ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Υλοποίηση Συστήματος Ανίχνευσης Εισβολών σε Περιβάλλον Android για Ασύρματα Δίκτυα Πρόσβασης

του

Ράδογλου-Γραμματίκη Ι. Παναγιώτη

Επιβλέπων Καθηγητής: Δρ. Παναγιώτης Σαρηγιαννίδης

Κοζάνη, Νοέμβριος 2016

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Υλοποίηση Συστήματος Ανίχνευσης Εισβολών σε Περιβάλλον Android για Ασύρματα Δίκτυα Πρόσβασης

του

Ράδογλου-Γραμματίκη Ι. Παναγιώτη

Επιβλέπων Καθηγητής: Δρ. Παναγιώτης Σαρηγιαννίδης

Εξεταστική Επιτροπή

Επίκουρος Καθηγητής: Δρ. Παναγιώτης Σαρηγιαννίδης

Επίκουρος Καθηγητής: Δρ. Θεόδωρος Ζυγκιρίδης

Κοζάνη, Νοέμβριος 2016

Ράδογλου-Γραμματίκης Ι. Παναγιώτης

Διπλωματούχος Μηχανικός Πληροφορικής και Τηλεπικοινωνιών Π.Δ.Μ.

Περίληψη

Τα τελευταία χρόνια οι έξυπνες κινητές συσκευές έχουν γνωρίσει ιδιαίτερα σημαντική πρόοδο τόσο σε επίπεδο υλικού, όσο και υπηρεσιών, με αποτέλεσμα η χρήση τους να αναπτύσσεται με ραγδαία ταχύτητα. Δεν αποτελεί υπερβολή, η παρατήρηση, ότι πλέον οι κινητές συσκευές αποτελούν αναπόσπαστο τμήμα της σημερινής καθημερινότητας. Ωστόσο παράλληλα με την ανάπτυξη των δυνατοτήτων τους, ο όγκος των πληροφοριών που επεξεργάζονται αποτελεί στόχο ενός ολοένα και αυξανόμενου πλήθους εισβολών κατά της ασφάλειάς τους. Παρά το πλήθος των τεχνικών ασφάλειας που ενσωματώνουν τα σύγχρονα λειτουργικά συστήματα κινητής υπολογιστικής, όπως οι μηχανισμοί ελέγχου προσπέλασης χρηστών και οι τεχνικές ετεροχρονισμένης αυθεντικοποίησης, δεν παρέχονται λύσεις προστασίας από άγνωστους τύπους εισβολών.

Συγκεκριμένα, η καθιέρωση των λειτουργικών συστημάτων Android και iOS στις κινητές συσκευές και η συνεχής ανάπτυξη κακόβουλων λογισμικών, ειδικά κατασκευασμένων για τα συγκεκριμένα λειτουργικά συστήματα, θέτουν νέα δεδομένα στην ανάπτυξη λύσεων ασφάλειας για τους χρήστες των κινητών συσκευών. Συμπερασματικά, κρίνεται απαραίτητη η ανάπτυξη αποδοτικότερων μηχανισμών ασφάλειας, ειδικά κατασκευασμένων για συστήματα κινητής υπολογιστικής.

Έξυπνοι μηχανισμοί, οι οποίοι μπορούν να ενισχύσουν σημαντικά την ασφάλεια μίας κινητής συσκευής, αποτελούν τα συστήματα ανίχνευσης εισβολών. Οι συγκεκριμένοι μηχανισμοί, εκτός από την παροχή υπηρεσιών για την αντιμετώπιση γνωστών επιθέσεων, περιλαμβάνουν τεχνικές για την αναγνώριση άγνωστου τύπου εισβολών. Ωστόσο παρά τη σημαντική ανάπτυξη των συστημάτων ανίχνευσης εισβολών σε σταθερά πληροφοριακά συστήματα, η έρευνα για την προσαρμογή τους σε κινητές συσκευές είναι αρκετά περιορισμένη.

Ο κύριος στόχος της συγκεκριμένης διπλωματικής εργασίας, αποτελεί η ανάπτυξη ενός συστήματος ανίχνευσης εισβολών για κινητές συσκευές με λειτουργικό σύστημα Android. Συγκεκριμένα η εφαρμογή που υλοποιήθηκε, στηρίζεται στη διαδικασία παρακολούθησης των δικτυακών ροών και στην ανάπτυξη ενός τεχνητού νευρωνικού δικτύου, εκπαιδευμένο κατάλληλα να αναγνωρίζει τις ύποπτες δικτυακές ροές, με βάση τα χαρακτηριστικά τους.

Λέξεις Κλειδιά: συστήματα ανίχνευσης εισβολών, ασφάλεια, δικτυακές ροές, κινητές συσκευές, Android, τεχνητά νευρωνικά δίκτυα

Abstract

Mobile devices have been rapidly evolved and experienced a vast popularity over the last few years. However, along with the expansion of their potential, the size of information that is processed is a potential target of an ever-increasing number of security threats. Despite the number of the security techniques that modern operating mobile computing systems incorporate, such as access control and (post) authentication techniques, protection solutions towards unknown and undefined threats, are not provided.

More specifically, new security gaps are identified in, yet powerful, operating systems, such as Android and iOS, capable of allowing to attackers of compromising the mobile devices and the stored data. This is attached to the fact that the growth of the mobile applications come at the cost of the mobile malware. Given that the malware traffic stream may comprise a serious threat in the near future, the research community seeks for solutions to cope with these newly introduced risks.

Intrusion detection systems are intelligent mechanisms that can greatly improve the security of a mobile device. These mechanisms provide services for addressing known attacks but also they include techniques for identifying unknown threat intrusions. However, despite the significant development of intrusion detection systems in usual information systems, the development of such detection mechanisms in mobile operating systems is limited.

Given the above remarks, the main objective of this thesis is the development of an intrusion detection system for mobile devices designed for the Android operating system. The application was implemented based on the monitoring process of NetFlows and the development of an artificial neural network, which is trained to identify properly suspect NetFlows based on their characteristics.

Keywords: intrusion detection system, security, NetFlows, mobile, Android, artificial neural networks

Ευχαριστίες

Η παρούσα διπλωματική εργασία αποτελεί κατακλείδα της φοίτησης μου στο Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών της Πολυτεχνικής Σχολής του Πανεπιστημίου Δυτικής Μακεδονίας. Κατά τη διάρκεια των σπουδών, μου δόθηκαν τα απαραίτητα εφόδια για την περαιτέρω πορεία μου στον επαγγελματικό τομέα και συνέβαλαν στην εν γένει διαμόρφωση του χαρακτήρα και της αντίληψής μου.

Αρχικά, θα ήθελα να ευχαριστήσω τον Επίκουρο Καθηγητή Δρ. Παναγιώτη Σαρηγιαννίδη για την υποστήριξη, τις ιδέες και την καθοδήγηση που μου προσέφερε για την περάτωση της συγκεκριμένης εργασίας. Επίσης, θα ήθελα να εκφράσω την ειλικρινή μου εκτίμηση στον Επίκουρο Καθηγητή Δρ. Θεόδωρο Ζυγκιρίδη για τη βοήθεια και τις γνώσεις που μου μετέδωσε.

Επιπλέον, θα ήθελα να ευχαριστήσω τους γονείς μου Ιωάννη και Πασχαλίνα για την σημαντική ηθική και οικονομική στήριξη, καθώς και την εμπιστοσύνη που μου επέδειξαν καθ' όλη τη διάρκεια των σπουδών μου.

Τέλος θα ήθελα να ευχαριστήσω τους φίλους μου για τις όμορφες στιγμές που μοιραστήκαμε στην Κοζάνη.

Ράδογλου-Γραμματίκης Ι. Παναγιώτης,
Κοζάνη, Νοέμβριος 2016

Αφιερώνεται στους γονείς μου

Συντομογραφίες

IDS: Intrusion Detection System

HIDS: Host Intrusion Detection System

NIDS: Network Intrusion Detection System

IPS: Intrusion Prevention System

ANN: Artificial Neural Network

MLP: Multilayer Perceptron

SOM: Self Organizing Map

SVM: Support Vector Machine

PCAP: Packet Capture

TCP/IP: Transmission Control Protocol/Internet Protocol

UDP: User Datagram Protocol

SNMP: Simple Network Management Protocol

P2P: Peer to Peer

RFC: Request for Comments

CPU: Central Processing Unit

WiFi: Wireless Fidelity

3g: Third generation of wireless mobile telecommunications technology

4g: Fourth generation of wireless mobile telecommunications technology

RFID: Radio Frequency Identification

GSM: Global System for Mobile communications

IrDA: Infrared Data Association

SMS: Short Message Service

MMS: Multimedia Messaging Service

UML: Unified Modeling Language

IDE: Integrated Development Environment

GUI: Graphical User Interface

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Η ασφάλεια των σύγχρονων υπολογιστικών συστημάτων αποτελεί ένα κρίσιμο ζήτημα και αντικείμενο έρευνας, διότι η καθολικότητα χρήσης του διαδικτύου και η ταχύτατη εξέλιξη των τεχνολογικών μέσων έχει ως επακόλουθο την ταυτόχρονη ανάπτυξη των κακόβουλων λογισμικών [1]. Η συγκεκριμένη εξέλιξη οδήγησε στην ανάπτυξη εναλλακτικών μεθόδων άμυνας, ικανών να αντιμετωπίζουν νέα μοντέλα εισβολών και να αναγνωρίζουν άγνωστες δικτυακές απειλές. Μία αποτελεσματική και συνεχώς αναπτυσσόμενη μέθοδος προστασίας αποτελεί η ανίχνευση εισβολών (intrusion detection), η οποία πρωτοεμφανίστηκε ως όρος στα τέλη της δεκαετίας του 1970 [2] και ορίζεται ως η διαδικασία ταυτοποίησης ενεργειών, οι οποίες στοχεύουν στην κατάχρηση ενός συστήματος, χωρίς την άδεια των ιδιοκτητών τους [4]. Με την πάροδο του χρόνου δημιουργήθηκαν τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS), τα οποία αποτελούν εργαλεία με μορφή λογισμικού ή και υλικού, τα οποία αυτοματοποιούν τη διαδικασία ελέγχου, ανάλυσης, αναγνώρισης και απόκρισης των ύποπτων ενεργειών [6].

Στο συγκεκριμένο κεφάλαιο πραγματοποιείται ιστορική αναδρομή στη δημιουργία των συστημάτων ανίχνευσης εισβολών, αναφέρονται οι στόχοι και το κίνητρο υλοποίησης της διπλωματικής εργασίας και παρουσιάζεται η δομή των επόμενων κεφαλαίων.

1.1 Εξέλιξη της Ανίχνευσης Εισβολών

Η έρευνα της μεθόδου της ανίχνευσης εισβολών ξεκίνησε στα μέσα της δεκαετίας του 1980, όπου ο James Anderson συμπέρανε ότι τα αρχεία καταγραφής ενός υπολογιστικού συστήματος, μπορούν να αποτελέσουν μία πολύ καλή πηγή για την παρακολούθηση της κατάστασής του και του τρόπου με τον οποίο ο εκάστοτε χρήστης

αλληλοεπιδρά με αυτό [3]. Στηριζόμενοι στην ιδέα του Anderson, ερευνητές άρχισαν να δημιουργούν τα πρώτα συστήματα ανίχνευσης εισβολών, τα οποία παρουσίαζαν και ταξινομούσαν με κατάλληλο τρόπο τα αρχεία καταγραφής συμβάντων, ώστε οι διαχειριστές ασφάλειας να μπορούν να επιβλέπουν την κατάσταση των υπολογιστικών συστημάτων. Το 1987 η Dorothy Denning πρότεινε ένα σύστημα ανίχνευσης εισβολών, το οποίο χρησιμοποιούσε ένα αφηρημένο πρότυπο χαρακτηριστικών, τα οποία αν δεν πληρούν τα πληροφοριακά συστήματα, υπάρχει σημαντική πιθανότητα να δέχονται κάποια μορφή απειλής [5]. Από το 1995 άρχισαν να εμφανίζονται οι πρώτες εμπορικές εκδώσεις των συστημάτων ανίχνευσης εισβολών, τα οποία χρησιμοποιήθηκαν κυρίως σε στρατιωτικές υπηρεσίες πληροφοριών.

1.2 Κίνητρο και Στόχοι Διπλωματικής Εργασίας

Εκτός από την εξέλιξη των πληροφοριακών συστημάτων, ταχεία ανάπτυξη έχει πραγματοποιηθεί και στην τεχνολογία της κινητής υπολογιστικής [7]. Κατά τη χρονική διάρκεια των τελευταίων ετών, οι κινητές συσκευές έχουν αποκτήσει αυξανόμενη δημοτικότητα, εξαιτίας των υπηρεσιών δεδομένων που προσφέρουν, όπως αυτές του ηλεκτρονικού ταχυδρομείου, της περιήγησης στο διαδίκτυο, της επεξεργασίας εγγράφων, κτλ. αλλά και των πολλαπλών τρόπων επικοινωνίας (3G / GSM, 4G, WiFi, RFID, IrDA, Bluetooth) που υποστηρίζουν [8] σε συνδυασμό με τις παραδοσιακές υπηρεσίες φωνής. Συγκεκριμένα από την πρωταρχική εμφάνιση του iPhone από την Apple το 2007, οι κινητές συσκευές έχουν εξελιχθεί σε σημαντικό επίπεδο, ικανές πλέον να επεξεργάζονται μεγάλο όγκο δεδομένων και να προσεγγίζουν τις δυνατότητες των παραδοσιακών υπολογιστικών συστημάτων. Ωστόσο παράλληλα με τις νέες δυνατότητες που προσφέρουν, ο όγκος των δεδομένων που περιλαμβάνουν αποτελεί ελκυστικό στόχο των κακόβουλων λογισμικών, σκοπός των οποίων είναι είτε να εκθέσουν ευαίσθητα δεδομένα των χρηστών ή να διαχειριστούν δημοφιλείς υπηρεσίες [9, 10, 11]. Συγκεκριμένα σημειώνεται πως το 2011 περίπου ένα εκατομμύριο κινητές συσκευές με λειτουργικό σύστημα Android είχαν μολυνθεί από κακόβουλο λογισμικό, ενώ το 33,9% των δωρεάν εφαρμογών για το λειτουργικό σύστημα iOS έκρυβαν κάποιο είδος κακόβουλου κώδικα [12, 13].

Τα κακόβουλα λογισμικά, τα οποία δημιουργούνται αποκλειστικά για συστήματα κινητής υπολογιστικής χρησιμοποιούν συνήθως παραδοσιακές τεχνικές κοινωνικής μηχανικής, όπως το ηλεκτρονικό ταχυδρομείο ή την P2P διαμοίραση αρχείων, καθώς και μοναδικά χαρακτηριστικά των κινητών συσκευών, όπως είναι η τεχνολογία Bluetooth, η υπηρεσία Short Message Service (SMS) και οι διαδικτυακές υπηρεσίες ανταλλαγής μηνυμάτων.

Αντίθετα η διαδικασία μοντελοποίησης ενός συστήματος ανίχνευσης εισβολών για κινητές συσκευές διαφοροποιείται σε σημαντικά σημεία, σε σύγκριση με τη διαδικασία υλοποίησής του, σε ένα σταθερό υπολογιστικό σύστημα. Αναλυτικότερα παρά την πληθώρα βιβλιογραφικών αναφορών για τα μοντέλα ανίχνευσης εισβολών στα συνήθη πληροφοριακά συστήματα, η ερευνητική δραστηριότητα που αφορά το συγκεκριμένο τομέα, σε συστήματα κινητής υπολογιστικής είναι αρκετά περιορισμένη. Ακριβέστερα οι περιορισμένοι πόροι επεξεργασίας, μνήμης και ενέργειας που διαθέτουν, η διαφορετική αρχιτεκτονική CPU και τα ιδιαίτερα χαρακτηριστικά των λειτουργικών

συστημάτων που χρησιμοποιούν, αυξάνουν την πολυπλοκότητα της ανίχνευσης εισβολών.

Στόχος της παρούσας διπλωματικής εργασίας αποτελεί η μελέτη των συστημάτων ανίχνευσης εισβολών και η ανάπτυξη μίας εφαρμογής αναγνώρισης απειλών, για κινητές συσκευές με λειτουργικό σύστημα Android. Συγκεκριμένα στην εφαρμογή ορίζονται δύο καταστάσεις λειτουργίας: η κατάσταση παρακολούθησης της δικτυακής κίνησης και η κατάσταση ανίχνευσης εισβολών. Στην πρώτη, η εφαρμογή παρακολουθεί την κίνηση του δικτύου και παρέχει στον χρήστη σημαντικές πληροφορίες, όπως είναι τα πακέτα που διακινήθηκαν, στατιστικές πληροφορίες της δικτυακής κίνησης και τις δικτυακές επικοινωνίες μεταξύ των συσκευών. Στη δεύτερη κατάσταση η εφαρμογή απομονώνει τις δικτυακές ροές από την κίνηση του δικτύου και βασιζόμενη σε ένα μοντέλο ανίχνευσης διαταραχών, προσδιορίζει τις ροές που παρουσιάζουν ύποπτη συμπεριφορά.

1.3 Σύνοψη Διπλωματικής Εργασίας

Το παρόν κείμενο δομείται από έξι κεφάλαια, τα οποία καλύπτουν το σύνολο των γνώσεων και των απαιτήσεων που χρειάστηκαν για την υλοποίηση της διπλωματικής εργασίας. Στο παρόν κεφάλαιο πραγματοποιείται η παρουσίαση του αντικειμένου και των στόχων που πραγματεύεται η εργασία και περιγράφεται το υπόλοιπο της δομής της.

Στο δεύτερο κεφάλαιο πραγματοποιείται θεωρητική ανάλυση των θεμάτων που αφορούν τα συστήματα ανίχνευσης εισβολών, όπως η αρχιτεκτονική τους, τα μοντέλα ανίχνευσης εισβολών, η κατηγοριοποίησή τους βάσει συγκεκριμένων κριτηρίων, καθώς και ο τρόπος απόκρισής τους στις εισβολές.

Το τρίτο κεφάλαιο αποτελεί μία εισαγωγή στην επιστήμη της επιβλεπόμενης μηχανικής μάθησης, μηχανισμοί της οποίας χρησιμοποιούνται για την ανάπτυξη των μοντέλων ανίχνευσης διαταραχών. Συγκεκριμένα, εξετάζεται ιδιαίτερα η λειτουργία των τεχνητών νευρωνικών δικτύων, στην οποία στηρίχθηκε η ανάπτυξη της εφαρμογής.

Το τέταρτο κεφάλαιο φέρει μια εκτενή αναφορά σχετικά με τον τρόπο και τα μέσα που χρησιμοποιήθηκαν για την κατασκευή του λογισμικού. Συγκεκριμένα, αναλύονται οι απαιτήσεις του συστήματος, ο σχεδιασμός του και τα προγραμματιστικά εργαλεία που χρησιμοποιήθηκαν για την υλοποίησή του.

