ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

ΜΑΝΤΑΣ ΕΛΕΥΘΕΡΙΟΣ

Α.Μ 1047128

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2019

ΠΕΡΙΕΧΟΜΕΝΑ

Α Κ Ρ Ω Ν Υ Μ Ι Α

CIA: Confidentiality, Integrity, Availability

DOS: Denial of Service

DDoS: Destributed Denial of Service

DNS: Domain Name System

ARP: Address Resolution Protocol

BCP38: Best Common Practise

TCP: Transmission Control Protocol

IP: Internet Protocol

PPMP: Ping Message Message Protocol

IMW: Instant Message Worm

P2P: Pear to Pear

DES: Data Encryption Standard

AES: Advanced Encryption Standard

XOR: Exclusive Or

RSA: Rivest-Shamir-Adleman

BCP: best Common Practice

CAGR: Compound Annual Growth Rate

ACL: Access Control Lists

UTM: Unified threat management

Κεφαλαιο 1: Εισαγωγη Στην Ασφαλεια Δικτυων

1.1 Γενικά

Η **Ασφάλεια των Δικτύων** είναι ένα μείζον ζήτημα από τότε που δημιουργήθηκε το διαδίκτυο. Δημιουργήθηκε ώς όρος κατά την διαδικασία αναζήτησης μεθόδων και τεχνικών διασφάλισης της μυστικότητας (**secrecy**) των πληροφοριών των υπολογιστικών συστημάτων που εμπλέκονταν στο δίκτυο και διατηρούσαν πολύ σημαντικά δεδομένα που δεν μπορούσαν να πέσουν στα χέρια κακόβουλων ή επιτήδειων ανθρώπων. Η Ασφάλεια σαν όρος αφορά την ασφάλεια των πληροφοριών (**information security**) όπου χρησιμοποιούνται μέθοδοι κρυπτογράφισης, την ασφάλεια λειτουργικών, υπολογιστικών συστημάτων και εφαρμογών (**system security**) και τέλος την ασφάλεια δικτύων υπολογιστών, δικτυακά πρωτόκολλα και ασφάλεια δικτυακών συσκευών(**network security**)[1].

1.2. Ορισμός

Οι τεχνολογίες ασφαλείας δικτύου προστατεύουν το δίκτυο από **κλοπή** και **κατάχρηση απόρρητων** επιχειρηματικών **πληροφοριών**, καθώς και από κακόβουλες επιθέσεις από ιούς του Internet και ιούς τύπου worm. Η ασφάλεια δικτύου συνδυάζει πολλαπλά στρώματα άμυνας στη συσκευή που συνδέεται και στο δίκτυο. Κάθε στρώμα ασφάλειας δικτύου εφαρμόζει πολιτικές και ελέγχους. Οι εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση σε πόρους δικτύου, αλλά οι κακόβουλοι χρήστες εμποδίζονται να πραγματοποιούν απειλές και επιθέσεις[2] [3].

.

1.3. Ιστορική Αναδρομή

Κατά τις πρώτες δεκαετίες της ‘ύπαρξής τους, τα δίκτυα υπολογιστών χρησιμοποιούνταν κυρίως από πανεπιστημιακούς **ερευνητές** για αποστολή ηλεκτρονικού ταχυδρομείου και από τους υπαλλήλους των εταιρειών για κοινή χρήση των εκτυπωτών. Υπό αυτή τη συνθήκη δεν δινόταν και πολλή σημασία στην έννοια της Ασφάλειας. Στις μέρες μας, όμως, που εκατομμύρια απλοί άνθρωποι χρησιμοποιούν τα δίκτυα για τραπεζικές συναλλαγές, αγορές, υποβολή φορολογικών δηλώσεων, και όπου ανακαλύπτεται η μια αδυναμία μετά την άλλη, η ασφάλεια των δικτύων προβάλλει στον ορίζοντα ως ένα δυνητικά τεράστιο πρόβλημα[4].

1.4. Αρχές της Ασφάλειας Δικτύων (CIA)

Οι χρήστες κάθε επικονωνίας που λαμβάνει χώρα επιζητούν σιγουριά για τον χρήστη με τον οποίο επικοινωνούν και πως τα μηνύματά του θα φτάσουν στο **σωστό παραλήπτη** και δεν θα γίνουν θύματα υποκλοπής. Επίσης, θέλουν να πιστοποιούν πως το περιεχόμενο των μηνυμάτων που στέλνουν δεν έχουν τροποποιηθεί κατά τη μεταφορά τους. Τέλος, θέλουν να είναι διασφαλισμένη η επικοινωνία τους στη πρώτη ζήτηση. Όλα αυτά μας οδηγούν στην ανάλυση των τριών Αρχών της Ασφάλειας Δικτύων που είναι οι παρακάτω[5]:

1.4.1. Εμπιστευτικότητα (Confidentiality)

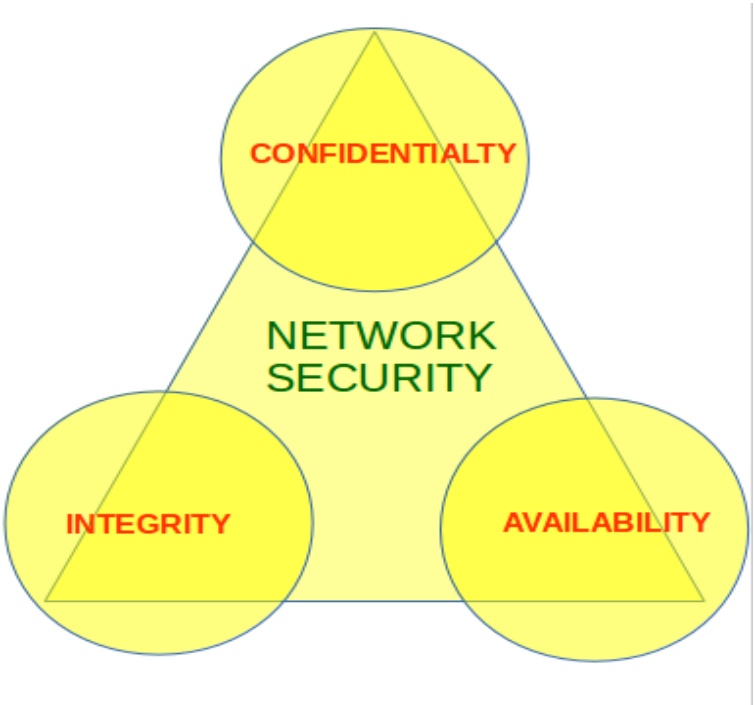
Εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Μόνο ο αποστολέας και ο παραλήπτης πρέπει να είναι σε θέση να κατανοούν τα περιεχόμενα του μεταδιδόμενου μηνύματος. Εδώ προκύπτει η ανάγκη της **κρυπτογράφισης (encryption),** ώστε να διασφαλιστεί πως ακόμα και όταν ένα μήνυμα πέσει θύμα υποκλοπής να είναι σε μορφή μη κατανοητή από τον υποκλοπέα.

1.4.2. Ακεραιότητα Δεδομένων (Data Integrity)

Η Ακεραιότητα είναι άρρηκτα συνδεδεμένη με τον όρο της **αξιόπιστης** πληροφορίας. Επιζητάμε εδώ την πρόληψη μη εξουσιοδοτημένης μεταβολής των πληροφοριών, δηλαδή την αδυναμία ενός επιτηθέμενου να **τροοποποιήσει**, διαγράψει το περιεχόμενο του μηνύματος που στέλνεται, ακόμα και να μην μπορεί να δημιουργήσει κάποια δεδομένα (fake data).

1.4.3. Διαθεσιμότητα (Availability)

Η Διαθεσιμότητα σημαίνει πως ανα πάσα στιγμή οι υπηρεσίες του δικτύου είναι **προσπελάσιμες** και χρησιμοποιούμενες χωρίς κάποια μη-ορθολογική καθυστέρηση. Κάθε χρήστης πρέπει να έχει πρόσβαση στη πληροφορία που επιθυμεί, εφόσον διαθέτει το **δικαίωμα** να τη προσπελάσει. Είναι δυνατόν κάποιος επιτήδειος να προσπαθήσει να κάνει την λεγόμενη επίθεση DOS, επίθεση άρνησης παροχής υπηρεσιών. Τα συστήματα οφείλουν να είναι ανθεκτικά σε τέτοιες κακόβουλες επιθέσεις που παρακωλύουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα.



Οι Τρείς αρχές της Ασφάλειας [6]

ΚΕΦΑΛΑΙΟ 2: ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΕΙΔΗ

2.1. Δούριοι Ίπποι (Trojan Horses)

Όπως ο Δούρειος ίππος της ελληνικής μυθολογίας, αυτός ο τύπος κακόβουλου λογισμικού χρησιμοποιεί μεταμφίεση ή παραπλάνηση για να αποκρύψει την πραγματική του λειτουργία. Αφού καταφέρει και φτάσει στο στόχο του, συχνά χρησιμοποιεί διάφορες τεχνικές για να εκτελεστεί από το χρήστη ή από άλλο λογισμικό που επίσης βρίσκεται στο μολυσμένο σύστημα.

Τα **Trojans** αποτελούν την πιο κοινή κατηγορία **κακόβουλου λογισμικού**. Χρησιμοποιούνται για να ανοίξουν «κερκόπορτες» σε ένα σύστημα με σκοπό οι επιτιθέμενοι να αποκτήσουν τον έλεγχο της προσβληθείσας συσκευής, να υποκλέψει προσωπικά δεδομένα του χρήστη, να κατεβάσει και να εκτελέσει άλλο κακόβουλο λογισμικό, καθώς και για πολλούς άλλους κακόβουλους σκοπούς. Οι άνθρωποι μερικές φορές σκέφτονται ένα Trojan ως ιό (virus) ή σκουλήκι (worm), αλλά στην πραγματικότητα δεν είναι τίποτα από τα δύο[7].

Τα Trojans παρομοιάζονται με τον ρόλο της ομπρέλας για την παράδοση κακόβουλων προγραμμάτων, επειδή υπάρχουν διάφορα είδη Trojans. Ανάλογα με την πρόθεση του εγκληματικού προγραμματιστή, ο Δούρειος ίππος μπορεί να λειτουργεί ως ένα κομμάτι από αυτόνομο κακόβουλο λογισμικό ή ως εργαλείο για άλλες δραστηριότητες, όπως η παροχή μελλοντικών ωφέλιμων φορτίων, η επικοινωνία με τον χάκερ σε μεταγενέστερο χρόνο, ή ανοίγοντας το σύστημα σε επιθέσεις, δηλαδή αποδυναμώνοντάς το.

