρώου που έχουν εγκατασταθεί από τα Windows Vista και προστατεύονται επίσης. Εάν ένα κλειδί προστατεύεται από το WRP, όλα τα δευτερεύων κλειδιά και τιμές μπορούν να προστατευθούν. Τέλος Η Προστασία Πόρων του συστήματος επιβάλλει αυστηρότερα μέτρα για την προστασία των αρχείων.

2.1.9.3 Πρωτόκολλο Ασφαλείας Διαδικτύου (IPSEC)

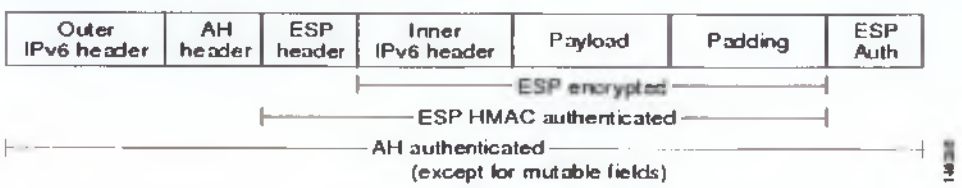
Το IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για τη διασφάλιση του απορρήτου των επικοινωνιών. Εγγυάται την εμπιστευτικότητα , ακεραιότητα και πίστωση ταυτότητας , τόσο τον δεδομένων όσο και τον επικοινωνιών που γίνονται με αυτό. Για να μπορέσει να τα καταφέρει, προσφέρει κρυπτογράφηση στο επίπεδο IP και καθορίζει πώς θα

γίνεται η κρυπτογράφηση των δεδομένων. Το IPSec υποστηρίζει, επίσης, ένα πλαίσιο ανταλλαγής κλειδιών (Internet Key Exchange – IKE) το οποίο διαπραγματεύεται τις σχέσεις ασφαλείας (Security Associations – SA) αλλά και να ανταλλάσσει τα κλειδιά αυτά. [15]



Εικόνα 11 : IPSec[16]

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



Εικόνα 12 : Πακέτο IPSec

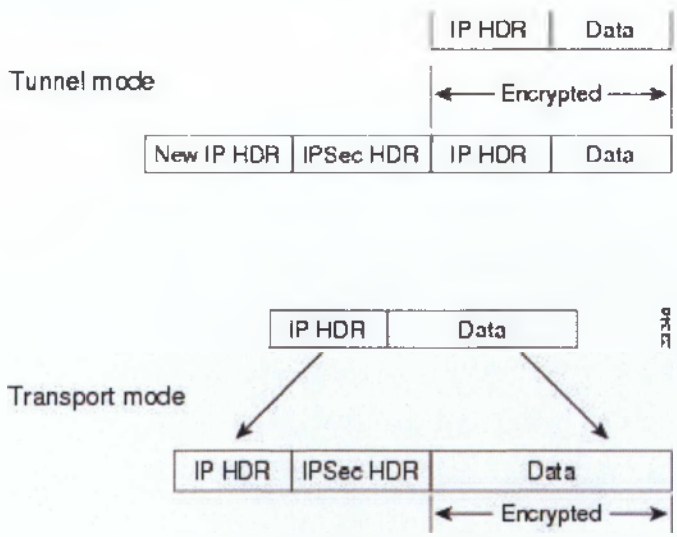
Το πρωτόκολλο IPSec επεμβαίνει αργά σε ένα IP πακέτο , βάζοντας μια επιπλέον επικεφαλίδα ενώ παράλληλα κρυπτογραφεί την καθαρή πληροφορία (payload) . Η επικεφαλίδα του IPSec μπορεί να είναι η :

- Επικεφαλίδα πιστοποίησης (Authentication Header – AH), η οποία προσφέρει ακεραιότητα και πιστοποίηση του περιεχομένου του πακέτου, καθώς και του μεγαλύτερου μέρους της IP επικεφαλίδας και γι αυτό το λόγο χρησιμοποίει μια συνάρτηση hash κλειδιού.

- Ενθυλάκωση ασφαλούς πληροφορίας (Encapsulation Security Payload – ESP), στην οποία λειτουργία παρέχεται εμπιστευτικότητα, ακεραιότητα και πιστοποίηση προέλευσης για το κάθε πακέτο, μια και κρυπτογραφείται πάντοτε ενώ παράλληλα δίνεται η επιλογή για πιστοποίηση του payload . Εάν γίνει συνδυασμός με πλήρη με χρήση της επικεφαλίδας πιστοποίησης, το IPSec παρέχει ταυτόχρονα όλες τις δυνατότητες, με πλήρη εμπιστευτικότητα και πιστοποίηση πακέτων. [15]

Το IPSec έχει δύο κύριους τρόπους λειτουργίας, ανάλογα με το αν τα τελικά συστήματα αντιλαμβάνονται και μπορούν να διαχειρισθούν τη συγκεκριμένη τεχνολογία

- Κατάσταση Μεταφοράς (Transport Mode) , η οποία είναι για χρήση του IPSec σε τελικά συστήματα τα οποία καταλαβαίνουν το πρωτόκολλο και μπορούν να το διαχειριστούν. Στον τρόπο αυτό, σε κάθε IP πακέτο προσαρτάται μια νέα IPSec επικεφαλίδα, ενώ κρυπτογραφείται μόνο το IP payload.
- Κατάσταση Διόδου (Tunnel Mode) , η οποία είναι για χρήση του IPSec σε τελικά συστήματα τα οποία δε καταλαβαίνουν αυτό το πρωτόκολλο και δεν μπορούν να το διαχειριστούν. Έτσι, μια ενδιάμεση πύλη (gateway) αναλαμβάνει τη διαχείριση των IPSec πακέτων και έπειτα τα παραδίδει αποκρυπτογραφημένα σαν IP πακέτα στο τελικό σύστημα. Αυτή η κατάσταση δημιουργεί ένα καινούριο IP πακέτο, μαζί με μία νέα IPSec επικεφαλίδα, ενώ μέσα του βρίσκεται κρυπτογραφημένο ολόκληρο το αρχικό IP πακέτο. [15]



Εικόνα 13 : Καταστάσεις διόδου και μεταφοράς[17]

Η κατάσταση διόδου (tunnel mode) χρησιμοποιείται πιό συχνά, μια και προσφέρει σε μια δικτυακή συσκευή τη δυνατότητα να λειτουργεί σαν πληρεξούσια (proxy) για άλλες, οπότε και δεν χρειάζεται να τροποποιηθούν τα τελικά συστήματα προκειμένου να αναγνωρίζουν το IPSec. Παράλληλα, δίνεται η δυνατότητα υλοποίησης του IPSec σε επίπεδο αρχιτεκτονικής δικτύου. Τέλος, προστατεύει από παθητικές επιθέσεις ανάλυσης της διακίνησης των πληροφοριών στο δίκτυο, μια και ο επιτιθέμενος μπορεί να δεί μόνο τα τυπικά σημεία της διόδου και όχι σε ποιά τελικά συστήματα παραδίδονται τα πακέτα. [15]

2.1.9.4 Transport Layer Security

Το Transport Layer Security (TLS) είναι ένα πρωτόκολλο κρυπτογράφησης που παρέχει ασφάλεια της επικοινωνίας μέσω του Διαδικτύου. Το TLS κρυπτογραφεί τα τμήματα των συνδέσεων του δικτύου πάνω από το στρώμα μεταφοράς, χρησιμοποιώντας ασύμμετρη κρυπτογράφηση για την προστασία προσωπικών δεδομένων και έναν κώδικα γνησιότητας για την αξιοπιστία του μηνύματος. Αρκετές εκδόσεις των πρωτοκόλλων είναι σε ευρεία χρήση σε εφαρμογές όπως η περιήγηση στο web, ηλεκτρονικό ταχυδρομείο, αποστολή φαξ μέσω διαδικτύου, εφαρμογές άμεσων μηνυμάτων και voice-over-IP.

Το πρωτόκολλο TLS επιτρέπει σε client / server εφαρμογές να επικοινωνούν μέσω δικτύου με έναν τρόπο που αποσκοπούν στην πρόληψη υποκλοπών και παραβιάσεων (eavesdropping and tampering). Όταν ένας πελάτης TLS και διακομιστής διαπραγματεύονται μια σύνδεση χρησιμοποιούν χειραψία και κατά τη διάρκεια αυτής, ο πελάτης και ο διακομιστής θα συμφωνήσουν σχετικά με διάφορες παραμέτρους που χρησιμοποιούνται για την εδραίωση της ασφάλειας της σύνδεσης.

Παράδειγμα χειραψίας :

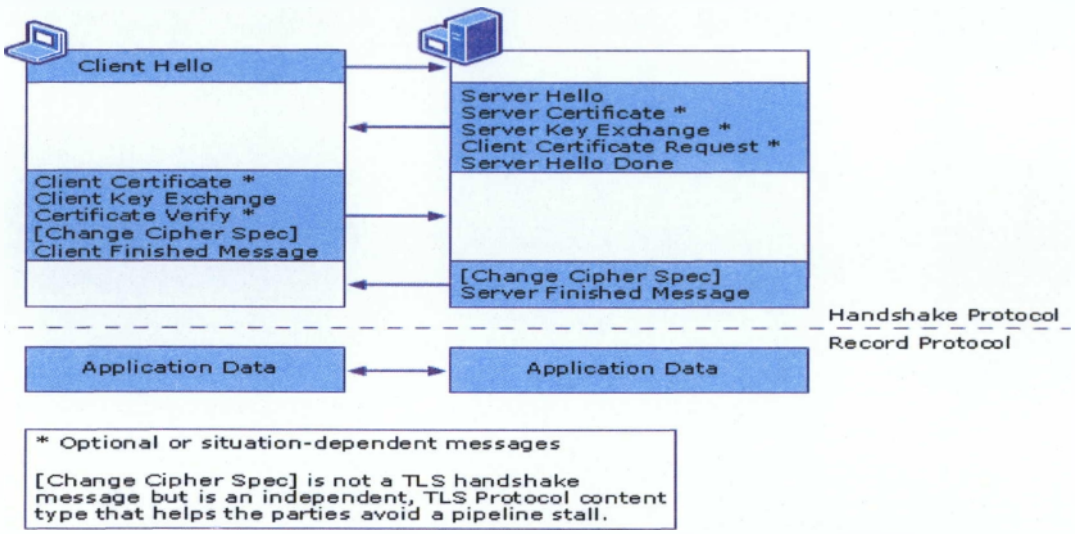
- Η χειραψία αρχίζει όταν ένας πελάτης συνδέεται σε έναν TLSενεργοποιημένο διακομιστή ζητώντας μια ασφαλή σύνδεση και παρουσιάζει μια λίστα με τα υποστηριζόμενα CipherSuites (αλγόριθμους κρυπτογράφησης και hash λειτουργίες).
- Από τον κατάλογο αυτό, ο server επιλέγει την ισχυρότερη κρυπτογραφημένη και hash λειτουργία που υποστηρίζει, και ειδοποιεί τον πελάτη (client) για την απόφαση.
- Ο διακομιστής στέλνει πίσω τη ταυτοποίησή του, με τη μορφή ενός ψηφιακού πιστοποιητικού. Το πιστοποιητικό περιέχει συνήθως το όνομα του διακομιστή,

τηναξιόπιστη αρχή έκδοσης πιστοποιητικών (CA) και το δημόσιο κλειδί κρυπτογράφησης του διακομιστή.

- Ο πελάτης μπορεί να επικοινωνήσει με το διακομιστή που εξέδωσε το πιστοποιητικό (η αξιόπιστη αρχή όπως παραπάνω) και να επιβεβαιώσει την εγκυρότητα του πιστοποιητικού πριν συνεχίσει.

- Για να δημιουργηθούν τα κλειδιά συνόδου που χρησιμοποιούνται για την ασφαλή σύνδεση, ο πελάτης κρυπτογραφεί ένα τυχαίο αριθμό με το δημόσιο κλειδί του διακομιστή και στέλνει το αποτέλεσμα στο διακομιστή. Μόνο ο server πρέπει να μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του.

- Από το τυχαίο αριθμό, αμφότερα τα μέρη παράγουν βασικά υλικά για την κρυπτογράφηση και την αποκρυπτογράφηση. Εδώ ολοκληρώνεται η χειραψία και αρχίζει η ασφαλής σύνδεση. Ωστόσο, εάν κάποιο από τα παραπάνω βήματα αποτύχει, η χειραψία TLS αποτυγχάνει και η σύνδεση δεν δημιουργείται.



Εικόνα 14: τυπική χειραψία TLS[18]

Τέλος Το TLS έχει μια ποικιλία μέτρων ασφαλείας. Αρχικά, παρέχει προστασία κατά της υποβάθμισης του πρωτοκόλλου σε προηγούμενη (λιγότερο ασφαλείς) έκδοση ή σε ασθενέστερο πρόγραμμα κρυπτογράφησης. Επίσης ,αριθμεί τα μετέπειτα αρχεία εφαρμογών με αριθμό σειράς και χρησιμοποιεί αυτόν τον αριθμό ακολουθίας στον κωδικό πιστοποίησης μηνύματος (MAC).Επιπλέον χρησιμοποιεί ένα μήνυμα συγχωνευμένο με ένα κλειδί (έτσι μόνο ένα κλειδί-κάτοχος να μπορεί να ελέγξει την MAC) . Η λειτουργία ψευδοτυχαίων διαχωρίζει τα δεδομένα εισόδου στο μισό και διαδικασίες το καθένα με διαφορετικό

αλγόριθμο hashing (MD5 και SHA-1), τότε XORs τους μαζί για να δημιουργήσουν την MAC. Αυτό παρέχει προστασία ακόμη και αν ένας από αυτούς τους αλγόριθμους βρίσκεται για να είναι ευάλωτες.

2.1.9.5 Αποτροπή εκτέλεσης δεδομένων

Η Αποτροπή εκτέλεσης δεδομένων (Data Execution Prevention - DEP) είναι ένα σύνολο τεχνολογιών υλικού και λογισμικού που πραγματοποιούν πρόσθετους ελέγχους στη μνήμη για να αποτρέψουν την εκτέλεση επιβλαβή κώδικα σε ένα σύστημα

Το κυριότερο πλεονέκτημα της δυνατότητας DEP είναι ότι βοηθά στην αποτροπή εκτέλεσης κώδικα από σελίδες δεδομένων. Τυπικά, ο κώδικας δεν εκτελείται από το προεπιλεγμένο heap και τη στοίβα. Η δυνατότητα DEP που επιβάλλεται από το υλικό ανιχνεύει κώδικα που εκτελείται από αυτές τις θέσεις και παρουσιάζει ένα μήνυμα εξαίρεσης κατά την εκτέλεση. Η δυνατότητα DEP που επιβάλλεται από το λογισμικό μπορεί να αποτρέψει τον επιβλαβή κώδικα να επωφεληθεί από τους μηχανισμούς χειρισμού εξαιρέσεων των Windows.

Η Δυνατότητα αποτροπής εκτέλεσης δεδομένων (DEP) που επιβάλλεται από το υλικό σημειώνει όλες τις θέσεις μνήμης σε μια διαδικασία ως μη εκτελέσιμες, εκτός αν η θέση περιέχει αποκλειστικά εκτελέσιμο κώδικα. Υπάρχει μια κλάση επιθέσεων που προσπαθεί να εισαγάγει και να εκτελέσει κώδικα από θέσεις μνήμης χωρίς δυνατότητα εκτέλεσης. Η δυνατότητα DEP βοηθά στην αποτροπή αυτών των επιθέσεων, αναχαιτίζοντάς τις και παρουσιάζοντας ένα μήνυμα εξαίρεσης.

Η δυνατότητα DEP που επιβάλλεται από το λογισμικό, έχει σχεδιαστεί με σκοπό τον αποκλεισμό επιβλαβούς κώδικα ο οποίος επωφελείται από τους μηχανισμούς χειρισμού εξαιρέσεων των Windows. Η δυνατότητα DEP που επιβάλλεται από το λογισμικό εκτελείται σε όλους τους επεξεργαστές που έχουν τη δυνατότητα εκτέλεσης του Windows XP SP2 και άνω. Από προεπιλογή, η δυνατότητα DEP που επιβάλλεται από το λογισμικό βοηθά στην προστασία μόνο περιορισμένων δυαδικών στοιχείων συστήματος, ανεξάρτητα από τις δυνατότητες της DEP που επιβάλλεται από το υλικό του επεξεργαστή.

2.2 Conclusion

Σε αυτό το κεφάλαιο αναλύσαμε τους μηχανισμούς ασφαλείας αλλά και τις καινοτομίες στα λειτουργικά συστήματα Windows που εισάχθηκαν με την κυκλοφορία της έκδοσης Vista. Επίσης, κάναμε αναφορά στο πώς αυτές οι καινοτομίες άλλαξαν τον τρόπο με

τον οποίο οι χρήστες προστατεύονται από τις καθημερινές απειλές. Τέλος, στο επόμενο κεφάλαιο θα αναπτύξουμε μεθόδους με τις οποίες οι εισβολείς επιτίθενται στα υπολογιστικά μας συστήματα καθώς και σε εξυπηρετητές.