Στο πέμπτο κεφάλαιο αναφέρονται τα τεχνικά χαρακτηριστικά της εφαρμογής και παρουσιάζονται οι λειτουργίες που διαθέτει. Συγκεκριμένα, παρουσιάζονται η διαδικασία εγκατάστασης και αρχικοποίησης της εφαρμογής, η λειτουργία ανάλυσης της δικτυακής κίνησης και η λειτουργία ανίχνευσης εισβολών.

Τέλος στο έκτο κεφάλαιο, παρατίθενται τα συμπεράσματα που προέκυψαν από τη διπλωματική εργασία και προτείνονται κατευθύνσεις προς τις οποίες μπορεί να επεκταθεί.

Κεφάλαιο 2

Συστήματα Ανίχνευσης Εισβολών

Την τελευταία δεκαετία η έννοια των δικτυακών ροών έχει αποκτήσει μεγάλη δημοτικότητα στο χώρο της παρακολούθησης και της ασφάλισης των υπολογιστικών συστημάτων, εξαιτίας των ζητημάτων που οφείλονται στην ταχύτητα των δικτύων. Συγκεκριμένα τη σημερινή εποχή, όλες οι μεγάλες εταιρίες τηλεπικοινωνιακών συστημάτων, κατασκευάζουν δικτυακές συσκευές με ενεργοποιημένη την επιλογή καταγραφής των δικτυακών ροών, όπως για παράδειγμα οι δρομολογητές της Cisco [14]. Συμπερασματικά τα νέα μοντέλα συστημάτων ανίχνευσης εισβολών, βασίζονται κυρίως στην ανάλυση των πληροφοριών που παρέχονται από τις δικτυακές ροές και όχι στο σύνολο της δικτυακής κίνησης.

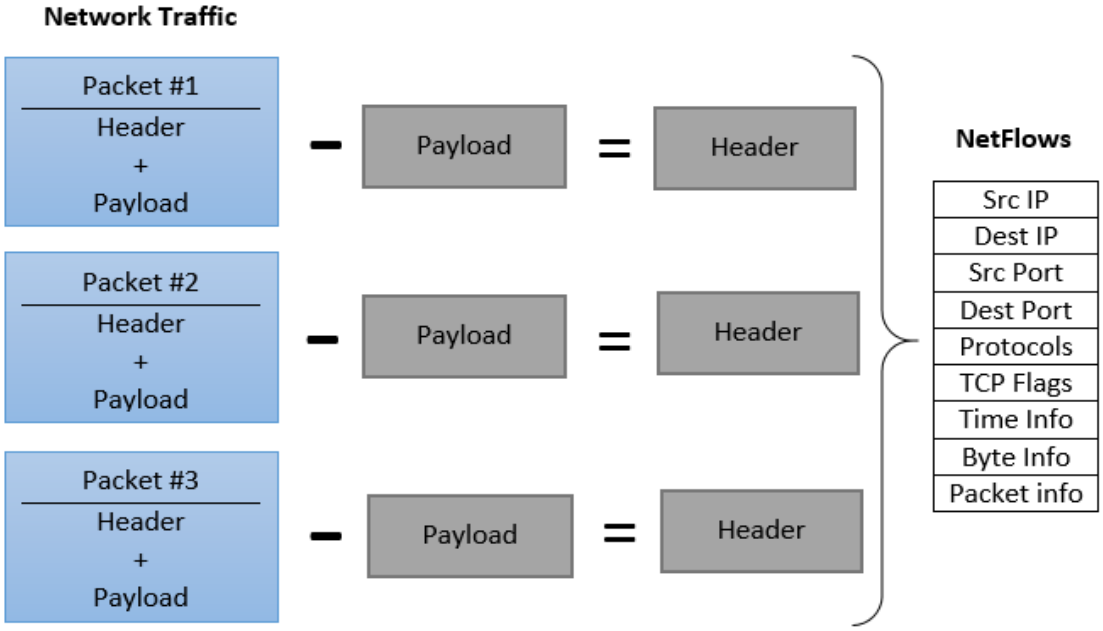
Στο παρόν κεφάλαιο αναπτύσσονται διεξοδικά θέματα σχετικά με μηχανισμούς και τεχνικές, οι οποίες αξιοποιούνται για την αποτελεσματική προστασία των συστημάτων, και των διαθέσιμων πόρων. Αναλυτικότερα εξηγείται η έννοια των δικτυακών ροών, και πραγματοποιείται θεωρητική ανάλυση των θεμάτων που αφορούν τα συστήματα ανίχνευσης εισβολών, όπως η αρχιτεκτονική τους, τα διάφορα μοντέλα εισβολών, η κατηγοριοποίηση τους βάσει συγκεκριμένων κριτηρίων, κτλ.

2.1 Δικτυακές Ροές

Σε βιβλιογραφικές αναφορές μπορούν να βρεθούν αρκετοί ορισμοί για την έννοια των δικτυακών ροών, ανάλογα με τον τύπο των δικτύων και του θέματος που εξετάζεται [15, 18]. Στη συγκεκριμένη διπλωματική εργασία χρησιμοποιήθηκε ο ορισμός του Internet Engineering Task Force (IETF): «Ως δικτυακή ροή ορίζεται ένα σύνολο από πακέτα IP τα οποία διέρχονται από ένα συγκεκριμένο σημείο στο δίκτυο, σε συγκεκριμένη χρονική διάρκεια. Όλα τα πακέτα που ανήκουν σε μία δικτυακή ροή, παρουσιάζουν ένα σύνολο κοινών χαρακτηριστικών» [16]. Τα κοινά χαρακτηριστικά, που ορίζονται σύμφωνα με τον παραπάνω ορισμό είναι: η IP διεύθυνση της πηγής, η

IP διεύθυνση του προορισμού, η δικτυακή θύρα της πηγής και η δικτυακή θύρα του προορισμού. Στο Σχήμα 2.1 απεικονίζεται η διαφορά μεταξύ της δικτυακής κίνησης και των δικτυακών ροών.

Επιπλέον με βάση τον παραπάνω ορισμό οι δικτυακές ροές μπορούν να ταξινομηθούν στην κατηγορία των δικτυακών ροών μονής κατεύθυνσης και στην κατηγορία των δικτυακών ροών αμφίδρομης κατεύθυνσης. Η πρώτη κατηγορία αφορά μόνο τη δικτυακή κίνηση, η οποία προέρχεται από την διεύθυνση της πηγής προς την διεύθυνση του προορισμού, ενώ η δεύτερη κατηγορία αφορά τη συνολική δικτυακή κίνηση που ανταλλάσσεται μεταξύ των δύο διευθύνσεων [17]. Στο σύστημα ανίχνευσης εισβολών που δημιουργήθηκε στο πλαίσιο της διπλωματικής εργασίας, χρησιμοποιήθηκαν ως δεδομένα εισόδου, οι δικτυακές ροές αμφίδρομης κατεύθυνσης.



Σχήμα 2.1: Σύγκριση δικτυακής κίνησης και δικτυακών ροών.

2.2 Στόχοι των Συστημάτων Ανίχνευσης Εισβολών

Όπως προαναφέρθηκε η συνεχής εξέλιξη των υπολογιστικών συστημάτων, έχει ως αρνητικό αποτέλεσμα την παράλληλη ανάπτυξη νέων, άγνωστων μορφών δικτυακών επιθέσεων. Σκοπός των συστημάτων ανίχνευσης εισβολών αποτελεί ο εντοπισμός ενδείξεων για πιθανές προσπάθειες εισβολής, στις οποίες εντοπίζονται ενέργειες παραβίασης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριακών πόρων. Ακριβέστερα, στόχοι των συστημάτων ανίχνευσης εισβολών αποτελούν:

- Η ανίχνευση μεγάλου εύρους εισβολών: Αναγνώριση απειλητικών ενεργειών, οι οποίες μπορεί να προέρχονται είτε από εξωτερικούς παράγοντες του δικτύου ή από εσωτερικούς χρήστες. Ακόμη, τα νέα μοντέλα συστημάτων ανίχνευσης εισβολών θα πρέπει να περιλαμβάνουν μηχανισμούς για την αντιμετώπιση άγνωστων μορφών επιθέσεων. Η δυνατότητα αυτή προϋποθέτει την ύπαρξη

ενός μηχανισμού εκμάθησης ή προσαρμογής σε νέους τύπους επιθέσεων, καθώς και στις αλλαγές της συνήθους δραστηριότητας των χρηστών.

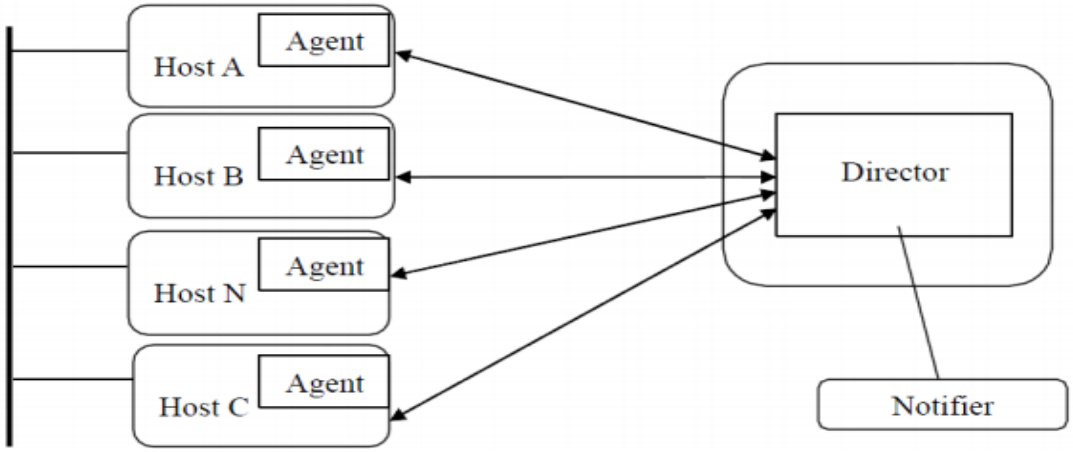
- Έγκαιρη ανίχνευση εισβολών: Ο όρος «έγκαιρη» δεν αναφέρεται κυριολεκτικά σε πραγματικό χρόνο (real time), διότι η αναγνώριση εισβολών σε πραγματικό χρόνο εισάγει σημαντικά ζητήματα ανταπόκρισης. Ωστόσο, απαιτείται η ανίχνευση μίας εισβολής σε εύλογο χρονικό διάστημα.

- Να παρέχουν ακριβείς πληροφορίες: Ένα ψευδές θετικό σήμα (false positive) προκύπτει, όταν ένα σύστημα ανίχνευσης εισβολών αναφέρει μία επίθεση, ενώ στην πραγματικότητα δεν υφίσταται [19]. Τα ψευδώς θετικά σήματα μειώνουν την αξιοπιστία του συστήματος και αυξάνουν αναιτίως την απαιτούμενη εργασία. Αντίθετα τα ψευδώς αρνητικά σήματα (false negative) παράγονται, όταν το σύστημα εντοπισμού εισβολών αποτυγχάνει να αναφέρει μία πραγματική επίθεση που βρίσκεται σε εξέλιξη [19]. Τα συγκεκριμένα είναι ιδιαίτερα αρνητικά, καθώς ο σκοπός των συστημάτων ανίχνευσης εισβολών είναι να προσδιορίζουν τις πραγματικές επιθέσεις.

- Απλή και εύχρηστη γραφική διεπαφή χρήστη (GUI): Τα αποτελέσματα μίας προσπάθειας ανίχνευσης εισβολής, είναι επιθυμητό να προκύπτουν από την τιμή μίας δυαδικής μεταβλητής. Ωστόσο, οι δικτυακές επιθέσεις δεν είναι λειτουργικά τόσο σαφείς και οι πληροφορίες που παράγονται από τα συστήματα ανίχνευσης εισβολών είναι αρκετά πιο σύνθετες. Επίσης, επειδή οι μηχανισμοί ανίχνευσης εισβολών μπορεί να παρακολουθούν περισσότερα από ένα συστήματα, οι πληροφορίες που παράγονται θα πρέπει να παρουσιάζονται στον υπεύθυνο ασφαλείας του συστήματος με κατάλληλο τρόπο.

2.3 Αρχιτεκτονική Συστημάτων Ανίχνευσης Εισβολών

Κάθε σύστημα ανίχνευσης εισβολών αποτελεί έναν αυτοματοποιημένο μηχανισμό παρακολούθησης και ελέγχου. Ο μηχανισμός αυτός, όπως απεικονίζεται στο Σχήμα 2.2 αποτελείται από τρία μέρη: έναν ή περισσότερους αντιπρόσωπους (agent), έναν διευθυντή (director) και έναν αγγελιοφόρο (notifier).



Σχήμα 2.2: Αρχιτεκτονική συστήματος ανίχνευσης εισβολών [20].

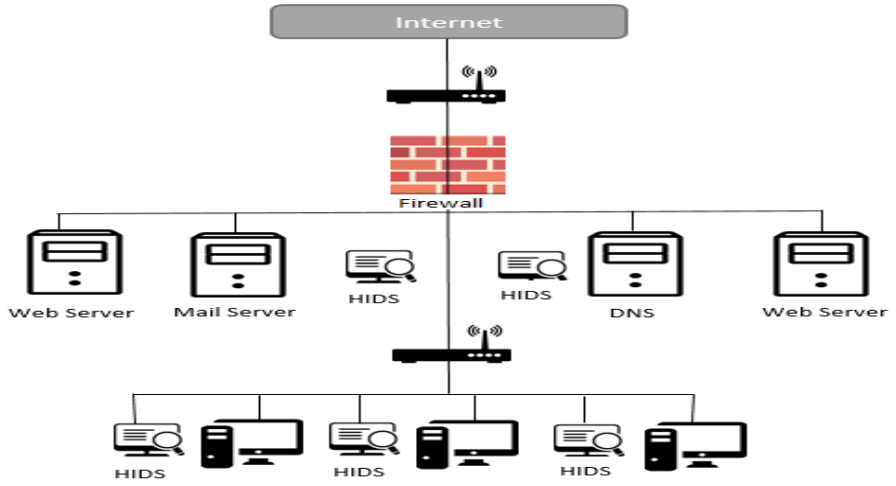
2.3.1 Αντιπρόσωπος

Σκοπός του αντιπροσώπου είναι η συλλογή χρήσιμων πληροφοριών, οι οποίες συνήθως επεξεργάζονται σε κατάλληλα πρότυπα και μεταδίδονται στον διευθυντή. Η πηγή προέλευσης των πληροφοριών μπορεί να προέρχεται είτε από αρχεία καταγραφής συμβάντων (log files), είτε από πληροφορίες που εξάγει το λειτουργικό σύστημα ή οι εφαρμογές του, είτε από χαρακτηριστικά της δικτυακής κίνησης των δικτύων.

Ανάλογα με την τοπολογία του δικτύου, ορίζεται ο αριθμός των αντιπροσώπων που θα χρησιμοποιεί το σύστημα ανίχνευσης εισβολών. Για παράδειγμα, αν η τοπολογία του δικτύου είναι από σημείο σε σημείο (point-to-point) όπως σε ένα δίκτυο Token Ring, οι αντιπρόσωποι θα πρέπει να κατανεμηθούν, προκειμένου να αποκτήσουν πλήρη εικόνα των μηνυμάτων του δικτύου. Αντίθετα, αν η τοπολογία του δικτύου είναι ευρείας μετάδοσης (broadcast), όπως σε ένα δίκτυο Ethernet, η ύπαρξη ενός αντιπροσώπου σε μία συσκευή είναι αρκετή. Συμπερασματικά οι πηγές πληροφορίας μπορούν να διαιρεθούν σε επίπεδο συστήματος (Host) και σε επίπεδο δικτύου (Network), δημιουργώντας κατά αυτόν τον τρόπο τις αντίστοιχες κατηγορίες των συστημάτων ανίχνευσης εισβολών.

2.3.1.1 Σύστημα Ανίχνευσης Εισβολών Μεμονωμένου Συστήματος

Τα συστήματα ανίχνευσης εισβολών μεμονωμένου συστήματος (Host Based IDS - HIDS) λειτουργούν χρησιμοποιώντας πληροφορίες, οι οποίες συλλέγονται από ένα μόνο σύστημα, το οποίο και προστατεύουν. Οι πληροφορίες αυτές αποτελούν συνήθως τα αρχεία καταγραφής του μεμονωμένου συστήματος, οι διεργασίες του λειτουργικού συστήματος και των εφαρμογών του, καθώς και η δικτυακή κίνηση που σχετίζεται με το συγκεκριμένο μηχάνημα. Η εφαρμογή που υλοποιήθηκε στο πλαίσιο της παρούσας διπλωματικής εργασίας, αποτελεί ένα σύστημα ανίχνευσης εισβολών μεμονωμένου συστήματος, το οποίο προσαρτάται σε κινητές συσκευές με λειτουργικό σύστημα Android. Στο Σχήμα 2.3 ορίζεται ένα δίκτυο, στο οποίο χρησιμοποιούνται HIDS σε συγκεκριμένους διακομιστές και προσωπικούς υπολογιστές.



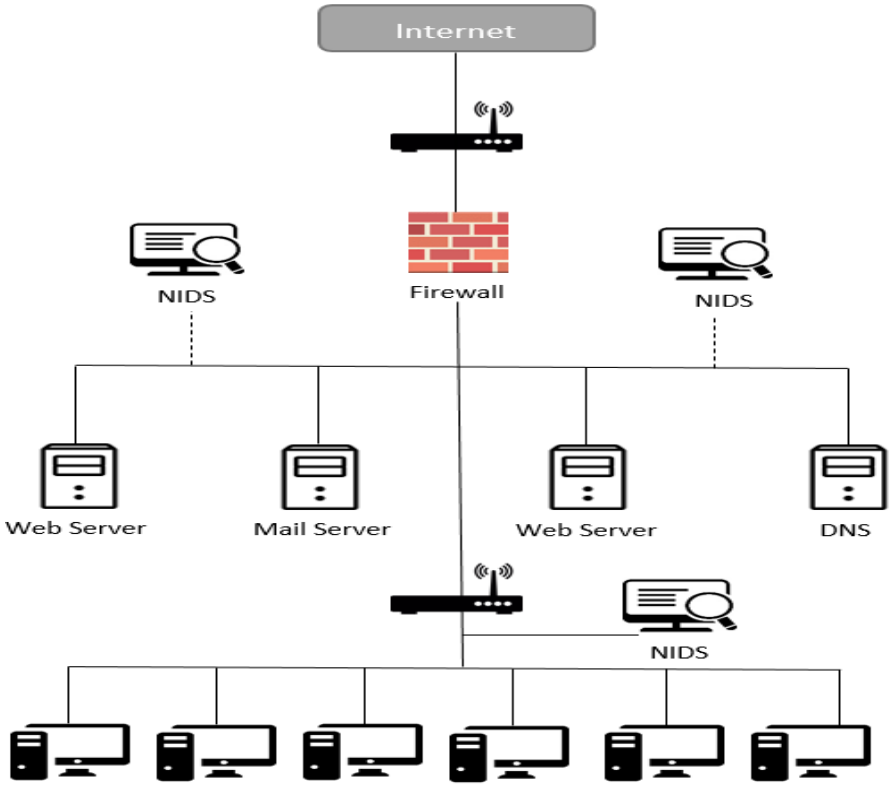
Σχήμα 2.3: Παράδειγμα HIDS.