Με άλλα λόγια, ένας Trojan είναι μια στρατηγική παράδοσης που χρησιμοποιούν οι **χάκερ** για να παραδώσουν οποιουδήποτε είδους απειλές, από το ransomware που απαιτεί άμεσα χρήματα, μέχρι το **spyware** που κρύβει, ενώ κλέβει πολύτιμες πληροφορίες όπως προσωπικά και οικονομικά δεδομένα.

Trojan Horse [8]

Μέθοδοι μόλυνσης από Trojan

Τα Trojans μπορούν να μοιάζουν σχεδόν με οτιδήποτε, από το ελεύθερο λογισμικό και τη μουσική, έως τις διαφημίσεις του προγράμματος περιήγησης σε φαινομενικά νόμιμες εφαρμογές. Οποιαδήποτε απρόσεκτη συμπεριφορά των χρηστών μπορεί να οδηγήσει σε μόλυνση από Trojan. Ακολουθούν μερικά παραδείγματα:

- **Λήψη cracked εφαρμογών**.

Ένα **παράνομο** δωρεάν αντίγραφο ενός λογισμικού μπορεί να είναι δελεαστικό, αλλά το cracked λογισμικό (ή γεννήτρια κλειδιού ενεργοποίησης) μπορεί να αποκρύψει μια επίθεση Trojan.

- **Λήψη άγνωστων δωρεάν προγραμμάτων**.

Αυτό που μοιάζει με ένα δωρεάν παιχνίδι ή μια προφύλαξη οθόνης θα μπορούσε να είναι πραγματικά ένας Δούρειος Ίππος, ειδικά αν το βρέθηκε σε μη-ασφαλή ιστοσελίδα.

- **Άνοιγμα μολυσμένων συνημμένων**.

Συνήθως υλοποιείται ως **παράξενο μήνυμα ηλεκτρονικού ταχυδρομείου** που μοιάζει με ένα σημαντικό συνημμένο, όπως ένα τιμολόγιο ή μια απόδειξη παραλαβής, αλλά ξεκινάει ένα Trojan όταν κάνετε κλικ σε αυτό[9].

Είδη του Trojan

- **Spyware:** παρακολουθεί την απόκτηση πρόσβασης σε λογαριασμούς στο διαδίκτυο ή την εισαγωγή των στοιχεία πιστωτικών καρτών. Στη συνέχεια μεταδίδουν τους κωδικούς πρόσβασής σας και άλλα στοιχεία ταυτοποίησης πίσω στον χάκερ.
- **Zombified Trojans:** παίρνουν τον έλεγχο του υπολογιστή για να το κάνουν σκλάβο σε ένα δίκτυο υπό τον έλεγχο του χάκερ. Αυτό είναι το πρώτο βήμα για τη δημιουργία ενός botnet (ρομπότ + δίκτυο), το οποίο χρησιμοποιείται συχνά για να εκτελέσει μια κατανεμημένη επίθεση κατάργησης υπηρεσίας (DDoS) που έχει σχεδιαστεί για να καταστρέψει ένα δίκτυο κατακλύζοντάς το με κυκλοφορία.
- **Backdoors:** δημιουργούν απομακρυσμένη πρόσβαση στε συστήματα. Αυτό το είδος κακόβουλου λογισμικού αλλάζει την ασφάλειά για να επιτρέψει στον χάκερ να ελέγξει τη συσκευή, να κλέψει δεδομένα και ακόμα να κατεβάσει περισσότερα κακόβουλα προγράμματα.

2.2. Σκουλίκια (Worms)

Τα **σκουλήκια υπολογιστών** είναι ειδικά είδη κακόβουλου λογισμικού που αναπαράγονται και εξαπλώνονται από μόνα τους χωρίς καμία ανθρώπινη αλληλεπίδραση, κάτι που τα κάνει πολύ επικίνδυνα[10].

Τα **σκουλήκια (worms)** είναι παρόμοια με τους ιούς, επειδή αναπαράγουν λειτουργικά αντίγραφα των ίδιων και μπορούν να προκαλέσουν τον ίδιο τύπο βλάβης. Σε αντίθεση με τους ιούς, οι οποίοι απαιτούν την εξάπλωση ενός μολυσμένου αρχείου ξενιστή, τα σκουλήκια είναι αυτόνομο λογισμικό και δεν απαιτούν πρόγραμμα

φιλοξενίας. Για να εξαπλωθούν, τα σκουλήκια είτε εκμεταλλεύονται μια ευπάθεια στο σύστημα στόχου είτε χρησιμοποιούν κάποιο είδος *κοινωνικής μηχανικής* για να εξαπατήσουν τους χρήστες να τους εκτελέσουν. Η κοινωνική μηχανική είναι η χρήση της εμπιστοσύνης για την εξαγωγή πληροφοριών από ομάδες ή άλλα άτομα.

Ένα **σκουλήκι** εισέρχεται σε έναν υπολογιστή μέσω μιας ευπάθειας στο σύστημα και εκμεταλλεύεται τις δυνατότητες μεταφοράς αρχείων ή μεταφοράς πληροφοριών στο σύστημα, επιτρέποντάς του να ταξιδεύει χωρίς βοήθεια. Τα πιο προηγμένα σκουλήκια εκμεταλλεύονται την κρυπτογράφηση και τις τεχνολογίες **ransomware** για να βλάψουν τους στόχους τους[11].

Εξάπλωση των worms

Ο συνηθέστερος τρόπος με τον οποίο οι ιοί συνήθως εξαπλώνονται είναι μέσω ενός χρήστη που εξαπατάται για να το κατεβάσει και να το εκτελέσει. Επίσης η εξάπλωση γίνεται με τους παρακάτω τρόπους αν ο χρήστης ενός υπολογιστή δεν είναι αρκετά προσεκτικός.

- Κάνοντας **κλικ** σε κακόβουλες διαφημίσεις
- Λήψη επιβλαβών συνημμένων ηλεκτρονικού ταχυδρομείου
- Εγκατάσταση **δωρεάν** λογισμικού
- Συμμετοχή σε κοινή χρήση **P2P**

Computer Worm [12]

Υπάρχουν παραλλαγές των σκουληκιών, όπως τα σκουλήκια **IMW** και τα σκουλήκια ηλεκτρονικού ταχυδρομείου, μπορούν να αναγκάσουν το μηχάνημα-στόχο να στείλει μηνύματα που περιέχουν τον ιό τύπου worm σε χρήστες σε μια λίστα αποθηκευμένων επαφών. Αυτό κάνει την διάκριση ιών και σκουλικιών ακόμα πιο δύσκολη και «θολή». Τα υβρίδια ιού / σκουληκιών είναι επίσης κοινά, όπου το κακόβουλο λογισμικό μπορεί να εξαπλωθεί χωρίς ανθρώπινη επαφή όπως το σκουλήκι, αλλά παράγει ωφέλιμο φορτίο σαν ιό για να προκαλέσει ζημιά σε κάθε μηχανή με την οποία αλληλεπιδρά[10].

Επίδραση ενός worm

Η ταχεία αναπαραγωγή και η εξάπλωση ενός ιού τύπου worm μέσω του δικτύου μπορεί να εκμεταλευτεί τους πόρους ενός υπολογιστή προς όφελός τους. Συνήθως ένας υπολογιστής που κινείται αργά ή το δίκτυό του φαίνεται να έχει επιβραδυνθεί έχει πολλές πιθανότητες να έχει προσβληθεί από **σκουλίκι**.

Στη συνέχεια ο υπολογιστής φαίνεται να έχει τις εξής συμπεριφορές.

- Εμφάνιση μηνυμάτων ασυνήθιστου σφάλματος.
- Παράξενες εικόνες.
- Ανεξήγητες αλλαγές στην εμφάνιση ή τη διάταξη των εικονιδίων.

Αντιμετώπιση – Μέτρα Ασφαλείας/ Προστασίας

Ως προς την αντιμετώπιση των σκουλικιών μπορεί να ακολουθηθεί εγκατάσταση **λογισμικού προστασίας** από κακόβουλο λογισμικό σε όλες τις συσκευές που διαθέτει κανείς, όπως των υπολογιστών, των φορητών υπολογιστών, των Mac και των smartphones. Ύστερα, απαραίτητη κρίνεται η τακτική ενημέρωση για να προστατεύεται κανείς από τις τελευταίες απειλές. Ένα καλό λογισμικό προστασίας από κακόβουλο λογισμικό θα εντοπίσει και θα αποτρέψει λοιμώξεις από ιούς και σκουλήκια στον υπολογιστή[14].

2.3. Ιοί (Viruses)

Ένας **ιός** είναι ένας αναγωγέας αρχείων ο οποίος μπορεί να αυτοαναδιπλασιαστεί και να εξαπλωθεί προσαρμόζοντάς τον σε ένα άλλο πρόγραμμα.

Η βασική ιδέα των ιών είναι η διαδικασία την αυτό-αναπαραγωγής τους και η μόνιμη διάδοσή τους από συσκευή σε συσκευή. Πρώτα μολύνεται ο υπολογιστής-στόχος και ύστερα αυτός σαν «πραγματικός ιός» εξαπλώνεται μέσα στο δίκτυο που ανήκει ο πρώτος υπολογιστής μολύνονται κι'άλλους σαν αυτόν. Συνήθως, οι ιοί είναι εκτελέσιμα αρχεία τα οποία αποθηκεύονται στο σύστημα αρχείων (**file system**) ενός υπολογιστή αλλά δεν τίθονται σε λειτουργία μέχρι ο χρήστης να τα εκτελέσει. Πολλοί **ιοί** είναι επιβλαβείς και μπορούν να υποκλέψουν δεδομένα, όπως κωδικούς πρόσβασης και λογαριασμούς, να επιβραδύνουν τους πόρους του συστήματος και να καταστρέψουν τα περιφερειακά του υπολογιστή. Μπορεί να εξαπλωθεί σε μία συσκευή όταν «κατεβάζουμε» ένα αρχείο ή ανοίγουμε μια ανεπιθύμητη αλληλογραφία.

Σε αυτό το σημείο θα εξηγήσουμε μερικά από τα είδη των ιών.

Είδη Ιών

1. **Boot Sector Virus**: Αυτός ο τύπος ιού μολύνει το κύριο αρχείο εκκίνησης και είναι πολύ δύσκολο και πολύπλοκο έργο να αφαιρέσει κανείς αυτόν τον ιό, ενώ απαιτεί συχνά το σύστημα να μορφοποιηθεί ("needs to be formatted"). Κυρίως εξαπλώνεται μέσω αφαιρούμενων μέσων.