ΚΕΦΑΛΑΙΟ 3
ΟΙ ΒΑΣΙΚΟΤΕΡΕΣ ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΩΝ WINDOWS

3 Οι βασικότερες επιθέσεις κατά των Windows

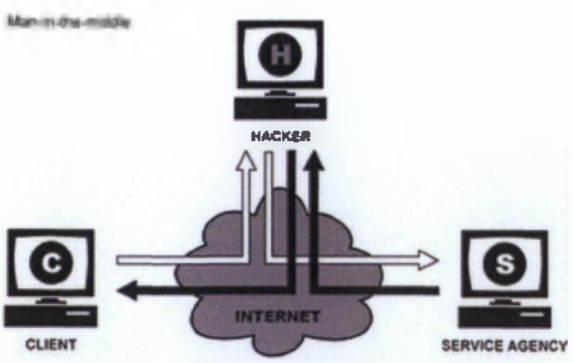
3.1 Εισαγωγή

Στο κεφάλαιο αυτό θα αναφερθούμε σε επιθέσεις ενάντια στα Windows και στο τρόπο υλοποίησής τους καθώς και στις μεθόδους προστασίας. Για τις ανάγκες τις εργασίας μας επιλέξαμε τις πέντε δημοφιλέστερες επιθέσεις, οι οποίες είναι :

- Man-In-The-middle Attack
- Denial Of Service
- Buffer Overflow
- DLL Hijacking
- Password Guessing/Cracking

3.2 Man-in-the-Middle Attack

Μια από τις πιο διαδεδομένες δικτυακές επιθέσεις που χρησιμοποιείται ενάντια σε χρήστες και οργανισμούς είναι η Man-in-the-Middle (MITM) επίθεση. Η επίθεση αυτή είναι μια μορφή υποκλοπής (eavesdropping) στη οποία ο επιτιθέμενος κάνει ανεξάρτητες συνδέσεις με τα θύματα του και αναμεταδίδει μηνύματα μεταξύ τους, δημιουργώντας την ψευδαίσθηση πως μιλούν απευθείας ο ένας στον άλλο με μια ιδιωτική σύνδεση, ενώ στην πραγματικότητα ολόκληρη η συνομιλία ελέγχεται από τον εισβολέα. [19] Η παρακάτω εικόνα περιγράφει τον τρόπο με τον οποίο ένας εισβολέας υποκλέπτει την συνομιλία μεταξύ δύο χρηστών.



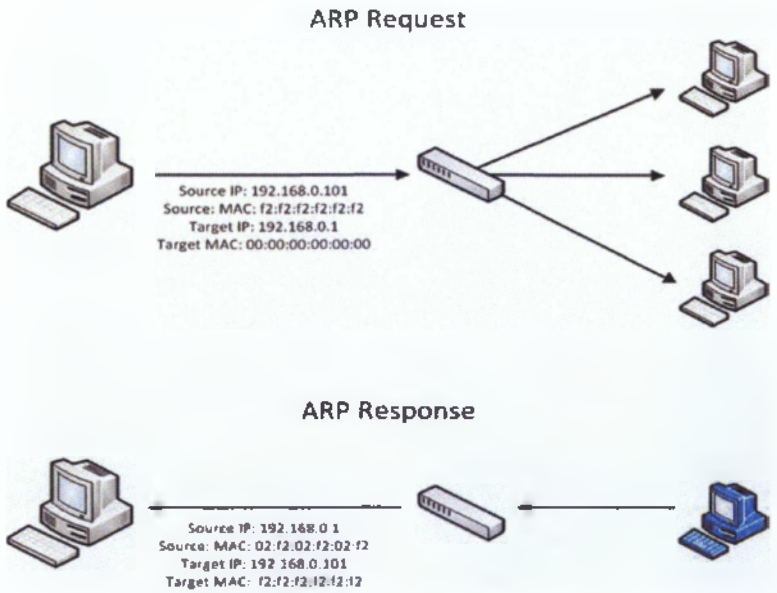
Εικόνα 15 : Man-in-the-Middle Attack [19]

Για την υλοποίηση επιθέσεων αυτού του είδους χρησιμοποιούνται πολλές μέθοδοι. Εμείς θα αναλύσουμε τις τέσσερις επικρατέστερες μεθόδους που χρησιμοποιούν οι εισβολείς.

3.2.1 Address Resolution Protocol

Μια από τις παλαιότερες μεθόδους υλοποίησης μια επίθεσης Man-in-the-Middle είναι η δηλητηρίαση του Πρωτόκολλου Μετατροπής Διεύθυνσης (ARP). Η μέθοδος αυτή επιτρέπει στον εισβολέα, με την προϋπόθεση να είναι στο ίδιο υποδίκτυο με τα θύματα της επίθεσης, να κρυφακούσει όλη την κίνηση του δικτύου ανάμεσα στα θύματα. Το ARP πρωτόκολλο σχεδιάστηκε από την ανάγκη για διευκόλυνση της μετάφρασης των διευθύνσεων μεταξύ του επίπεδου σύνδεσης δεδομένων και επιπέδου δικτυού του μοντέλου OSI. Το επίπεδο σύνδεσης δεδομένων χρησιμοποιεί φυσικές διευθύνσεις, έτσι ώστε οι συσκευές υλικού να μπορούν να επικοινωνούν μεταξύ τους απευθείας σε μικρή κλίμακα, ενώ το επίπεδο δικτύου χρησιμοποιεί IP διευθύνσεις (συνήθως) για να δημιουργήσει μεγάλα και ευέλικτα δίκτυα που μπορούν να επικοινωνούν σε όλη την υδρόγειο.

Το πιο σημαντικό μέρος της λειτουργίας του πρωτοκόλλου ARP επικεντρώνεται γύρω από δύο πακέτα, ένα αίτημα και μια απάντηση ARP. Ο σκοπός της αίτησης και της απάντησης είναι να εντοπίσει τη φυσική διεύθυνση του υλικού που συνδέεται με μια συγκεκριμένη IP διεύθυνση, έτσι ώστε η κίνηση των πακέτων να μπορεί να φτάσει στον προορισμό της σε ένα δίκτυο.

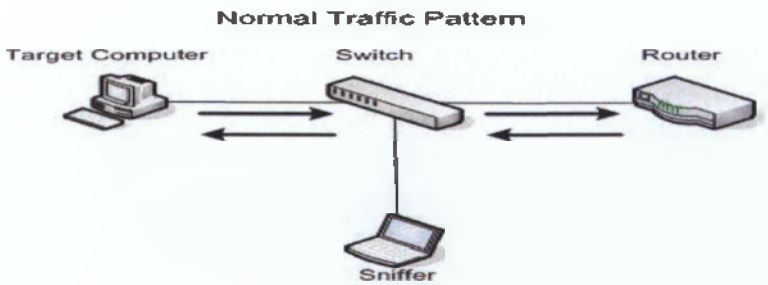


Εικόνα 16 : ARP Αίτηση και Απάντηση[20]

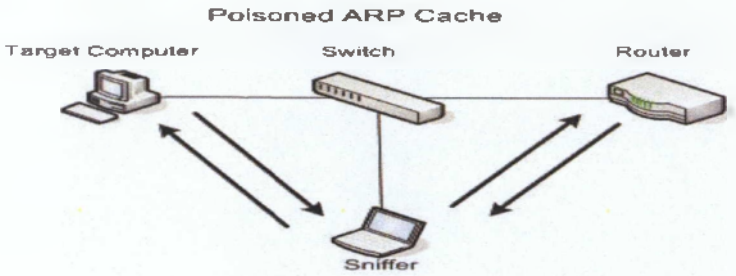
Ένας πίνακας, που ονομάζεται μνήμη cache ARP, χρησιμοποιείται για να διατηρεί την αντιστοίχηση της φυσικής διεύθυνση και της IP διεύθυνσης. Το πρωτόκολλο παρέχει τους κανόνες για την πραγματοποίηση αυτής της αντιστοίχισης καθώς την ανάλυση των διευθύνσεων και στις δύο κατευθύνσεις. Όταν ένα εισερχόμενο πακέτο που αποστέλλεται σε ένα μηχάνημα ενός δικτυού φτάσει σε ένα δρομολογητή, ζητεί από το ARP πρόγραμμα να βρει την φυσική διεύθυνση της αντίστοιχης IP διεύθυνσης. Το πρόγραμμα κοιτάει στον ARP πίνακα και αν βρει την αντίστοιχη φυσική διεύθυνση, την παρέχει έτσι ώστε να το πακέτο να μπορεί να σταλθεί στο μηχάνημα. Εάν δεν βρεθεί κάποια διεύθυνση, τότε το πρωτόκολλο στέλνει μια αίτηση σε όλους τους υπολογιστές του δικτύου έτσι ώστε να βρει την κατάλληλη IP διεύθυνση. Ένας υπολογιστής που αναγνωρίζει τη διεύθυνση IP ως δίκια του στέλνει μια απάντηση στην ARP αίτηση. Τότε το πρωτόκολλο ενημερώνει τον πίνακα για μελλοντική μεταφορά πακέτων και στη συνέχεια στέλνει το πακέτο στην φυσική διεύθυνση.[20]

3.2.1.1 ARP cache poisoning

Η δηλητηρίαση του ARP πίνακα εκμεταλλεύεται την επισφαλή φύση του πρωτοκόλλου. Σε αντίθεση με πρωτόκολλα ,όπως το DNS που μπορεί να ρυθμιστεί ώστε να δέχεται μόνο δυναμικές ενημερώσεις οι οποίες είναι ασφαλείς, οι συσκευές που χρησιμοποιούν ARP δέχονται ενημερώσεις ανά πάσα στιγμή. Αυτό σημαίνει , ότι οποιαδήποτε συσκευή μπορεί να στείλει μία ARP απάντηση με τη μορφή πακέτου σε μια άλλη συσκευή και να την εξαναγκάσει να ενημερώσει τον πίνακα της με τη νέα τιμή. Επίσης, όταν στέλνουμε μια ARP απάντηση χωρίς να έχει προηγηθεί μία αίτηση, τότε λέμε ότι στέλνουμε μια αβάσιμη ARP απάντηση. Έτσι , όταν κάποιος εισβολέας θέλει να κρυφακούσει κάποια δεδομένα στο δίκτυο, τότε στέλνει μερικά αβάσιμα ARP πακέτα κάνοντας την συσκευή A να νομίζει οτι επικοινωνεί με την συσκευή B ενώ στην πραγματικότητα ο εισβολέας τους υποκλέπτει τις πληροφορίες.



Εικόνα 17 : Συνήθης επικοινωνία δύο συσκευών[20]



Εικόνα 18 : Παρεμβολή εισβολέα στην επικοινωνία[20]

3.2.1.2 Μέθοδοι προστασίας ενάντια στο ARP Poisoning

Από άποψη Λειτουργικού Συστήματος η αντιμετώπιση της μορφής αυτής της Man-in-the-Middle επίθεσης είναι πολύ δύσκολη. Ένας τρόπος προστασίας είναι να αλλάξουμε τις ARP αιτήσεις και απαντήσεις, οι οποίες είναι ανασφαλείς, από δυναμικές σε στατικές. Αυτό είναι μια καλή επιλογή διότι οι υπολογιστές που έχουν Λειτουργικά Συστήματα Windows, τους δίνεται η δυνατότητα να προσθέσουν στατικές καταχωρήσεις στο ARP πίνακα χρησιμοποιώντας την εντολή *arp –s <IP> <mac address>*. Αυτό βοηθάει σε περιπτώσεις που το δίκτυο δεν αλλάζει συχνά και είναι προτιμότερο να λειτουργεί με μια λίστα από στατικές ARP καταχωρήσεις. Στη συνέχεια, τις γνωστοποιούν στις συσκευές του δικτύου μέσω ενός αυτοματοποιημένου script παρά να βασίζονται σε ARP απαντήσεις και αιτήσεις. Επιπλέον, ένας άλλος τρόπος για την προστασία ενάντια σε ARP poisoning επιθέσεις είναι η συνεχής παρακολούθηση της κίνησης του δικτύου χρησιμοποιώντας κάποιο πρόγραμμα όπως το Snort το οποίο ανιχνεύει οποιαδήποτε παράβαση στο σύστημα. Συνοψίζοντας, η δηλητηρίαση ARP πίνακα είναι μια μεγάλη εισαγωγή στον κόσμο των Man-in-the-Middle επιθέσεων επειδή είναι πολύ απλή ως προς την εκτέλεσή της. Επίσης, είναι μια πολύ μεγάλη απειλή για τα σύγχρονα δίκτυα, διότι είναι δύσκολο να την ανιχνεύσουμε και να την αντιμετωπίσουν έγκαιρα. Τέλος η επόμενη μέθοδος που θα εξετάσουμε είναι το DNS spoofing [20].

3.2.2 Domain Name System Spoofing

Στο πρώτο μέρος αναλύσαμε την επικοινωνία μέσω του Πρωτόκολλου Μετατροπής Διεύθυνσης καθώς και την εκμετάλλευση αυτού από εισβολείς. Τώρα θα αναλύσουμε μια παρόμοια μέθοδο υλοποίησης Man-in-the-Middle επιθέσεων την DNS Spoofing.

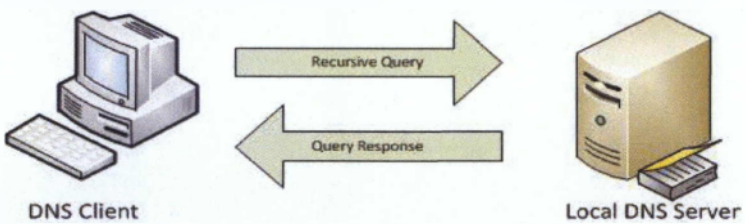
Το DNS spoofing είναι μια MITM τεχνική η οποία χρησιμοποιείτε για την παροχή ψευδών πληροφοριών DNS σε μια συσκευή έτσι ώστε όταν προσπαθήσει να συνδεθεί σε μία ιστοσελίδα οι πληροφορίες σύνδεσης του (συνθηματικό και όνομα χρήστη) αυτομάτως πηγαίνουν στον εισβολέα και όχι στη σελίδα. Για παράδειγμα, κάποιος συνδέεται στην

ιστοσελίδα μιας τράπεζας ,με IP XXX.XX.XX.XX για να τροποποιήσει κάποια στοιχειά του ενώ στην πραγματικότητα ο χρήστης συνδέεται στην YYY.YY.YY.YY που είναι η ψεύτικη σελίδα που έχει δημιουργήσει ο εισβολέας.

3.2.2.1 Κανονική Επικοινωνία DNS

Το πρωτόκολλο Σύστημα Ονομάτων Περιοχών (DNS) είναι ένα από τα σημαντικότερα πρωτόκολλα που χρησιμοποιούνται από το διαδίκτυο. Κάθε φορά που πληκτρολογούμε μια διεύθυνση, όπως www.google.com στον περιηγητή μας, δημιουργείτε μια αίτηση DNS σε ένα εξυπηρετητής ονόματος για να καταλάβει σε ποία IP αναφέρετε η διεύθυνση που πληκτρολογήσαμε. Αυτό συμβαίνει επειδή οι δρομολογητές και οι συσκευές που διασυνδέονται στο διαδίκτυο δεν καταλαβαίνουν τις διευθύνσεις σαν γράμματα παρά μόνο σαν IP.[22]

Ένας εξυπηρετητής ονόματος λειτουργεί αποθηκεύοντας μια βάση δεδομένων των εγγραφών των αντιστοιχίσεων από διευθύνσεις σε ονόματα και το αντίστροφο, κοινοποιώντας τα στοιχεία των πόρων προς τους πελάτες, και σε αντίστοιχους εξυπηρετητές ονόματος .



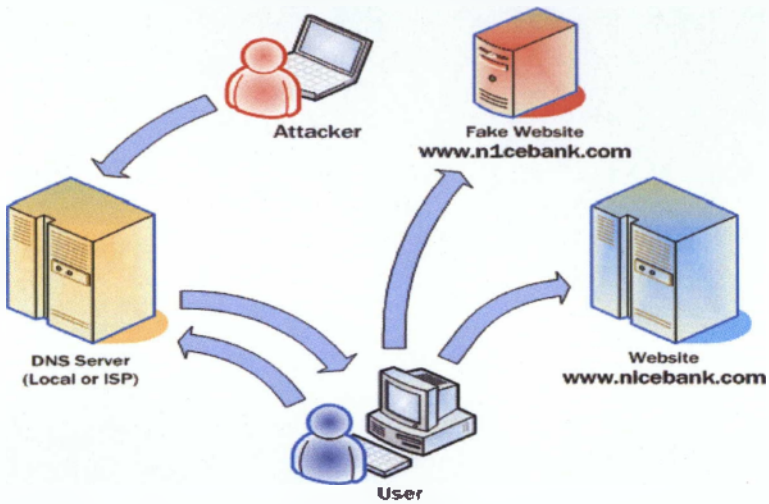
Εικόνα 19 : Domain Name System Συναλλαγή[22]

Το DNS λειτουργεί σε μια μορφή τύπου ερώτηση/απάντηση. Ένας πελάτης που επιθυμεί να αλλάξει ένα όνομα DNS σε μια διεύθυνση IP στέλνει ένα ερώτημα σε ένα εξυπηρετητή ονόματος.

3.2.2.2 Τρόπος εξαπάτησης DNS

Το DNS spoofing λειτουργεί αναγκάζοντας ένα πελάτη να δημιουργήσει ένα DNS αίτημα σε έναν εξυπηρετητή ονόματος, και στη συνέχεια να πλαστογραφήσει την απάντηση από τον εξυπηρετητή αυτό. Ένας τρόπος για να δουλέψει αυτό είναι με τον τρόπο που οι περισσότεροι εξυπηρετητές ονόματος υποστηρίζουν τα αναδρομικά ερωτήματα. Μπορούμε να στείλουμε ένα αίτημα σε κάθε εξυπηρετητή ζητώντας να μεταφράσει ένα όνομα στην ανάλογη διεύθυνση. Στη συνέχεια, θα στείλει τα κατάλληλα ερωτήματα προκειμένου να ανακαλύψει τις κατάλληλες πληροφορίες. Ωστόσο, ένας εισβολέας μπορεί να προβλέψει τι αίτηση θα στείλει ο εξυπηρετητής ονόματος και μπορεί να πλαστογραφήσει την απάντηση, η

οποία θα φτάσει πριν από την πραγματική. Δηλαδή όταν ένας χρήστης θα θελήσει να περιηγηθεί σε μια ιστοσελίδα ο εισβολέας θα έχει πλαστογραφήσει την διεύθυνση και ο χρήστης αντί να συνδεθεί στην σελίδα που επιθυμεί, θα συνδεθεί εκεί που τον κατευθύνει ο εισβολέας.



Εικόνα 20 : DNS Spoofing[22]

3.2.2.3 Πρόληψη και προστασία DNS spoofing

Για να αποφευχθούν πολλές πηγές επιθέσεων στο Internet, είναι απαραίτητο να υπάρχει ενσωματωμένη ασφάλεια στα DNS συστήματα. Για να ελαχιστοποιηθεί ο κίνδυνος μιας επίθεσης spoofing, κάθε οργάνωση ή άτομο που είναι υπεύθυνο για έναν τομέα πρέπει πρώτα να ελέγξει ποιος τύπος του εξυπηρετητή ονόματος χρησιμοποιείται και να διαβουλεύεται με τους προγραμματιστές της, κατά πόσον είναι ασφαλή ενάντια στη πλαστογράφησης DNS.