2.3.1.2 Συστήματα Ανίχνευσης Εισβολών Δικτυακού Συστήματος

Τα συστήματα ανίχνευσης εισβολών δικτυακού συστήματος (Network Based IDS – NIDS) λειτουργούν, χρησιμοποιώντας πληροφορίες, οι οποίες προκύπτουν από τη συνολική δικτυακή δραστηριότητα. Σε αντίθεση με τα HIDS, στόχος τους αποτελεί η παρακολούθηση της αθροιστικής δικτυακής κίνησης και όχι ενός μεμονωμένου υπολογιστικού συστήματος. Ωστόσο δεν επεξεργάζονται περαιτέρω πληροφορίες, όπως οι κλήσεις των λειτουργικών συστημάτων ή τα αρχεία καταγραφής συμβάντων.

Ακριβέστερα, αποτελούνται από αισθητήρες (sensors), οι οποίοι τοποθετούνται σε συγκεκριμένα σημεία του δικτύου και αναλύουν κάθε πακέτο της δικτυακής κίνησης. Οι αισθητήρες είναι συνήθως πληροφοριακά συστήματα με ισχυρές δυνατότητες επεξεργαστικής ισχύς και δικτύωσης, τα οποία καταγράφουν την ανάλυση του δικτύου, είτε τοπικά είτε σε απομακρυσμένους χώρους αποθήκευσης. Ακόμη, διαθέτουν τη δυνατότητα απόκρυψης της παρουσίας τους (Stealth Mode), με αποτέλεσμα ο επιτιθέμενος να μην είναι σε θέση να γνωρίζει την ύπαρξη ή τη θέση τους.

Συγκεκριμένα, μία κάρτα δικτύου λειτουργεί συνήθως σε κατάσταση, όπου λαμβάνει μόνο εκείνα τα δικτυακά πακέτα, τα οποία προορίζονται για την προσωπική της φυσική διεύθυνση (nonpromiscuous mode). Συνεπώς σύμφωνα με τον ορισμό των NIDS, ή κάρτα δικτύου του αντίστοιχου μηχανισμού άμυνας θα πρέπει να τεθεί σε κατάσταση παρακολούθησης (promiscuous mode), προκειμένου να αφουγκράζεται τη συνολική δικτυακή δραστηριότητα. Στο παρακάτω σχήμα απεικονίζεται ένα δίκτυο, το οποίο χρησιμοποιεί τρία NIDS, δύο για τους διακομιστές και ένα για τις εσωτερικές συσκευές.

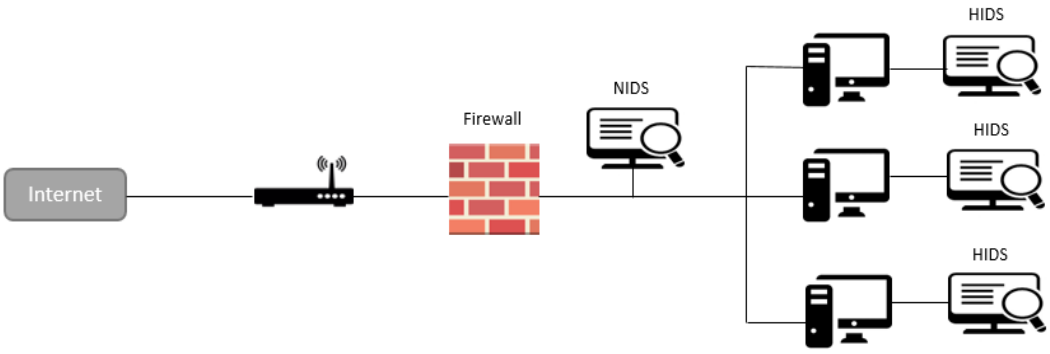


Σχήμα 2.4: Παράδειγμα NIDS.

2.3.1.3 Συνδυαστική Λύση Μεμονωμένου και Δικτυακού Συστήματος Ανίχνευσης Εισβολών

Αποτελεσματικότερος μηχανισμός ασφάλειας των δικτύων υπολογιστών, όσον αφορά τον τομέα ανίχνευση εισβολών, αποτελεί η συνδυαστική χρήση των μοντέλων HIDS και NIDS. Η συγκεκριμένη λύση, αν και περιέχει ιδιαίτερο φόρτο εργασίας για τις διαδικασίες εγκατάστασης και διαχείρισης, καθιστά δυνατή τη διαδικασία ανίχνευσης εισβολών σε όλα τα επίπεδα ενός δικτύου, δηλαδή από το επίπεδο εισόδου μέχρι το κάθε μεμονωμένο υπολογιστικό σύστημα.

Επίσης, αυξάνεται σημαντικά η ακρίβεια αναγνώρισης πιθανών προσπαθειών εισβολής, καθώς από την ένωση των πληροφοριών των δύο προτύπων, προκύπτουν πιο σαφή αποτελέσματα για την κατάσταση του δικτύου. Στο Σχήμα 2.5 παρουσιάζεται η τοποθέτηση των μοντέλων HIDS και NIDS σε ένα δίκτυο.



Σχήμα 2.5: Συνδυασμός HIDS και NIDS.

2.3.2 Διευθυντής

Ο στόχος της λειτουργίας του διευθυντή είναι η επεξεργασία των δεδομένων που έχουν συγκεντρωθεί από του αντιπροσώπους, προκειμένου να διαπιστωθεί αν μία επίθεση ή ο πρόδρομος μίας επίθεσης βρίσκεται σε εξέλιξη. Ακριβέστερα χρησιμοποιεί μία μηχανή ανάλυσης, η οποία περιλαμβάνει ένα η περισσότερα πρότυπα ανίχνευσης εισβολών, τα οποία καθορίζουν βάσει συγκεκριμένων κανόνων ή μεθόδων τεχνικής νοημοσύνης, αν υφίσταται κάποια απειλητική ενέργεια.

Ακόμη, διαθέτει την ικανότητα αποστολής συγκεκριμένων οδηγιών στους αντιπροσώπους, προκειμένου οι δεύτεροι να συλλέξουν περισσότερες πληροφορίες για συγκεκριμένες ενέργειες.

Τέλος, επειδή ο ρόλος του διευθυντή είναι κρίσιμος για την αποτελεσματικότητα της ανίχνευσης εισβολών, σε πολλές περιπτώσεις προτιμάται να εκτελείται σε εξωτερικό σύστημα, από τα υπόλοιπα δομικά στοιχεία του συστήματος ανίχνευσης εισβολών.

2.3.3 Αγγελιοφόρος

Σκοπός του αγγελιοφόρου αποτελεί η ενημέρωση του υπεύθυνου ασφάλειας του συστήματος, για τα αποτελέσματα της μηχανής ανάλυσης του διευθυντή. Ανάλογα με τον προγραμματισμό του συστήματος ανίχνευσης εισβολών, σε κάποιες περιπτώσεις ο

αγγελιοφόρος αποστέλλει μία ειδοποίηση στον διαχειριστή ασφάλειας, ενώ σε άλλες περιπτώσεις εκτελεί συγκεκριμένες ενέργειες, προκειμένου να «απαντήσει» στις επιθέσεις, με στόχο τον άμεσο τερματισμό τους.

2.4 Μοντέλα Εισβολών

Όπως αναφέρθηκε παραπάνω ο διευθυντής του συστήματος ανίχνευσης εισβολών, χρησιμοποιεί ένα ή περισσότερα μοντέλα εισβολών (models of intrusion) προκειμένου να ελέγχει τις πληροφορίες που παρέλαβε από τους αντιπροσώπους και να τις ταξινομεί ως «καλές» (δεν υπάρχουν πιθανές εισβολές) ή ως «κακές» (υπάρχουν πιθανές εισβολές). Προσδιορίζονται κυρίως τρεις κατηγορίες μοντέλων ανίχνευσης εισβολών: Το μοντέλο κακής συμπεριφοράς (misuse model), τα μοντέλα ανίχνευσης διαταραχών (anomaly models) και τα μοντέλα ανίχνευσης διαταραχών πρωτοκόλλων (protocol anomaly detection). Τα μοντέλα μπορεί να είναι είτε προσαρμοστικά, δηλαδή να μεταβάλλουν τη συμπεριφορά τους ανάλογα με τις ενέργειες των συστημάτων, είτε στατικά δηλαδή η λειτουργία τους να στηρίζεται σε ένα αρχικό μη τροποποιήσιμο σύνολο δεδομένων.

2.4.1 Μοντέλο Κακής Συμπεριφοράς

Το μοντέλο κακής συμπεριφοράς αποτελεί ένα από τα πιο χρησιμοποιούμενα πρότυπα στα εμπορικά συστήματα ανίχνευσης εισβολών. Συγκεκριμένα, η λειτουργία του βασίζεται στην αντιστοίχιση των ενεργειών που λαμβάνουν χώρα σε ένα πληροφοριακό σύστημα, με ένα προκαθορισμένο σύνολο προτύπων εισβολών, τα οποία ονομάζονται υπογραφές (signatures). Στην περίπτωση που τα χαρακτηριστικά της συμπεριφοράς μίας ενέργειας ταυτίζονται με μία από τις υπογραφές, τότε συνάγεται ότι μία πιθανή εισβολή βρίσκεται σε εξέλιξη. Συνεπώς η ανίχνευση κακής συμπεριφοράς απαιτεί τη γνώση όλων των ευπαθειών των συστημάτων ή των δυνητικών ευπαθειών που οι επιτιθέμενοι προσπαθούν να εκμεταλλευτούν [20].

Η χρήση του συγκεκριμένου μοντέλου αποφέρει μεγάλη αξιοπιστία, με μηδαμινό ποσοστό ψευδών θετικών σημάτων, ωστόσο αρνητικό σημείο αποτελεί η αδυναμία αναγνώρισης άγνωστων προσπαθειών εισβολών, οι οποίες δεν συμπεριλαμβάνονται στα σύνολα υπογραφών των γνωστών επιθέσεων. Συμπερασματικά τα συστήματα ανίχνευσης εισβολών που χρησιμοποιούν το συγκεκριμένο μοντέλο, θα πρέπει να ανανεώνουν τακτικά το σύνολο των υπογραφών, προκειμένου να συμπεριλαμβάνονται οι νέες επιθέσεις που εμφανίζονται.

2.4.2 Μοντέλα Ανίχνευσης Διαταραχών

Στα μοντέλα ανίχνευσης διαταραχών, ως τεκμήριο εισβολής θεωρείται μία απροσδόκητη συμπεριφορά του συστήματος. Για την υλοποίηση των συγκεκριμένων μοντέλων, θα πρέπει αρχικά να δημιουργηθεί ένα σύνολο δεδομένων και στατιστικών στοιχείων, τα οποία θα ορίζουν τη φυσιολογική δραστηριότητα του συστήματος ή των συστημάτων, στα οποία θα εφαρμόζεται το σύστημα ανίχνευσης εισβολών. Με βάση τα συγκεκριμένα στοιχεία, αν κάποια υπό εξέταση ενέργεια δεν ορίζεται στα πλαίσια

του συνόλου δεδομένων φυσιολογικής συμπεριφοράς, το μοντέλο ενημερώνει τον διαχειριστή ασφάλειας, για την ενεργοποίηση μίας διαταραχής.

Ο ορισμός των στατιστικών μέτρων που ορίζουν τη φυσιολογική συμπεριφορά ενός συστήματος, αποτελεί το δυσκολότερο τμήμα εργασιών για την υλοποίηση των συγκεκριμένων μοντέλων, καθώς η δραστηριότητα ενός συστήματος εμφανίζει πολλές διακυμάνσεις, με συνέπεια να παρουσιάζεται μεγάλη δυσκολία στη μοντελοποίησή του. Για το συγκεκριμένο έργο οι L.Lankewicz και M. Benard [21] εξέτασαν τη χρήση μη παραμετρικών στατιστικών τεχνικών, δηλαδή στατιστικών μοντέλων, τα οποία δεν υποθέτουν καμία a priori κατανομή γεγονότων. Η συγκεκριμένη τεχνική που χρησιμοποίησαν και πλέον έχει καθιερωθεί στα σύγχρονα μοντέλα ανίχνευσης διαταραχών, ονομάζεται ανάλυση συστοιχιών (clustering analysis) και απαιτεί να υπάρχει διαθέσιμο κάποιο σύνολο δεδομένων, το οποίο προκύπτει από την παρακολούθηση του συστήματος για κάποια χρονική περίοδο. Ακολούθως τα δεδομένα ομαδοποιούνται σε υποσύνολα ή σε συστοιχίες με βάση κάποια ιδιότητα που αποκαλείται χαρακτηριστικό (feature).

Η χρήση των συγκεκριμένων μοντέλων είναι περισσότερο ανακριβή από το μοντέλο κακής συμπεριφοράς, ωστόσο παρουσιάζει το πλεονέκτημα αναγνώρισης άγνωστων επιθέσεων. Στη συνέχεια αναλύονται ορισμένα μοντέλα αυτής της κατηγορίας. Στο πλαίσιο της διπλωματικής εργασίας υλοποιήθηκε ένα μοντέλο ανίχνευσης διαταραχών, βασιζόμενο στη λειτουργία των τεχνητών νευρωνικών δικτύων.

2.4.2.1 Μοντέλο Τιμών Κατωφλίου

Στο μοντέλο αυτό καταμετρούνται κάποια συγκεκριμένα χαρακτηριστικά της συμπεριφοράς του χρήστη και του συστήματος και ελέγχεται το πλήθος τους, σε σχέση με κάποιο ανώτατο όριο που θεωρείται επιτρεπτό. Τέτοιου είδους χαρακτηριστικά αποτελούν ο αριθμός των αρχείων, στα οποία έχει πρόσβαση ένας χρήστης, σε μία συγκεκριμένη χρονική περίοδο, το πλήθος των αποτυχημένων προσπαθειών εισόδου ενός χρήστη σε ένα σύστημα, το ποσοστό χρήσης της CPU, κτλ. Το ανώτατο επιτρεπτό όριο μπορεί να αρχικοποιηθεί σε μία στατική τιμή ή να μεταλλάσσεται δυναμικά, προσαρμόζοντας την τιμή του, σύμφωνα με τις ενέργειες που παρατηρούνται στη διάρκεια του χρόνου και θεωρούνται φυσιολογικές. Η λειτουργία του μοντέλου ορίζεται ως εξής: Κάποια συγκεκριμένη ενέργεια αναμένεται να εμφανιστεί κατά ελάχιστο αριθμό m και κατά μέγιστο n. Αν κατά τη διάρκεια μίας συγκεκριμένης χρονικής περιόδου, η συγκεκριμένη δραστηριότητα εμφανίζεται λιγότερο από m ή περισσότερο από n φορές, τότε η συμπεριφορά θεωρείται διαταραγμένη.

Χαρακτηριστικό παράδειγμα του συγκεκριμένου μοντέλου αποτελεί η αποτροπή της εισόδου ενός χρήστη στο λειτουργικό σύστημα MS-Windows NT 4.0, ύστερα από κάποιον αριθμό n αποτυχημένων προσπαθειών εισόδου [22].

2.4.2.2 Μοντέλο Στατιστικών Ροπών

Στο συγκεκριμένο μοντέλο χρησιμοποιούνται στατιστικά μέτρα, όπως η μέση τιμή, η τυπική απόκλιση, η διακύμανση, η επικρατούσα τιμή, κτλ. ενός γνωστού συνόλου δεδομένων φυσιολογικής δραστηριότητας, τα οποία ονομάζονται στατιστικές ροπές.

Αν τα χαρακτηριστικά των υπό εξέταση ενεργειών βρίσκονται εκτός των αναμενόμενων ορίων της εκάστοτε στατιστικής ροπής, τότε η συμπεριφορά της αντίστοιχης ενέργειας θεωρείται διαταραγμένη. Ακόμη, επειδή η κατατομή (profile) της περιγραφής του υπό εξέταση συστήματος μπορεί να εμπεριέχει καθυστερήσεις, το μοντέλο στατιστικών ροπών συνυπολογίζει αυτές τις αλλαγές, είτε σταθμίζοντας τα δεδομένα είτε τροποποιώντας τους στατιστικούς κανόνες, με βάση τους οποίους λαμβάνονται οι αποφάσεις.

Το μοντέλο στατιστικών ροπών παρέχει μεγαλύτερη ευελιξία από το μοντέλο τιμών κατωφλίου, ωστόσο εμφανίζει μεγαλύτερη πολυπλοκότητα στη σχεδίαση του. Αναλυτικότερα για την υλοποίηση του, θα πρέπει να μοντελοποιηθεί η συμπεριφορά τόσο των χρηστών, όσο και των διεργασιών του λειτουργικού συστήματος σε μία από τις ήδη γνωστές στατιστικές κατανομές, όπως είναι η κατανομή Gauss. Ωστόσο η συγκεκριμένη εργασία, εμφανίζει μεγάλή δυσκολία εξαιτίας, των απρόβλεπτων ενεργειών των χρηστών. Στην περίπτωση, όπου το σύνολο των διεργασιών των χρηστών και του λειτουργικού συστήματος δεν μπορεί να αντιστοιχηθεί σε μία από τις ήδη γνωστές κατανομές, τότε χρησιμοποιούνται άλλες ενέργειες, όπως η ανάλυση συστοιχιών [21].

2.4.2.3 Μαρκοβιανό Μοντέλο

Το συγκεκριμένο μοντέλο εξετάζει το σύστημα χρησιμοποιώντας τις Μαρκοβιανές αλυσίδες. Μία στοχαστική διαδικασία Markov ορίζει πως μία μελλοντική κατάσταση ενός συστήματος, εξαρτάται αποκλειστικά από την αμέσως προηγούμενη κατάσταση. Επομένως, η πιθανότητα μία νέας κατάστασης i σε χρόνο t, σύμφωνα με τις διαδικασίες Markov ορίζεται ως:

$$pij = P\{Xt{=}i|Xt\text{-}1{=}j\},\ \ i = 1,2,...,n\ \ j = 0,1,...,n \qquad (2.1)$$

όπου i η νέα μελλοντική κατάσταση σε χρόνο t και j η προηγούμενη κατάσταση του συστήματος σε χρόνο t-1.

Προσαρτώντας τον παραπάνω ορισμό στα συστήματα ανίχνευσης εισβολών, συνάγεται το συμπέρασμα πως το σύνολο των γεγονότων που έχουν προηγηθεί, έχουν θέσει το υπό εξέταση σύστημα σε μία συγκεκριμένη κατάσταση. Η πραγματοποίηση μία νέας ενέργειας θέτει το σύστημα σε μία διαφορετική κατάσταση και με την πάροδο του χρόνου δημιουργείται ένα σύνολο πιθανοτήτων μετάβασης από την μία κατάσταση στις επόμενες. Έτσι δημιουργείται ένας πίνακας πιθανοτήτων μετάβασης καταστάσεων, όπως ο παρακάτω, ο οποίος ορίζει μία αλυσίδα Markov.