2. **Direct Action Virus**: Αυτός ο τύπος ιού εγκαθίσταται ή παραμένει κρυμμένος στη μνήμη του υπολογιστή. Παραμένει συνδεδεμένο με τον συγκεκριμένο τύπο αρχείων που μολύνει. Δεν επηρεάζει την απόδοση του συστήματος και δεν γίνεται αντιληπτή κάποια ιδιαίτερη διαφορά στον χρήστη.
3. **Overwrite Virus:** Αυτός ο τύπος ιού διαγράφει όλα τα αρχεία που μολύνει. Ο μόνος πιθανός μηχανισμός που κατάργησης του ιού είναι να διαγραφούν όλα τα μολυσμένα αρχεία με προφανή απώλεια των πληροφοριών αυτών. Ο εντοπισμός του ιού αντικατάστασης είναι δύσκολος καθώς εξαπλώνεται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου.
4. **Polymorphic Virus** – Αυτος ο τύπος ιών είναι δύσκολο να εντοπιστεί με ένα παραδοσιακό πρόγραμμα προστασίας από ιούς. Αυτό συμβαίνει επειδή οι πολυμορφικοί ιοί αλλάζουν το πρότυπο υπογραφής τους κάθε φορά που αναπαράγονται. Δεδομένου ότι τα προγράμματα κατάργησης ιών εξαρτώνται από τον εντοπισμό υπογραφών κακόβουλου λογισμικού, αυτοί οι ιοί σχεδιάζονται προσεκτικά για να αποφύγουν την ανίχνευση και την ταυτοποίηση. Όταν ένα λογισμικό ασφαλείας ανιχνεύει έναν πολυμορφικό ιό, ο ιός που τροποποιείται με τον τρόπο αυτό, δεν είναι πλέον ανιχνεύσιμος χρησιμοποιώντας την προηγούμενη υπογραφή[14].

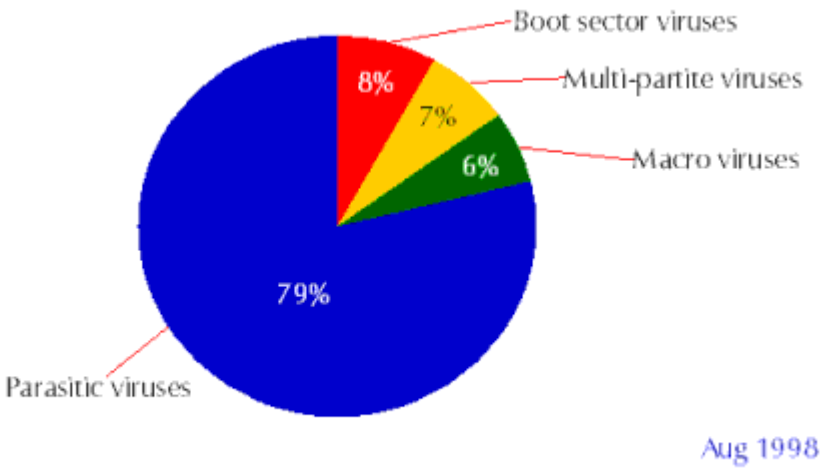


Fig.2 - Known viruses

Types of viruses [15]

Οι 3 χειρότεροι ιοί που εμφανίστηκαν ποτέ περιληπτικά

1. **Melissa Virus (1999)**

Αυτός ο ιός στελνόταν μέσω ηλεκτρονικού ταχυδρομείου ως ένα mail με περιεχόμενο που έγραφε τη σημαντικότητα του απεσταλμένου αρχείου, και ένα αρχείο **list.doc** το οποίο μόλις ανοιγόταν από το χρήστη άνοιγαν δεκάδες ιστοσελίδες με ύποπτο περιεχόμενο και επίσης το ίδο mail στελνόταν σε άλλες 20 επαφές του μολυσμένου χρήστη. Εξαπλώθηκε σε εκατοντάδες χιλιάδες υπολογιστές χωρίς να κάνει κακό σε αυτούς αλλά στις υπηρεσίες email κοστίζοντας συνολικά 80 εκατομμύρια δολάρια.

2. **“I love you” Virus (2000)**

Αυτός ο ιός βασίστηκε στο social engineering και εξαπλώθηκε σε 45 εκατομμύρια υπολογιστές μέσα σε 2 μέρες. Και αυτός ο ιός εξαπλώθηκε μέσω e-mail με περιεχόμενο ένα αρχείο **Love-Letter-for-you.txt,** το οποίο όταν ανοιγόταν έβρισκε φακέλους στον υπολογιστή του χρήστη τους οποίους αντικαθιστούσε με αντίγραφα του εαυτού του, καταστρέφοντας έτσι τα δεδομένα της μνήμης του υπολογιστή. Φυσικά και αυτός ο ιός στελνόταν σε όλες τις επαφές του χρήστη μέσω email.

3. **SQL Slammer (2003)**

Αποτέλεσμα αυτού του ιού ήταν να «πέσει» το internet, επηρεάζοντας αεροπορικές εταιρείες, ATM μηχανήματα, αστυνομικές υπηρεσίες, χρήστες κ.λ.π. Αξιοποιώντας ένα bug στο λογισμικό της Microsoft, Microsoft SQL **Server**, στέλνοντας ένα αρχείο που έμοιαζε με απλή αίτηση στο server ουσιαστικά εξάπλωνε τον ιό μέσω του server σε άλλους servers και ύστερα στους υπολογιστές που αυτοί εξυπηρετούσαν. Εξαπλώθηκε, εν τέλει, πιο γρήγορα από κάθε άλλο ιό που έχει εντοπιστεί στην ιστορία [16].

2.4. Λυτρισμικό (Ransomware)

Το **Ransomware(Λυτρισμικό)** είναι κακόβουλο λογισμικό που μπορεί να κλειδώσει μια συσκευή ή να κρυπτογραφήσει τα περιεχόμενά της, προκειμένου να ζητήσει χρήματα ως λύτρα από τον ιδιοκτήτη της. Σε αντάλλαγμα, οι δημιουργοί του κακόβουλου κώδικα υπόσχονται, φυσικά χωρίς καμία εγγύηση, να αποκαταστήσουν την πρόσβαση στο μολυσμένο μηχάνημα ή τα δεδομένα. Ουσιαστικά ο επιτηθέμενος απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβασή του θύματος σε αυτά, μέχρι να δοθούν **λύτρα από το θύμα**. Αν και τα απλά ransomware προγράμματα μπορεί να κλειδώσουν ένα σύστημα με τέτοιον τρόπο που δεν είναι δύσκολο να ξεκλειδωθεί από ένα άτομο έμπειρο στον τομέα, τα πιο εξελιγμένα προγράμματα του είδους χρησιμοποιούν τεχνικές που συνδυάζουν την κρυπτογραφία με την κακόβουλη σχεδίαση λογισμικού (**cryptoviral extortion**), ώστε να πετύχουν την κρυπτογράφηση των αρχείων του θύματος, καθιστώντας τα μη προσβάσιμα και ζητώντας λύτρα για την αποκρυπτογράφησή τους [17].

Οι **επιθέσεις** ransomware υλοποιούνται συνήθως με την χρήση ενός ιού **Trojan** ο οποίος φαίνεται σαν ένα καλόβουλο αρχείο επισυναπτόμενο συνήθως σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου και ο χρήστης παραπλανάται και το κατεβάζει ή το τρέχει στον υπολογιστή του.

Ransomware example [19]

Ας εξηγήσουμε πιο αναλυτικά το πώς λειτουργεί το Ransomware:

Υπάρχουν πολλές τεχνικές που χρησιμοποιούνται από τους δημιουργούς ransomware:

- Το ransomware **Diskcoder** κρυπτογραφεί όλο το δίσκο και εμποδίζει την πρόσβαση στο λειτουργικό σύστημα.
- Το **Screen locker** αποκλείει την πρόσβαση στην οθόνη της συσκευής.
- Το **Crypto-ransomware** κρυπτογραφεί τα δεδομένα που είναι αποθηκευμένα στο δίσκο του θύματος.
- Το **PIN locker** επιτίθεται σε συσκευές Android αλλάζοντας τους κωδικούς πρόσβασης κλειδώνοντας το χρήστη απ' έξω.

Σε μια καταλλήλως υλοποιημένη επίθεση αυτού του είδους η ανάκτηση των αρχείων χωρίς το κλειδί αποκρυπτογράφησης αποτελεί ένα ιδιαίτερα δυσεπίλυτο πρόβλημα και καθίσταται εξαιρετικά δύσκολος ο εντοπισμός των ψηφιακών νομισμάτων που χρησιμοποιήθηκαν ως λύτρα για τη συναλλαγή, όπως κρυπτονομίσματα (πχ bitcoin, xmr, etherium κ.λ.π.), και για τον λόγο αυτό υπάρχει μεγάλη δυσκολία στον εντοπισμό και τη σύλληψη των δραστών. Σε αντάλλαγμα, οι επιτιθέμενοι υπόσχονται να αποκρυπτογραφήσουν τα δεδομένα ή να αποκαταστήσουν την πρόσβαση στη μολυσμένη συσκευή [18].

2.5. Spoofing

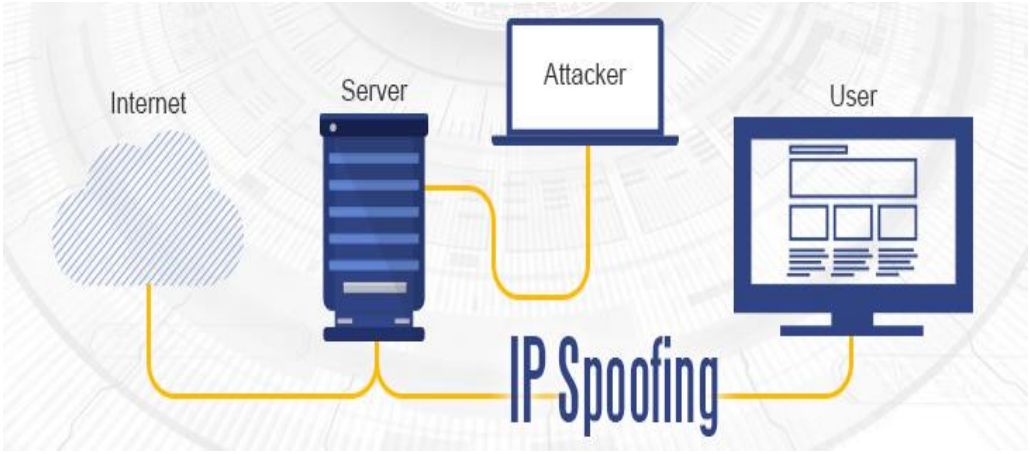
Το επονομαζόμενο Spoofing, σε μετάφραση «**Πλαστογραφία της IP διεύθυνσης**» είναι άλλη μία τεχνική επίθεσης διαδικτύου. Η πλαστογράφηση IP είναι η δημιουργία πακέτων πρωτοκόλλου Internet (IP) με διεύθυνση IP πηγής που έχει τροποποιηθεί για να μιμηθεί άλλο σύστημα υπολογιστή ή να αποκρύψει την ταυτότητα του αποστολέα ή και τα δύο. Στην πλαστογράφηση IP, το πεδίο κεφαλίδας για τη διεύθυνση IP προέλευσης περιέχει διεύθυνση διαφορετική από την πραγματική διεύθυνση IP πηγής [20].