Η πλαστογράφηση αυτή έχει γίνει πολύ δύσκολη να εντοπιστεί λόγω της δημιουργίας νέων μεθόδων και νέων επιθέσεων. Συνήθως, δεν γνωρίζουμε πότε το DNS είναι πλαστογραφημένο μέχρι να συμβεί.

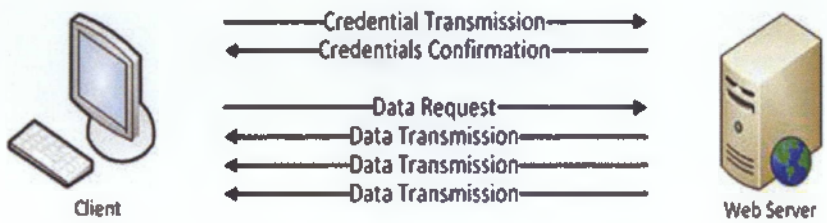
Από πλευράς λογισμικού μια αποτελεσματική λύση ενάντια στο DNS spoofing είναι η ασφάλιση των διακομιστών με την χρήση ενός τείχους προστασίας που θα παρέχει anti-spoofing. Επειδή η πλειοψηφία των επιθέσεων γίνεται από το ίδιο δίκτυο, όταν έχουμε ασφαλίσει τις συσκευές μας η πιθανότητα μειώνεται. Επίσης, μια καινούρια λύση η οποία σχεδιάστηκε έτσι ώστε να αντιμετωπίσει την εκμετάλλευση του DNS είναι το Domain Name System Security Extensions το οποίο είναι μια πιο ασφαλή έκδοση του προκατόχου του. Επιπλέον, όταν δεν χρησιμοποιούμε το διαδίκτυο καλό είναι να μην χρησιμοποιείτε το

πρωτόκολλο αυτό διότι δεν είναι ασφαλές. Αντιθέτως, εάν χρησιμοποιούμε ένα λογισμικό το οποίο βασίζεται στα ονόματα των host για να λειτουργήσει τότε αυτά μπορούν να οριστούν στο αρχείο των host της συσκευής. Και τέλος η χρησιμοποίηση IDS (Intrusion Detection System) αποτρέπει τις περισσότερες επιθέσει που υλοποιούνται με APR Poisoning και DNS spoofing

3.2.3 Session Hijacking

Η εισβολή σε περίοδο λειτουργίας ή αλλιώς Session Hijacking ονομάζεται οποιαδήποτε ManInTheMiddle επίθεση υλοποιείται ανάμεσα σε μια περίοδο λειτουργίας δύο συσκευών. Όταν αναφερόμαστε σε μια περίοδο λειτουργίας, μιλάμε για μια σύνδεση μεταξύ των συσκευών. Δηλαδή, υπάρχει ένας καθιερωμένο διάλογος με τον οποίο η σύνδεση έχει τυπικά συσταθεί, η σύνδεση διατηρείται, και μια καθορισμένη διαδικασία πρέπει να χρησιμοποιηθεί για να τερματίσει τη σύνδεση.

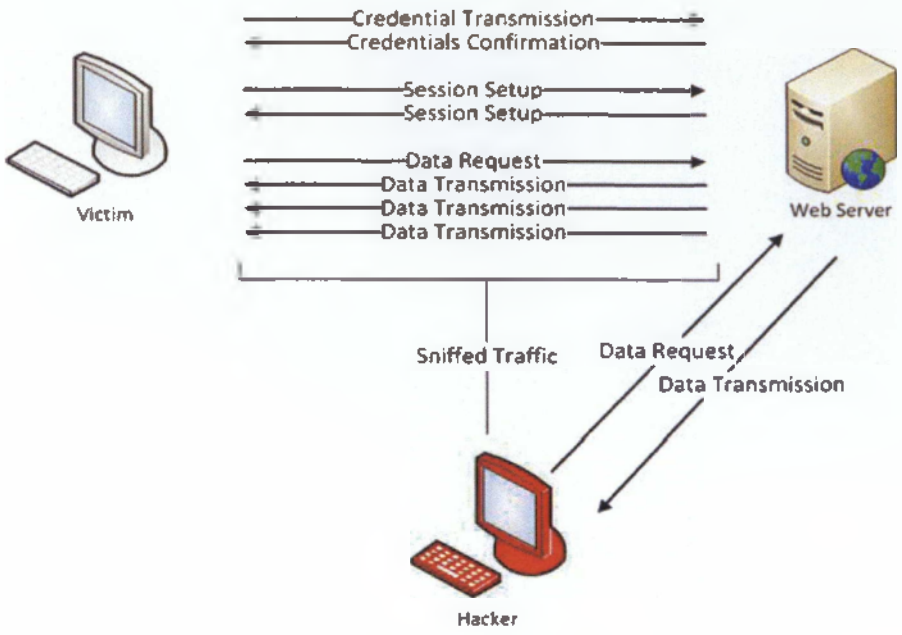
Εμείς θα αναφερθούμε σε εισβολή περιόδου λειτουργίας μέσω υποκλοπής των cookies. Μια τέτοια περίοδος λειτουργίας είναι όταν συνδεόμαστε σε μια ιστοσελίδα και μας ζητάει συνθηματικό και όνομα χρήστη. Τότε δημιουργείτε μία αμφίδρομη περίοδος λειτουργίας που μας επιτρέπει να είμαστε συνδεδεμένοι στην ιστοσελίδα και να μπορούμε να χρησιμοποιήσουμε τους πόρους της.



Εικόνα 21 : Μία κανονική περίοδος λειτουργίας[22]

3.2.3.1 Session Hijacking

Όπως είδαμε και στις προηγούμενες επιθέσεις, οτιδήποτε κινείται μέσα στο δίκτυο δεν είναι ασφαλές. Η αρχή λειτουργίας σε αυτού του τύπου τις επιθέσεις είναι ότι αν μπορέσει κάποιος να παρέμβει σε ένα μέρος της περιόδου λειτουργίας τότε μπορεί να χρησιμοποιήσει τα δεδομένα που έχει για να παραστήσει τον έναν από τους δύο που βρίσκονται στη περίοδο αύτη και να υποκλέψει στοιχεία που θα είναι ικανά στο να του δώσουν πρόσβαση.



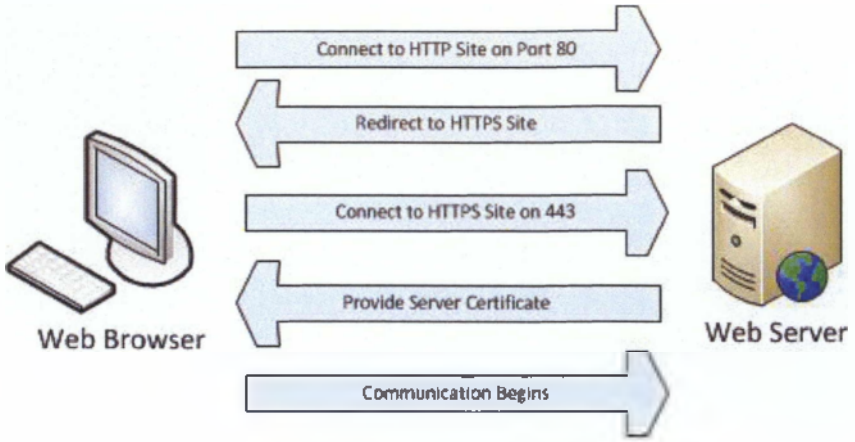
Εικόνα 22 : Session Hijacking[22]

3.2.4 SSL Hijacking

Η τελευταία μέθοδος υλοποίησης μιας ManInTheMiddle επίθεσης είναι η παραβίαση SSL. Η παραβίαση SSL είναι εκ φύσεως μια από τις πιο ισχυρές επιθέσεις MITM , επειδή επιτρέπει την εκμετάλλευση των υπηρεσιών που οι χρήστες υποθέτουν ότι είναι ασφαλής.

Τα πρωτόκολλα SSL και TLS έχουν σχεδιαστεί για να παρέχουν προστασία για επικοινωνία μέσω δικτύου χρησιμοποιώντας κρυπτογράφηση. Αυτά τα πρωτόκολλα συνήθως συνδυάζονται με άλλα πρωτόκολλα για την παροχή προστασίας όπως το HTTPS στο οποίο θα αναφερθούμε και εμείς καθώς το SSL εκεί χρησιμοποιείται περισσότερο.

Η διαδικασία που χρησιμοποιεί το HTTPS για να διασφαλίσει ότι τα δεδομένα είναι ασφαλή επικεντρώνεται γύρω από την κατανομή των πιστοποιητικών μεταξύ του διακομιστή και του πελάτη, καθώς και ένα έμπιστο τρίτο μέρος.



Εικόνα 23 : Επικοινωνία HTTPS[22]

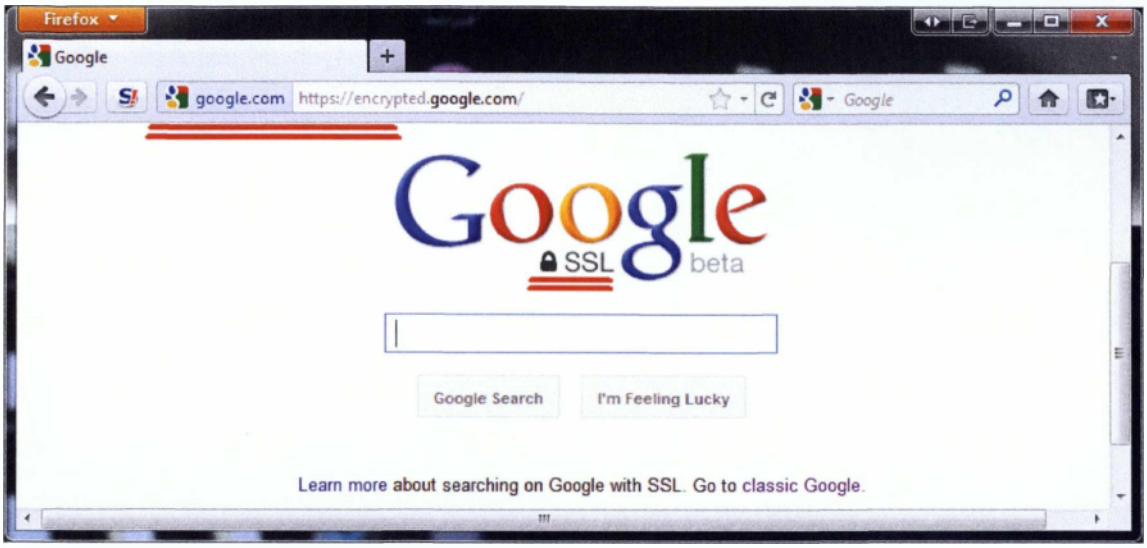
Η επικοινωνία αυτή πριν μερικά χρόνια θεωρούνταν ασφαλής μέχρι που εισάχθηκε το SSL hijacking, με το οποίο ουσιαστικά δεν παρακάμπτει το SSL αλλά τη γέφυρα μεταξύ των κρυπτογραφημένων και μη επικοινωνιών. Το SSL ποτέ δεν αντιμετωπίστηκε άμεσα. Τις περισσότερες φορές που μια ασφαλής σύνδεση εκκινείτε μέσω HTTPS, είναι επειδή κάποιος είχε ανακατευθυνθεί σε HTTPS μέσω ενός κωδικού απάντησης HTTP 302 ή κάνοντας κλικ σε μια σύνδεση που τους κατευθύνει σε μια ιστοσελίδα HTTPS, όπως ένα κουμπί login. Η ιδέα είναι ότι αν επιτεθεί κάποιος κατά τη μετάβαση από μη ασφαλή σύνδεση σε μια ασφαλή, στην προκειμένη περίπτωση από HTTP σε HTTPS επιτίθενται στη γέφυρα επικοινωνίας και μπορούν να κάνουν ManInTheMiddle επίθεση πριν η ασφαλής σύνδεση πραγματοποιηθεί.

Εικόνα 24 : SSL Hijacking[22]

Όπως έχουμε ήδη αναφερθεί, η συγκεκριμένη παράβαση στην πραγματικότητα δεν μπορεί να ανιχνευθεί από την πλευρά των εξυπηρετητών γιατί θεωρείται ως μια κανονική επικοινωνία με τον πελάτη. Δεν μπορεί να αντιληφθεί ότι η επικοινωνία του με τον πελάτη γίνεται μέσω ενός διακομιστή μεσολάβησης. Μπορούμε όμως να προστατευτούμε από αυτού του είδους τις επιθέσεις καθώς ο πελάτης από την πλευρά του μπορεί να τις ανιχνεύσει και να τις αποτρέψει.

Ένας τρόπος αντιμετώπισης μιας τέτοιας επίθεσης είναι η εξασφάλιση ασφαλούς σύνδεσης χρησιμοποιώντας HTTPS. Παραδείγματος χάρη, κατά τη διάρκεια μιας ασφαλούς

σύνδεσης σε μια ιστοσελίδα, ανάλογα τον περιηγητή μας εμφανίζεται μια ένδειξη γνωστοποίησης όπως στη παρακάτω εικόνα



Εικόνα 25 : Σύνδεση https στον περιηγητή μας

Κατά τη διάρκεια μιας επίθεσης SSL Hijacking ενώ έχουμε συνδεθεί με ασφαλή σύνδεση και ο περιηγητής μας την αναγνωρίζει δεν εμφανίζονται τα διακριτικά αυτής διότι συνδεόμαστε με απλή σύνδεση.

Επίσης, η ασφάλιση των υπολογιστών στο δίκτυο μας αποτρέπει τέτοιου είδους επιθέσεις. Οι SSL Hijacking επιθέσεις πραγματοποιούνται συχνότερα μέσα από το δικό μας δίκτυο.[22][23]

3.3 Denial of Service (Άρνηση Παροχής Υπηρεσιών)

3.3.1 Τι είναι Άρνηση Παροχής Υπηρεσιών

Όπως υποδηλώνει το όνομα, Denial of Services (DoS) είναι μια επίθεση σε ένα σύστημα υπολογιστή ή σε ένα δίκτυο που προκαλεί απώλεια της παροχής υπηρεσιών προς τους χρήστες, συνήθως την απώλεια της σύνδεσης με το δίκτυο και τις υπηρεσίες του μέσα από την κατανάλωση του εύρους ζώνης του δικτύου του θύματος, ή την υπερφόρτωση των υπολογιστικών πόρων του συστήματος.

3.3.2 Ιστορία Επιθέσεων Άρνησης Παροχής Υπηρεσιών

Στα μέσα της δεκαετίας του 90 αρχίζουν να κάνουν την εμφάνιση τους οι πρώτες επιθέσεις DoS. Για να τρέχεις τα κατάλληλα προγράμματα χρειαζόσουν έναν καλό

υπολογιστή και κάποιο γρήγορο δίκτυο οπότε οι περισσότεροι χρησιμοποιούσαν το δίκτυο των πανεπιστήμιων.

Αργότερα το 1996 ανακαλύφθηκε μια "τρυπά" στο TCP/IP πρωτόκολλο που επέτρεπε τον μεγάλο αριθμό SYN πακέτων (SYN flood). Το 1997 μεγάλες DoS επιθέσεις ξεκινάμε να γίνονται σε IRC δίκτυα. Σε μια επίθεση ατέλειες σε Windows συστήματα ο επιτιθέμενος μπορούσε απάθειας να θέσει εκτός λειτουργίας τα συστήματα IRC χρηστών με προγράμματα όπως το teardrop, boink, bonk. Τα προβλήματα αυτά διορθώθηκαν με διαφορά τροποποιήσεις στα πρωτόκολλα παρόλα αυτά άλλες τεχνικές επίθεσης ανακαλύφθηκαν όπως η Smurf attack.