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} \qquad (2.2)$$

Συμπερασματικά, κάθε γεγονός που προκαλεί μία μετάβαση από την υπάρχουσα κατάσταση σε μία άλλη και δεν ορίζεται στην αλυσίδα Markov ή παρουσιάζει μικρή πιθανότητα, θεωρείται διαταραγμένο. Η αποτελεσματικότητα των μοντέλων Markov εξαρτάται από την εγκυρότητα των δεδομένων που χρησιμοποιούνται για την αρχικοποίηση του μοντέλου. Τα δεδομένα αυτά αποκαλούνται δεδομένα εκμάθησης και αποκτώνται συνήθως πειραματικά από την παρακολούθηση των συστημάτων.

Χαρακτηριστικό παράδειγμα υλοποίησης του συγκεκριμένου μοντέλου αποτελεί το σύστημα TIM της DEC [23]. Οι ερευνητές Teng Henry, Kaihu Chen και Stephen C. Lu, χρησιμοποιώντας επιβλεπόμενη μάθηση βασισμένη στο χρόνο (time-based inductive learning) εκπαίδευσαν το μοντέλο να προβλέπει τη χρονική στιγμή κατά την οποία θα συνέβαινε ένα γεγονός. Επομένως αν η πραγματοποίηση μίας ενέργειας σε συγκεκριμένο χρονικό διάστημα, παρουσίαζε μικρή πιθανότητα εμφάνισης, τότε το μοντέλο προειδοποιούσε τον διαχειριστή ασφάλειας για την εμφάνιση πιθανής εισβολής.

2.4.3 Μοντέλα Ανίχνευσης Διαταραχών Πρωτοκόλλων

Τα συγκεκριμένα μοντέλα ελέγχουν τη δραστηριότητα του δικτύου όσον αφορά τη σωστή χρήση των πρωτοκόλλων επικοινωνίας και κυρίως εκείνων που ανήκουν στην οικογένεια του TCP/IP. Τα πρωτόκολλα επικοινωνίας αποτελούν σύνολα από αρχές και κανόνες, τα οποία ορίζουν τον τρόπο με τον οποίο επιτυγχάνεται η επικοινωνία μεταξύ δύο διασυνδεδεμένων συστημάτων. Οι ορισμοί υλοποίησης των πρωτοκόλλων αυτών, ορίζονται σε επίσημα, ευρέως αποδεκτά έγγραφα, τα οποία ονομάζονται RFC (Request For Comments) και περιγράφουν τα πρότυπα των ενεργειών, που κάθε πρωτόκολλο θα πρέπει να ακολουθεί κατά την εφαρμογή του.

Οι επιθέσεις, οι οποίες στηρίζονται στη μη φυσιολογική χρήση των πρωτοκόλλων επικοινωνίας, αποβλέπουν στο γεγονός ότι αυτού του είδους οι ενέργειες έχουν παραλειφθεί από τα RFC ή διαφορετικά στηρίζονται σε ελλείψεις που δεν προβλέφθηκαν, κατά την αρχική υλοποίηση των πρωτοκόλλων.

Συνεπώς, τα μοντέλα ανίχνευσης διαταραχών πρωτοκόλλων, αναλύουν τη δραστηριότητα που σχετίζεται με τη χρήση των πρωτοκόλλων επικοινωνίας και ελέγχουν αν αυτή συμφωνεί με κάποια συγκεκριμένα πρότυπα, τα οποία περιγράφουν τη φυσιολογική και νόμιμη εφαρμογή των πρωτοκόλλων.

Η δημιουργία των συγκεκριμένων μοντέλων αποτελεί πιο εύκολη διαδικασία σε σύγκριση με τα μοντέλα ανίχνευσης διαταραχών, καθώς στην προκειμένη περίπτωση χρησιμοποιούνται προκαθορισμένοι κανόνες που περιγράφονται από τα RFC και όχι σύνολα εκπαίδευσης, τα οποία περιγράφουν τη φυσιολογική δραστηριότητα ενός συστήματος.

Ακόμη συγκριτικά με την ανίχνευση κακής συμπεριφοράς, το παρόν μοντέλο στηρίζεται στην υπόθεση πως αν εφαρμόζονται όλες οι προδιαγραφές των πρωτοκόλλων επικοινωνίας, η πολιτική ασφάλειας του συστήματος δεν μπορεί να παραβιαστεί. Αντίθετα, το μοντέλο κακής συμπεριφοράς δεν πραγματοποιεί καμία παρόμοια υπόθεση και εστιάζει στη γενική πολιτική ασφάλειας του συστήματος.

2.5 Οργάνωση των Συστημάτων Ανίχνευσης Εισβολών

Ανάλογα με τους τρόπους παρακολούθησης των συστημάτων και της επιλογή των μοντέλων εισβολών, ένα σύστημα ανίχνευσης εισβολών μπορεί να οργανωθεί με διάφορους τρόπους. Στη συγκεκριμένη ενότητα μελετώνται τρεις προσεγγίσεις οργάνωσης των συστημάτων ανίχνευσης εισβολών, οι οποίες έχουν αναπτυχθεί ερευνητικά.

2.5.1 Παρακολούθηση της κυκλοφορίας στο Δίκτυο: NSM

Το σύστημα Network Security Monitor (NSM) [24] αποτελεί ένα σύστημα ανίχνευσης εισβολών δικτυακού συστήματος, του οποίου ο διευθυντής χρησιμοποιεί τον συνδυασμό του μοντέλου κακής συμπεριφοράς και του μοντέλου ανίχνευσης διαταραχών. Αναλυτικότερα, κατά την πρώτη του έκδοση, το NSM εκπαιδευόταν αρχικά με ένα προκαθορισμένο σύνολο ενεργειών φυσιολογικής συμπεριφοράς του υπό εξέταση δικτύου, το οποίο βασιζόταν στο πλήθος των πακέτων της δικτυακής κίνησης μεταξύ μίας πηγής και ενός προορισμού, στο πλαίσιο μίας συγκεκριμένης δικτυακής υπηρεσίας. Κατά τη διάρκεια της παρακολούθησης του δικτύου, έθετε σε κάθε επικοινωνία μία μοναδική ταυτότητα σύνδεσης (connection ID), η οποία χρησιμοποιούταν για τον καθορισμό των συνδέσεων, που αποτελούσαν πιθανές εισβολές. Η μηχανή ανάλυσης συνέκρινε το πλήθος των πακέτων κάθε σύνδεσης, με τις αναμενόμενες τιμές του συνόλου φυσιολογικής συμπεριφοράς και στην περίπτωση, που μία επικοινωνία παρουσίαζε δεδομένα εκτός του αναμενόμενου εύρους τιμών, τότε σημειωνόταν ως πιθανή εισβολή.

Κατά την πρώτη αξιολόγηση του συστήματος, οι υπεύθυνοι ανάπτυξης του NSM διαπίστωσαν πως κατά τη διάρκεια ανάλυσης της δικτυακής κίνησης, παράγονταν μεγάλος όγκος δεδομένων, γεγονός που χαρακτήριζε το σύστημα ως χρονικά δαπανηρό. Για τη μείωση του σχετικού κόστους, προτιμήθηκε η ομαδοποίηση του συνόλου της δικτυακής κίνησης, μεταξύ μίας συγκεκριμένης πηγής και προορισμού, ανεξαρτήτως της δικτυακής υπηρεσίας.

Με την πάροδο του χρόνου η διάρκεια χρήσης του NSM οδήγησε στη δημιουργία συγκεκριμένων κανόνων (υπογραφές) οι οποίοι αποτέλεσαν τη βάση για την εξέλιξη του συστήματος σε ένα υβριδικό μοντέλο ανίχνευσης διαταραχών και κακής συμπεριφοράς. Οι κανόνες που χρησιμοποιήθηκαν αρχικά, αφορούσαν τον έλεγχο για τυχόν υπερβολικό αριθμό προσπαθειών σύνδεσης, για τυχόν επικοινωνία ενός υπολογιστικού συστήματος με δεκαπέντε ή περισσότερα συστήματα, ή για οποιαδήποτε προσπάθεια επικοινωνίας με ανύπαρκτο σύστημα.

2.5.2 Συνδυασμένη Προσέγγιση: DIDS

Το σύστημα Distributed Instruction Detection System – DIDS [25] αποτελεί μία συνδυαστική λύση μεμονωμένου και δικτυακού συστήματος ανίχνευσης εισβολών, καθώς συνδυάζει τις λειτουργίες του NSM, με τη δυνατότητα παρακολούθησης εισβολών σε μεμονωμένα συστήματα. Χαρακτηριστικό γνώρισμα των αντιπροσώπων του δικτυακού συστήματος, αποτελεί η απόδοση ενός συγκεκριμένου αριθμού ταυτότητας δικτύου (NID) σε κάθε χρήστη. Η συγκεκριμένη ενέργεια οφείλεται στην

αδυναμία των αντιπροσώπων, των μεμονωμένων συστημάτων να ανιχνεύσουν την περίπτωση, όπου ο εισβολέας μετακινείται από σύστημα σε σύστημα, μεταβάλλοντας την τοπική του ταυτότητα. Ύστερα από τη συλλογή των υπό εξέταση δεδομένων από τους αντιπροσώπους, χρησιμοποιείται ένα έμπειρο σύστημα ανάλυσης, το οποίο περιλαμβάνει πέντε επίπεδα λειτουργίας:

- Συλλογή των υπό εξέταση πληροφοριών από τους αντιπροσώπους του δικτύου και των μεμονωμένων συστημάτων.
- Σε κάθε χρήστη, που εντοπίστηκε από τους αντιπροσώπους του δικτυακού συστήματος, αντιστοιχείται ένα υποκείμενο, στο οποίο καταχωρείται η ταυτότητα του χρήστη και οι υπό εξέταση ενέργειες που σχετίζονται με αυτόν.
- Επεξεργάζονται διάφορες συναφείς πληροφορίες, όπως ο χρόνος χρήσης του επεξεργαστή, το ποσοστό χρήσης μνήμης, πληροφορίες ομοιότητας γεγονότων, κτλ. Χαρακτηριστικό παράδειγμα των συγκεκριμένων πληροφοριών, αποτελεί η περίπτωση που ένας χρήστης προσπαθεί να συνδεθεί στο σύστημα σε κάποια συγκεκριμένη χρονική περίοδο, κατά την οποία δεν είχε συνδεθεί σε προηγούμενη χρονική στιγμή. Συνεπώς βάση της συγκεκριμένης πληροφορίας συνάγεται το συμπέρασμα ότι πρόκειται για ύποπτη συμπεριφορά.
- Διαχειρίζεται τις απειλές προς το δίκτυο (network threats) οι οποίες αποτελούν συνδυασμούς διάφορων γεγονότων. Μία απειλή θεωρείται εξαπάτηση (abuse) αν μεταβάλλεται η κατάσταση προστασίας του συστήματος. Παράδειγμα αποτελεί η αλλαγή των δικαιωμάτων ανάγνωσης, εγγραφής ή εκτέλεσης ενός αρχείου. Μία απειλή χαρακτηρίζεται ως κακή συμπεριφορά (misuse) αν παραβιάζει την πολιτική ασφάλειας του συστήματος, χωρίς όμως να μεταβάλει την κατάσταση του. Ένα παράδειγμα στη συγκεκριμένη περίπτωση αποτελεί η αντιγραφή και η κοινοποίηση ενός απαγορευμένου αρχείου. Τέλος μία απειλή θεωρείται ύποπτη πράξη (suspicious act) αν δεν παραβιάζει την πολιτική ασφάλειας ενός συστήματος, αλλά θεωρείται πρόδρομος για την πραγματοποίηση μίας επίθεσης.
- Βαθμολογεί την κατάσταση ασφάλειας του δικτύου με βάση τις απειλές προς το σύστημα που αναπτύσσονται στο προηγούμενο επίπεδο.

Στο DIDS κάθε κανόνας προσδιορίζεται από μια αξία, οι οποίες χρησιμοποιούνται για τον υπολογισμό της εκάστοτε βαθμολογίας. Ο υπεύθυνος ασφάλειας των συστημάτων ανατροφοδοτεί το έμπειρο σύστημα ανάλυσης, ενώ σε περίπτωση ψευδών ειδοποιήσεων η μηχανή ανάλυσης μειώνει την αντίστοιχη αξία, η οποία συνδέεται με τους κανόνες που οδήγησαν στον ψευδή συναγερμό.

2.5.3 Αυτόνομοι Πράκτορες

Οι M.Crosbie και E.Spafford πρότειναν μία διαφορετική αρχιτεκτονική για τα συστήματα ανίχνευσης εισβολών, όπου ο κάθε αντιπρόσωπος παρακολούθησης του συστήματος περιλάμβανε ένα εσωτερικό μοντέλο διευθυντή, το οποίο διέθετε τη δυνατότητα ανάλυσης των πληροφοριών του συγκεκριμένου αντιπροσώπου. Οι

συνδυασμοί αυτοί ονομάστηκαν αυτόνομοι αντιπρόσωποι. Στην περίπτωση, που κάποιος από τους αυτόνομους αντιπροσώπους ανίχνευε κάποια ύποπτη συμπεριφορά του συστήματος, τότε ενημέρωνε το υπόλοιπο σύνολο των αντιπροσώπων και από κοινού καθόριζαν αν το πλήθος των ειδοποιήσεων ήταν επαρκές, ώστε να αποτελέσει μία δυνητική εισβολή [26].

Σημαντικό πλεονέκτημα της συγκεκριμένης αρχιτεκτονικής αποτελεί το γεγονός πως ο συνολικός μηχανισμός άμυνας, δεν επηρεάζεται στην περίπτωση που κάποιος από τους αντιπροσώπους τεθεί εκτός λειτουργίας, καθώς οι υπόλοιποι συνεχίζουν αδιάκοπα τη λειτουργία τους. Επιπλέον, το συγκεκριμένο σχήμα καθιστά δυνατή την εξειδίκευση παρακολούθησης των πληροφοριών του συστήματος, καθώς ο κάθε αντιπρόσωπος μπορεί να αναπτυχθεί, ώστε να ελέγχει συγκεκριμένη ποσότητα πόρων, ικανοποιώντας τη βασική αρχή της οικονομίας μηχανισμών (economy of mechanisms).

Αντίστοιχα, τα συνήθη μειονεκτήματα υλοποίησης του μοντέλου των αυτόνομων αντιπροσώπων, εντοπίζονται κυρίως στο αυξημένο υπολογιστικό κόστος των απαιτούμενων επικοινωνιών. Συγκεκριμένα καθώς μειώνεται η λειτουργικότητα του κάθε αντιπροσώπου, απαιτείται περισσότερο πλήθος αντιπρόσωπων για τη συνολική παρακολούθηση του συστήματος, με επακόλουθο την αύξηση του υπολογιστικού κόστους επικοινωνίας.

2.6 Απόκριση στις Εισβολές

Το επόμενο ζήτημα έρευνας, ύστερα από την ανάλυση της διαδικασίας ανίχνευσης εισβολών, αποτέλεσε η δημιουργία αυτόματων μηχανισμών άμυνας, στόχος των οποίων είναι η αντιμετώπιση των αποπειραθείς επιθέσεων με συγκεκριμένο τρόπο, ώστε να ελαχιστοποιούνται οι επιπτώσεις της εκάστοτε επίθεσης, όπως αυτές ορίζονται στην πολιτική ασφάλειας του συστήματος.

2.6.1 Συστήματα Πρόληψης Εισβολών

Τα συστήματα πρόληψης εισβολών (Intrusion Prevention System – IPS) αποτελούν το επόμενο βήμα εξέλιξης των συστημάτων ανίχνευσης εισβολών, στοχεύοντας στην αντιμετώπιση των επιθέσεων πριν την ολοκλήρωση τους. Αναλυτικότερα, κατά την ανίχνευση μία εισβολής, επιθυμητός στόχος αποτελεί η άμεση αυτόματη διακοπή της, χωρίς την παρέμβαση του ανθρώπινου παράγοντα, προκειμένου να ελαχιστοποιηθεί η χρονική διάρκεια εξέλιξης της επίθεσης.

2.6.2 Ενεργές Αποκρίσεις

Οι ενεργές αποκρίσεις αποτελούν αυτοματοποιημένες ενέργειες, οι οποίες εκτελούνται από τα συστήματα ανίχνευσης εισβολών, και στοχεύουν στην άμεση αντιμετώπιση συγκεκριμένου τύπου επιθέσεων. Σε αντίθεση με τα συστήματα πρόληψης εισβολών, στην προκειμένη περίπτωση η διαδικασία της επίθεσης υφίσταται ήδη στο προστατευόμενο σύστημα. Προς την κατεύθυνση αυτή το σύστημα ανίχνευσης εισβολών μπορεί να προβεί σε μία ή περισσότερες από τις ακόλουθες ενέργειες:

- Συλλογή επιπρόσθετων πληροφοριών: Η λειτουργία της συγκεκριμένης αντίδρασης ορίζει τη συλλογή περισσότερων δεδομένων για μία πιθανή εισβολή, με στόχο την αύξηση της ακρίβειας που αφορά τον τύπο της ενέργειας ή το είδος της επίθεσης. Ανάλογα με τις συγκεκριμένες πληροφορίες το σύστημα ανίχνευσης εισβολών λαμβάνει την κατάλληλη απόφαση για το αν θα πρέπει να οριστούν επιπλέον μέτρα προστασίας.

- Παρεμπόδιση του επιτιθέμενου: Η συγκεκριμένη αντίδραση αποσκοπεί στον άμεσο τερματισμό της επίθεσης ή στην παρεμπόδιση της εξάπλωσης της στο προστατευόμενο σύστημα. Αναλυτικότερα, η διαδικασία πραγματοποίησης της, στηρίζεται στον επαναπροσδιορισμό των κανόνων ασφαλείας του τείχους προστασίας (firewall) ή των δρομολογητών του συστήματος, ώστε να αποκλείσουν τη δικτυακή κίνηση, η οποία προέρχεται από την IP διεύθυνση του επιτιθέμενου.

- Αντεπίθεση στον επιτιθέμενο: Η απόκριση αυτή λαμβάνει συνήθως δύο μορφές. Η πρώτη μορφή εξελίσσεται στο πλαίσιο υπάρχοντών νομικών μηχανισμών, οι οποίοι όμως απαιτούν την υποστήριξη αποδεικτικών στοιχείων (chain of evidence), προκειμένου οι δικαστικές αρχές να μπορούν να προσδιορίσουν πως πρόκειται για πραγματική επίθεση. Η δεύτερη λύση, η οποία δεν προτείνεται, αφορά τη σχεδίαση μίας νέας τεχνικής επίθεσης, με στόχο την επίτευξη σοβαρών αρνητικών επιπτώσεων στον επιτιθέμενο, προκειμένου να τερματίσει την τρέχουσα επίθεση και παράλληλα να αποθαρρυνθεί για μελλοντικές επιθέσεις. Η εκτέλεση της δεύτερης προσέγγισης μπορεί να προκαλέσει σημαντικές συνέπειες όπως στην άσκηση αντίστροφης ποινικής δίωξης, την πρόκληση αρνητικών επιπτώσεων σε «αθώα» υπολογιστικά συστήματα και στη δημιουργία διάφορων άλλων παρενεργειών.