Οι τρείς πιο συνηθησμένες μορφές του spoofing είναι οι παρακάτω:

- **Spoofing διακομιστή DNS**: Τροποποιεί έναν διακομιστή DNS, προκειμένου να ανακατευθύνει ένα όνομα τομέα σε διαφορετική διεύθυνση IP. Χρησιμοποιείται συνήθως για την εξάπλωση ιών.

- **<u>ARP spoofing</u>**: Συνδέει τη διεύθυνση MAC του δράστη σε μια νόμιμη διεύθυνση IP μέσω παραποιημένων μηνυμάτων ARP. Χρησιμοποιείται συνήθως στην άρνηση εξυπηρέτησης (DoS) και στην επιθετικότητα man-in-the-middle.

- **<u>Διευθυνσιοδότηση διευθύνσεων IP</u>**: Αποκρύπτει την IP προέλευσης του εισβολέα. Χρησιμοποιείται συνήθως σε επιθέσεις DoS[21].



Spoofing Example [22]

Όσον αφορά αυτά τα κακόβουλα λογισμικά, πάντα θέμα της συζήτησης είναι οι πιθανοί τρόποι που έχει κάποιος στη διάθεσή του ώστε να τα αντιμετωπίσει. Ας το αναλύσουμε.

Ενώ δεν μπορεί να προληφθεί η πλαστογράφηση IP, μπορούν να ληφθούν μέτρα για να σταματήσουν τα παρωχημένα πακέτα από την διείσδυση ενός δικτύου. Μια πολύ κοινή άμυνα κατά της πλαστογραφίας είναι η το φιλτράρισμα εισόδου, η οποία περιγράφεται στο BCP38 (έγγραφο Best Common Practice). Το φίλτρο Ingress είναι μια μορφή φιλτραρίσματος πακέτων που συνήθως εφαρμόζεται σε μια συσκευή ακμής δικτύου η οποία εξετάζει τα εισερχόμενα πακέτα IP και εξετάζει τις κεφαλίδες πηγής τους. Εάν οι κεφαλίδες πηγών σε αυτά τα πακέτα δεν ταιριάζουν με την προέλευσή τους ή διαφορετικά φαίνονται ύποπτα, τα πακέτα απορρίπτονται**.** Ορισμένα δίκτυα θα εφαρμόσουν επίσης **το φιλτράρισμα εξόδου**, το οποίο εξετάζει τα πακέτα IP που εξέρχονται από το δίκτυο, εξασφαλίζοντας ότι τα πακέτα αυτά

έχουν νόμιμες κεφαλίδες πηγών για να εμποδίσουν κάποιον εντός του δικτύου να ξεκινήσει μια εξερχόμενη κακόβουλη επίθεση χρησιμοποιώντας spoofing IP[21].

Οι επιθέσεις τύπου "IP spoofing" είναι γενικά δύσκολο να εντοπιστούν, αφού η **πρώτη εντύπωση** είναι ότι η επίθεση έχει προέλθει από την πλαστή διεύθυνση. Η επαλήθευση συνήθως αργεί, επιτρέποντας στον hacker να δρα ανενόχλητος για κάποιο διάστημα. Η πιο επαρκής «**θεραπεία**» είναι η χρήση δρομολογητών που έχουν κατάλληλα διαμορφωθεί ώστε να αποτρέπουν είσοδο πακέτων από το εξωτερικό interface με εσωτερικές διευθύνσεις του δικτύου του (δρώντας ως φίλτρο εισόδου) [23].

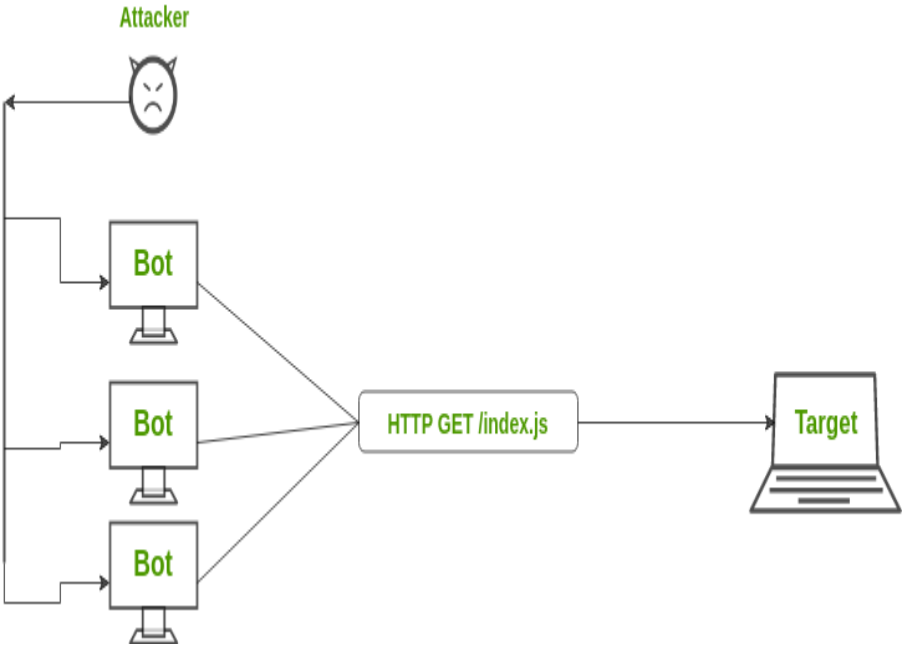
2.6. Κατανεμημένη Άρνηση Παροχής Υπηρεσιών (DDOS)

Η επίθεση Άρνησης Παροχής Υπηρεσιών (DoS, Denial of Service) είναι από τις πλέον χρησιμοποιούμενες επιθέσεις, καθώς καθιστούν εξαιρετικά δύσκολη την αντιμετώπισή τους. Ως σκοπός του επιτηθέμενου τίθεται η υπερφόρτωση μιας σελίδας με ανεπιθύμητο **traffic** (**συμφόρηση**) ώστε αυτή να τεθεί εκτός λειτουργίας και αυτός να πάρει στα χέρια του την λειτουργία της σελίδας. Ουσιαστικά πολλοί υπολογιστές ζητάνε **εξυπηρέτηση από μία σελίδα**, μέχρι που αυτές οι αιτήσεις για εξυπηρέτηση γίνονται πάρα πολλές και είναι αδύνατον να εξυπηρετηθούν. Έτσι το σύστημα καταρρέει.

Η επίθεση αυτή υλοποιείται από τον επιτηθέμενο ως εξής.

- Αρχικά χτίζει ένα δίκτυο από «μολυσμένες» μηχανές, υπολογιστές, το γνωστό **botnet**, μέσω αποστολής κακόβουλου λογισμικού χρησιμοποιώντας ανεπιθύμητη αλληλογραφία, ιστοσελίδες και μέσα κοινωνικής δικτύωσης (social media).

- Στη συνέχεια το botnet μπορεί να ελεγχεί και να **καθοδηγηθεί** από το δημιουργό του σαν στρατός ώστε να στείλει μια σαρωτική συμφόρηση (traffic), ακόμα και σε εκτός δικτύου (offline) σελίδες.



Botnet Example [25]

Οι διάφορες μορφές αυτού του είδους επίθεσης παρατίθονται παρακάτω:

1. **Επιθέσεις σύνδεσης TCP (TCP Connection Attacks)** – Κατάληψη συνδέσεων

Σε αυτές γίνεται προσπάθεια να χρησιμοποιηθούν όλες οι διαθέσιμες συνδέσεις με συσκευές υποδομής όπως ισορροπιστές φορτίου (**load-balancers**), firewalls και διακομιστές εφαρμογών (**application servers**). Ακόμη και οι συσκευές που είναι ικανές να διαχειριστούν καταστάσεις με εκατομμύρια κλήσεις/συνδέσεις μπορεί να μην τα καταφέρουν σε τέτοιες επιθέσεις.

2. **Ογκομετρικές Επιθέσεις (Volumetric Attacks)** – Χρήση του εύρους ζώνης

Σε αυτές γίνεται προσπάθεια να καταναλωθεί το εύρος ζώνης που είναι διαθέσιμο είτε εντός του δικτύου του στόχου/της υπηρεσίας ή μεταξύ του δικτύου/των υπηρεσιών στόχος και του υπόλοιπου διαδικτύου. Αυτές οι επιθέσεις είναι απλά για να προκαλέσουν κυκλοφοριακή συμφόρηση με τον όγκο των δεδομένων.

3. **Smurfs**

Αυτός ο τύπος επίθεσης χρησιμοποιεί μεγάλες ποσότητες στόχου επισκεψιμότητας του Ping Message Message Protocol (PMMP) σε μια διεύθυνση Broadcast Internet. Η διεύθυνση IP απάντησης είναι πλαστογραφημένη με εκείνη του θύματος που σκοπεύει. Όλες οι απαντήσεις αποστέλλονται στο θύμα αντί για το IP που χρησιμοποιείται για τους pings. Δεδομένου ότι μια ενιαία Διεύθυνση Broadcast Internet μπορεί να υποστηρίξει μέχρι και 255 κεντρικούς υπολογιστές, μια επίθεση smurf ενισχύει ένα μόνο ping 255 φορές. Το αποτέλεσμα αυτής είναι η **επιβράδυνση του δικτύου** σε σημείο όπου είναι αδύνατο να χρησιμοποιηθεί.