Και ενώ μέχρι εκείνη την στιγμή ο αποστολέας εκμεταλλευόταν κάποιο πρόβλημα, αργότερα απλά έστελναν πολλά πακέτα σε κάποιον χρηστή. Αν ο χρηστής χρησιμοποιούσε κάποια dial-up σύνδεση και ο αποστολέας μπορούσε να χρησιμοποιήσει το δίκτυο κάποιο πανεπιστήμιου μπορούσαν να στείλουν πακέτα προκαλώντας DoS. Το 1998 ενώ οι συνδέσεις άρχιζαν να μεγαλώνουν οι συνδέσεις και οι υπολογιστές να γίνονται πιο γρήγοροι έτσι οι επιθέσεις άρχισαν να γίνονται πιο συχνές. Αργότερα εμφανίστηκε ένα άλλο είδος DoS επιθέσεων, οι DDos επιθέσεις οπού εκεί χρησιμοποιούνταν μεγάλα δίκτυα υπολογιστών για να σταλούν τα πακέτα. [24]

3.3.3 Κίνητρα και τρόποι υλοποίησης Denial Of Service

Το κίνητρο για των επιθέσεων DoS δεν είναι η ρήξη ενός συστήματος. Αντ' αυτού, είναι να αρνηθούμε τη νόμιμη χρήση του συστήματος ή του δικτύου σε άλλους που χρειάζονται τις υπηρεσίες του. Οι Denial of Service επιθέσεις έρχονται σε μια ποικιλία μορφών και αποσκοπούν σε διάφορες υπηρεσίες. Υπάρχουν τρεις βασικοί τύποι επιθέσεων:

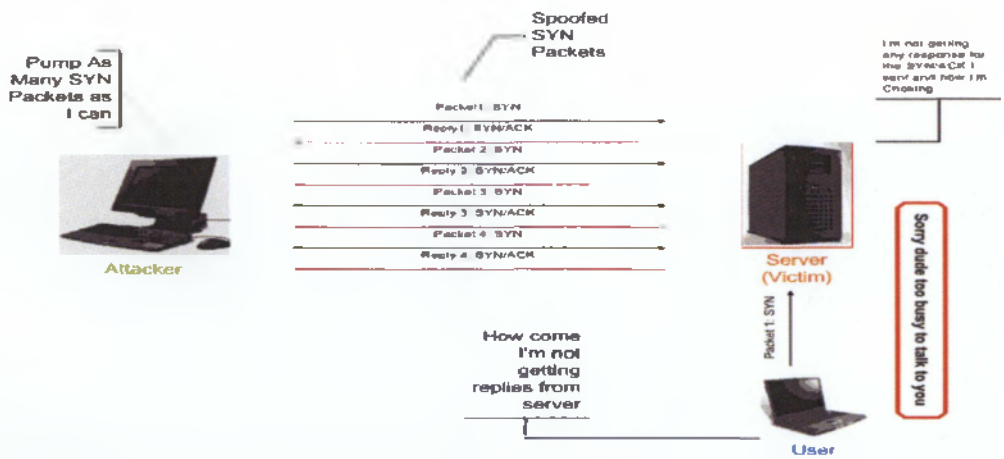
- χρήσης των πενιχρών, περιορισμένων ή μη ανανεώσιμων πόρων
- καταστροφή ή αλλοίωση των πληροφοριών ρύθμισης παραμέτρων
- φυσική καταστροφή ή αλλοίωση των στοιχείων του δικτύου [25]

3.3.4 Είδη επιθέσεων Denial of Service

3.3.4.1 TCP SYN attack

Μια Transmission Control Protocol (TCP) SYN flood επίθεση είναι ένα είδος άρνησης υπηρεσιών που υπάγετε στην κατηγορία εκμετάλλευσης υπολογιστικών πόρων. Σε μία TCP SYN υπερχείλιση ένας υπολογιστής υπερφορτώνεται με αιτήσεις για TCP συνδέσεις οι οποίες έρχονται πιο γρήγορα απ' ότι μπορεί να τις απαντήσει. Το"SYN"

αναφέρεται σε μια TCP header synchronization flag (Whitman & Mattord, 2004). Κάθε πακέτο SYN περιέχει μια τυχαία ή μια πλαστογραφημένη IP διεύθυνση. Έπειτα, απαιτεί μία νέα σύνδεση με το μηχάνημα-στόχο από την ψεύτικη διεύθυνση. Τότε ο υπολογιστής απαντάει στην ψευδή IP διεύθυνση και περιμένει λίγα λεπτά για την απάντηση. Ο πίνακας των συνδέσεων του υπολογιστή που έχει γίνει στόχος είναι συνεχώς απασχολημένος με αιτήσεις που δεν έχουν αναγνωριστεί και οι συνδέσεις που προσπαθούν να κάνουν υπολογιστές που τους γνωρίζουμε απορρίπτονται. Ουσιαστικά έχουμε άρνηση της υπηρεσίας.[24] Το είδος αυτό DoS ουσιαστικά παρεμβαίνει ανάμεσα σε μία τυπική SYN ACK χειραψία μεταξύ δύο υπολογιστών όπως φαίνεται στη παρακάτω εικόνα



Εικόνα 26 : SYN ACK Flood[26]

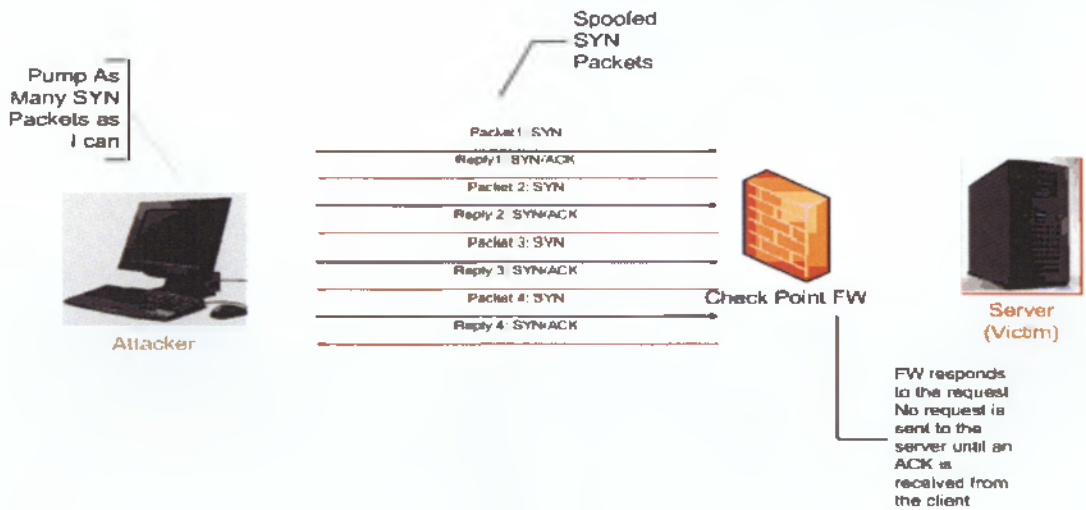
3.3.4.2 Τρόποι προστασίας από υπερχείλιση SYN ACK

Τα Microsoft Windows έχουν ένα μηχανισμό ο οποίος προστατεύει τον υπολογιστή μας όταν ανιχνευθεί μια υπερχείλιση SYN. Το χαρακτηριστικό αυτό ανιχνεύει τα συμπτώματα μιας τέτοιας υπερχείλισης και απαντάει μειώνοντας το χρόνο που ο Server ξοδεύει σε μια αίτηση σύνδεσης η οποία δεν μπορεί να αναγνωριστεί. Ουσιαστικά μειώνει το απαιτούμενο διάστημα μεταξύ της SYN ACK αναμετάδοσης. Το TCP αναμεταδίδει τα πακέτα SYN-ACK όταν αυτά δεν απαντώνται με αποτέλεσμα οι αιτήσεις που δεν αναγνωρίζονται να απορρίπτονται γρήγορα.[26]

Επίσης, άλλες τεχνικές προστασίας περιλαμβάνουν SYN cookies και RST cookies. Το SYN cookie είναι μία κρυπτογραφική τιμή που περιλαμβάνετε σε μια SYN απάντηση από τον αποστολέα. Εάν ο αποστολέας είναι πραγματικός και δεν είναι κάποιος εισβολέας η αναγνώριση (ACK) από τον αποστολέα θα περιέχει την τιμή αυτή. Αλλιώς η σύνδεση δεν

δημιουργείτε. Επίσης κάθε φορά που μια λανθασμένη αναγνώριση έρχεται σαν απάντηση , ένα RST cookie πρέπει να επιστραφεί. Αν δεν επιστραφεί τότε η σύνδεση απορρίπτεται.[25]

Και τέλος, μία άλλη μέθοδος είναι να τοποθετήσουμε ένα Τείχος Προστασίας πριν τον server, που θα λειτουργεί σαν σημείο ελέγχου. Αυτό θα λαμβάνει και θα απαντάει σε όλες τις αιτήσεις για συνδέσεις. Οι μόνες συνδέσεις που θα περνάνε στον server θα είναι αυτές που θα έχουν σωστή αναγνώριση. Όπως μας δείχνει η εικόνα



Εικόνα 27 : Check Point firewall acting as a proxy[26]

3.3.4.3 Smurf Attack

Το είδος αυτό των επιθέσεων Άρνησης Υπηρεσιών είναι ένα από τα πιο καταστροφικά. Ο εισβολέας στέλνει μια ICMP echo αίτηση (ping), δηλαδή μια χρησιμότητα για να ελέγξουμε αν μια συσκευή είναι προσβάσιμη σε ένα IP δίκτυο, [27] σε μία broadcast IP διεύθυνση. Η πηγαία διεύθυνσης του ping είναι η IP διεύθυνση του θύματος (χρησιμοποιεί την IP διεύθυνση του θύματος σαν την διεύθυνση επιστροφής). Αφότου το Ping έχει ληφθεί όλοι οι υπολογιστές στο broadcast domain στέλνουν απαντήσεις στην IP διεύθυνση του θύματος με αποτέλεσμα ο επιτιθέμενος να συγκρουστεί ή να παγώσει όταν λάβει όλες αυτές τις απαντήσεις .

Οι επιθέσεις smurf είναι ένα παράδειγμα επιθέσεων που αποσκοπούν στην κατανάλωση των πόρων του δικτύου και με αυτό το τρόπο να του απαγορέψει να χρησιμοποιήσει του πόρους του δικτύου του. Αυτό το πετυχαίνει χρησιμοποιώντας ενίσχυση από το εύρος του δικτύου του εισβολέα. Αν για παράδειγμα το δίκτυο αυτό έχει 100 υπολογιστές το σήμα ενισχύεται 100 φορές με αυτό να σημαίνει ότι ένας εισβολέας με εύρος δικτύου 56K μπορεί να υπερχειλίσει μια σύνδεση δικτύου T1. [28]

Αυτό έχει σαν αποτέλεσμα ένα μεγάλο αριθμό από απαντήσεις από το συγκεκριμένο δίκτυο το οποίο εάν είναι αρκετά μεγάλο έχει τη δυνατότητα να καταστρέψει το δίκτυο του θύματος. Άξιο αναφοράς είναι ότι ο χρήστης-θύμα δε μπορεί να κάνει τίποτα για αυτή την επίθεση καθώς η σύνδεση απλά υπερφορτώνεται με πακέτα.

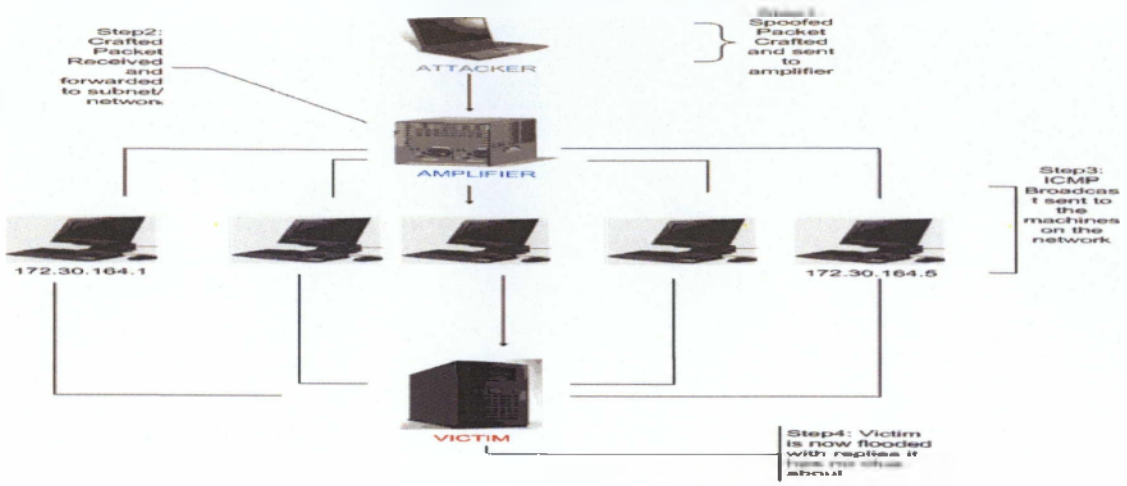
Σε αυτό το είδος Άρνησης Παροχής Υπηρεσιών υπάρχουν πάντα τρία μέρη

- Ο Επιτιθέμενος
- Ένας ενισχυτής – συνήθως ο δρομολογητής λειτουργεί έτσι
- Και το θύμα-χρήστης

Η επίθεση πετυχαίνει διότι ο ενισχυτής έχει παραμετροποιηθεί επίτηδες λανθασμένα έτσι ώστε να προωθεί τις κατευθυνόμενες μεταδόσεις πακέτων.

Ένα παράδειγμα αυτής της επίθεσης είναι το εξής : Έστω σε μια εταιρία έχει ανατεθεί το συγκεκριμένο εύρος IP διευθύνσεων από 172.30.164.0 έως 172.30.164.255 η οποία εταιρία έχει έναν ενισχυτή και ο εισβολέας στέλνει πακέτα με προορισμό την IP 172.30.164.255 η οποία είναι και η διεύθυνση εκπομπής του υποδικτύου. Όλοι οι δρομολογητές και τα συστήματα από τον εισβολέα μέχρι τον ενισχυτή δε θα καταλάβουν τη διαφορά από αυτή την IP και μία IP από το εύρος αυτού του υποδικτύου. Όταν το πακέτο φτάσει στον ενισχυτή και αυτή συνειδητοποιήσει ότι είναι η διεύθυνση εκπομπής (broadcast IP) προωθεί την αίτηση σε ολόκληρο το υποδίκτυο. Αυτό είναι γνωστό και ως κατευθυνόμενη εκπομπή. Τα δύο κύρια χαρακτηριστικά αυτής της επίθεσης είναι ένα λανθασμένα παραμετροποιημένος δρομολογητής που προώθησε την αίτηση για εκπομπή στο δίκτυο και οι υπολογιστές που απάντησαν σε αυτή την αίτηση ping.

Τα θύματα διαλέγονται κυρίως μέσω του Internet Relay Chat ή αλλιώς γνωστό και ως mIRC , όπου κάποια αυτοματοποιημένα προγράμματα (bots) κοιτάνε τις διευθύνσεις των θυμάτων. Οι εισβολείς συνήθως ανταλλάσουν πληροφορίες για όλους τους ενισχυτές μεταξύ τους , οπότε όταν μία μαζική επίθεση πραγματοποιείται φαίνεται ότι προέρχεται απ' όλη την υδρόγειο. Στην εικόνα βλέπουμε μια επισκόπηση της επίθεσης Smurf.



Εικόνα 28 : smurf attack [26]

3.3.4.4 Τρόποι Προστασίας από smurf attack

Ο δρομολογητής πρέπει να παραμετροποιηθεί έτσι ώστε να μην προωθεί κατευθυνόμενες εκπομπές μέσα στο δίκτυο. Κάτι τέτοιο για παράδειγμα γίνεται στους δρομολογητές της Cisco με την απλή εντολή no ip directed-broadcast

Οι εξυπηρετητές πρέπει να παραμετροποιήσουν τα Λειτουργικά τους Συστήματα ώστε να μην δέχονται τέτοιου είδους αιτήματα [26]

3.3.5 LAND Attack

Αυτό το είδος Denial-Of-Service επίθεσης βασίζεται στο να στέλνει το πλαστογραφημένο TCP SYN πακέτο με την διεύθυνση του θύματος. Πρωτοεμφανιζόμενη το 1997 , η επίθεση LAND εκμεταλλεύεται ένα σφάλμα στην TCP/IP στοίβα των Windows και με αυτό τον τρόπο το σύστημα θα απαντάει στον εαυτό του συνεχόμενα μέχρι που θα κλειδώσει και θα προκαλέσει άρνηση των υπηρεσιών. [29].

3.3.5.1 Teardrop Attack

Αυτή η επίθεση εκμεταλλεύεται την αδυναμία του πρωτοκόλλου TCP/IP στην επανασύνδεση (reassembly) των πακέτων δεδομένων (data packets) κατά την λήψη τους. Όταν στέλνονται δεδομένα στο διαδίκτυο αυτά κατανέμονται σε μικρότερα κομμάτια στην υπολογιστή που κάνει την μετάδοση και συναρμολογούνται πάλι στον υπολογιστή που λαμβάνει. Ας υποθέσουμε ότι θέλουμε να στείλουμε 8000 bytes από έναν υπολογιστή σε έναν άλλον. Δεν θα τα στείλουμε όλα μαζί με μία μετάδοση (transmission) αλλά θα κοπούν σε μικρότερα πακέτα δεδομένων (data packets) και κάθε πακέτο θα έχει συγκεκριμένο κομμάτι από τα 8000 bytes όπως : πακέτο 1ο θα έχει byte 1 έως byte 1500, πακέτο 2ο θα έχει byte 1501 έως byte 3000, πακέτο 3ο θα έχει byte 3001 έως byte 4000, και ούτω καθ έξης.

Αυτά τα πακέτα έχουν στο αρχικό τους κομμάτι (TCP header) ένα πεδίο (offset) που περιγράφει πως θα γίνει η συναρμολόγηση στο σύστημα που θα λάβει τα πακέτα. Στην επίθεση αυτή τα πακέτα που στέλνονται υπερκαλύπτουν το ένα το άλλο με αποτέλεσμα όταν το σύστημα που τα λαμβάνει προσπαθεί να τα συναρμολογήσει (reassembly) παθαίνει κατάρρευση (crash) ή/και "πάγωμα" (hang) ή/και επανεκκίνηση (reboot).

3.4 Επίθεση Υπερχείλισης Μνήμης (Buffer Overflow)

Τι είναι αυτό που προκαλεί την υπερχείλιση μνήμης; Γενικά μιλώντας η υπερχείλιση μνήμης συμβαίνει κάθε φορά που ένα πρόγραμμα γράφει περισσότερες πληροφορίες στο buffer από το κενό που του έχει κατανεμηθεί στην μνήμη. Αυτό επιτρέπει σε ένα εισβολέα να ξανά γράψει δεδομένα τα οποία ελέγχουν τη διαδρομή εκτέλεσης του προγράμματος και καταλαμβάνουν τον έλεγχο ενός προγράμματος έτσι ώστε να εκτελεστεί ο κώδικας ενός εισβολέα αντί του κώδικα της διεργασίας. [30]

3.4.1 Τι είναι το buffer;

Το Buffer είναι ένα συνεχόμενο κομμάτι της μνήμης του υπολογιστή που κρατά πωλλαπλά στιγμιότυπα του ίδιου τύπου δεδομένων. Στην πράξη στις περισσότερες γλώσσες προγραμματισμού αυτό εκφράζεται με την δομή του πίνακα(array). Αυτοί οι πίνακες στην C/C++ αλλά και σε άλλες γλώσσες δεσμεύονται στην μνήμη είτε στο σωρό (Heap) είτε στην Στοίβα (stack). Τα Buffer τα χωρίζουμε σε διάφορες κατηγόριες αναλόγως με το που βρίσκονται αλλά και με την συμπεριφορές τους. Τα Buffer που βρίσκονται στο σωρό τα λέμε heap Buffer ενώ αυτά που βρίσκονται στην στοίβα Stack Buffers. Όταν ένα Buffer βρίσκεται στο σωρό τότε η μνήμη για αυτά δεσμεύεται κατά την διαδικασία του φορτώματος στην μνήμη(Load time) ενώ όταν βρίσκεται στην στοίβα δεσμεύεται δυναμικό κατά την διάρκεια που το πρόγραμμα «τρέχει» (Run time).

Ένας άλλος διαχωρισμός είναι ότι τα Buffer μπορεί να έχουν στατικό μέγεθος που το προκαθορίζει ο προγραμματιστής ή δυναμικό μέγεθος που καθορίζεται από κατάλληλες συναρτήσεις όπως η malloc και η realloc στην γλώσσα C.