2.6.3 Παθητικές Αποκρίσεις

Στόχος των παθητικών αντιδράσεων είναι η ειδοποίηση του υπεύθυνου ασφαλείας του συστήματος, για την πραγματοποίηση πιθανών εισβολών. Οι ειδοποιήσεις αυτές μπορούν να παρουσιάζουν κυμαινόμενο βαθμό λεπτομέρειας και να εμφανίζονται είτε σε συγκεκριμένο χώρο του συστήματος ανίχνευσης εισβολών, είτε σε συσκευές τηλεειδοποίησης, είτε με τη χρήση αναδυόμενων παραθύρων, κτλ.

Ακόμη κάποια συστήματα ανίχνευσης εισβολών διαθέτουν τη δυνατότητα αποστολής των ειδοποιήσεων που παράγουν, σε ένα κεντρικό σύστημα διαχείρισης του δικτύου, με τη χρησιμοποίηση του πρωτοκόλλου SNMP. Η μαζική αποθήκευση των ειδοποιήσεων που προκύπτουν από τα διάφορα συστήματα ανίχνευσης εισβολών, καθώς και από πληροφορίες που εξάγονται από άλλους μηχανισμούς ασφάλειας, καθιστούν περισσότερο σαφή την κατάσταση του δικτύου, καθώς διαμέσου της συγκεκριμένης αρχιτεκτονικής διευκολύνεται η διαδικασία συσχέτισης των αποτελεσμάτων μεταξύ των διαφορετικών πηγών.

Κεφάλαιο 3

Τεχνητά Νευρωνικά Δίκτυα

Τα μοντέλα ανίχνευσης διαταραχών δανείζονται από την επιστήμη της τεχνητής νοημοσύνης συγκεκριμένους αλγόριθμους, προκειμένου να αναγνωρίσουν άγνωστους τύπους εισβολών, οι οποίοι δεν περιλαμβάνονται στα σύνολα υπογραφών κακής συμπεριφοράς. Ακριβέστερα, οι τεχνικές που χρησιμοποιούνται εντάσσονται στο πεδίο της μηχανικής μάθησης, η οποία αναπτύσσεται ως επιστήμη από τη δεκαετία του 1950 και διερευνά τη μελέτη και την κατασκευή αλγορίθμων, που στοχεύουν στην πρόβλεψη άγνωστων καταστάσεων, χρησιμοποιώντας συγκεκριμένους μηχανισμούς.

Στο παρόν κεφάλαιο πραγματοποιείται μία εισαγωγή στον τομέα της μηχανικής μάθησης, εξετάζοντας τις κατηγορίες στις οποίες διακρίνεται, και τους τύπους των προβλημάτων που επιλύει. Επιπλέον, περιγράφονται οι πιο διαδεδομένοι αλγόριθμοι μηχανικής μάθησης, εστιάζοντας στη χρήση των τεχνικών νευρωνικών δικτύων, στα οποία στηρίχθηκε η ανάπτυξη του συστήματος ανίχνευσης εισβολών, που υλοποιήθηκε στο πλαίσιο της διπλωματικής εργασίας. Τέλος αναλύονται μέτρα αξιολόγησης, τα οποία καθορίζουν το ποσοστό επιτυχίας ενός μοντέλου στην επίλυση ενός προβλήματος.

3.1 Μηχανική Μάθηση

Η μηχανική μάθηση (machine learning) έχει ως αντικείμενο την κατασκευή προγραμμάτων, ικανών να βελτιώνονται αυτόματα ανάλογα με την εμπειρία που αποκτούν κατά τη διάρκεια της εκπαίδευσής τους. Χρησιμοποιεί έννοιες από διάφορα επιστημονικά πεδία και κυρίως από τη στατιστική, την τεχνητή νοημοσύνη και τη θεωρία πληροφορίας. Τη δεκαετία του 1950 ο Arthur Samuel προσδιόρισε τη μηχανική μάθηση «ως το πεδίο μελέτης που δίνει στους υπολογιστές την ικανότητα να μαθαίνουν χωρίς να έχουν προγραμματιστεί για αυτό» [27]. Το 1997 ο E. Mitchell διατύπωσε έναν πιο ακριβή ορισμό για την έννοια της μηχανικής μάθησης, ο οποίος αναφέρει ότι: «Τα

προγράμματα υπολογιστών μπορούν να μάθουν την εμπειρία Ε, όσον αφορά μερικές τάξεις έργων Τ (tasks) και μέτρων απόδοσης Ρ (performance measures), αν οι αποδόσεις τους στα έργα Τ, όπως μετρήθηκαν με Ρ βελτιώνονται με την εμπειρία Ε» [28].

Για παράδειγμα στη διαδικασία ανίχνευσης εισβολών ως μέτρο αξιολόγησης μπορεί να θεωρηθεί το ποσοστό των ενεργειών που αναγνωρίστηκαν σωστά (ενέργειες που αποτελούν απειλές ή ασφαλείς ενέργειες), βάσει ενός συνόλου δεδομένων ενεργειών, οι οποίες είναι χαρακτηρισμένες εκ των προτέρων.

3.2 Κατηγορίες Μηχανικής Μάθησης

Οι εργασίες της μηχανικής μάθησης ταξινομούνται κυρίως στις τέσσερις παρακάτω κατηγορίες, ανάλογα με τις ανάγκες του προβλήματος και τις ιδιότητες του συνόλου των δεδομένων εκπαίδευσης.

- Επιβλεπόμενη ή επιτηρούμενη μάθηση: Η διαδικασία της συγκεκριμένης μάθησης στοχεύει στη δημιουργία ενός μοντέλου, ικανού να προβλέπει κάποιες μη παρατηρούμενες ιδιότητες σε άγνωστα αντικείμενα, χρησιμοποιώντας ως σώμα εκπαίδευσης, παραδείγματα, στα οποία οι ιδιότητες αυτές είναι γνωστές. Με άλλα λόγια, έχοντας ένα προκαθορισμένο κατηγοριοποιημένο σύνολο εκπαίδευσης, στόχο αποτελεί τα προς εξέταση αντικείμενα να ταξινομηθούν σε μία από τις συγκεκριμένες κατηγορίες. Η ιδέα της επιβλεπόμενης μάθησης θα μπορούσε να παρομοιαστεί με την κατάσταση ενός ανθρώπου, ο οποίος εκπαιδεύεται από τις εμπειρίες του, ώστε να λαμβάνει καλύτερες μελλοντικές αποφάσεις. Αυτό το είδος μάθησης χρησιμοποιήθηκε για την ανάπτυξη του μοντέλου εισβολών που υλοποιήθηκε στο πλαίσιο της διπλωματικής εργασίας.

- Μη επιβλεπόμενη μάθηση: Στο συγκεκριμένο είδος δεν ορίζεται κάποιο σύνολο δεδομένων εκπαίδευσης, με το οποίο μπορεί να εκπαιδευτεί το αντίστοιχο μοντέλο. Επομένως, χρησιμοποιούνται άλλες τεχνικές για την επίλυση του προβλήματος από τις οποίες ξεχωρίζουν η ομαδοποίηση (clustering) και η εκτίμηση παραμέτρων (parameter estimation). Η ομαδοποίηση συνιστάται στην ανακάλυψη ομάδων από αντικείμενα, τα οποία παρουσιάζουν μεταξύ τους κοινά χαρακτηριστικά [29]. Οι κατηγορίες στην περίπτωση αυτή δεν είναι γνωστές εκ των προτέρων, αλλά προκύπτουν δυναμικά κατά την εκτέλεση του αλγόριθμου ομαδοποίησης. Στην εκτίμηση παραμέτρων κατασκευάζεται ένα στατιστικό μοντέλο προς αντιμετώπιση του προβλήματος, το οποίο διαθέτει ένα σύνολο παραμέτρων, οι τιμές των οποίων πρέπει να προσδιοριστούν. Για το σκοπό αυτό χρησιμοποιείται ένας αλγόριθμος μάθησης, ο οποίος εκπαιδεύεται με αντιπροσωπευτικά δεδομένα, προκειμένου να προσεγγίσει τις ζητούμενες παραμέτρους [30].

- Ημι-επιβλεπόμενη μάθηση: Στη συγκεκριμένη κατηγορία χρησιμοποιούνται προταξινομημένα δεδομένα σε συνδυασμό με μη ταξινομημένα παραδείγματα. Στόχος αποτελεί η ενίσχυση του αποτελέσματος της μαθησιακής διαδικασίας, χρησιμοποιώντας όσο δυνατόν λιγότερα προταξινομημένα δεδομένα.

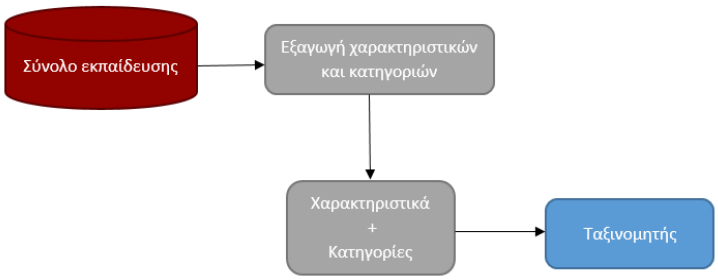
- Ενισχυτική μάθηση: Αυτό το είδος μάθησης χρησιμοποιεί παρατηρημένες ειδικές αναδράσεις (ανταμοιβές ή ενισχύσεις) για τη μάθηση σχεδόν βέλτιστων πολιτικών για το περιβάλλον του προβλήματος. Βέλτιστη πολιτική αποτελεί αυτή που μεγιστοποιεί την αναμενόμενη συνολική ανταμοιβή. Σε αρκετά πολύπλοκα πεδία θεωρείται ότι αποτελεί τη μοναδική εφικτή λύση για την εκπαίδευση προγραμμάτων, έτσι ώστε να επιτυγχάνονται υψηλά επίπεδα επιδόσεων.

3.3 Ταξινόμηση

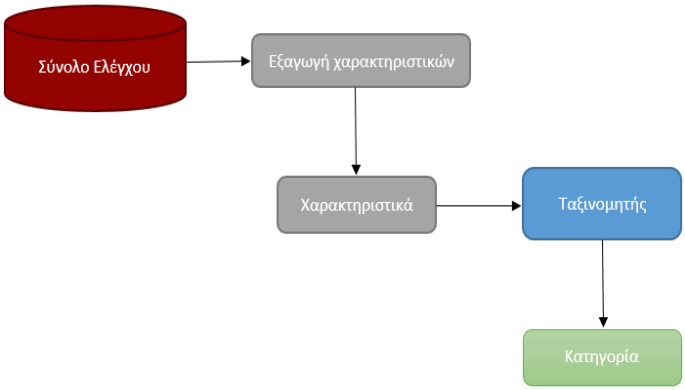
Ανάλογα με τον τύπο της πρόβλεψης, ορίζονται διάφορες κατηγορίες προβλημάτων, στις οποίες μπορούν να χρησιμοποιηθούν τεχνικές μηχανικής μάθησης. Αναφορικά, χρησιμοποιούνται κυρίως σε προβλήματα ταξινόμησης, παλινδρόμησης, εκτίμησης της πυκνότητας και ομαδοποίησης. Στη συγκεκριμένη ενότητα αναλύεται το πρόβλημα της ταξινόμησης, για το οποίο χρησιμοποιούνται αλγόριθμοι από την κατηγορία της επιβλεπόμενης μηχανικής μάθησης.

Αναλυτικότερα, η ταξινόμηση (classification) συνιστάται στην εκμάθηση μίας συνάρτησης στόχου, ικανής να αντιστοιχεί άγνωστα αντικείμενα σε ένα προκαθορισμένο σύνολο κατηγοριών. Στόχος της διαδικασίας μάθησης αποτελεί η δημιουργία ενός μοντέλου, έργο του οποίου θα αποτελεί η πρόβλεψη των κατηγοριών, ενός άγνωστου συνόλου αντικειμένων (test set), βάσει ορισμένων χαρακτηριστικών (features) που το προσδιορίζουν. Για την αντιμετώπιση του συγκεκριμένου προβλήματος προϋποτίθεται η συγκέντρωση ενός κατηγοριοποιημένου συνόλου εκπαίδευσης (training set) από αντιπροσωπευτικά για την κάθε κατηγορία παραδείγματα, τα οποία έχουν ταξινομηθεί από ανθρώπινες ενέργειες. Στη συνέχεια χρησιμοποιούνται αλγόριθμοι μηχανικής μάθησης, στους οποίους παρέχεται ως είσοδος το σύνολο εκπαίδευσης και τα χαρακτηριστικά των υπό εξέταση αντικειμένων και βάσει των στοιχείων αυτών, ταξινομείται το εκάστοτε αντικείμενο σε μία από τις προκαθορισμένες κατηγορίες.

Οι αλγόριθμοι μηχανικής μάθησης που χρησιμοποιούνται σε προβλήματα ταξινόμησης ονομάζονται ταξινομητές (classifiers). Οι πιο διαδεδομένοι ταξινομητές είναι τα δέντρα αποφάσεων, ο Naive Bayes, ο Support Vector Machine (SVM), και τα τεχνητά νευρωνικά δίκτυα. Τα τελευταία χρησιμοποιήθηκαν για την ανάπτυξη του μοντέλου ανίχνευσης εισβολών, που υλοποιήθηκε στο πλαίσιο της διπλωματικής εργασίας. Στα παρακάτω σχήματα απεικονίζονται οι διαδικασίες εκπαίδευσης και πρόβλεψης του ταξινομητή.



Σχήμα 3.1: Διαδικασία εκπαίδευσης του ταξινομητή.



Σχήμα 3.2: Διαδικασία πρόβλεψης του ταξινομητή.

3.4 Τεχνικά Νευρωνικά Δίκτυα

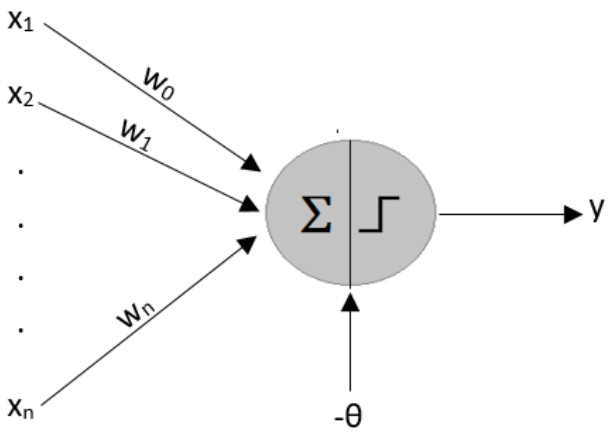
Τα τεχνητά νευρωνικά δίκτυα (Artificial Neural Networks - ANN) αποτελούν μία προσπάθεια προσέγγισης της λειτουργίας των βιολογικών νευρωνικών δικτύων. Συγκεκριμένα αποτελούν τομέα της τεχνητής νοημοσύνης και συγκροτούνται από ένα σύνολο απλών, διασυνδεδεμένων και προσαρμοστικών μονάδων, οι οποίες συνιστούν ένα παράλληλο πολύπλοκο υπολογιστικό μοντέλο. Μέχρι σήμερα έχουν εφαρμοστεί επιτυχημένα σε ένα ευρύ φάσμα περιοχών για την επίλυση προβλημάτων ταξινόμησης ή πρόβλεψης, όπως η βιολογία, η ιατρική, η πληροφορική, η φυσική, κτλ.

Αν και πρόκειται για σχετικά νέο ερευνητικό πεδίο της τεχνητής νοημοσύνης, καθώς η κύρια ανάπτυξη τους ξεκίνησε από τη δεκαετία του 1980, έχουν ήδη αναπτυχθεί αρκετά λογισμικά για τη δημιουργία και τη διαχείριση τους. Ένα από τα πιο διαδεδομένα αποτελεί το εργαλείο Network Neural Toolbox του λογισμικού Matlab, το οποίο χρησιμοποιήθηκε στην παρούσα διπλωματική εργασία.

Στην ενότητα αυτή εξετάζεται μία συγκεκριμένη οικογένεια των τεχνητών νευρωνικών δικτύων, τα οποία ονομάζονται δίκτυα εμπρόσθιας τροφοδότησης. Η ιδιότητα που χαρακτηρίζει τα συγκεκριμένα δίκτυα είναι ότι κάθε επίπεδο νευρώνων επικοινωνεί αποκλειστικά με τους νευρώνες του αμέσως επόμενου επιπέδου.

3.4.1 Το Μοντέλο του Αισθητήρα

Το μοντέλο του αισθητήρα ή αλλιώς Perceptron του Rosenblatt αποτελεί το πιο απλό τεχνητό νευρωνικό δίκτυο, καθώς συγκροτείται από μόνο ένα νευρώνα. Το συγκεκριμένο μοντέλο περιλαμβάνει έναν πολλαπλό αριθμό εισόδων, αλλά παράγει μόνο μία έξοδο, όπως απεικονίζεται στο Σχήμα 3.3. Σε κάθε είσοδο x_i αντιστοιχεί ένα συναπτικό βάρος w_i, το οποίο ορίζει την επίδραση του εισερχόμενου σήματος στο νευρώνα. Ο νευρώνας υπολογίζει την εκάστοτε έξοδο, αθροίζοντας αρχικά τα γινόμενα των εισερχόμενων σημάτων επί των συναπτικών βαρών και χρησιμοποιώντας στη συνέχεια μία συνάρτηση ενεργοποίησης, στην οποία μεταβιβάζεται ως παράμετρος, το προηγούμενο άθροισμα, αφαιρώντας από αυτό έναν μεροληπτικό παράγοντα θ.



Σχήμα 3.3: Μοντέλο του αισθητήρα.