4. **Buffer Overflow (Υπερχείλιση των Buffer)**

Ένα buffer είναι μια προσωρινή θέση αποθήκευσης στη μνήμη RAM που χρησιμοποιείται για τη συγκράτηση δεδομένων έτσι ώστε η CPU να μπορεί να την χειριστεί πριν την επιστρέψει στο δίσκο. Τα buffer έχουν όριο μεγέθους. Αυτός ο τύπος επίθεσης φορτώνει το buffer με περισσότερα δεδομένα που μπορεί να κρατήσει. Αυτό προκαλεί υπερχείλιση του buffer και καταστροφή των δεδομένων που κατέχει. Ένα παράδειγμα μιας υπερχείλισης buffer είναι η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου με ονόματα αρχείων που έχουν 256 χαρακτήρες [26].

5. **Επιθέσεις σε Εφαρμογές (Application Attacks)** – Με στόχευση τις εφαρμογές

Σε αυτές γίνεται προσπάθεια να συντριβεί μια συγκεκριμένη πτυχή κάποιας εφαρμογής ή υπηρεσίας και μπορεί να είναι αποτελεσματικές, ακόμη και με πολύ λίγες επιτιθέμενες μηχανές, δημιουργώντας μόνο ένα χαμηλό ποσοστό κυκλοφορίας (καθιστώντας έτσι δύσκολο τον εντοπισμό τους και την λήψη μέτρων για την αντιμετώπισή τους) [24].

Ένας δημιουργός ενός **botnet** έχει τη δυνατότητα επίσης να πουλήσει αυτό το δίκτυο υπολογιστικής ισχύος και οι αγοραστές να το κατευθύνουν προς τους στόχους τους. Αυτό το φαινόμενο παίρνει τεράστιες διαστάσεις όταν οι σελίδες που δέχονται επίθεση είναι media και λόγω του μεγάλου πλήθους χρηστών που τις επισκέπτονται, οι επιτηθέμενοι μπορούν να επηρεάσουν την κοινή γνώμη με ψεύτικες ειδήσεις. Αντιλαμβανόμαστε, λοιπόν, πως το ζήτημα ενεπλέκεται και σε πολιτικές αντιπαλότητες. Χρησιμοποιώντας αυτές τις υπόγειες αγορές, ο καθένας μπορεί να πληρώσει μια αμοιβή για να φιμώσει τις ιστοσελίδες που διαφωνούν μαζί του ή να

διαταράξει τις online λειτουργίες ενός οργανισμού. Η επίθεση DDoS διάρκειας μιας εβδομάδας, ικανή να υπερφορτώσει την σύνδεση ενός μικρού οργανισμού, κοστίζει πολύ λίγα χρήματα στον επιτηθέμενο, άλλο ένα πλεονέκτημα της επίθεσης αυτής[27].

ΚΕΦΑΛΑΙΟ 3: ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

3.1. Κρυπτογραφία και ανάγκη για κρυπτογραφία

Η ανάγκη που υπάρχει για κρυπτογραφία από τα παλιά χρόνια είναι αρκετά προφανής και γνωστή διαισθητικά σε όλους. Για παράδειγμα, οι μεγάλοι στρατηγοί ήθελαν να έχουν τρόπους επικοινωνίας με τους αγγελιαφόρους τους ώστε να σταλθούν «μηνύματα» για έφοδο στα εχθρικά στρατεύματα, τα οποία όμως να μην μπορούν να γίνουν κατανοητά αν πέσουν στα χέρια κάποιου εχθρού. Έτσι έκανε τη πρώτη εμφάνισή της η έννοια της **κρυπτογραφίας** και μαζί της η λογική και οι βασικές αρχές αυτής. Δηλαδή, ότι ένα κείμενο – μήνυμα που αποστέλεται πρώτα κρυπτογραφείται και όταν ο παραλήπτης το λάβει, το αποκρυπτογραφεί δίνοντας νόημα στο «ανεξήγητο» πλέον αυτό μήνυμα. Βέβαια, οι τρόποι της (απο)κρυπτογράφισης πρέπει να είναι κοινοί για παραλήπτη και αποστολέα για την επιτυχή μεταφορά κάποια πληροφορίας.

Η λέξη κρυπτογραφία προέρχεται από τις ελληνικές λέξεις «κρυφή γνώση». Στο [4] ο **Tanembaum** υποστηρίζει, χαριτολογώντας, πως οι πιο σημαντικές ομάδες ανθρώπων που έχουν συνεισφέρει στην ύπαρξης της τέχνης της **κρυπτογραφίας** είναι ο στρατός, το διπλωματικό σώμα, όσοι τηρούν τα ημερολόγια και οι εραστές. Σαφώς και το σημαντικότερο ρόλο ανάμεσα σε αυτούς τον έχει ο στρατός. Η κρυπτογραφία υπήρχε και πριν την ύπαρξη των υπολογιστών, όμως ήταν εξαιρετικά επικίνδυνη, συχνά στο πεδίο της μάχης, και δύσκολη στη μετάβασή της από μέθοδο σε μέθοδο αφού έπρεπε να εκπαιδευτεί όλο το ανθρώπινο δυναμικό στη καινούργια μέθοδο εκ νέου.

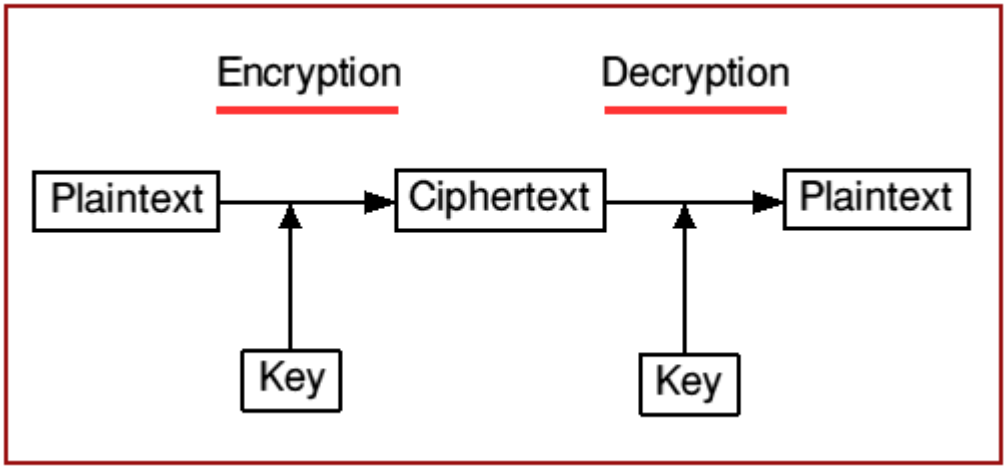
Ένας θεμελιώδης κανόνας της κρυπτογραφίας είναι ότι πρέπει να υποθέτουμε πως ο **κρυπταναλυτής** γνωρίζει τις μεθόδους που χρησιμοποιούνται για (απο)κρυπτογράφιση. Αναπόσπαστο κομμάτι της τέχνης αυτής είναι το λεγόμενο **κλειδί** (**key**), το οποίο ορίζεται ως ένα σύντομα αλφαριθμητικό που επιλέγει μια από τις πιθανές κρυπτογραφήσεις και μπορεί να αλλάζει όσο συχνά απαιτείται. Επομένως, έχουμε μια σταθερή, γνωστή, δημόσια μέθοδο που παραμετροποιείται με ένα μυστικό, εύκολα μεταβαλλόμενο κλειδί.

> **Αρχή του Kerchkoff (Kerchkoff's principle):** Όλοι οι αλγόριθμοι πρέπει να είναι δημόσιοι, μόνο τα κλειδιά πρέπει είναι μυστικά.

3.2. Είδη Κρυπτογραφίας

3.2.1. Συμμετρική Κρυπτογραφία

Η **Συμμετρική Κρυπτογραφία** (συμβατική) χρησιμοποιεί ένα κοινό **κλειδί** μεταξύ πηγής (**αποστολέα**) και πομπού (**παραλήπτη**) για την κωδικοποίηση ενός μηνύματος μεταξύ αυτών. Η εισαγωγή της έννοιας του κλειδιού γίνεται με κύριο σκοπό την αποκρυπτογράφιση του μηνύματος σε επόμενο στάδιο. Το κοινό κλειδί δεν πρέπει να σταλθεί ως ξεχωριστό μήνυμα καθώς μπορεί να πέσει θύμα υποκλοπής από κάποιον επιτήδειο, επομένως γίνεται κομμάτι του ίδιου του μηνύματος και κωδικοποιείται και αυτό με τον ίδιο τρόπο όπως το μήνυμα. Με αυτό το τρόπο ο παραλήπτης μπορεί να μάθει το κλειδί του αποστολέα ώστε να κάνει τη σωστή **αποκρυπτογράφιση**. Επομένως, το κείμενο σε αρχικό στάδιο είναι στη μορφή plain text, ύστερα **κρυπτογραφείται** με το κλειδί και μετατρέπεται σε κρυπτογραφημένο **(cyphertext),** μετά ξανά χρησιμοποιείται το κλειδί και το κείμενο επιστρέφει στην αρχική του μορφή. Αυτή είναι και η διαδιασία της **Κρυπτογράφισης** και **Αποκρυπτογράφισης** ενός κειμένου - μηνύματος.



Encryption and Decryption of plaintext [28]

Η συμμετρική Κρυπτογραφία υλοποιείται από δύο γνωστούς αλγορίθμους τον DES και τον AES.

DES: πρόκειται για block cipher αλγόριθμο συμμετρικού κλειδιού όπου διαχειρίζεται 2 παραμέτρους, το μέγεθος του κλειδιού, συνήθως 64 bits και το μέγεθος του μπλοκ, επίσης 64 bits. Επαναλαμβάνονται 16 στάδια επεξεργασίας πληροφορίας **(κύκλοι)**. Η λογική πίσω από τον αλγόριθμο είναι το σταδιακό «ανακάτεμα» των bits του κλειδιού, ώστε το τελικό μήνυμα να εξαρτάται ολόκληρο από το κλειδί. Ουσιαστηκά τα μισά bit του μηνύματος περνάνε από πύλη **XOR** με τα bit του κλειδιού για 16 γύρους, πράγμα που τα κάνει πολύ πολύπλοκα ώστε να αναλυθούν χωρίς γνώση του κλειδιού ή του μηνύματος.