Εδώ θα εξετάσουμε τις περιπτώσεις υπερχείλισης των Buffer που βρίσκονται στην στοίβα όπου το μέγεθος τους είναι προκαθορισμένο από τον προγραμματιστή.

3.4.2 Stack Overflow

Στην στοίβα το πρόβλημα της υπερχείλισης(Overflow) παρουσιάζεται όταν βάλουμε μέσα σε ένα Buffer που έχει προκαθοριστεί στατικά από τον προγραμματιστή, ένα String που έχει αριθμό χαρακτήρων μεγαλύτερο από αυτόν που μπορεί να χωρέσει μέσα στο Buffer.

Αυτό πολλές φορές μπορεί να μην γίνει αντιληπτό και το πρόγραμμα να συνεχίζει να δουλεύει χωρίς κανένα πρόβλημα. Όμως τις περισσότερες φορές το πρόβλημα εμφανίζεται με δυσάρεστα αποτελέσματα και μάλιστα σε σημείο του κώδικα που δεν είναι αναμενόμενο καθιστώντας την αποσφαλμάτωση (Debugging) εξαιρετικά δύσκολη. Το πρόβλημα λύνεται πολύ εύκολα αρκεί κάθε φορά να κάνουμε έλεγχο ορίων (Boundary Checking) ώστε να μην παρουσιάζονται τέτοια φαινόμενα. Την στιγμή που δεν έχουμε έλεγχο ορίων στη C είναι εξαιρετικά πιθανό να έχουμε το φαινόμενο του Stack Buffer Overflow.

3.4.2.1 Παράδειγμα Buffer Overflow

Όταν ένας εισβολέας επιλέγει να χρησιμοποιήσει την μέθοδο buffer overflow έχει ένα σημαντικό στόχο να μπορέσει να αναγκάσει το πρόγραμμα να εκτελέσει το κομμάτι του κώδικα που αυτός επιλέγει παραβιάζοντας την φυσιολογική ροή προγράμματος.

Ένα Buffer Overflow προκαλείται όταν βάλουμε περισσότερα δεδομένα από όσα ένα Buffer έχει προκαθοριστεί να χειρίζεται(να χωράει). Η περίπτωση του Buffer Overflow που μας ενδιαφέρει είναι η τρίτη από τις περιπτώσεις που περιγράφονται παραπάνω δηλαδή αυτή που προκαλεί κάποιο System Error. Στο παρακάτω παράδειγμα παρουσιάζεται μία τέτοια περίπτωση

```
/* C/C++ code */
void function(char *str) {
char buffer[16];
/* Αντιγραφή του μεγάλου String στο μικρό Buffer*/
strcpy(buffer,str);
}
main () {
char large_string[256];
int i;
for(i=0;i<255;i++)
large_string[i]='A';
function(large_string);
```

Αυτό το πρόγραμμα έχει μία συνάρτηση με ένα τυπικό Buffer Overflow σφάλμα κατά την συγγραφή του κώδικα. Η function αντιγράφει χωρίς έλεγχο ορίων (Boundary Checking) το string που της παραδίδεται από την main, με την strcpy(), σε ένα buffer που προηγουμένως έχει οριστεί να έχει μεγέθους 16 χαρακτήρων δηλαδή 16 byte. Είναι προφανές ότι όταν εκτελεστεί αυτό το πρόγραμμα επειδή ούτε η strcpy() δεν κάνει έλεγχο ορίων πριν αντιγράψει τα περιεχόμενα του large_string στο buffer θα προκληθεί segmentation violation και κατασυνέπεια υπερχείληση. [31]

3.4.2.2 Προστασία από υπερχείλησεις Στοίβας

Η πιο αποτελεσματική λύση στις επιθέσεις υπερχείλισης μνήμης είναι να χρησιμοποιήσουμε πιο ασφαλή κώδικες. Στην αγορά κυκλοφορούν πολλές δωρεάν λύσεις οι οποίες σταματούν τα buffer overflow. Κάποιες μέθοδοι είναι οι εξής :

- Άμυνες βασισμένες στις βιβλιοθήκες οι οποίες ξανά εφαρμόζουν τις μη ασφαλείς συναρτήσεις και διαβεβαιώνουν ότι αυτές οι συναρτήσεις δεν θα ξεπεράσουν ποτέ το μέγεθος του buffer. Ένα παράδειγμα τέτοιας λύσης είναι το Libsafe project

- Άμυνες βασισμένες στις βιβλιοθήκες που εντοπίζουν και αποτρέπουν την εφαρμογή οποιουδήποτε μη νόμιμου κώδικα στη στοίβα. Μία τέτοια αξιόπιστη λύση είναι η SecureStack της SecureWave.

- Μια άλλη τεχνική πρόληψης είναι η χρήση compiler με βάση το χρόνο εκτέλεσης ορίων, ελέγχοντας το τι είναι πρόσφατα διαθέσιμο. Κανένα μέτρο ασφαλείας δεν είναι τέλειο, η καλύτερη λύση είναι πάντα η αποφυγή των σφαλμάτων προγραμματισμού.[32]

3.4.3 Heap Overflow

Το Heap Based Buffer Overflow δεν έχει σημαντικές διαφορές στην φιλοσοφία του με το Stack Based Buffer Overflow. Είναι πολύ πιο εξειδικευμένη επίθεση και επίσης είναι αρκετά ποιο δύσκολο να βρεθεί μια τέτοιου είδους αδυναμία. Λόγο της δυσκολίας αυτής πολύ λίγοι ασχολούνται με αυτές τις περιπτώσεις. Οι λόγοι λοιπόν που τα Heap Buffer Overflow Exploits είναι λιγότερο διαδεδομένα είναι οι εξής :

- Η υπερχείλιση μνήμης στο σωρό είναι πολύ δυσκολότερο να επιτευχθεί σε σχέση με την υπερχείλιση μνήμης στη στοίβα.

- Βασίζονται σε ειδικές λειτουργία περιπτώσεις τις ίδιας της εφαρμογής και όχι σε μια μόνο γενική λειτουργία όπως το αυτή της διαδικασία κλήσης μίας συνάρτησης.
- Πρέπει να είναι γνωστές ακριβώς οι συνθήκες που θα επικρατούν την μνήμη την στιγμή που θα γίνει η υπερχείλιση μνήμης.

Η επικινδυνότητα αυτών των επιθέσεων δεν οφείλεται μόνο στο γεγονός ότι ελάχιστοι ασχολούνται με αυτές (συνεπώς πολλή λιγότεροι ασχολούνται με το πώς θα τις αποτρέψουν) αλλά πολύ περισσότερο γιατί οι τεχνικές υπερχείλισης μνήμης εκμεταλλευόμενοι τον σωρό χρησιμοποιούνται για να παρακάμψουν πολλές από τις μεθόδους προστασίας του συστήματος από τα Stack Based Buffer Overflow Exploits.

Η γενική ιδέα του Stack Based BOE είναι να αλλάξει την ροή του προγράμματος ώστε να μπορέσει το σύστημα να εκτελέσει αυθαίρετο κώδικα(arbitrary code). Η λογική της υπερχείλισης της μνήμης εκμεταλλευόμενοι το σωρό είναι ίδια αλλά με κάποιες διαφορές που το κάνουν αρκετά πιο δύσκολο να υλοποιηθεί. Η βασική δυσκολία όμως είναι ότι στο σωρό που στην πράξη είναι η συνέχεια του χώρου των δεδομένων είναι ότι δεν αποθηκεύονται συχνά πληροφορίες που αφορούν την ροή του προγράμματος. Επίσης όταν υπάρχουν πληροφορίες που αφορούν την φυσική ροή του προγράμματος αυτές δεν συνορεύουν πάντα με Buffers που πάσχουν από την αδυναμία υπερχείλισης. Αυτό αποτελεί μία επιπλέον δυσκολία στις υπάρχουσες που έχουν να αντιμετωπισθούν από ένα Stack Based BOE. Συνεπώς και στα Heap Bases BOE συνεχίζει να υπάρχει η δυσκολία του εντοπισμού την κατάλληλης διεύθυνσης όπου θα βρεθεί ο ShellCode ώστε η ροή του προγράμματος να οδηγηθεί προς αυτόν και να εκτελεστεί. [33]

3.4.4 Σύνοψη

Τα περισσότερα Λειτουργικά Συστήματα περιέχουν μία ή περισσότερες υπερχειλίσεις μνήμης. Συχνά, οι επιτιθέμενοι ανακαλύπτουν συμπτωματικά αυτά τα ψεγάδια ή χρησιμοποιούν προγράμματα ανίχνευσης αυτών και σαν αποτέλεσμα είναι οι επιτιθέμενοι να μπορούν να έχουν πρόσβαση σε υπηρεσίες του Λειτουργικού Συστήματος. Είναι μια πανίσχυρη επίθεση καθώς όταν χρησιμοποιηθεί σε συνδυασμό με μία επίθεση Άρνησης Εξυπηρέτησης μπορεί ένα εισβολέας να έχει πρόσβαση σε χιλιάδες υπολογιστές και να του χρησιμοποιήσει για τους σκοπούς του. Όμως οι μέθοδοι προστασίας που προτείναμε είναι αποτελεσματικοί και αποτρέπουν σχεδόν πάντα τέτοιου είδους επιθέσεις.

3.5 DLL Hijacking

Το είδος της επίθεσης αυτής πρώτο ανακαλύφθηκε τον Αύγουστο του 2010 από ερευνητές συστημάτων ασφαλείας όταν άρχισαν να δημοσιεύουν λεπτομέρειες από μια τάξη ευπαθειών που είχαν επιρροές μεγάλης κλίμακας. Η συγκεκριμένη ευπάθεια όμως απέκτησε γρήγορα μεγάλη φήμης καθώς βρέθηκαν εκατοντάδες εφαρμογές που αντιμετώπιζαν κενά ασφαλείας μέσω DLL και σαν αποτέλεσμα εισβολείς να μπορούν να εισάγουν στο σύστημα μας κακόβουλο κώδικα που εκμεταλλεύεται την ακεραιότητα της συγκεκριμένης εφαρμογής καθώς και τα δικαιώματα που έχει αυτή. Το είδος της συγκεκριμένης επίθεσης ονομάστηκε DLL Hijacking.

Το συγκεκριμένο είδος επίθεσης, μπορεί να υλοποιηθεί διότι όλες οι εφαρμογές των Windows βασίζονται στις Βιβλιοθήκες Δυναμικού Συνδέσμου (DLL) διότι αποτελούν μέρος της βασικής τους λειτουργίας. Οι DLL περιέχουν ξεχωριστά κομμάτια κώδικα τα οποία οι προγραμματιστές μπορούν να τα καλέσουν μέσα στις εφαρμογές που αναπτύσσουν να εκτελέσουν διάφορες λειτουργίες. Τα Windows από μόνα τους βασίζονται στον ίδιο τύπο αρχιτεκτονικής και περιέχουν μια πληθώρα από τις συγκεκριμένες Βιβλιοθήκες που εκτελούν διάφορες λειτουργίες.

Μαζί με τα DLL που κατασκευάστηκαν στα Windows , οι προγραμματιστές εφαρμογών συχνά δημιουργούν δικά τους DLL που περιέχουν τις συναρτήσεις που χρησιμοποιούνται από το πρόγραμμα. Όταν γίνεται αυτό οι Δυναμικές Βιβλιοθήκες που δημιουργήθηκαν από τον προγραμματιστή εγκαθίστανται μέσα στο πρόγραμμα. Το πρόβλημα έγκειται στο πώς οι εφαρμογές φορτώνουν τα DLL δηλαδή όταν μια εφαρμογή δεν έχει μία στατικά ορισμένη διαδρομή σε μία Βιβλιοθήκη που χρειάζεται τότε η εφαρμογή αυτή μπαίνει σε μια διαδικασία να βρει τη διαδρομή αυτή δυναμικά. Για να το κάνει αυτό η εφαρμογή πρώτα ψάχνει τον κατάλογο από τον οποίο εκτελέστηκε, έπειτα ψάχνει στη τον κατάλογο συστήματος, τον κατάλογο συστήματος 16-bit, τον κατάλογο των Windows και τον τρέχων κατάλογο και μετά όλους του καταλόγους που παρατίθενται στη διαδρομή του λειτουργικού συστήματος. Καθώς η εφαρμογή ψάχνει σε αυτούς τους καταλόγους το DLL που θα χρησιμοποιήσει η εφαρμογή θα είναι το πρώτο που θα βρει.

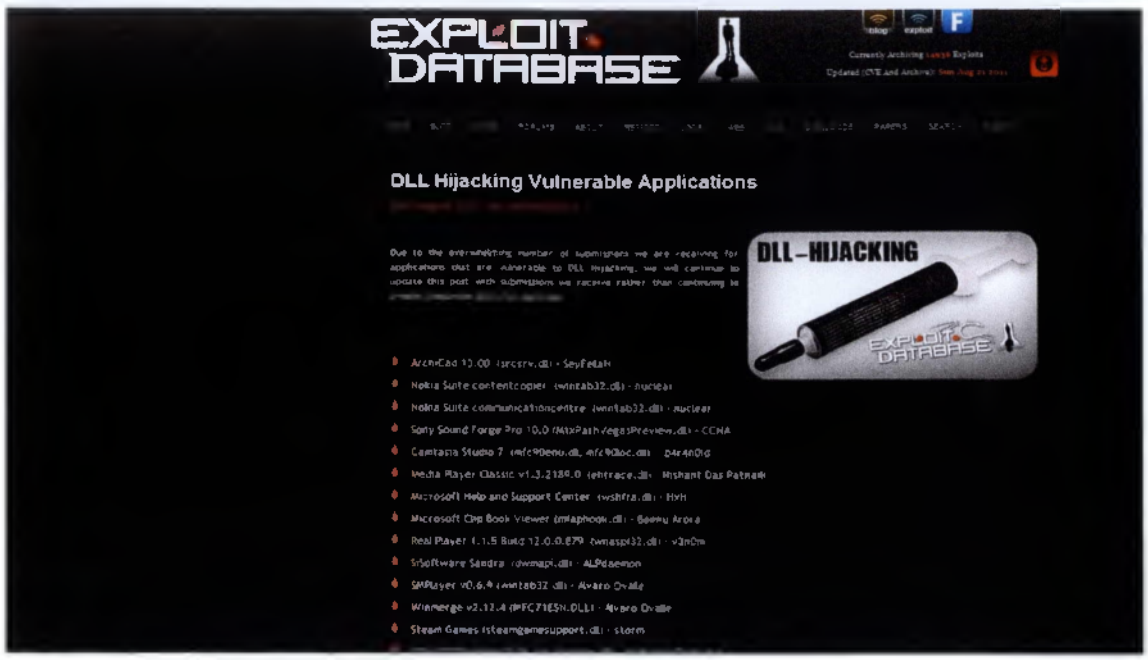
Πώς όμως η δυναμική μέθοδος εύρεσης του απαιτούμενου DLL δημιουργεί κενό ασφαλείας στο σύστημα μας; Ας υποθέσουμε ότι εκτελούμε μια εφαρμογή η οποία εκτελούμε ψάχνει για ένα απαιτούμενο DLL καθώς εκκινεί. Η πρώτη διαδρομή που θα ψάξει είναι αυτή που εκτελέστηκε και έστω βρίσκει τη βιβλιοθήκη που έψαχνε εκεί. Δυστυχώς για

τον χρήστη οι βιβλιοθήκες αυτές που συσχετίζονται με την εφαρμογή βρίσκονται στο κατάλογο του συστήματος των Windows και το DLL που ταιριάζει που βρήκε η εφαρμογή έχει τοποθετηθεί εκεί από τον εισβολέα και έχει μετατραπεί έτσι ώστε να δημιουργήσει άνοιγμα στην ασφάλεια του συστήματος μας.

3.5.1 Αναγνωρίζοντας τις ευπαθείς εφαρμογές

Η Microsoft μετά την ανακάλυψη αυτής της ευπάθειας, που οδηγεί σε κενό ασφαλείας το σύστημα μας, δεν μπόρεσε να βγάλει ένα διορθωτικό πρόγραμμα το οποίο θα διόρθωνε όλα τα σφάλματα και τα κενά εκατοντάδων εφαρμογών καθώς αυτό θα δημιουργούσε πρόβλημα στην εκτέλεση των εφαρμογών. Αντιθέτως, οι εταιρίες και οι προγραμματιστές που δημιουργούν τις εφαρμογές ανέλαβαν να αναγνωρίσουν όλες τις ευπαθείς εφαρμογές και να διορθώσουν τον κώδικα του και να παρέχουν δωρεάν τις αναβαθμισμένες εκδόσεις στους χρήστες. Επιπροσθέτως, οι χρήστες και κυρίως οι διαχειριστές δικτύων και συστημάτων πρέπει να καθορίσουν αν στο δίκτυό τους εκτελούνται εφαρμογές οι οποίες έχουν ευπάθεια ως προς τα DLL και να εγκαταστήσουν τα κατάλληλα διορθωτικά προγράμματα τα οποία θα εξαλείψουν αυτό το σφάλμα.

Μια πολύ απλή μέθοδος για να βρούμε ποιές εφαρμογές είναι προβληματικές είναι να διαβάσουμε άρθρα και ενημερώσεις από ερευνητές ασφάλειας οι οποίοι έχουν δημοσιεύσει την πλειονότητα των εφαρμογών αυτών. Μια πολύ καλή πηγή αυτών είναι η ιστοσελίδα http://www.exploit-db.com στην οποία αναφέρετε μια μεγάλη γκάμα από εφαρμογές που κρίθηκαν προβληματικές και μας παρέχει τις ανάλογες αναβαθμίσεις οι οποίες εξαλείφουν το πρόβλημα αυτό.



Εικόνα 29 : DLL Hijacking Vulnerable Applications [38]

3.5.2 Αποτρέποντας την επίθεση

Μέχρι την δημοσίευση της πλήρης λίστας με τις ευπαθείς εφαρμογές και την αντικατάσταση των προβληματικών βιβλιοθηκών υπάρχουν μερικά βήματα που πρέπει να ακολουθηθούν έτσι ώστε να διασφαλίσουμε κάποια ασφάλεια.