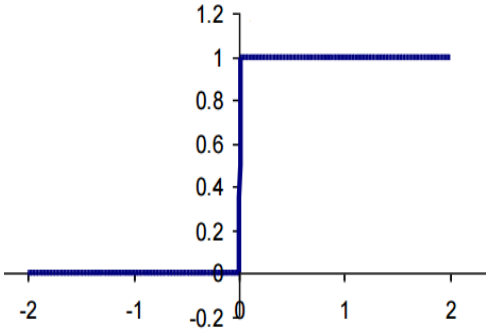
Αναλυτικότερα για τον υπολογισμό της εξόδου χρησιμοποιούνται οι ακόλουθες εξισώσεις, σύμφωνα με το μοντέλο McCulloch-Pitts [31].

$$u = \sum_{i=1}^{n} w_i x_i - \theta \quad (3.1)$$

$$y = f(u) = f\left(\sum_{i=1}^{n} w_i x_i - \theta\right) \quad (3.2)$$

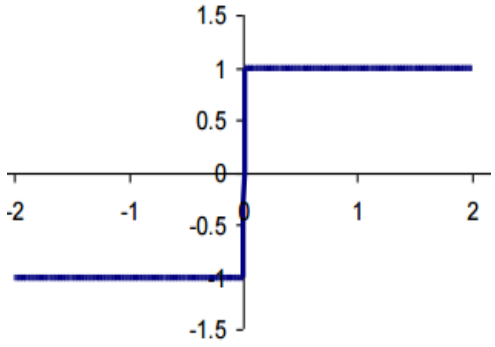
Η συνάρτηση ενεργοποίησης f που ορίζεται συνήθως για το μοντέλο του αισθητήρα είναι συνήθως είτε η βηματική συνάρτηση, είτε η συνάρτηση προσήμου, οι οποίες ορίζονται αντίστοιχα, σύμφωνα με τις ακόλουθες εξισώσεις.

$$\text{Βηματική } \sigma\text{υνάρτηση} : y = f(u) = \begin{cases} 0, & u<0 \\ 1, & u\geq 0 \end{cases} \quad (3.3)$$



Σχήμα 3.4: Γραφική παράσταση βηματικής συνάρτησης.

$$\text{Συνάρτηση προσήμου} : y = f(u) = \begin{cases} -1, & u<0 \\ 1, & u\geq 0 \end{cases} \quad (3.4)$$



Σχήμα 3.5: Γραφική παράσταση συνάρτησης προσήμου.

Συνήθως ο μεροληπτικός παράγοντας θ, θεωρείται ως ένα επιπλέον εσωτερικό συναπτικό βάρος w_0, το οποίο ονομάζεται πόλωση (bias) και αντιστοιχεί στην είσοδο $x_0 = 1$. Έτσι η τιμή u διαμορφώνεται σύμφωνα με την παρακάτω εξίσωση, η οποία αποτελεί το εσωτερικό γινόμενο των διανυσμάτων $w = [w_0, w_1, \ldots, w_n]$ και $x=[x_0, x_1, \ldots, x_n]$.

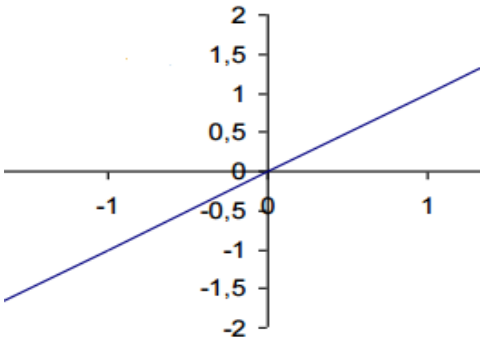
$$u = \sum_{i=1}^{n} w_i x_i - \theta = \sum_{i=1}^{n} w_i x_i + w_0 x_0 = \sum_{i=0}^{n} w_i x_i \qquad (3.5)$$

Το μοντέλο του αισθητήρα χρησιμοποιείται αποκλειστικά για γραμμικά διαχωρίσιμα προβλήματα ταξινόμησης, δύο κατηγοριών. Αναλυτικότερα ο Rosenblatt απέδειξε ότι αν το σύνολο εκπαίδευσης που παρέχεται στον αλγόριθμο εκπαίδευσης του μοντέλου, προέρχεται από δύο γραμμικά διαχωρίσιμες κατηγορίες, τότε ο αλγόριθμος συγκλίνει σε πεπερασμένο αριθμό επαναλήψεων, διαχωρίζοντας τα δεδομένα με τη μορφή ενός υπερεπιπέδου, μεταξύ των δύο κλάσεων. Συνεπώς τα δεδομένα εισόδου διαχωρίζονται σε δύο κατηγορίες, ανάλογα με την έξοδο του μοντέλου (+1 και -1 ή 0). Αν το πρόβλημα δεν είναι γραμμικά διαχωρίσιμο, τότε το μοντέλο του αισθητήρα αποτυγχάνει. Χαρακτηριστικό παράδειγμα μη διαχωρίσιμου προβλήματος αποτελεί η πρόβλεψη της τιμής που εξάγει η συνάρτηση XOR.

3.4.2 Συναρτήσεις Ενεργοποίησης

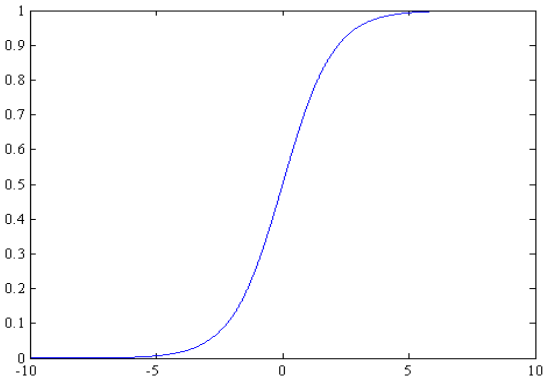
Παραπάνω αναφέρθηκαν οι συναρτήσεις ενεργοποίησης που χρησιμοποιούνται στο μοντέλο του αισθητήρα. Σε τεχνητά νευρωνικά δίκτυα πολλαπλών επιπέδων χρησιμοποιούνται συνήθως η σιγμοειδής ή η γραμμική συνάρτηση, οι οποίες ορίζονται παρακάτω. Οι συνήθεις μορφές της σιγμοειδούς συνάρτησης είναι είτε η λογαριθμική είτε η εφαπτομενική.

$$\text{Γραμμική συνάρτηση} : y = f(u) = u \qquad (3.6)$$



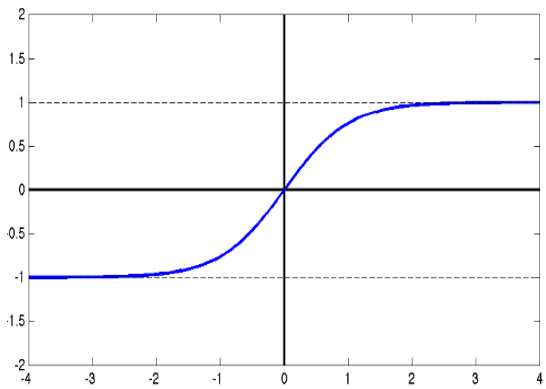
Σχήμα 3.6: Γραφική παράσταση γραμμικής συνάρτησης.

$$\text{Λογαριθμική σιγοειδής συνάρτηση} : y = f(u) = \frac{1}{1+e^{-u}} \qquad (3.7)$$



Σχήμα 3.7: Γραφική παράσταση λογαριθμικής σιγμοειδής συνάρτησης.

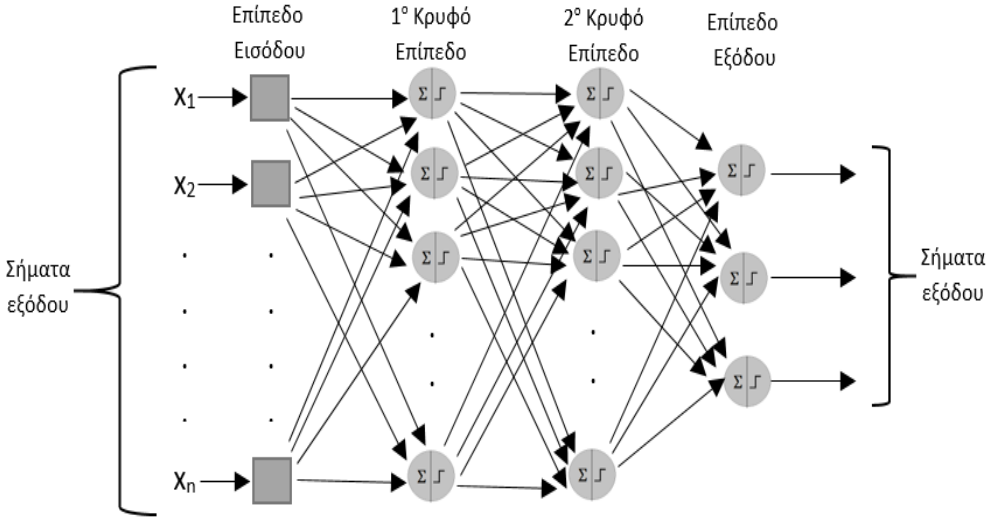
$$\text{Εφαπτομενική σιγοειδής συνάρτηση} : y = f(u) = \frac{2}{1+e^{-2u}} - 1 \qquad (3.8)$$



Σχήμα 3.8: Γραφική παράσταση εφαπτομενικής σιγμοειδής συνάρτησης.

3.4.3 Τεχνικά Νευρωνικά Δίκτυα Πολλαπλών Επιπέδων Perceptron

Τα τεχνικά νευρωνικά δίκτυα πολλαπλών επιπέδων Perceptron (Multi-Layer Perceptron - MLP) αποτελούν μία γενίκευση του μοντέλου του απλού αισθητήρα. Συγκεκριμένα αποτελούνται από ένα σύνολο νευρώνων, οι οποίοι συγκροτούν ένα επίπεδο εισόδου, ένα ή περισσότερα κρυφά επίπεδα και ένα επίπεδο εξόδου. Κάθε επίπεδο μπορεί να περιλαμβάνει οποιοδήποτε αριθμό νευρώνων. Στο Σχήμα 3.9 απεικονίζεται ένα παράδειγμα, ενός τεχνητού νευρωνικού δικτύου πολλαπλών επιπέδων, με δύο κρυφά επίπεδα.



Σχήμα 3.9: Παράδειγμα τεχνητού νευρωνικού δικτύου πολλαπλών επιπέδων με δύο κρυφά επίπεδα.

Όπως παρατηρείται και στο παραπάνω σχήμα, το δίκτυο απαιτείται να είναι πλήρως διασυνδεδεμένο, δηλαδή οι νευρώνες ενός επιπέδου πρέπει να επικοινωνούν αποκλειστικά με όλους τους νευρώνες του αμέσως επόμενου επίπεδου.

Ακριβέστερα, η λειτουργία των συγκεκριμένων μοντέλων ορίζεται ως εξής: Οι νευρώνες στο επίπεδο εισόδου λαμβάνουν τα εισερχόμενα σήματα και τα μεταβιβάζουν χωρίς καμία επεξεργασία στου νευρώνες του πρώτου κρυφού επιπέδου. Η συμπεριφορά των επόμενων νευρώνων στα κρυφά επίπεδα και στο επίπεδο εξόδου είναι η ίδια με αυτή που παρουσιάστηκε στο μοντέλο του αισθητήρα. Δηλαδή, υπολογίζουν την εκάστοτε έξοδο, αθροίζοντας αρχικά τα γινόμενα των εξερχόμενων σημάτων, των προηγούμενων επιπέδων, επί τα αντίστοιχα συναπτικά βάρη και έπειτα χρησιμοποιούν μία συνάρτηση ενεργοποίησης, στην οποία μεταβιβάζεται ως παράμετρος το προηγούμενο άθροισμα, αφαιρώντας από αυτό την πόλωση του εκάστοτε νευρώνα.

Το πλήθος των κρυμμένων επιπέδων, καθώς και ο αριθμός των νευρώνων που περιλαμβάνουν καθορίζουν την αρχιτεκτονική του τεχνητού νευρωνικού δικτύου. Η προσθήκη επιπλέον επιπέδων σε σύγκριση με το μοντέλο του αισθητήρα, οδηγεί στη δυνατότητα επίλυσης μη διαχωρίσιμων γραμμικών προβλημάτων, καθώς και προβλημάτων ταξινόμησης, που περιλαμβάνουν παραπάνω από δύο κατηγορίες. Συγκεκριμένα δίκτυα, τα οποία περιλαμβάνουν τρία επίπεδα νευρώνων (ένα επίπεδο εισόδου, ένα κρυφό επίπεδο, ένα επίπεδο εξόδου) έχουν τη δυνατότητα να

προσεγγίσουν οποιαδήποτε συνεχή συνάρτηση, σε οποιαδήποτε επιθυμητή ακρίβεια [32,33].

3.4.4 Εκπαίδευση Τεχνητών Νευρωνικών Δικτύων

Η εκπαίδευση των τεχνητών νευρωνικών δικτύων, αφορά τον καθορισμό των τιμών, των συνοπτικών βαρών και των πολώσεων των νευρώνων, όλων των κρυφών επιπέδων και του επιπέδου εξόδου, ώστε τα υπό εξέταση αντικείμενα ενός προβλήματος ταξινόμησης, να κατηγοριοποιούνται με υψηλό ποσοστό ακρίβειας στις αντίστοιχες κατηγορίες.

Συγκεκριμένα, στόχος ενός αλγόριθμου εκπαίδευσης σε ένα τεχνητό νευρωνικό δίκτυο, δεδομένου της ύπαρξης ενός κατηγοριοποιημένου συνόλου εκπαίδευσης, αποτελεί ο καθορισμός ενός διανύσματος βαρών w, το οποίο θα ελαχιστοποιεί το συνολικό άθροισμα των τετραγωνικών σφαλμάτων, που ορίζεται από την εξίσωση (3.9). Στη συγκεκριμένη σχέση, όπου t_i ορίζεται η εκάστοτε έξοδος του συνόλου εκπαίδευσης, ενώ ως y_i ορίζεται η τρέχουσα έξοδος που υπολόγισε το μοντέλο.

$$E(w) = \frac{1}{2} \sum_{i=1}^{N} (t_i - y_i)^2 \qquad (3.9)$$

Έχουν αναπτυχθεί αρκετοί αλγόριθμοι για την εκπαίδευση τεχνητών νευρωνικών δικτύων. Γενικότερα, δεν προτείνεται η χρησιμοποίηση κάποιου με καθολική ισχύ, καθώς η απόδοσή τους εξαρτάται από το πρόβλημα που εξετάζεται. Χαρακτηριστική κατηγορία αποτελούν οι αλγόριθμοι που στηρίζονται στη μέθοδο της βαθμωτής κατάβασης. Η σχέση ενημέρωσης των βαρών που χρησιμοποιείται για τη συγκεκριμένη μέθοδο, περιγράφεται από την εξίσωση (3.10). Όπου n θεωρείται ο ρυθμός μάθησης, ο οποίος αποτελεί μία σταθερά στο διάστημα (0,1] και καθορίζει το βαθμό με τον οποίο θα μεταβάλλονται τα βάρη σε κάθε επαναληπτική διαδικασία.

$$w_j \leftarrow -n \frac{\partial E(w)}{\partial w_j} \qquad (3.10)$$

Η μέθοδος της βαθμωτής κατάβασης εμφανίζει συγκεκριμένα μειονεκτήματα. Αναλυτικότερα, ο δεύτερος όρος της εξίσωσης (3.10) ορίζει πως το εκάστοτε βάρος θα πρέπει να αυξάνεται προς την κατεύθυνση που μειώνεται ο συνολικός όρος σφάλματος. Ωστόσο, αν η συνάρτηση ενεργοποίησης που χρησιμοποιείται είναι μη γραμμική, τότε είναι πιθανό η μέθοδος της βαθμωτής κατάβασης να παγιδευτεί σε ένα τοπικό ελάχιστο όριο. Ακόμη παρουσιάζει αδυναμία, στον υπολογισμό των βαρών των κρυφών νευρώνων, καθώς δεν είναι δυνατή η εκτίμηση του όρου σφάλματος $\partial E/\partial w_j$, στην περίπτωση που δεν παρέχονται από το σύνολο εκπαίδευσης, οι τιμές των εξόδων, των κρυφών νευρώνων.

Για την επίλυση των συγκεκριμένων προβλημάτων, αναπτύχθηκε ο αλγόριθμος οπισθοδιάδοσης του σφάλματος (back-propagation), στον οποίο στηρίζονται οι περισσότεροι σύγχρονοι αλγόριθμοι εκπαίδευσης τεχνητών νευρωνικών δικτύων. Στον

συγκεκριμένο αλγόριθμο, ορίζονται δύο σύνολα ενεργειών σε κάθε επανάληψη, τα οποία ονομάζονται εμπρόσθια και οπίσθια φάση. Κατά την εμπρόσθια φάση, τα βάρη που λαμβάνονται από την προηγούμενη επανάληψη, χρησιμοποιούνται για τον υπολογισμό της τιμής εξόδου του κάθε νευρώνα. Ο υπολογισμός συνεχίζει σε μία κατάσταση προς τα εμπρός, δηλαδή τα αποτελέσματα των νευρώνων στο επίπεδο k υπολογίζονται πριν από τα αποτελέσματα στο επίπεδο k+1. Κατά τη διάρκεια της οπίσθιας φάσης, εφαρμόζεται η σχέση ενημέρωσης των βαρών στην αντίθετη κατεύθυνση. Με άλλα λόγια, τα βάρη στο επίπεδο k+1 ενημερώνονται πριν ανανεωθούν τα βάρη του επιπέδου k. Συμπερασματικά, η συγκεκριμένη προσέγγιση οπισθοδιάδοσης επιτρέπει να χρησιμοποιηθούν τα σφάλματα των νευρώνων στο επίπεδο k+1 για να εκτιμηθούν τα σφάλματα στο επίπεδο k.

Για την εκπαίδευση του τεχνητού νευρωνικού δικτύου που υλοποιήθηκε στο πλαίσιο της διπλωματικής εργασίας, χρησιμοποιήθηκε ο αλγόριθμός Levenberg – Marquardt. Η συγκεκριμένη τεχνική εμφανίζει γρήγορη σύγκλιση, συνδυάζοντας τους αλγόριθμους εκπαίδευσης Back-Propagation και Gauss-Newton [50].

3.4.5 Τεχνητά Νευρωνικά Δίκτυα στην Ανίχνευση Εισβολών

Αν και τα συστήματα ανίχνευσης εισβολών έχουν σημειώσει σημαντική εξέλιξη με την πάροδο του χρόνου, κύρια αδυναμία τους παραμένει η ανίχνευση άγνωστων κακόβουλων λογισμικών, καθώς και τα υψηλά ποσοστά εσφαλμένων ειδοποιήσεων, τα οποία οφείλονται κυρίως στη δυναμική φύση των συστημάτων και των δικτύων. Από διάφορα ερευνητικά μοντέλα, έχει διαπιστωθεί πως η χρησιμοποίηση τεχνητών νευρωνικών δικτύων, στο πλαίσιο ενός προτύπου ανίχνευσης διαταραχών, αποτελεί μία αρκετά υποσχόμενη λύση για την αντιμετώπιση των παραπάνω προβλημάτων. Συγκεκριμένα, η ικανότητά τους να προβλέπουν άγνωστες μορφές επιθέσεων, αλλά και η δυνατότητα ταξινόμησης ήδη γνωστών κακόβουλων ενεργειών σε συγκεκριμένες κατηγορίες, αποτέλεσαν την αφορμή για τη μελέτη της εφαρμογής τους, στον τομέα της ανίχνευσης εισβολών.