Παρά την πολυπλοκότητα που φαίνεται να έχει ο **DES**, στην πραγματικότητα έχει πολύ μικρό κλειδί και έτσι είναι ευάλωτος σε επιθέσεις και επομένως ακατάλλλος για εφαρμογές διαδικτύου. Το 1998 κατασκευάστηκε υπολογιστής που μόνος του έσπασε τον DES μέσα σε 5 μέρες μόνο, μέγεθος υπέρογκο για την εποχή και την εξέλιξη που είχαν μέχρι τότε οι υπολογιστές[1].

AES: Η αδυναμία του DES οδήγησε στην δημιουργία του AES, ενός πιο γρήγορου και ασφαλούς αλγορίθμου κρυπτογράφισης. Εδώ τα μπλοκ έχουν μέγεθος 128 bits και το κλειδί φτάνει τα 256 ή και 512 bits, ενώ η διαδικασία ολοκληρώνεται

μετά από 14 ή 16 γύρους, ανάλογα το μέγεθους που έχει το κλειδί. Ο AES τοποθετεί το κείμενο σε ένα πίνακα τον οποίο επεξεργάζεται σε κάθε βήμα με XOR.

Αυτός ο αλγόριθμος, όπως και πολλοί άλλοι που χρησιμοποιούνται σήμερα, είναι ασφαλής έναντι όλων των γνωστών μεθόδων κρυπτοανάλυσης. Ειδικότερα, δεν υπάρχει γνωστή μέθοδος πυρόλυσης που να είναι πιο αποτελεσματική από την «**ωμή βία**», δηλαδή να δοκιμάζει όλα τα πιθανά κλειδιά μέχρι να βρεθεί το σωστό, το οποίο με τη σειρά του δεν είναι εφικτό με οποιαδήποτε γνωστή τεχνολογία. Αυτό καθιστά τον κωδικό ισχυρό και μας επιτρέπει να λάβουμε μια ποσοτική εκτίμηση της ισχύος του. Γενικότερα, η αποτροπή της δυνατότητας των αλγορίθμων ωμής βίας από την εύρεση της κρυπτογραφίας είναι μείζον ζήτημα στην Ασφάλεια των Υπολογιστών και των Δικτύων[28].

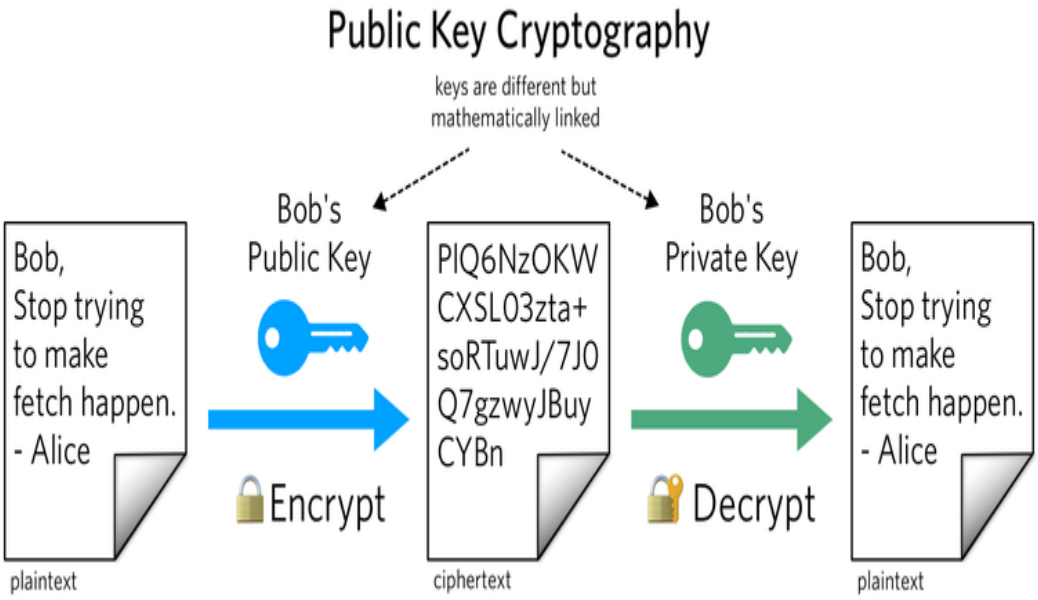
3.2.2. Κρυπτογραφία Δημόσιου Κλειδιού

Η Κρυπτογραφία Δημόσιου Κλειδιού ή **Ασύμμετρη Κρυπτογραφία** γίνεται με τη χρήση **2 κλειδιών** για την κρυπτογράφισης και την αποκρυπτογράφιση ενός μηνύματος. Σε αυτό το τύπο κρυπτογραφίας ο αποστολέας ορίζει ένα δημόσιο κλειδί το οποίο θα χρησιμοποιήσει όποιος θέλει να λάβει μήνυμα από αυτόν. Αρχικά, ο αποστολέας χρησιμοποιεί ένα ιδιωτικό κλειδί για την κρυπτογράφιση και ύστερα ο παραλήπτης το αποκρυπτογραφεί με το δημόσιο κλειδί που έχει οριστεί. Η ασσύμετρη κρυπτογραφία παρέχει εμπιστευτικότητα και εγγύηση με την έννοια ότι ο παραλήπτης χρειάζεται εγγύηση για την ταυτοποίηση του αποστολέα.

Η συμμετρική κρυπτογραφία έχει ένα σοβαρό **μειονέκτημα**, γνωστό ως το βασικό πρόβλημα διανομής. Δεδομένου ότι το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση, δύο μέρη που επιθυμούν να επικοινωνήσουν με ασφάλεια πρέπει να υιοθετήσουν με κάποιο τρόπο ένα αμοιβαία συμφωνημένο κλειδί πριν ανταλλάξουν μηνύματα. Φυσικά, αυτό είναι δυνατό αν συναντηθούν εκ των προτέρων αυτοπροσώπως, πράγμα οριακά αδύνατο σε επίπεδο διαδικτύου. Όλες οι διαθέσιμες μορφές ηλεκτρονικής επικοινωνίας μπορούν να παρεμποδιστούν από τους ηλεκτρονικούς υπολογιστές. Εάν τα δύο μέρη είχαν κάποιο ασφαλές κανάλι επικοινωνίας για να ανταλλάξουν ένα **μυστικό κλειδί**, θα μπορούσαν επίσης να το χρησιμοποιήσουν για να ανταλλάξουν το ίδιο το μήνυμα.

RSA: Ο αλγόριθμος αυτός υλοποιεί την ασύμετρη κρυπτογραφία. Η ιδέα του RSA βασίζεται στο γεγονός ότι είναι δύσκολο να παραγοντοποιηθεί ένας μεγάλος ακέραιος αριθμός. Το δημόσιο κλειδί αποτελείται από δύο αριθμούς όπου ένας αριθμός είναι πολλαπλασιασμός δύο μεγάλων πρώτων αριθμών. Και το ιδιωτικό κλειδί προέρχεται επίσης από τους ίδιους δύο πρώτους αριθμούς. Έτσι, αν κάποιος μπορεί να παραγοντοποιήσει τον μεγάλο αριθμό, το ιδιωτικό κλειδί παραβιάζεται. Επομένως, η αντοχή κρυπτογράφησης βρίσκεται **εξ ολοκλήρου στο μέγεθος του κλειδιού** και αν διπλασιάσουμε ή τριπλασιάσουμε το μέγεθος του κλειδιού, η δύναμη της κρυπτογράφησης αυξάνεται εκθετικά. Τα κλειδιά RSA μπορούν να είναι συνήθως 1024 ή 2048 bit, αλλά οι ειδικοί πιστεύουν ότι τα κλειδιά 1024 bit θα μπορούσαν να σπάσουν στο εγγύς μέλλον. Αλλά μέχρι τώρα φαίνεται να είναι ένα ανέφικτο έργο[29].

- Ένας πελάτης (για παράδειγμα πρόγραμμα περιήγησης) στέλνει το δημόσιο κλειδί του στο διακομιστή και ζητά κάποια δεδομένα.
- Ο διακομιστής κρυπτογραφεί τα δεδομένα χρησιμοποιώντας το δημόσιο κλειδί του πελάτη και αποστέλλει τα κρυπτογραφημένα δεδομένα.
- Ο πελάτης λαμβάνει αυτά τα δεδομένα και το αποκρυπτογραφεί.



Public key cryptography [29]

Ο RSA λειτουργεί πιο αναλυτικά ως εξής.

- Διαλέγουμε 2 μεγάλους πρώτους αριθμούς p, q (τουλάχιστον 512 bits) και το γινόμενό τους το ονομάζουμε **n=p*q.**
- Στη συνέχεια διαλέγουμε 1 ακέραιο αριθμό e, έτσι ώστε με τον αριθμό **(p-1)*(q-1)** να είναι σχετικά πρώτοι, δηλαδή να έχουν μέγιστο κοινό διαιρέτη τον αριθμό 1.
- Στη συνέχεια διαλέγουμε έναν αριθμό d τέτοιον ώστε να ισχύει η σχέση**: e*d = 1 mod (p-1)*(q-1).**
- Συχνά χρησιμοποιείται ο πρώτος αριθμός **e=65537** γιατί απλοποιεί τους υπολογισμούς κατά την κρυπτογράφηση
- Το **δημόσιο** κλειδί είναι το **(e,n)**
- Το **ιδιωτικό** κλειδί είναι το **(d,n)**
- Η **κρυπτογράφιση** του μηνύματος P γίνεται με το δημόσιο κλειδί που είναι γνωστό σε όλους και έχουμε

$$\mathbf{C = P^e \bmod n}$$

- Η **αποκρυπτογράφιση** του μηνύματος C γίνεται με το ιδιωτικό κλειδί και έχουμε

$$\mathbf{P = C^d \bmod n}$$

Όλοι γνωρίζουν τα (e,n) , αλλά κανείς τα d,q,p και για την έυρεση του d ώστε να γίνει η αποκρυπτογράφηση χρειάζεται η παραγοντοποίηση του n[1].

3.3. Ψηφιακές Υπογραφές (Digital Singatures)

Μια ψηφιακή υπογραφή δεν είναι τίποτα άλλο παρά μια υπογραφή για ένα αρχείο (ψηφιακό). Η «συμβατική» υπογραφή, στον φυσικό κόσμο, είναι ένας τρόπος πιστοποίησης του κατόχου ενός εγγράφου ή υποδηλώνει πως κάποιος συμφωνεί με το συγκεκριμένο έγγραφο, για παράδειγμα, μια συμφωνία με μία τράπεζα. Προκύπτουν, λοιπόν, **ανάγκες** κατά την υπογραφή των αρχείων, όπως το να μην μπορεί να πλαστογραφηθεί από κάποιον επιτήδειο τρίτο που προσπαθεί να κατευθύνει υπέρ του το συγκεκριμένο έγγραφο ή θέλει να εξαπατήσει κάποιον βάζοντας την υπογραφή αυτού σε αντίστοιχο αρχείο[3].