- Χρησιμοποίηση του διορθωτικού προγράμματος CWDIllegalllnDll search . Αυτή ήταν και η αρχική αντίδραση της Microsoft σε αυτό το θέμα ασφαλείας. Δηλαδή παρείχε στους χρήστες μια παραμετροποίηση της registry ως προς τον τρόπο λειτουργίας των δυναμικών Βιβλιοθηκών.

- Τον αποκλεισμό της εξερχόμενης Server Message Block στο firewall.

- Απεγκατάσταση προβληματικών εφαρμογών. Αν έχουμε μια ανασφαλή εφαρμογή η οποία μπορεί να αντικατασταθεί με μια παρόμοια τότε καλό είναι να απεγκατασταθεί.

- Χρησιμοποίηση κάποιου Intrusion Detection Software (IDS) το οποίο θα βοηθήσει στην εύρεση του εισβολέα πριν την επίθεση

3.5.3 Σύνοψη

Το DLL Hijacking είναι πολύ δύσκολα αντιμετωπίσιμο από πλευράς λειτουργικού συστήματος καθώς οι εφαρμογές που εμπλέκονται σε αυτή την ευπάθεια είναι εκατοντάδες και επηρεάζουν ένα πολύ μεγάλο εύρος άλλων μη ευπαθών εφαρμογών. Το μόνο που

μπορούμε να κάνουμε είναι να μένουμε ενημερωμένοι για όλες τις καινούριες εφαρμογές που προστίθενται στην ήδη μεγάλη λίστα των εφαρμογών αυτών καθώς και στην αντικατάσταση τους με ενημερωμένες εκδόσεις αλλά και να συμβάλουμε στον εντοπισμό αυτών.[34]

3.6 Logon Credential Password Guessing/Cracking

Η πειρατεία των κωδικών, που χρησιμοποιούν οι χρήστες για να εισέλθουν στο σύστημα τους, είναι ανάμεσα στις πιο δημοφιλή μεθόδους που χρησιμοποιούν οι εισβολείς. Πολλές πηγές ονομάζουν αυτή τη τεχνική σπάσιμο των κωδικών κάτι που δεν είναι απόλυτα σωστό καθώς οι χρήστες εκτός από κωδικούς χρησιμοποιούν και άλλες μεθόδους ταυτοποίησης όπως οι έξυπνες κάρτες. Έτσι έχουμε δύο ειδών πειρατείας το μάντεμα και το σπάσιμο.

3.6.1 Password Guessing

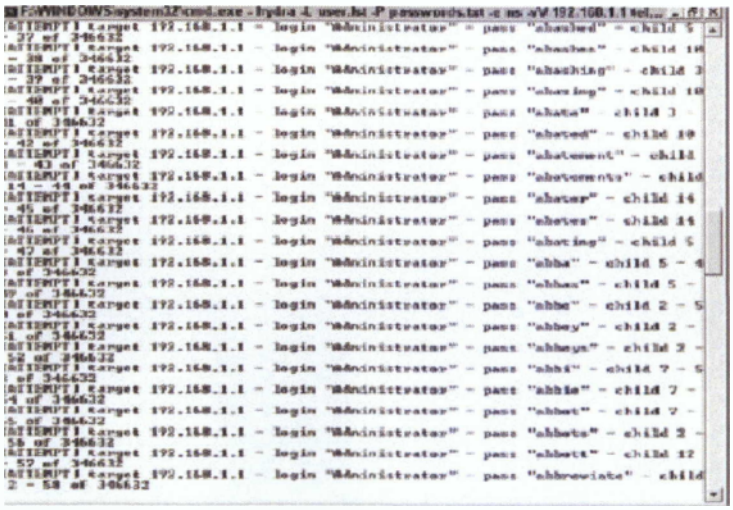
Με τον ορισμό αυτό εννοούμε τον τρόπο με τον οποίο ο εισβολέας μαντεύει τον κωδικό, είτε μόνος του είτε μέσω κάποιου αυτόματου προγράμματος με αποτέλεσμα να μπορεί να εισέλθει στο σύστημά μας. Στα Windows άν οι κατάλληλες υπηρεσίες είναι ενεργοποιημένες, η επίθεση αυτή μπορεί να γίνει ενάντια σε πολλές εφαρμογές εξυπηρετητών όπως η απομακρυσμένη επιφάνεια εργασίας, Τερματικές Υπηρεσίες, Telnet αλλά και στο κανονικό Windows logon και γενικά οπουδήποτε ο εισβολέας μπορεί να δει μια προτροπή (prompt) για να εισαχθούν τα στοιχεία του χρήστη (credentials) .

Το να μαντέψει ένας εισβολέας είναι κάτι πολύ κοινότυπο αλλά ταυτόχρονα πολύ αργό. Πρέπει να εκτελεστεί ενάντια σε μία προτροπή για εισαγωγή στοιχείων εισόδου και να περιμένει μέχρι η υπηρεσία σύνδεσης να απαντήσει θετικά ή αρνητικά μέχρι να ξεκινήσει ο εισβολέας μια νέα προσπάθεια.

3.6.1.1 Automated Password Guessers

Επειδή, η παραπάνω διαδικασία μπορεί να διαρκέσει πάρα πολύ χρόνο οι εισβολείς συνήθως χρησιμοποιούν αυτόματα προγράμματα για την εκπόνηση της ενέργειας αυτής. Ένα τέτοιο πρόγραμμα μπορεί να εισάγει τον ένα κωδικό μετά τον άλλο μέχρι το μάντεμα να εξαντληθεί και ο λογαριασμός να ξεκλειδώσει. Επιπλέον, ένα όφελος της τεχνικής αυτής είναι ότι ο εισβολέας μπορεί να αρχίσει ταυτόχρονα πολλές προσπάθειες εισόδου. Μερικά εργαλεία αφήνουν τον εισβολέα να ξεκινήσει όσες ταυτόχρονες επιθέσεις θέλει κάτι που περιορίζεται μόνο από το εύρος του δικτύου και επίσης αυξάνει την πιθανότητα στο να γίνει αντιληπτός.

Ένα τέτοιο αυτόματο πρόγραμμα που μαντεύει κωδικούς είναι το HYDRA από το The Hacker's Choice. Είναι ένα πρόγραμμα που λειτουργεί σε γραμμή εντολών και επιτρέπει στον εισβολέα να μαντέψει πολλαπλά ονόματα χρήστη με κωδικούς πολλαπλούς κωδικούς ενάντια σε πολλούς εξυπηρετητές και υπολογιστές με τη μία. Υποστηρίζει πολλές υπηρεσίες που χρησιμοποιούνται για την ταυτοποίηση χρηστών περιλαμβανομένων των υπηρεσιών των Windows που αναφέρθηκαν προηγουμένως αλλά και της Cisco, mySQL, oracle και πολλών άλλων. Στην παρακάτω εικόνα βλέπουμε το πρόγραμμα Hydra να εκτελείτε ενάντια στην υπηρεσία telnet των Windows .



Εικόνα 30 : Hydra against telnet[35]

Η διαδικασία αυτή μπορεί να γίνει πιο εύκολα εάν είναι γνωστός κάποιος περιορισμός στο κωδικό ή κάποια συγκεκριμένη πολιτική όπως για παράδειγμα μέγιστο μήκος κωδικού έξι γράμματα κ.ο.κ .

3.6.1.2 Είδη Password Guessing

Εάν μια επίθεση password guessing ξεκινάει χρησιμοποιώντας όλα τα πιθανά σύμβολα τα οποία μπορεί να βρίσκονται σε ένα κωδικό (όπως αα , αβα ,αββ , ββα ,ββ κλπ) αντί για ολόκληρες λέξεις θεωρείτε ως brute force επίθεση. Η επίθεση αυτού του είδους από υπολογιστική σκοπιά είναι οι πιο δύσκολες επιθέσεις κατακερματισμού κωδικών που υπάρχουν.

Οι περισσότεροι χρήστες χρησιμοποιούν ένα κωδικό με μία κοινή ρίζα με άλλους κωδικούς η συσχετιζόμενη με το αντικείμενο (παράδειγμα password, guess, frog κλπ). Επιθέσεις που μαντεύουν ολόκληρη τη λέξη ονομάζονται επιθέσεις λεξικού ή dictionary attacks.

Αλλά συνήθως πολιτικές διαφόρων οργανισμών δεν αφήνουν τον χρήστη να βάλει μια λέξη ατόφια για κωδικό αλλά τον προτρέπει να χρησιμοποιήσει και άλλα σύμβολα ανάμεσα στη λέξη. Υπάρχουν όμως επιθέσεις παρόμοιες με τις επιθέσεις λεξικού οι οποίες ειδικεύονται στο να σπάνε τέτοιου είδους κωδικούς και ονομάζονται υβριδικές επιθέσεις (hybrid attacks) .

Γενικά επιθέσεις brute force χρησιμοποιούνται μόνο όταν ο εισβολέας δεν έχει καμία ιδέα για τον κωδικό που πρόκειται να κατακερματίσει ούτε πόσο πολύπλοκος είναι. Επιπροσθέτως, οι επιθέσεις λεξικού είναι οι πιο κοινότυπες όταν υπάρχει χρόνος και τέλος οι υβριδικές επιθέσεις είναι αναγκαίες μόνο όταν υπάρχουν παραπάνω σύμβολα στις λέξεις.

3.6.1.3 Προβλήματα με το μάντεμα των κωδικών

Υπάρχουν τρία βασικά προβλήματα με το μάντεμα των κωδικών. Αυτά είναι ο χρόνος που απαιτείται για να αποκτηθεί ο κωδικός, το κλείδωμα του λογαριασμού και ότι μπορεί να παρατηρηθούν οι λανθασμένες προσπάθειες του εισβολέα από τον χρήστη (event logging).

Εάν ο χάκερ δεν ξέρει την πολιτική χρησιμοποίησης του κωδικού μπορεί να του πάρει χρόνια ακόμα και με μία αυτοματοποιημένη επίθεση. Επιπλέον, η προστασία ενάντια σε αυτές τις επιθέσεις (account lockout) κάνει τα πράγματα πολύ πιο δύσκολα διότι μετά από πολλές λανθασμένες προσπάθειες για είσοδο θα προτρέψουν τον λογαριασμό να κλειδώσει. Επιπλέον, ακόμα και αν δεν είναι ενεργοποιημένος ο μηχανισμός ασφαλείας πολλά λειτουργικά συστήματα περιλαμβανομένων και των Windows καθυστερούν μελλοντικές προσπάθειες για είσοδο.

3.6.2 Κατακερματισμός Κωδικών

Όταν ένας εισβολέας αντιμετωπίσει προβλήματα με το μάντεμα ενός κωδικού θα επιλέξει να κατακερματίσει τον κωδικό παρά να τον μαντέψει. Ο κατακερματισμός των κωδικών αποτελεί μια μέθοδο η οποία θα αποσπάσει τον κωδικό σε οποιαδήποτε μορφή (παραδείγματος χάρη κωδικοποιημένο) και μέσω του υπολογιστικού του συστήματος θα προσπαθήσει να τον επαναφέρει στην αρχική του μορφή.

Στα Windows οι κωδικοί εισόδου είναι αποθηκευμένοι σαν hash κωδικών στη βάση δεδομένων της ταυτοποίησης. Για να επιτευχθεί αυτό στα Windows ο χάκερ πρέπει να έχει δικαιώματα διαχειριστή για να έχει πρόσβαση στον υπολογιστή. Όταν έχει τα δικαιώματα ο εισβολέας μπορεί να αποσπάσει τα hashes από τοπικά ή ασύρματα. Επίσης ο εισβολέας μπορεί να πάρει τους κωδικούς χρησιμοποιώντας sniffing με κάποιο πρόγραμμα σαν τον

Abel και Cain. Η μεγαλύτερη διαφορά του κατακερματισμού των κωδικών από το μάντεμα είναι η ταχύτητα και ειδικά αν το Bitlocker Drive Encryption δεν είναι ενεργοποιημένο τότε η απόσπαση αυτών γίνεται πολύ εύκολα.

Όμως ανάλογα την πολυπλοκότητα των κωδικών μπορεί να πάρει εκατομμύρια προσπάθειες για να μαντέψει τον κωδικό. Γι αυτό έχουν εφευρεθεί νέες τεχνικές απόσπασης κωδικών δημιουργήθηκαν. Μία από αυτές τις μεθόδους ονομάζεται pre-computed hash tables. Με αυτή τη μέθοδο κάθε πιθανός κωδικός σε απλό κείμενο δημιουργείται εκ των προτέρων , hashed, και τοποθετείται σε ένα πίνακα που αναζητάει τον κωδικό σε μια βάση δεδομένων. Μετά ο χάκερ τοποθετεί το κατειλημμένο hash στο πρόγραμμα αναζήτησης κωδικών και αναζητεί όλα τα παρόμοια hashes και του εμφανίζει τον κωδικό.[35]

3.6.2.1 Μέθοδοι προστασίας

Οι μέθοδοι προστασίας για τον κατακερματισμό και μάντεμα των κωδικών είναι περισσότερο κάποια βήματα που πρέπει να ακολουθεί ο χρήστης. Αρχικά το Bitlocker Drive Encryption πρέπει να είναι ενεργοποιημένο καθώς ασφαλίζει όλα τα δεδομένα στο δίσκο μας. Επιπλέον το τείχος προστασίας μας πρέπει να είναι πάντα ενεργό και να έχει παραμετροποιηθεί έτσι ώστε να επικοινωνούν συγκεκριμένες πόρτες όπως η 80 για το διαδίκτυο η 21 για τον FTP και συγκεκριμένες θύρες για παιχνίδια. Και τέλος όσο πιο μεγάλο μήκος έχει ένας κωδικός και όση μεγαλύτερη η πολυπλοκότητα του τόσο πιο δύσκολο και χρονοβόρο είναι για τον εισβολέα να τον αποσπάσει. [36]

ΚΕΦΑΛΑΙΟ 4 : ΥΛΟΠΟΙΗΣΗ ΕΠΙΘΕΣΗΣ

4 Υλοποίηση Επίθεσης

4.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο αναλύσαμε πέντε μεθόδους με τις οποίες οι εισβολείς καταφέρνουν να εισχωρήσουν στο σύστημα μας και να υποκλέψουν τα δεδομένα μας ή να κάνουν ζημίες με δικό τους συμφέρον. Σε αυτό το κεφάλαιο θα υλοποιήσουμε μια από τις παραπάνω μεθόδους με σκοπό να δείξουμε πώς οι εισβολείς διαβάζουν τα δεδομένα ή υποκλέπτουν σημαντικές πληροφορίες του συστήματος μας. Η επίθεση που αποφασίσαμε να υλοποιήσουμε είναι η Man-In-The-Middle attack με τη μέθοδο Arp Cache Poisoning. Επιλέξαμε τη συγκεκριμένη μέθοδο διότι μας περιόριζε ο εξοπλισμός και η τεχνογνωσία που διαθέταμε , αλλά είναι μια σημαντική και εύκολα υλοποιήσιμη επίθεση που μπορεί να την κάνει οποιοσδήποτε συνδέεται σε ένα δίκτυο. Για την υλοποίηση της χρειαστήκαμε

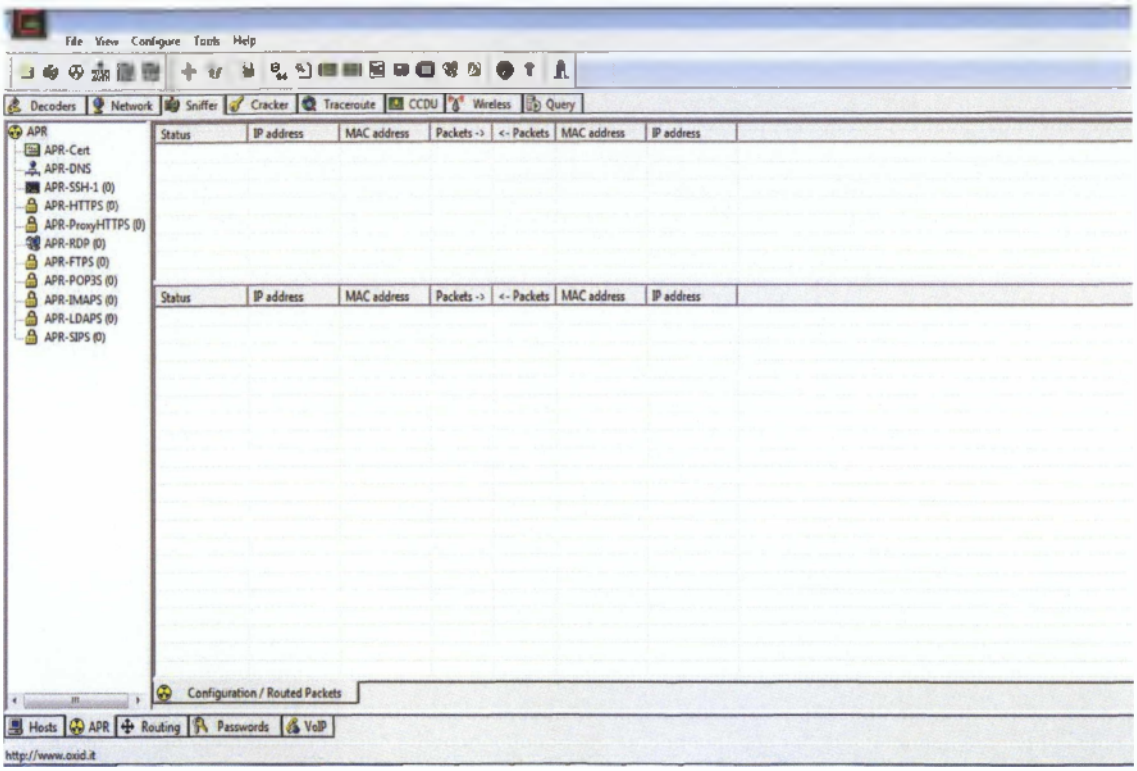
- Τρείς φορητούς υπολογιστές
- Ένα switch
- Τρία καλώδια τύπου RJ-45
- Το πρόγραμμα Cain & Abel