Η πιο διαδομένη κατηγορία τεχνητών νευρωνικών δικτύων που χρησιμοποιείται στον τομέα της ανίχνευσης εισβολών, είναι τα τεχνικά νευρωνικά δίκτυα πολλαπλών επιπέδων Perceptron. Αρχικές προσπάθειες ανίχνευσης εισβολών που αναπτύχθηκαν, στηριζόμενες στη συγκεκριμένη κατηγορία τεχνητών νευρωνικών δικτύων, παρουσιάζονται στις βιβλιογραφικές αναφορές [34, 35, 36,37,38]. Αρχικά, ερευνήθηκε η χρήση τους στην ανίχνευση πιθανών άγνωστων διαταραχών και στη συνέχεια εφαρμόστηκαν στο μοντέλο κακής συμπεριφοράς, για την ταξινόμηση μίας εισβολής, σε έναν συγκεκριμένο τύπο επίθεσης. Μία σχετικά νέα προσέγγιση αποτέλεσε ο συνδυασμός των παραπάνω περιπτώσεων.

Πιο πρόσφατες μελέτες εφαρμογής των τεχνητών νευρωνικών δικτύων στο πεδίο της ανίχνευσης εισβολών, βασίστηκαν στο μη εποπτευόμενο μοντέλο εκπαίδευσης και κυρίως στην κατηγορία των αυτοοργανούμενων τεχνητών νευρωνικών δικτύων (Self Organizing Map – SOM). Η συγκεκριμένη τεχνική χρησιμοποιήθηκε κυρίως σε συστήματα ανίχνευσης εισβολών μεμονωμένου συστήματος, για την ανάλυση της συμπεριφοράς του χρήστη [39,40].

3.5 Μέτρα Αξιολόγησης

Στόχος ενός αλγόριθμου ταξινομητή αποτελεί η σωστή κατηγοριοποίηση όλων των εισερχόμενων αντικειμένων εξέτασης. Στην παρούσα ενότητα αναλύονται ορισμένες μετρικές, οι οποίες αξιολογούν την εξόρυξη της πληροφορίας του ταξινομητή. Αναλυτικότερα οι εξισώσεις που αναλύονται στις παρακάτω υποενότητες, χρησιμοποιούν τις ακόλουθες τέσσερις δυνατές εκβάσεις μιας προσπάθειας δυαδικής ταξινόμησης.

- TP (True Positive): Δηλώνει το πλήθος των περιπτώσεων ορθής ταξινόμησης ενός θετικού παραδείγματος, στην κατηγορία των θετικών παραδειγμάτων. Αντίστοιχα στη διαδικασία ανίχνευσης εισβολών, θεωρείται ως το πλήθος των περιπτώσεων ορθής ταξινόμησης, μίας επιθετικής δραστηριότητας, στην κατηγορία των ενεργειών μη φυσιολογικής συμπεριφοράς.
- TN (True Negative): Δηλώνει το πλήθος των περιπτώσεων ορθής ταξινόμησης, ενός αρνητικού παραδείγματος, στην κατηγορία των αρνητικών παραδειγμάτων. Αντίστοιχα στη διαδικασία ανίχνευσης εισβολών, θεωρείται ως το πλήθος των περιπτώσεων ορθής ταξινόμησης, μίας μη επιθετικής δραστηριότητας, στην κατηγορία των ενεργειών φυσιολογικής συμπεριφοράς.
- FN (False Negative): Δηλώνει το πλήθος των περιπτώσεων εσφαλμένης ταξινόμησης, ενός θετικού παραδείγματος, στην κατηγορία των αρνητικών παραδειγμάτων. Αντίστοιχα στη διαδικασία ανίχνευσης εισβολών, θεωρείται ως το πλήθος των περιπτώσεων εσφαλμένης ταξινόμησης, μίας επιθετικής δραστηριότητας, στην κατηγορία των ενεργειών φυσιολογικής συμπεριφοράς.
- FN (False Positive): Δηλώνει το πλήθος των περιπτώσεων εσφαλμένης ταξινόμησης, ενός αρνητικού παραδείγματος, στην κατηγορία των θετικών παραδειγμάτων. Αντίστοιχα στη διαδικασία ανίχνευσης εισβολών, θεωρείται ως το πλήθος των περιπτώσεων εσφαλμένης ταξινόμησης μίας μη επιθετικής δραστηριότητας, στην κατηγορία των ενεργειών μη φυσιολογικής συμπεριφοράς.

3.5.1 Ακρίβεια

Ως ακρίβεια (accuracy) ορίζεται η αναλογία των συνολικών προβλέψεων που ήταν ορθές:

$$\text{Ακρίβεια} = \frac{\text{Σύνολο ορθών προβλέψεων}}{\text{Σύνολο προβλέψεων}} \qquad (3.12)$$

Σε ένα πρόβλημα ταξινόμησης δύο κατηγοριών, ο τύπος της ακρίβειας διαμορφώνεται σύμφωνα με την ακόλουθη εξίσωση.

$$\text{Ακρίβεια} = \frac{TP+TN}{TP+TN+FP+FN} \qquad (3.13)$$

3.5.2 Ορθότητα

Ως ορθότητα (precision) ορίζεται η δεσμευμένη πιθανότητα, αν ταυτίζεται η κατηγορία που προβλέπει ένας ταξινομητής, για ένα στιγμιότυπο με την πραγματική του κατηγορία:

$$\text{Ορθότητα} = \frac{\text{Σύνολο ορθών προβλέψεων κλάσης } c}{\text{Σύνολο προβλέψεων κλάσης } c} \quad (3.14)$$

Σε ένα πρόβλημα ταξινόμησης δύο κατηγοριών, η εξίσωση της ορθότητας διαμορφώνεται σύμφωνα με τους ακόλουθους τύπους.

$$\text{Ορθότητα}_P = \frac{TP}{TP+FP} \quad (3.15)$$

$$\text{Ορθότητα}_N = \frac{TN}{TN+FN} \quad (3.16)$$

3.5.3 Ανάκληση

Ως ανάκληση (recall) ορίζεται η δεσμευμένη πιθανότητα, αν ένα στιγμιότυπο ανήκει σε μία κλάση, έστω c και αυτή αναγνωριστεί ορθά από τον ταξινομητή:

$$\text{Ανάκληση} = \frac{\text{Σύνολο προβλέψεων κλάσης } c}{\text{Δεδομένα κλάσης } c} \quad (3.17)$$

Σε ένα πρόβλημα ταξινόμησης δύο κατηγοριών, η εξίσωση της ανάκλησης διαμορφώνεται σύμφωνα με τους ακόλουθους τύπους.

$$\text{Ανάκληση}_P = \frac{TP}{TP+FN} \quad (3.18)$$

$$\text{Ανάκληση}_N = \frac{TN}{TN+FP} \quad (3.19)$$

3.5.4 Μέτρο F

Πρακτικά, οι δύο παραπάνω μετρικές δεν μπορούν να εκτιμηθούν χωριστά, καθώς παρέχουν μια αλληλοσυμπληρούμενη εικόνα της αποτελεσματικότητας ενός

ταξινομητή. Ένα μέτρο που τα συνδυάζει είναι η συνάρτηση F (F–score), που ορίζεται από την ακόλουθη εξίσωση.

$$F_C = \frac{2 \times \text{Ορθότητα}_C \times \text{Ανάκληση}_C}{\text{Ορθότητα}_C + \text{Ανάκληση}_C} \quad (3.20)$$

Κεφάλαιο 4

Ανάλυση και Σχεδίαση της Εφαρμογής

Στο συγκεκριμένο κεφάλαιο θα αναλυθεί η μεθοδολογία ανάπτυξης και σχεδίασης της εφαρμογής ανίχνευσης εισβολών «EyeSec» που υλοποιήθηκε στο πλαίσιο της παρούσας διπλωματικής εργασίας. Αναλυτικότερα, θα παρουσιαστεί η περιγραφή των απαιτήσεων της εφαρμογής, οι βασικές λειτουργίες που επιτελεί, καθώς και η ανάλυση των περιπτώσεων χρήσης. Τέλος, θα αναλυθούν οι τεχνικές ανάπτυξης που ακολουθήθηκαν και θα πραγματοποιηθεί σχετική αναφορά στα προγραμματιστικά εργαλεία που χρησιμοποιήθηκαν κατά την υλοποίηση.

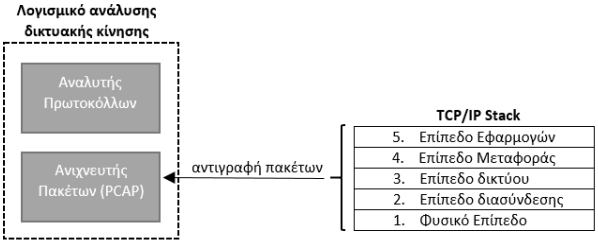
4.1 Περιγραφή Εφαρμογής «EyeSec»

Το σύστημα ανίχνευσης εισβολών «EyeSec» αποτελεί ένα μοντέλο μεμονωμένου συστήματος, για κινητές συσκευές με λειτουργικό σύστημα Android, στο οποίο ο χρήστης θα πρέπει να διαθέτει δικαιώματα διαχειριστή. Αναλυτικότερα, εντάσσεται στην κατηγορία ανίχνευσης διαταραχών, καθώς η λειτουργία του βασίζεται στη χρήση ενός τεχνητού νευρωνικού δικτύου πολλαπλών επιπέδων Perceptron, το οποίο αναλύει τις αμφίδρομες δικτυακές ροές, για την αναγνώριση άγνωστων πιθανών εισβολών. Έχει διαπιστωθεί πως η ανάλυση των χαρακτηριστικών των δικτυακών ροών, μπορεί να εντοπίσει πληθώρα δικτυακών εισβολών, όπως επιθέσεις άρνησης υπηρεσιών, ενέργειες σάρωσης των δικτυακών θυρών, καθώς και αυτοαναπαραγόμενα κακόβουλα λογισμικά (worms). Συγκεκριμένα, στην εφαρμογή ορίζονται δύο καταστάσεις λειτουργίας: η ανάλυση της δικτυακής κίνησης και η ανίχνευση εισβολών.

4.1.1 Ανάλυση Δικτυακής Κίνησης

Η ανάλυση του δικτύου (network analysis) ορίζεται ως η διαδικασία κατά την οποία καταγράφονται και αναλύονται όλα τα δικτυακά πακέτα που διακινούνται σε ένα δίκτυο υπολογιστικών συστημάτων. Συγκεκριμένα, τα λογισμικά ανάλυσης της δικτυακής κίνησης αποτελούνται από δύο δομικά στοιχεία: έναν ανιχνευτή πακέτων (sniffer) και έναν αναλυτή πρωτοκόλλων (protocol analyzer).

Ο ανιχνευτής πακέτων παρατηρεί και καταγράφει τα πακέτα που διακινούνται στο δίκτυο, χωρίς να επεμβαίνει στην κατάσταση του δικτύου. Συγκεκριμένα, λαμβάνει ένα αντίγραφο των πακέτων που αποστέλλονται ή λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που εκτελούνται στα υπολογιστικά συστήματα. Αντίστοιχα, ο αναλυτής πρωτοκόλλων αναλαμβάνει την αποκωδικοποίηση και την ταξινόμηση των δικτυακών πακέτων σε γνωστά πρωτόκολλα επικοινωνίας. Στο Σχήμα 4.1 απεικονίζεται η δομή ενός λογισμικού ανάλυσης της δικτυακής κίνησης, που αφορά τη στοίβα TCP/IP.



Σχήμα 4.1: Δομή ενός λογισμικού ανάλυσης δικτυακής κίνησης.

Συμπερασματικά, η συγκεκριμένη λειτουργία της εφαρμογής παρακολουθεί την κίνηση του δικτύου και παρέχει στον χρήστη σημαντικές πληροφορίες, αναφορικά με αυτή. Αναλυτικότερα, παρουσιάζει μία αναγνώσιμη μορφή των δικτυακών πακέτων που καταγράφηκαν, καθώς και τη δεκαεξαδική αναπαράσταση τους. Επιπλέον, παρέχει συγκεκριμένα στατιστικά στοιχεία, σχετικά με τα πρωτόκολλα των πακέτων και των δεδομένων που έχουν παραληφθεί από τα σημεία τερματισμού, ομόλογων επιπέδων. Τέλος, εμφανίζει στον χρήστη τις δικτυακές επικοινωνίες και το πλήθος των πακέτων που ανταλλάχθηκαν, μεταξύ δύο σημείων τερματισμού.

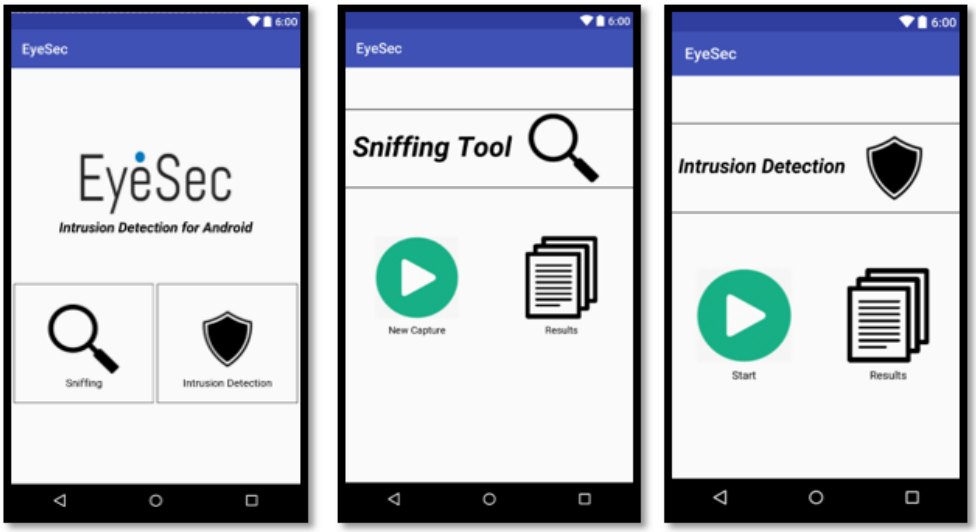
4.1.2 Ανίχνευση Εισβολών

Αυτή η λειτουργία της εφαρμογής αποτελεί στην ουσία το σύστημα ανίχνευσης εισβολών, το οποίο όπως αναφέρθηκε βασίζεται στις υπολογιστικές διαδικασίες ενός τεχνητού νευρωνικού δικτύου. Αναλυτικότερα η συγκεκριμένη λειτουργία, ύστερα από μία παρακολούθηση του δικτύου, εμφανίζει στον χρήστη το σύνολο των αμφίδρομων δικτυακών ροών, που εμφάνισαν ύποπτη δραστηριότητα.

4.2 Πρότυπο Εφαρμογής «EyeSec»

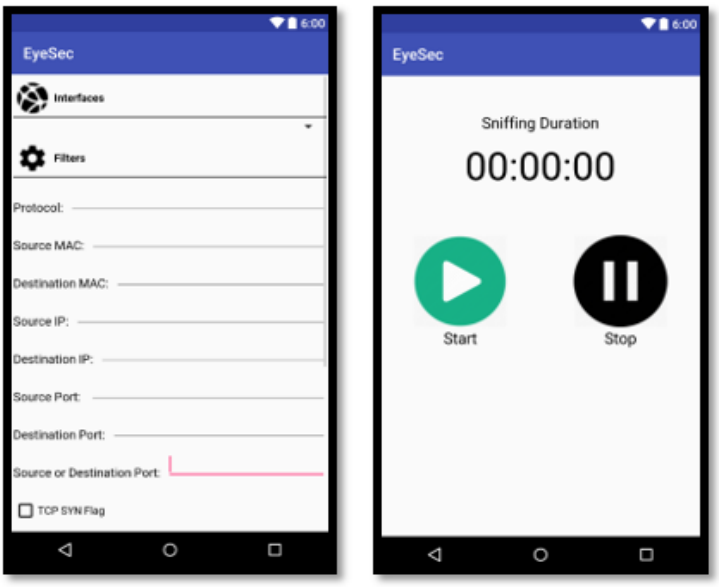
Πριν τη διαδικασία προγραμματισμού της εφαρμογής, δημιουργήθηκε ένα προσχέδιο των βασικών οθονών και των λειτουργιών της. Το πρότυπο αυτό

δημιουργήθηκε, ώστε να εντοπιστεί η κατάλληλη διεπαφή χρήστη της εφαρμογής. Συγκεκριμένα στο Σχήμα 4.2 απεικονίζονται τρεις οθόνες της εφαρμογής, όπου αντίστοιχα παρουσιάζουν το αρχικό μενού εργαλείων, το μενού επιλογών για τη διαδικασία ανάλυση της δικτυακής κίνησης και το μενού επιλογών για τη λειτουργία της ανίχνευσης εισβολών.



Σχήμα 4.2: Προσχέδιο οθόνης αρχικό μενού επιλογών, οθόνης μενού επιλογών ανάλυσης δικτυακής κίνησης, οθόνης μενού επιλογών ανίχνευσης εισβολών.

Αντίστοιχα στο Σχήμα 4.3 παρουσιάζονται δύο οθόνες, όπου η πρώτη απεικονίζει έναν κατάλογο από παραμέτρους που μπορούν να επιλεγούν κατά τη διαδικασία μίας νέα ανάλυσης του δικτύου, ενώ η δεύτερη απεικονίζει τη χρονική διάρκεια που πραγματοποιείται η παρακολούθηση του δικτύου και για τις δύο καταστάσεις λειτουργίας της εφαρμογής.



Σχήμα 4.3: Προσχέδιο οθόνης επιλογής παραμέτρων ανάλυσης του δικτύου και οθόνης εμφάνισης χρονικής διάρκειας παρακολούθησης της δικτυακής κίνησης.

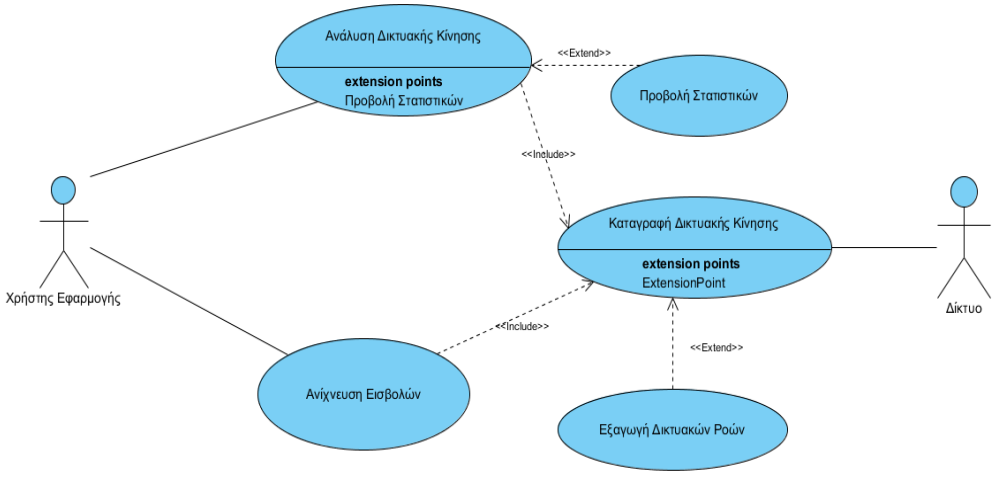
4.3 Περιγραφή Απαιτήσεων Εφαρμογής

Στη διαδικασία περιγραφής των απαιτήσεων της εφαρμογής θα αναλυθούν οι οντότητες του συστήματος, οι περιπτώσεις χρήσης που παρουσιάζει, καθώς και το σύνολο των διασυνδεδεμένων μονάδων που συνθέτουν την εφαρμογή.