Ο λόγος που οι ψηφιακές υπογραφές είναι σημαντικές αποτυπώνεται φανερά στην εποχή που διανύουμε, μια εποχή κατά την οποία αρχεία αποστέλονται και λαμβάνοντας αδιάλειπτα μεταξύ μηχανημάτων σε όλον το κόσμο. Οι ψηφιακές υπογραφές προσφέρουν 3 πολύ σημαντικά προνόμοια σε ένα υπογεγραμμένο αρχείο.

1. **Αυθεντικοποίηση:** Προσδίδει στον παραλήπτη ένα λόγο για να πιστέψει ότι το μήνυμα που έλαβε, στάλθηκε πράγματι από αυτόν που ισχυρίζεται ότι είναι ο αποστολέας.

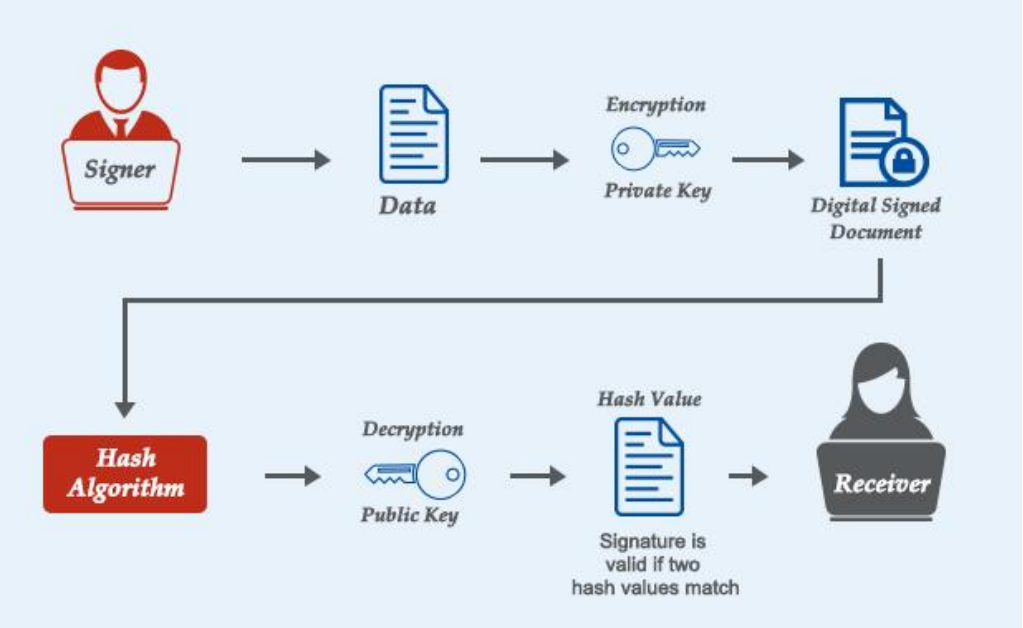
2. **Μη-απόρριψη**: Δεν μπορεί κάποιος που έχει στείλει ένα αρχείο να αρνηθεί ότι το έστειλε αργότερα.

3. **Ακεραιότητα:** Διαβεβαιώνεται πως το μήνυμα δεν τροποποιήθηκε κατά την μεταβίβασή του.

Ας αναλύσουμε την λειτουργία της ψηφιακής υπογραφής

Όταν ένας **υπογράφοντας** υπογράφει ηλεκτρονικά ένα έγγραφο, η υπογραφή δημιουργείται χρησιμοποιώντας το **ιδιωτικό** κλειδί του υπογράφοντος, το οποίο διατηρείται πάντα ασφαλώς από τον υπογράφοντα. Ο μαθηματικός αλγόριθμος λειτουργεί ως ένας κρυπτογραφημένος κώδικας, δημιουργώντας δεδομένα που ταιριάζουν με το υπογεγραμμένο έγγραφο, που ονομάζεται **hash**, και κρυπτογραφεί τα δεδομένα αυτά. Τα κρυπτογραφημένα δεδομένα που προκύπτουν είναι η **ψηφιακή υπογραφή**. Η υπογραφή σημειώνεται επίσης με την **ώρα υπογραφής** του εγγράφου. Αν το έγγραφο αλλάξει μετά την υπογραφή, η ψηφιακή υπογραφή ακυρώνεται.

Για παράδειγμα, η Alice υπογράφει μια συμφωνία για την πώληση μιας κατοικίας χρησιμοποιώντας το ιδιωτικό της κλειδί. Ο αγοραστής παραλαμβάνει το έγγραφο. Ο αγοραστής που λαμβάνει το έγγραφο λαμβάνει επίσης αντίγραφο του δημόσιου κλειδιού της Alice. Εάν το δημόσιο κλειδί δεν μπορεί να από-κρυπτογραφήσει την υπογραφή (μέσω του κρυπτογράφου, ο οποίος δημιούργησε τα κλειδιά), σημαίνει ότι η υπογραφή δεν είναι της Alice ή έχει αλλάξει από τότε που υπογράφηκε. Η υπογραφή στη συνέχεια θεωρείται άκυρη[31].



Digital Signature Procedure [32]

Η αύξηση των περιστατικών **παραβίασης δεδομένων** προκάλεσε σημαντική ανοδική τάση όσον αφορά την αποδοχή των ψηφιακών υπογραφών. Πρόσφατη έρευνα που πραγματοποιήθηκε από την Credence Research Inc. δείχνει ότι η παγκόσμια αγορά Digital Signature αυξάνεται με εκπληκτική **CAGR** από 24,2% από το 2017 έως το 2025. Επιπλέον, σε πολλές χώρες, οι ψηφιακές υπογραφές είναι ισοδύναμες με τις χειρόγραφες υπογραφές. Για παράδειγμα, η αμερικανική κυβέρνηση επικυρώνει τις ψηφιακές εκδόσεις εγγράφων μέσω ψηφιακών υπογραφών[33].

ΚΕΦΑΛΑΙΟ 4: ΛΕΙΤΟΥΡΓΙΚΗ ΑΣΦΑΛΕΙΑ

4.1. Ορισμός και ανάγκη

Όπως και στο φυσικό κόσμο έτσι και στο κόσμο του διαδικτύου η ασφάλεια, όπως παρουσιάσαμε και παραπάνω, είναι μείζον ζήτημα. Όπως σε ένα κάστρο της αρχαίοτητας υπήρχε μία πόρτα, «κερκόπορτα», από την οποία εισέρχονταν και εξέρχονταν αγαθά καθώς και άνρθωποι, και γινόταν όλος ο έλεγχος, έτσι σε μια εταιρεία για παράδειγμα πρέπει να ελέγχεται ποιος θα έχει πρόσβαση στους πόρους του δικτύου και ταυτόχρονα, πολύ πιο εξονυχιτστικά, το σε ποιόν απαγορεύεται. Γίνεται έτσι ένας διαχωρισμός μεταξύ «καλών» και «κακών» χρηστών, στους οποίους θέλουμε να παρέχουμε αντίστοιχες δυνατότητες ή μη. Ως λειτουργική ασφάλεια μπορούμε να ορίσουμε τον **έλεγχο** την κίνησης **εισόδου** και **εξόδου** στο δίκτυο, την **καταγραφή**, **απόρριψη** και/ή **προώθηση** συσκευών γνωστών ως **firewalls** (τοίχοι προστασίας), συστήματα **ανίχνευσης** παρείσφρησης και συστήματα **αποτροπής** παρείσφρησης.

4.2. Firewalls (Τείχοι Προστασίας)

Πριν από τα τείχη προστασίας, η ασφάλεια δικτύου πραγματοποιήθηκε από **λίστες ελέγχου πρόσβασης** (ACL) που διαμένουν σε δρομολογητές. Οι ACL είναι κανόνες που καθορίζουν κατά πόσο η πρόσβαση στο δίκτυο θα πρέπει να χορηγείται ή να απαγορεύεται σε συγκεκριμένη διεύθυνση IP.

Αλλά οι **ACL** δεν μπορούν να καθορίσουν τη φύση του πακέτου που εμποδίζει. Επίσης, η ACL από μόνη της δεν έχει την ικανότητα να κρατήσει απειλές έξω από το δίκτυο. Ως εκ τούτου, εισήχθη το Firewall[34].

Τα firewalls (τείχη προστασίας) είναι ένας συνδυασμός **υλικού** και **λογισμικού** που απομονώνει το εσωτερικό δίκτυο ενός οργανισμού από το υπόλοιπο Διαδίκτυο επιτρέποντας σε κάποια πακέτα να εισέρχονται σε αυτό και μπλοκάροντας τα υπόλοιπα. Ένα firewall επιτρέπει σε ένα διαχειριστεί να ελέγχει την προσπέλαση ανάμεσα στον έξω κόσμο και στους **πόρους** μέσα στο διαχειριζόμενο δίκτυο, προσέχοντας τη ροή προς και από αυτούς τους πόρους[3].

4.2.1. Δυνατότητες-Στόχοι

- **Filtering**

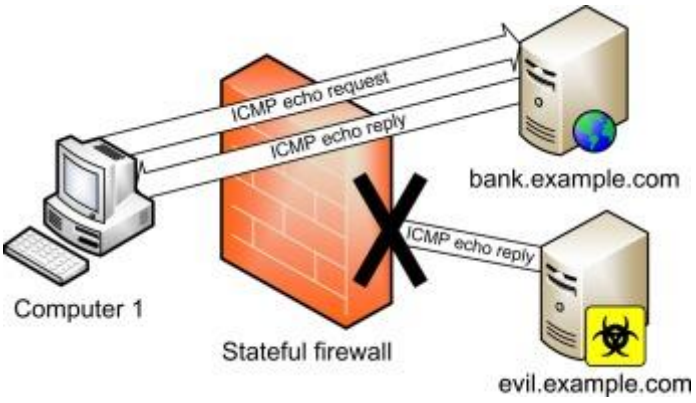
Ο πρωταρχικός σκοπός ενός τείχους προστασίας είναι το **filtering** ή αλλιώς **φιλτράρισμα πακέτων**. Όταν ένας υπολογιστής στέλνει ένα αίτημα μέσω του Διαδικτύου, παίρνει τη μορφή μικρών **πακέτων δεδομένων**, τα οποία ταξιδεύουν μέσω του δικτύου προς τον προορισμό τους. Ο διακομιστής προορισμού ανταποκρίνεται με τα δικά του πακέτα δεδομένων, τα οποία επιστρέφουν κατά μήκος της ίδιας διαδρομής. Ένα τείχος προστασίας παρακολουθεί κάθε πακέτο που περνά μέσα από αυτό, λαμβάνοντας υπόψη την πηγή, τον προορισμό του και τον τύπο δεδομένων που περιέχει και συγκρίνει αυτές τις πληροφορίες με το εσωτερικό του σύνολο **κανόνων**. Εάν το τείχος προστασίας εντοπίσει ότι το πακέτο δεν είναι **εξουσιοδοτημένο**, απορρίπτει τα δεδομένα. Συνήθως, τα τείχη προστασίας επιτρέπουν την κυκλοφορία από κοινά προγράμματα όπως προγράμματα ηλεκτρονικού ταχυδρομείου ή προγράμματα περιήγησης στο Web, ενώ απορρίπτουν τα περισσότερα εισερχόμενα αιτήματα.