4.2 Από τη θεωρία στη πράξη

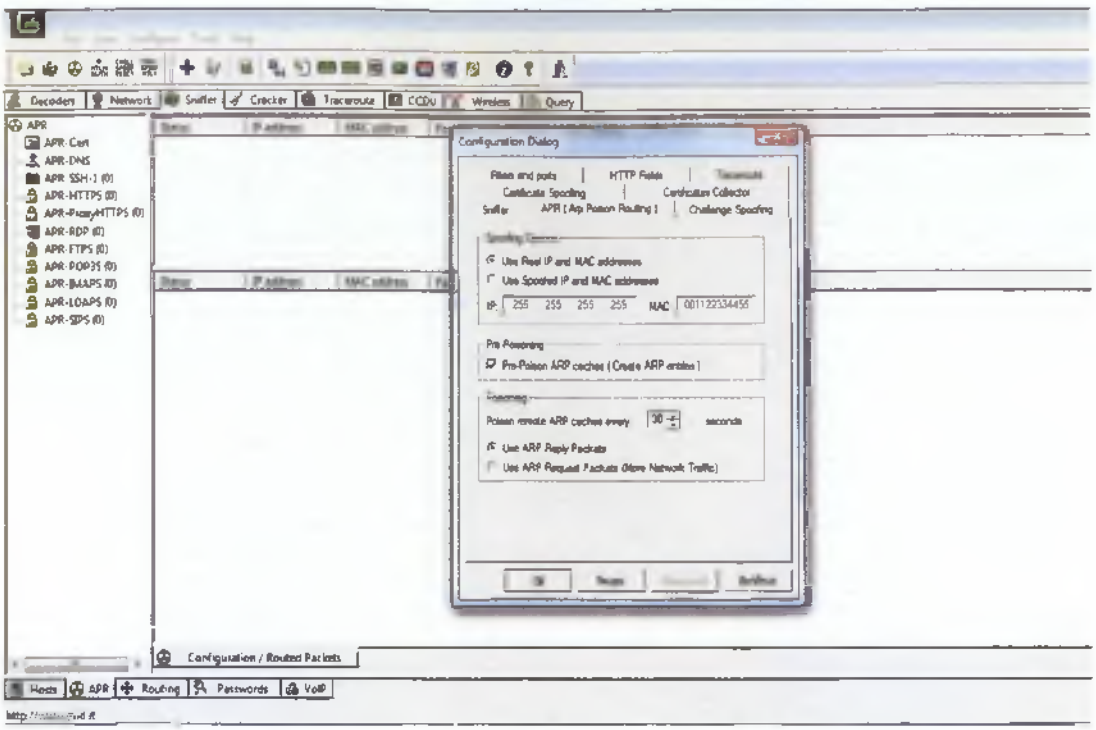
Υπάρχουν πολλά εργαλεία τα οποία μας βοηθάνε στο να πάρουμε τα κατάλληλα βήματα έτσι ώστε να πετύχουμε μια δηλητηρίαση του πίνακα ARP μεταξύ των υπολογιστών των θυμάτων εμείς επιλέξαμε το εργαλείο Cain and Abel το οποίο το πήραμε από το www.oxid.it . Αρχικά δημιουργήσαμε ένα τοπικό δίκτυο μεταξύ δύο υπολογιστών που συνδεόντουσαν μέσω του switch και έκαναν ανταλλαγές κάποιων αρχείων. Πριν ξεκινήσουμε οποιαδήποτε ενέργεια φροντίσαμε να γνωρίζουμε τις δύο IP διευθύνσεις των δύο θυμάτων καθώς και τη δικτυακή συσκευή που χρησιμοποιήθηκε και ακολουθώντας τα παρακάτω βήματα υλοποιήσαμε την επίθεση.

Πρώτα κατεβάσαμε το Cain and Abel πρόγραμμα και το εγκαταστήσαμε στον υπολογιστή που θα λειτουργήσει ως sniffer. Έπειτα συνδέσαμε τον υπολογιστή αυτό στο ίδιο δίκτυο με τους άλλους δύο και ξεκινήσαμε το πρόγραμμα.

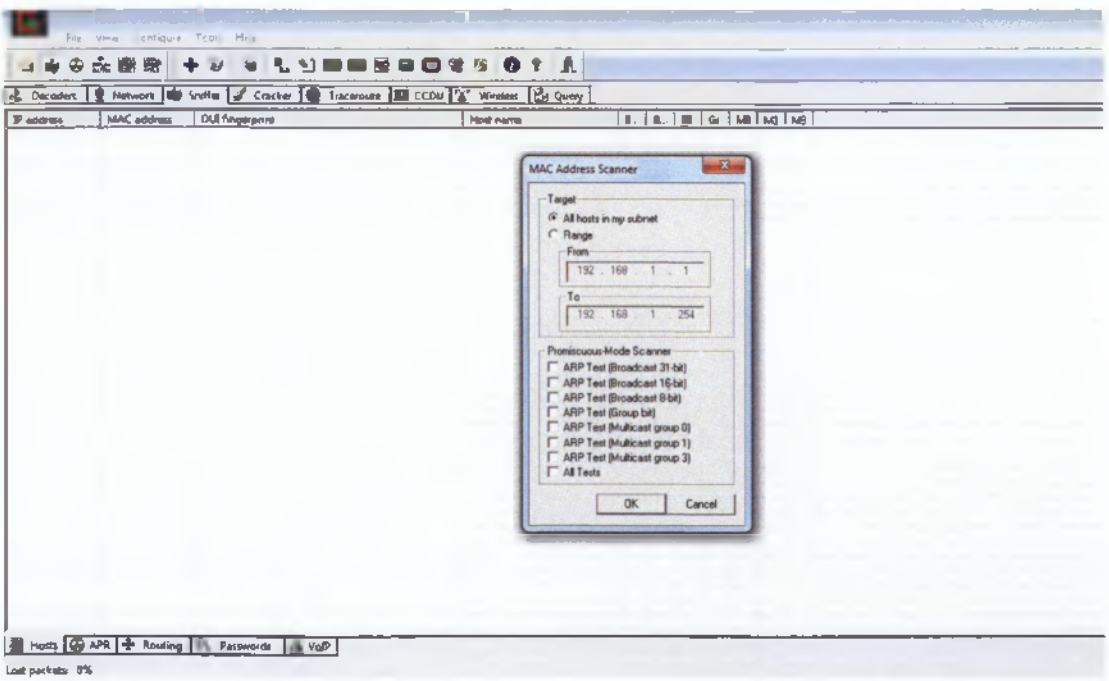
Κατά την εκκίνηση του προγράμματος εμφανίζονται πολλά εικονίδια εμείς επιλέγουμε, για τους σκοπούς της εργασίας μας, την καρτέλα sniffer όπως φαίνεται στη παρακάτω εικόνα



Έπειτα πατήσαμε στο configuration για να βεβαιωθούμε ότι χρησιμοποιούμε τη πραγματική μας IP και φυσική διεύθυνση όπως βλέπουμε παρακάτω

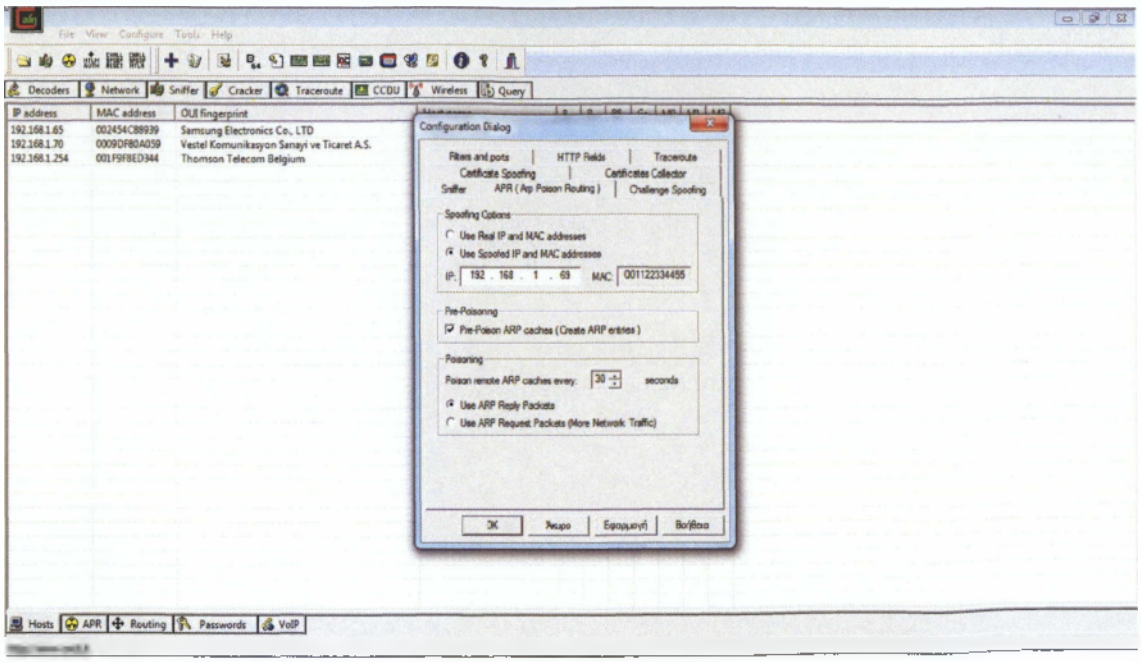


Μετά ξεκινήσαμε το sniffer και πατήσαμε το σύμβολο με τον μπλε σταυρό όπως μας δείχνει η επόμενη εικόνα

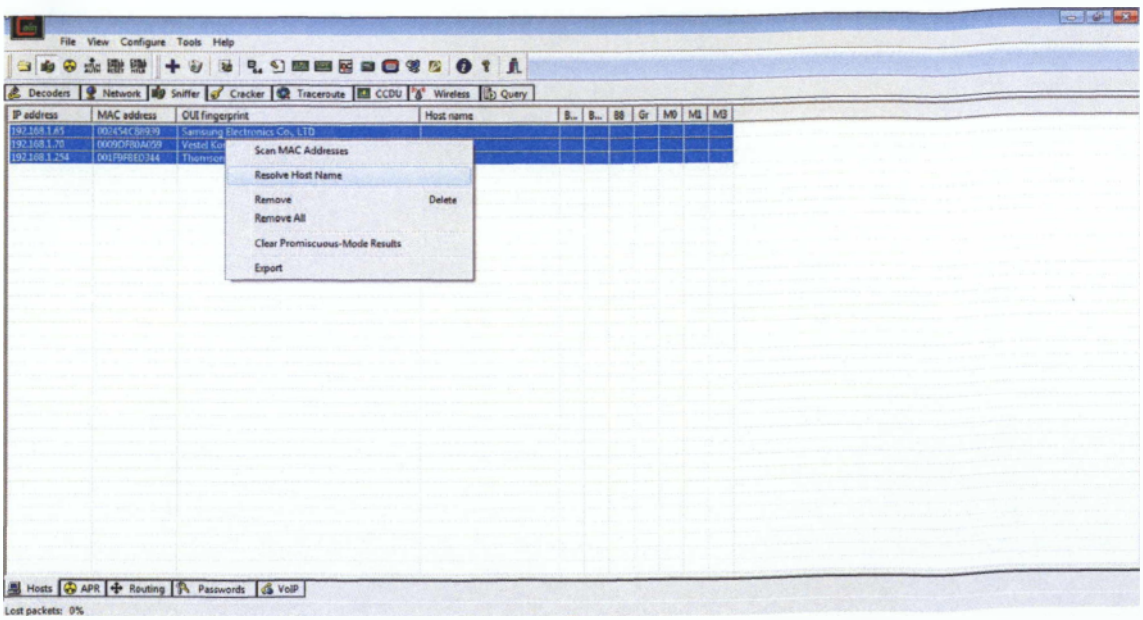


Πατώντας αυτό το σύμβολο το πρόγραμμα μας επιτρέπει να δούμε όλους τους υπολογιστές και τις δικτυακές συσκευές στο δίκτυο μας. Έπειτα πάμε στην επιλογή configure και

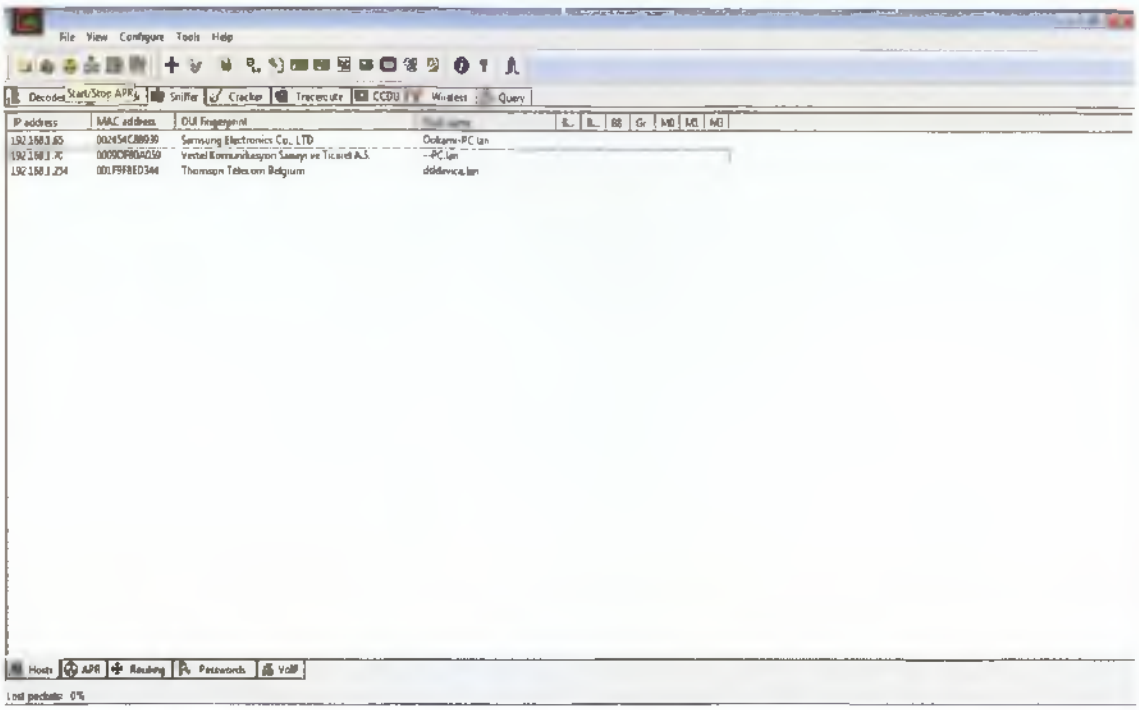
επιλέγουμε να χρησιμοποιήσουμε μια ψευδή IP διεύθυνση η οποία ομως θα ανήκει στο υποδίκτυο που βρισκόμαστε



Μετά επιλέξαμε όλες τις συσκευές στο υποδίκτυο μας πατήσαμε δεξί κλικ και Resolve Host Name έτσι ώστε να γνωρίζουμε ποιός είναι ποιός στο δίκτυο μας.

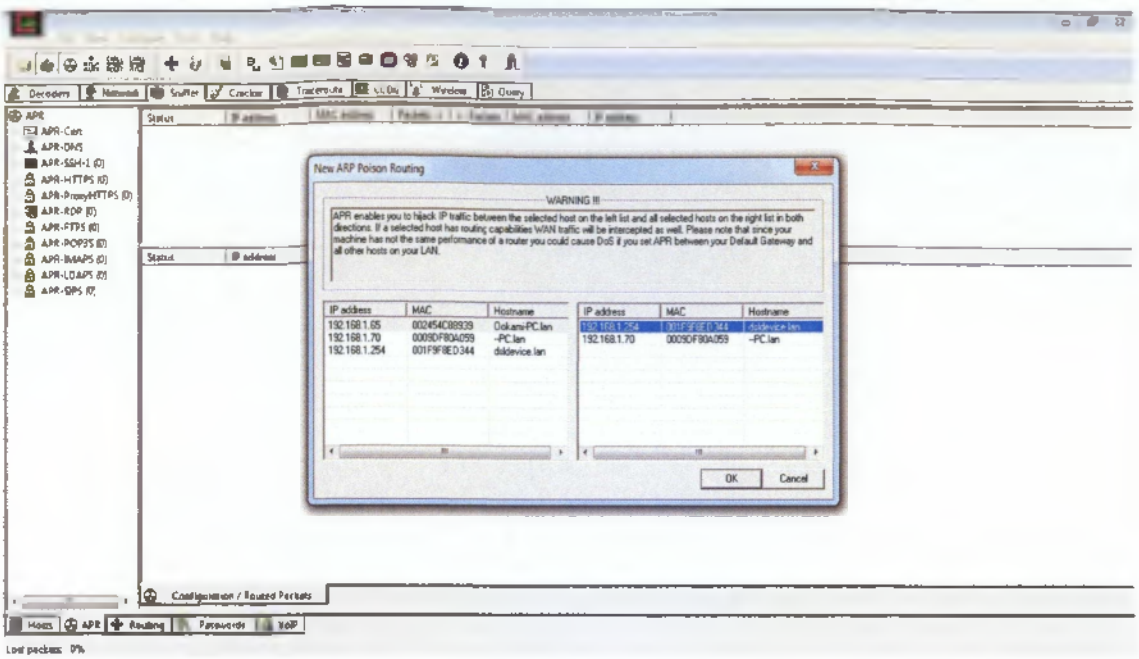


Και το αποτέλεσμά μας ήταν το παρακάτω

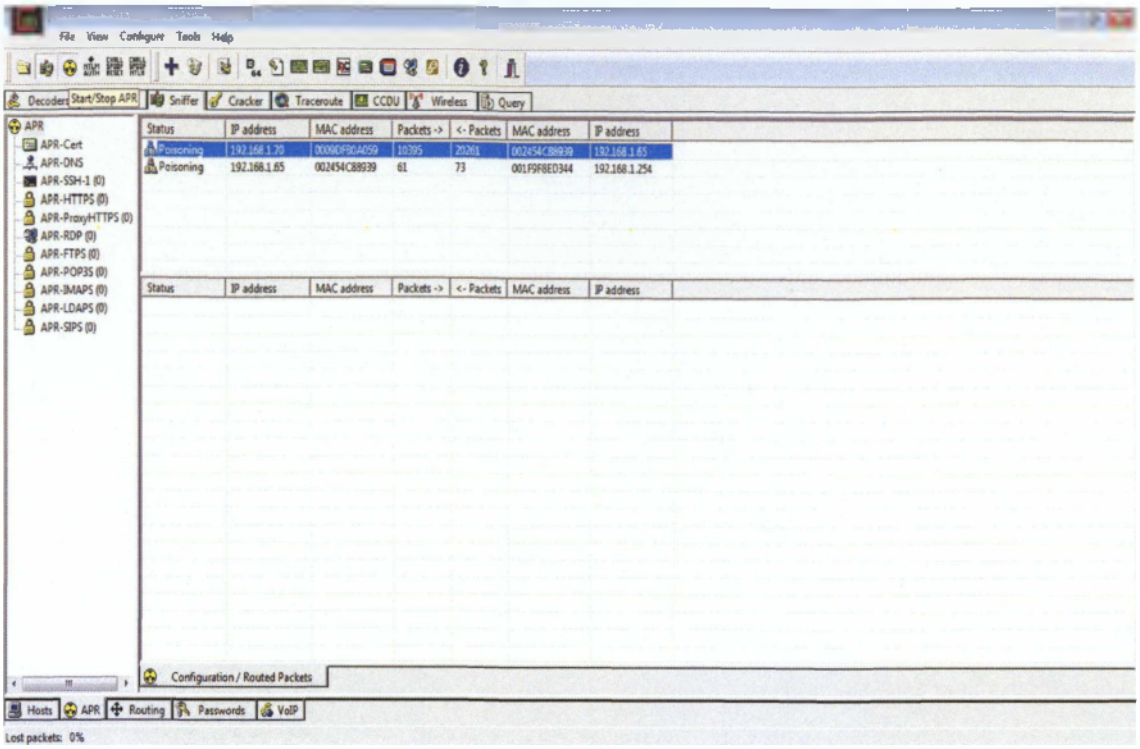


Έτσι τώρα ξέρουμε ποίοι είναι οι υπολογιστές στο δίκτυο μας και ποία η συσκευή διασύνδεσης αυτών.