- **Logging**

Μια άλλη σημαντική πτυχή ενός τείχους προστασίας είναι η ικανότητά του να καταγράφει κάθε κίνηση που περνά μέσα από αυτό. Καταγράφοντας τις πληροφορίες από πακέτα που περνούν ή που απορρίπτονται, μπορεί να σας δώσει μια σαφή εικόνα του είδους κίνησης που βιώνει το σύστημά σας. Αυτό μπορεί να είναι πολύτιμο για τον **προσδιορισμό της πηγής** μιας εξωτερικής επίθεσης, αλλά χρησιμοποείται επίσης από εταιρείες στη παρακολούθηση των δραστηριοτήτων των υπαλλήλων τους online για να αποτρέψουν τη χαμένη παραγωγικότητα.

- **Internal Threats**

Ενώ ο πρωταρχικός στόχος ενός τείχους προστασίας είναι να κρατήσει τους επιτιθέμενους έξω, εξυπηρετεί επίσης έναν πολύτιμο σκοπό με την παρακολούθηση **εξερχόμενων συνδέσεων**. Πολλοί τύποι κακόβουλου λογισμικού στέλνουν ένα μήνυμα μόλις αναλάβουν ένα σύστημα, επιτρέποντας στον δημιουργό του να ενεργοποιήσει συγκεκριμένες ενέργειες ή ακόμα και να ελέγξει τον υπολογιστή εξ αποστάσεως. Ένα τείχος προστασίας μπορεί να σας ειδοποιήσει όταν ένα άγνωστο πρόγραμμα επιχειρεί να επιτεθεί, προειδοποιώντας τον χρήστη για πιθανή λοίμωξη κακόβουλου λογισμικού και επιτρέποντάς τον να τον απενεργοποιήσετε προτού προκαλέσει σημαντική ζημιά στο δίκτυό του. Ο αποκλεισμός από μια επίθεση κακόβουλου λογισμικού προτού ενεργοποιηθεί προστατεύσει ζωτικά δεδομένα της εταιρείας και εξοικονομήσει το κόστος για την συντήρηση από ζημιές του λογισμικού[35].



Firewall Example [36]

4.2.2. Είδη firewalls

- **Proxy firewall**

Ένας πρώιμος τύπος τείχους προστασίας, ένα τείχος προστασίας μεσολάβησης χρησιμεύει ως **πύλη** από ένα δίκτυο σε άλλο για μια συγκεκριμένη εφαρμογή. Οι διακομιστές μεσολάβησης μπορούν να παρέχουν πρόσθετες λειτουργίες όπως η προσωρινή αποθήκευση περιεχομένου και η ασφάλεια, εμποδίζοντας τις απευθείας συνδέσεις εκτός δικτύου. Ωστόσο, αυτό μπορεί επίσης να επηρεάσει τις δυνατότητες διεκπεραίωσης και τις εφαρμογές που μπορούν να υποστηρίξουν.

- **Stateful inspection firewall**

Το πλέον "παραδοσιακό" τείχος προστασίας, ένα κρατικό τείχος επιθεώρησης επιτρέπει ή αποκλείει την κίνηση με βάση την κατάσταση, τη θύρα και το πρωτόκολλο. Παρακολουθεί όλη τη δραστηριότητα από το άνοιγμα μιας σύνδεσης μέχρι να κλείσει. Οι αποφάσεις φιλτραρίσματος γίνονται με βάση και τους κανόνες που ορίζονται από τον διαχειριστή καθώς και το πλαίσιο, το οποίο αναφέρεται στη χρήση πληροφοριών από προηγούμενες συνδέσεις και πακέτα που ανήκουν στην ίδια σύνδεση.

- **Unified threat management (UTM) firewall**

Μια συσκευή UTM συνδυάζει συνήθως, με έναν χαλαρά συζευγμένο τρόπο, τις λειτουργίες ενός κρατικού τείχους επιθεώρησης με πρόληψη εισβολής και antivirus. Μπορεί επίσης να περιλαμβάνει πρόσθετες υπηρεσίες και συχνά διαχείριση cloud. Τα UTM επικεντρώνονται στην απλότητα και την **ευκολία χρήσης**[37].

4.3. Antiviruses (Αντιβιωτικά)

Το **antivirus** είναι ένα πρόγραμμα που έχει σχεδιαστεί για την προστασία των χρηστών και των συσκευών τους από δυνητικούς επιβλαβείς **ιούς** υπολογιστών, **κακόβουλο λογισμικό** και άλλες **κυβερνοαπειλές**. Είναι σημαντικό τόσο οι επιχειρήσεις όσο και οι οικιακοί χρήστες να προστατεύονται από ιούς και άλλες επιθέσεις που θα μπορούσαν να διαταράξουν, να επιβραδύνουν, ακόμα και να καταστρέψουν τη συσκευή τους. Το antivirus είναι το βασικό εργαλείο που βοηθάει στην ασφαλή και ομαλή λειτουργία του υπολογιστή και των άλλων συσκευών.

Τα διάφορα antivirus διαφέρουν σε ότι αφορά τις μεθόδους τους, ωστόσο όλα έχουν τον ίδιο στόχο: **να προστατέψουν τις συσκευές.**

Αφού το antivirus εγκατασταθεί, λειτουργεί στο παρασκήνιο, εκτελώντας τακτικές σαρώσεις και ελέγχους στις συσκευές σας, παρακολουθώντας τα αρχεία, τα προγράμματα και τις ιστοσελίδες για πιθανές απειλές. Το antivirus **ανιχνεύει** οποιαδήποτε κακόβουλη ή απειλητική συμπεριφορά θα μπορούσε να θεωρηθεί ως μορφή κακόβουλου λογισμικού, αφαιρώντας το από τη συσκευή σας όσο το δυνατόν γρηγορότερα, ενώ εργάζεται για να αποτρέψει μελλοντικές επιθέσεις.

Πως λειτουργεί το antivirus

- **Ενεργώντας** ως **ασπίδα** κατά των ιών και των κακόβουλων προγραμμάτων. Το antivirus εντοπίζει, αφαιρεί και αποτρέπει τις **κυβερνοαπειλές** από το να προκαλέσουν βλάβη.
- **Προστατεύοντάς** σας σε όλες τις online δραστηριότητες σας. Είτε πραγματοποιείτε online **τραπεζικές συναλλαγές**, αγορές, είτε εργάζεστε, τα προσωπικά στοιχεία και τα δεδομένα σας παραμένουν ασφαλή.
- **Διασφαλίζοντας** online προστασία ακόμη και σε κινητά και tablet.
- **Στοχεύοντας** συγκεκριμένο **λογισμικό** που κινδυνεύει [38].

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]https://eclass.upatras.gr/modules/document/index.php?course=EE678&openDir=/5a014e94eMoa

[2] https://www.glavas.gr/pages.asp?pid=28&subid=30

[3]https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

[4] Δίκτυα Υπολογιστών, Tanenbaum, Wetherall, Πέμπτη Έκδοση, 2011

[5] Δικτύωση Υπολογιστών, Kurose, Ross, Έβδομη Έκδοση, 2017

[6] https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/

[7] https://www.eset.com/gr/trojan-horse/

[8] https://enterprise.comodo.com/what-is-the-trojan-horse-virus.php

[9] https://www.malwarebytes.com/trojan/

[10]https://www.safetydetectives.com/blog/what-is-a-computer-worm-tips-to-protect-your-computer-in/

[11] https://tools.cisco.com/security/center/resources/virus_differences#4

[13]https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms

[12]https://fossbytes.com/difference-viruses-worms-ransomware-trojans-bots-malware-spyware-etc/

[13]https://antivirus.comodo.com/blog/computer-safety/what-is-virus-and-its-definition/

[14] http://ivanlef0u.fr/repo/madchat/vxdevl/vdat/epfutur3.htm

[15] https://en.wikipedia.org/wiki/Malware

[16] https://www.youtube.com/watch?v=DF8Ka8Jh0BQ

[17]https://securityintelligence.com/wp-content/uploads/2018/08/si-8-21-19-news-article2x-630x330.jpg

[18] https://el.wikipedia.org/wiki/Ransomware

[19]https://www.eset.com/gr/ransomware/

[20]https://searchsecurity.techtarget.com/definition/IP-spoofing

[21]https://www.imperva.com/learn/application-security/ip-spoofing/

[22]https://www.iplocation.net/ip-spoofing

[23]https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

[24] https://www.cloudwards.net/what-is-a-botnet/

[25]http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/136/tlp_000409.pdf?sequence=1

[26]https://privacy.ellak.gr/2017/04/24/ti-ine-mia-epithesi-ddos-mia-isagogi-stis-epithesis-distributed-denial-of-service-ddos/

[27]https://www.geeksforgeeks.org/denial-of-service-ddos-attack/

[28] http://www.queen.clara.net/pgp/art6.html

[29] https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

[30] https://www.twilio.com/blog/what-is-public-key-cryptography

[31]https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq

[32]https://comodosslstore.com/blog/what-is-digital-signature-how-does-it-work.html

[33]https://comodosslstore.com/blog/what-is-digital-signature-how-does-it-work.html

[34]https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

[35]https://smallbusiness.chron.com/purpose-firewall-53858.html

[36]https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~types-of-firewalls

[37]https://www.sciencedirect.com/topics/computer-science/stateful-firewall

[38] https://www.eset.com/gr/antivirus-software/