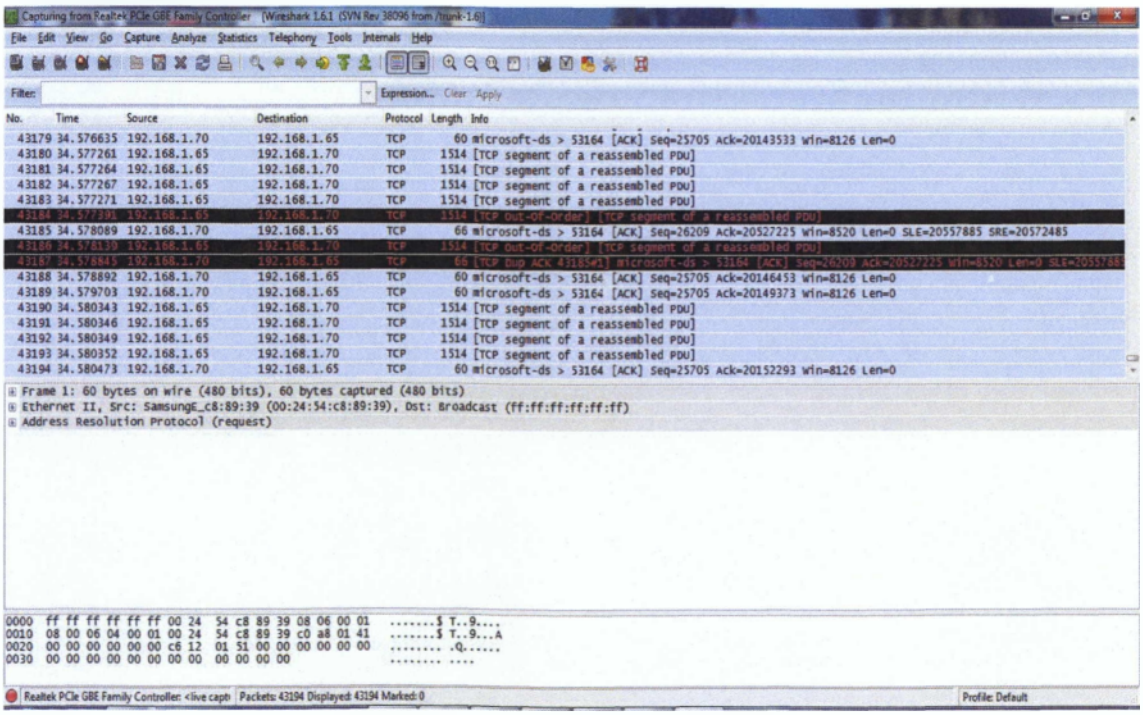
Στη συνέχεια πατήσαμε την καρτέλα Arp Poisoning και εμφανίστηκαν δύο νέες καρτέλες κάναμε κλικ στη πρώτη καρτέλα και πατήσαμε το σύμβολο με το μπλε σταυρό και εμφανίστηκαν οι συσκευές που είναι συνδεμένες στο δίκτυό μας και επιλέξαμε τις δικτυακές συσκευές που θέλαμε όπως φαίνεται παρακάτω



Αφού επιλέξαμε τις συσκευές που θέλαμε να κρυφακούσουμε πατάμε την επιλογή ARP Poisoning και βλέπουμε τη μεταφορά των πακέτων μεταξύ των υπολογιστών χωρίς αυτοί να υποψιάζονται το παραμικρό ότι τους παρακολουθούμε. Τώρα μας δίνεται η επιλογή πατώντας την καρτέλα Passwords και επείτα SendToCracker να δούμε διάφορους κωδικούς όπως εάν ο χρήστης συνδεθεί στο λογαριασμό του ηλεκτρονικό ταχυδρομείο του αλλά για λόγους εχεμύθειας δεν θα το προβάλλουμε σε αυτή την εργασία



Για περισσότερη ακρίβεια στη μεταφορά των δεδομένων κατεβάσαμε το πρόγραμμα Wireshark για να βλέπουμε σε μεγαλύτερη ανάλυση τη μεταφορά των πακέτων καθώς και την χειραψία που συνάπτουν αυτοί οι δύο υπολογιστές (SYN-ACK) .



4.3 Σύνοψη

Με την υλοποίηση αυτής της επίθεσης κατανοήσαμε περισσότερο το τρόπο με τον οποίο λειτουργούν οι ManInTheMiddle επιθέσεις το τρόπο λειτουργίας τους και πώς μπορούν να υποκλέψουν στοιχεία σχεδόν ανώδυνα και χωρίς να αφήσουν ίχνη όπως άλλες μέθοδοι. Η τεχνική Arp Cache Poisoning είναι η πιο απλή και πιο διαδεδομένη μορφή καθώς εκτελείται απλά ακολουθώντας μερικά απλά βήματα. Ελπίζουμε ότι οι αναγνώστες αυτής της πτυχιακής να κατανόησαν τη μέθοδο αυτή καθώς και τον τρόπο υλοποίησης της και να είναι πλέον ικανοί να την υλοποιήσουν και οι ίδιοι όταν χρειαστεί. Τέλος, όλες οι εικόνες που χρησιμοποιήθηκαν για το τέταρτο κεφάλαιο της εργασίας αυτής έχουν τραβηχθεί από τον υπολογιστή που χρησιμοποιήσαμε σαν sniffer.

ΑΝΑΦΟΡΕΣ ΚΑΙ ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Παπακωνσταντίνου Γ., Τσανάκα Π., Κοζύρη Ν., Μανουσοπούλου Α., Ματζάκου Π. (1999), *Τεχνολογία Υπολογιστικών Συστημάτων & Λειτουργικά Συστήματα*, p.176-201.

[2] Wikipedia (2011), *WinLogon*, [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση: http://en.wikipedia.org/wiki/Winlogon [πρόσβαση 12 Ιουλίου 2011].

[3]Dan Griffin (2011) , *Create Custom Login Experiences With Credential Providers For Windows Vista,*. [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση:http://msdn.microsoft.com/en-us/magazine/cc163489.aspx [Πρόσβαση 12 Ιουλίου 2011]

[4] Microsoft TechNet (2011) , *Bitlocker*, [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση http://technet.microsoft.com/en-us/library/cc766200%28WS.10%29.aspx#BKMK_WhatIsBitLocker [Πρόσβαση 13 Ιουλίου]

[5]Wikipedia (2011), Bitlocker Drive Encryption ,. [Online] Διαθέσιμο στην ηλεκτρονική διεύθυνση: http://en.wikipedia.org/wiki/Bitlocker_Drive_Encryption [Πρόσβαση 13 Ιουλίου]

[6]Microsoft (2011), BitlockerDriveEncryption, [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση: http://windows.microsoft.com/en-US/windows-vista/Bitlocker-Drive-Encryption-Overview [Πρόσβαση 13 Ιουλίου 2011].

[7] Wikipedia (2011), *Cryptographic API,* [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση http://en.wikipedia.org/wiki/Cryptographic_API [Πρόσβαση 13 Ιουλίου 2011].

[8] Roger A. Grimes, Jespen M. Johansson ., (2007) *Windows Vista Security* , Εκδόσεις Wiley , Έκδοση Πρώτη, p.13

[9] IT SECURITY(2011), *Windows Defender*, [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση: http://www.itsecurity.com/features/microsoft-windows-vista-033007/ [Πρόσβαση 15 Ιουλίου]

[10] MSDN Microsoft(2011), *Windows Filtering Platform*, [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση: http://msdn.microsoft.com/en-us/library/aa366509(v=vs.85).aspx

[11] Adopenstatic (2011) , *Mandatory Integrity Control* [Online],. Διαθέσιμο στην ηλεκτρονική διεύθυνση : http://www.adopenstatic.com/cs/blogs/ken/archive/2006/08/18/Why-Vista_3F00_-Mandatory-Integrity-Control-_2800_MIC_2900_-_2800_Security_2C00_-Stability_2C00_-System-Integrity_2900_.aspx [Προσβαση 15 Ιουλίου]

[12] Βικιπέδια (2011), Secure Socket Layer , [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση http://el.wikipedia.org/wiki/SSL [Πρόσβαση 17 Ιουλίου]

[14] Μάγκος Κ., Νιξαρλίδης Α.,(1999), Κατάταξη Δικτυακών Συστημάτων Ασφάλειας, [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση: http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kefalaio5.htm [πρόσβαση 18 Ιουλίου 2011].

[15] Σουρής Α., Πατσός Δ., Γρηγοριάδης Ν., (2004), *Ασφάλεια Της Πληροφορίας*, Εκδόσεις Νέων Τεχνολογιών, Έκδοση Πρώτη, p. 285-287.

[16] Μάγκος Κ., Νιξαρλίδης Α.,(1999), Κατάταξη Δικτυακών Συστημάτων Ασφάλειας, [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση: http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kefalaio5.htm [πρόσβαση 18 Ιουλίου 2011].

[17] IPSecHOWTO (2011) , Ipsec Tunnel and transport mode, [online],. Διαθέσιμο στην ηλεκτρονική διεύθυνση http://www.ipsec-howto.org/x202.html [Πρόσβαση 15 Ιουλίου]

[18]Microsoft Technet (2011) , How TLS works , [Online],. Διαθέσιμο στην ηλεκτρονική διεύθυνση : http://technet.microsoft.com/en-us/library/cc783349(WS.10).aspx [Πρόσβαση 15 Ιουλίου]

[19] Coressec (2011), ManInTheMiddle attack, [Online] ,. Διαθέσιμο στην ηλεκτρονική διεύθυνση : (http://www.coresec.org/2011/04/07/man-in-the-middle-attack-using-ettercap/ [Πρόσβαση 17 Ιουλίου 2011]

[20] Chris Sanders,. (2010) , *Understanding ManInTheMiddle Attack,* [Online] ,. Διαθέσιμο στην ηλεκτρονική έκδοση : http://www.windowsecurity.com/articles/understanding-man-in-the-middle-attacks.htm [Πρόσβαση 18 ιουλιου 2011]

[21] P. RameshBabu,. D.Lalitha Bhaskari ,. CH.Satyanarayana ,. (2010), *A Comprehensive Analysis of Spoofing* [Online] ,. Διαθέσιμο στην ηλεκτρονική έκδοση http://thesai.org/Downloads/Volume1No6/Paper_23_A_Comprehensive_Analysis_of_Spoofing.pdf III ARP SPOOFING III [Πρόσβαση 18 Ιουλιου 2011]

[22] Chris Sanders,. (2010) , *Understanding ManInTheMiddle Attack,* [Online] ,. Διαθέσιμο στην ηλεκτρονική έκδοση http://www.windowsecurity.com/articles/understanding-man-in-the-middle-attacks-arp-part2.htm

[23] Ian Green,. (2005) *DNS Spoofing by ManInTHeMiddleAttack* ,. [Online] Διαθέσιμο σε ηλεκτρονική έκδοση : http://www.sans.org/reading_room/whitepapers/dns/dns-spoofing-man-middle_1567 [Πρόσβαση 19 Ιουλίου 2011]

[24] Μαργαρίτης Γ,. *DoS ATTACKS* ,. [Online], Διαθέσιμο στην ηλεκτρονική έκδοση : http://www.secbible.org/Files/papers/Simple_Dos_attacks.pdf [Πρόσβαση 19 Ιουλίου 2011]

[25] David Slee,. Common Denial Of Service attacks , (2007) , [Online], Διαθέσιμο στην ηλεκτρονική έκδοση : http://www.infosecwriters.com/text_resources/pdf/DSlee_Denial_of_Service_Attacks.pdf] [Πρόσβαση 19 Ιουλίου 2011]

[26] Abhishek Singh,. *Demystifying Denial Of Service Attacks*, **(2010)**,. [Online] Διαθέσιμο στην ηλεκτρονική διεύθυνση : http://www.symantec.com/connect/articles/demystifying-denial-service-attacks-part-one [Πρόσβαση 15 Ιουλίου 2011]

[27]Wikipedia (2011) , *Ping*, [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση: http://en.wikipedia.org/wiki/Ping [Πρόσβαση 18 Ιουλίου 2011]

[28] Hang Chau (2011),. Network *Security – Defense Against DoS/DDoS Attacks* , [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση:http://www.infosecwriters.com/text_resources/pdf/Defense_DDoS.pdf [Πρόσβαση 22 Ιουλίου 2011]

[29] Kioskea (2008) ,. *Land Attack* , [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση: http://en.kioskea.net/contents/attaques/attaque-land.php3 [Προσβαση 5 Αυγούστου 2011]

[30] Maciej Ogorkiewicz,. Piotr Frej ,. (2002) *Analysis of buffer Overflow Attacks*, [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση : http://www.windowsecurity.com/articles/Analysis_of_Buffer_Overflow_Attacks.html [Πρόσβαση 7 Αυγούστου 2011]

[31] Πρίτσος Δ,. Buffer Overflow Exploits,. [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση : http://www.islab.demokritos.gr/gr/html/ptixiaki_dpritsos/kefalaio_1.pdf [Πρόσβαση 18 Αυγούστου 2011]

[32] Maciej Ogorkiewicz,. Piotr Frej ,. (2002) Analysis of buffer Overflow Attacks, [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση : http://www.windowsecurity.com/articles/Analysis_of_Buffer_Overflow_Attacks.html [Πρόσβαση 7 Αυγούστου 2011]

[33] Πρίτσος Δ,. Buffer Overflow Exploits,. [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση : http://www.islab.demokritos.gr/gr/html/ptixiaki_dpritsos/kefalaio_1.pdf [Πρόσβαση 18 Αυγούστου 2011]

[34]Chris Sanders,. (2010) ,. Analyzing DLL Hijacking Attacks [Online]. Διαθέσιμο στην ηλεκτρονική διεύθυνση : http://www.windowsecurity.com/articles/Analyzing-DLL-Hijacking-Attacks.html [Πρόσβαση 21 Αυγούστου 2011]

[35] Roger A. Grimes, Jespen M. Johansson ., (2007) *Windows Vista Security* , Εκδόσεις Wiley , Έκδοση Πρώτη, p.44-50

[36] Microsoft Technet (2009) ,. Protecting Against Brute Force Attacks ,. [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση : [http://social.technet.microsoft.com/Forums/en/winservers ecurity/thread/f97ff18e-dd41-4e57-94a5-0f47b6d85b54] [Πρόσβαση 21 Αυγούστου 2011]

[37]Exploit Database (2011),. DLL hijacking vulnerable applications ,. [Online]. Διαθέσιμο στην ηλεκτρονική έκδοση : www.exploit-db.com [Προσβαση 21 αυγούστου 2011]

Whitman, M.E. & Mattord, H.J. (2004). *Management of Information Security.*

Roger A. Grimes, Jespen M. Johansson., (2007) *Windows Vista Security*

Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reiher, (2004) *Internet Denial of Service: Attack and Defense Mechanisms*

Matthew Conover., *Analysis of the Windows Vista Security Model*

James C Foster., Vitaly Osipov., Nish Bhalla., (2004) *Buffer Overflow Attacks: Detect, Exploit, Prevent*

Σουρής Α., Πατσός Δ., Γρηγοριάδης Ν., (2004), *Ασφάλεια Της Πληροφορίας*

Andy Walker,. (2008). *Windows Lockdown!: Your XP and Vista Guide Against Hacks, Attacks, and Other Internet Mayhem*

Gary B. Shelly., Steven M. Freund., Reymond E. Enger (2007) *Microsoft Windows Vista: Complete Concepts and Techniques*
David Leblanc., Michael Howard (2007) *Writing Secure Code for Windows Vista*

Ed Bott., Craig Stinson., Carl Siechert (2008) *Windows Vista Inside Out*

Joel Scambray., George Kurtz., Stuart McClure(2010) *Hacking Exposed, Sixth Edition*

Books LLC, Wiki Series Books LLC, Wiki Series (2011) *Cryptographic Attacks, Cryptanalysis, Dictionary Attack, Differential cryptanalysis, Brute Force Attack, Keystroke Logging*

Chris Sanders (2011) *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*

Mike Danseglio., Robbie Allen, (2006) Windows *Server 2003 security cookbook*

Mark Burnett, Anonymous, L. J. Locher , Chris Doyle, Chris Amaris, Rand Morimoto, (2001) *Maximum Windows 2000 Security*