4.3.1 Περιπτώσεις Χρήσης

Η ανάλυση των απαιτήσεων χρήσης (use case analysis) ή ανάλυση ευρωστίας (robustness analysis) αποτελεί μία μέθοδο για τον προσδιορισμό της συμπεριφοράς του συστήματος, για την κάλυψη των απαιτήσεων που είναι καταγεγραμμένες στις περιπτώσεις χρήσης [41]. Στη συγκεκριμένη ενότητα θα περιγραφούν οι περιπτώσεις χρήσης για την πλοήγηση του χρήστη στην εφαρμογή.

Αναλυτικότερα, η εφαρμογή περιλαμβάνει μία βασική οντότητα που είναι ο χρήστης της εφαρμογής και μία δευτερεύουσα οντότητα που αποτελεί το εκάστοτε δίκτυο. Οι λειτουργίες που εκτελούνται από τον χρήστη της εφαρμογής, όπως απεικονίζονται και στο διάγραμμα περιπτώσεων χρήσης στο Σχήμα 4.4, είναι η ανάλυση της δικτυακής κίνησης και η ανίχνευση εισβολών, όπως αυτές αναλύθηκαν στην ενότητα της περιγραφής της εφαρμογής.



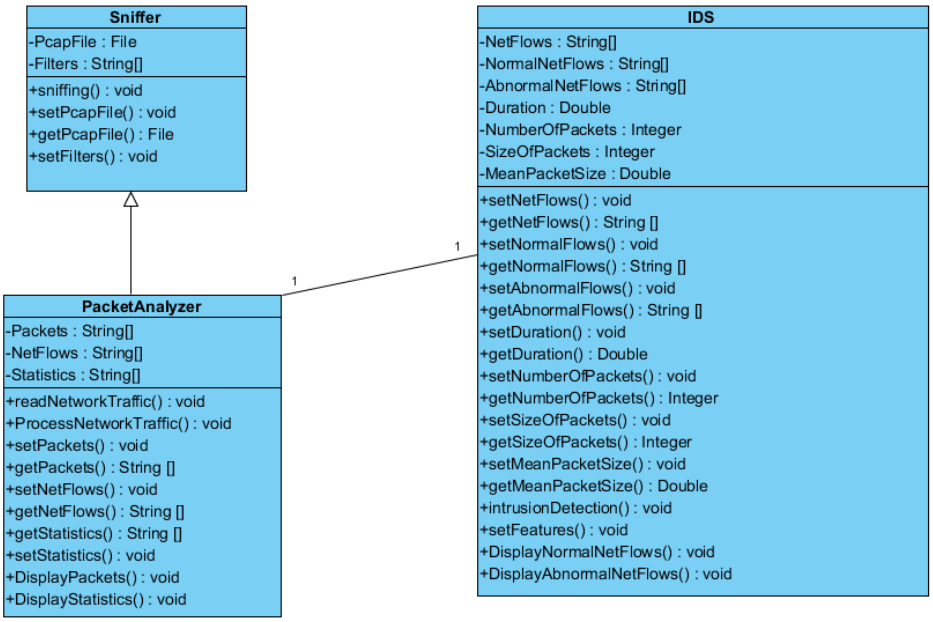
Σχήμα 4.4: Διάγραμμα περίπτωσης χρήσης εφαρμογής.

4.3.2 Διάγραμμα Κλάσεων

Το διάγραμμα κλάσεων χρησιμοποιείται στην ανάλυση για την ανάδειξη των σημαντικότερων εννοιών του προβλήματος, όπως επίσης και στη σχεδίαση για τη λεπτομερέστερη προδιαγραφή των βασικότερων μονάδων του αντικειμενοστραφούς προγραμματισμού, που είναι οι κλάσεις του λογισμικού. Αποτελεί ένα από τα σημαντικότερα διαγράμματα της Unified Modeling Language (UML) και χρησιμοποιείται καθ' όλη τη διάρκεια του κύκλου ζωής του λογισμικού [41].

Εξαιτίας της επιλογής υλοποίησης της εφαρμογής «EyeSec» σε κινητές συσκευές με λειτουργικό σύστημα Android, χρησιμοποιήθηκε η γλώσσα προγραμματισμού Java. Λόγω της αντικειμενοστραφούς φύσης της συγκεκριμένης γλώσσας, κρίθηκε

απαραίτητο η σχεδίαση ενός διαγράμματος, το οποίο θα περιλαμβάνει τις κλάσεις που θα πρέπει να υλοποιηθούν κατά τον προγραμματισμό της εφαρμογής. Το συγκεκριμένο διάγραμμα απεικονίζεται στο Σχήμα 4.5, στο οποίο αποτυπώνονται οι κλάσεις του συστήματος, συμπεριλαμβανομένου των πεδίων και των μεθόδων που υποστηρίζουν, καθώς και των τρόπων διασύνδεσης, μεταξύ τους.



Σχήμα 4.5: Διάγραμμα κλάσεων εφαρμογής.

4.4 Προγραμματιστικά Εργαλεία Ανάπτυξης

Η υλοποίηση της εφαρμογής «EyeSec» βασίστηκε σε πληθώρα προγραμματιστικών τεχνολογιών και εργαλείων. Συγκεκριμένα για τη σχεδίαση και την ανάπτυξη της λειτουργικότητας της εφαρμογής, χρησιμοποιήθηκε κατά κόρον το ολοκληρωμένο περιβάλλον ανάπτυξης (Integrated Development Environment - IDE) Android Studio και η συνδυαστική χρήση των γλωσσών προγραμματισμού Java και XML. Επιπλέον, η διαδικασία καταγραφής και ανάλυσης της δικτυακής κίνησης πραγματοποιήθηκε, χρησιμοποιώντας μία στατική έκδοση της γλώσσας προγραμματισμού Python και συγκεκριμένα της βιβλιοθήκης διαχείρισης δικτυακών πακέτων, Scapy. Τέλος για τη διαδικασία εκπαίδευσης του τεχνητού νευρωνικού δικτύου, χρησιμοποιήθηκε το λογισμικό MATLAB και η ειδικότερα το υπολογιστικό πακέτο Neural Network Toolbox.

4.4.1 Android Studio

Το μεγαλύτερο τμήμα της εφαρμογής «EyeSec» υλοποιήθηκε, χρησιμοποιώντας το λογισμικό Android Studio. Το Android Studio αποτελεί ένα IDE, βασισμένο στο λογισμικό της JetBrains' IntelliJ IDEA, και διατίθεται για λειτουργικά συστήματα Windows, Mac OS X και Linux. Από το Δεκέμβριο του 2014 αντικατέστησε το

λογισμικό Eclipse Android Development Tools (ADT) ως το κύριο IDE της Google, για την ανάπτυξη εφαρμογών Android.

Οι εφαρμογές Android που υλοποιούνται με το προαναφερθέν λογισμικό, χρησιμοποιούν για τον προγραμματισμό τους, τον συνδυασμό των γλωσσών προγραμματισμού Java και XML. Η πρώτη χρησιμοποιείται για τον προγραμματισμό της λειτουργικότητας της εφαρμογής, ενώ η δεύτερη για τη σχεδίαση της διεπαφής χρήστη.

Τέλος για τη δημιουργία διαγραμμάτων στατιστικών περιεχομένων, που παρέχει η εφαρμογή, χρησιμοποιήθηκε η εξωτερική βιβλιοθήκη Androidplot. Η συγκεκριμένη βιβλιοθήκη παρέχει τη δυνατότητα κατασκευής στατικών και δυναμικών γραφικών αναπαραστάσεων και η λειτουργικότητά της προσαρτάται στην εφαρμογή, διαμέσου ειδικών επεκτάσεων που προσφέρονται από το Android Studio.

4.4.2 Python και Scapy

Η Python αποτελεί μία υψηλού επιπέδου αντικειμενοστρεφή και διαδικαστική γλώσσα προγραμματισμού, η οποία μπορεί να εφαρμοστεί σε πολλαπλές αρχιτεκτονικές λειτουργικών συστημάτων [42]. Η χρησιμοποίησή της στην εφαρμογή «EyeSec» δικαιολογείται από την ύπαρξη της βιβλιοθήκης Scapy, η οποία απλοποιεί ιδιαίτερα την υλοποίηση της διαδικασίας καταγραφής και ανάλυσης της δικτυακής κίνησης. Συγκεκριμένα για τη δημιουργία της εφαρμογής χρησιμοποιήθηκε μία στατική έκδοση της Python 2.7, της οποίας τα σενάρια (python scripts) εκτελούνται από κλήσεις exec του λειτουργικού συστήματος.

Η βιβλιοθήκη Scapy αποτελεί στην ουσία ένα πρόγραμμα διαχείρισης δικτυακών πακέτων, υλοποιημένο στη γλώσσα προγραμματισμού Python, με παρόμοια χρήση, όπως αυτή των λογισμικών Wireshark, Tcpdump, Kismet, κτλ. Το κύριο πλεονέκτημα που παρουσιάζει, είναι ότι παρέχει προγραμματιστική πρόσβαση στις μεθόδους και στις δομές δεδομένων, που χρησιμοποιεί για τη λειτουργία της.

4.4.3 MATLAB και Neural Network Toolbox

Το MATLAB αποτελεί ένα διαδραστικό (interactive) πρόγραμμα για αριθμητικούς υπολογισμούς και οπτικοποίηση δεδομένων (data visualization) με δυνατότητες προγραμματισμού, οι οποίες το καθιστούν ένα σημαντικό εργαλείο στις θετικές επιστήμες. Η χρησιμοποίησή του, οφείλεται στην ύπαρξη του λογισμικού Neural Network Toolbox (nntool) το οποίο απλοποιεί τις διαδικασίες μοντελοποίησης και διαχείρισης των τεχνητών νευρωνικών δικτύων, παρέχοντας υλοποιημένες μεθόδους για την εφαρμογή των αλγόριθμων εκπαίδευσης και τους υπολογισμούς των συναρτήσεων ενεργοποίησης.

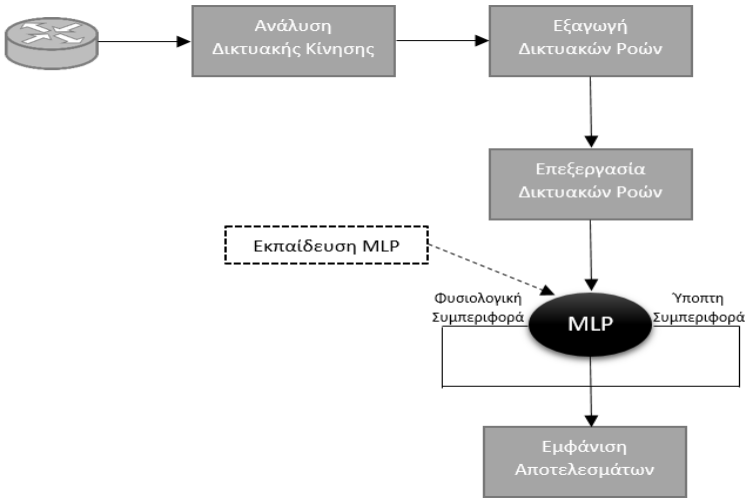
4.5 Λεπτομερής Ανάλυση Εφαρμογής

Η διαδικασία της λεπτομερούς σχεδίασης επικεντρώνεται στην εσωτερική δομή των μονάδων, τις δομές δεδομένων και τους αλγόριθμους που αυτές χρησιμοποιούν. Η λεπτομερής παρουσίαση των δεδομένων, η περιγραφή της επεξεργασίας των

αλγορίθμων, η σχέση δεδομένων και επεξεργασιών, καθώς και η εσωτερική οργάνωση της κάθε μονάδας παρέχουν την αναγκαία λεπτομέρεια για να καταστεί δυνατή η υλοποίηση των μονάδων [41].

Συγκεκριμένα στην παρούσα ενότητα, θα αναλυθούν οι διαδικασίες που ακολουθήθηκαν για την κατασκευή των λειτουργιών της εφαρμογής. Η ανάλυση επικεντρώνεται κυρίως στη λειτουργία της ανίχνευσης εισβολών, καθώς η διαδικασία ανάλυσης της δικτυακής κίνησης, επιτυγχάνεται μέσω αυτοματοποιημένων μεθόδων της βιβλιοθήκης Scapy.

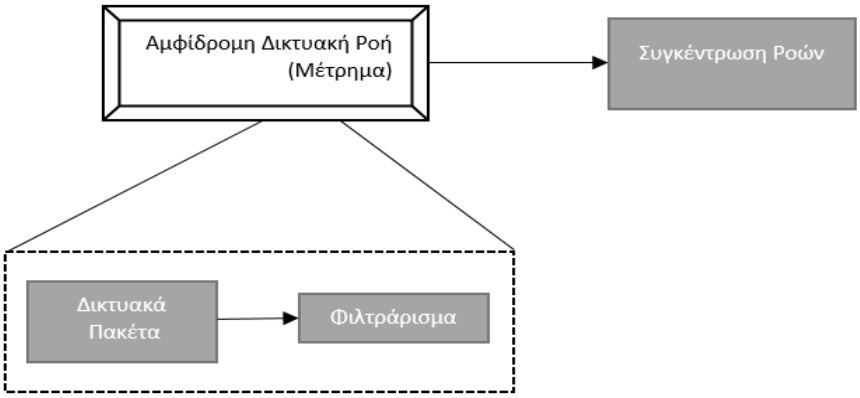
Όπως έχει αναφερθεί το σύστημα ανίχνευσης εισβολών που ενσωματώνει η εφαρμογή «EyeSec» στηρίζεται στις υπολογιστικές διαδικασίες ενός τεχνητού νευρωνικού δικτύου πολλαπλών Perceptron. Ακριβέστερα το MLP που σχεδιάστηκε, επεξεργάζεται συγκεκριμένα χαρακτηριστικά των δικτυακών ροών και βάσει αυτών τις ταξινομεί είτε στην κατηγορία «φυσιολογικής συμπεριφοράς» (normal), είτε στην κατηγορία «ύποπτης συμπεριφοράς» (abnormal). Το Σχήμα 4.6 απεικονίζει τη συνολική δομή των επιμέρους διεργασιών της λειτουργίας ανίχνευσης εισβολών, οι οποίες είναι η εκπαίδευση του τεχνητού νευρωνικού δικτύου, η ανάλυση της δικτυακής κίνησης, η εξαγωγή των αμφίδρομών δικτυακών ροών, η επεξεργασία των δικτυακών ροών και η εφαρμογή των υπολογιστικών διαδικασιών του τεχνητού νευρωνικού δικτύου.



Σχήμα 4.6: Δομή λειτουργίας ανίχνευσης εισβολών.

4.5.1 Εξαγωγή Δικτυακών Ροών

Στο Σχήμα 4.7 απεικονίζεται η διαδικασία που πραγματοποιείται για την απομόνωση και τη συγκέντρωση των αμφίδρομων δικτυακών ροών από το σύνολο της δικτυακής κίνησης. Συγκεκριμένα σύμφωνα με τον ορισμό που αποδόθηκε στο Κεφάλαιο 2, η ανίχνευση των αμφίδρομων δικτυακών ροών, απαιτεί μηχανισμούς σύγκρισης, οι οποίοι θα ελέγχουν τα πακέτα που ανταλλάσσονται μεταξύ δύο συγκεκριμένων διευθύνσεων IP, με συγκεκριμένες δικτυακές θύρες. Η διαδικασία αυτή, διευκολύνεται σε μεγάλο βαθμό από την προγραμματιστική πρόσβαση που παρέχει η βιβλιοθήκη Scapy, στις δομές δεδομένων που χρησιμοποιεί.



Σχήμα 4.7: Εξαγωγή αμφίδρομων δικτυακών ροών IP.

4.5.2 Επεξεργασία Δικτυακών Ροών

Κατά την επεξεργασία των αμφίδρομων δικτυακών ροών, αποσπώνται από αυτές συγκεκριμένα χαρακτηριστικά, σύμφωνα με τα οποία πραγματοποιήθηκε η εκπαίδευση του τεχνητού νευρωνικού δικτύου. Ακριβέστερα, επιλέχθηκαν τα ακόλουθα χαρακτηριστικά:

- Διάρκεια δικτυακής ροής: Δηλώνει το χρονικό διάστημα μεταξύ του χρόνου λήψης του πρώτου και του τελευταίου πακέτου μίας δικτυακής ροής. Το συγκεκριμένο χαρακτηριστικό μπορεί να υποδείξει πολλές μορφές δικτυακών επιθέσεων.

- Αριθμός πακέτων: Αναφέρεται στο συνολικό αριθμό των πακέτων της δικτυακής ροής. Επίσης αποτελεί σημαντικό παράγοντα, ο οποίος μπορεί να υποδείξει αρκετούς τύπους εισβολών.

- Μέγεθος δικτυακής ροής: Δηλώνει το συνολικό μέγεθος των πακέτων της δικτυακής ροής σε bytes. Χαρακτηριστικά, αν το μέγεθος μίας δικτυακής ροής είναι αρκετά μικρό, τότε υπάρχει σημαντική πιθανότητα να υφίσταται κάποια εισβολή, όπως οι επιθέσεις σάρωσης των δικτυακών θυρών.

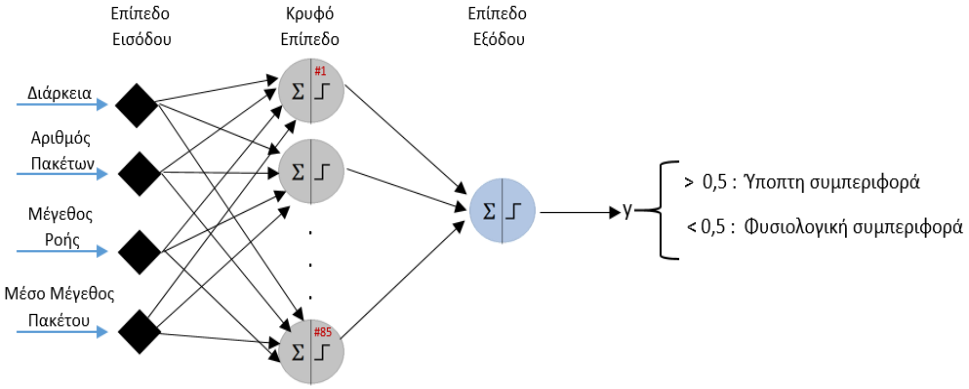
- Μέσο μέγεθος πακέτων: Δηλώνει το αναμενόμενο μέγεθος ενός πακέτου της δικτυακής ροής. Για παράδειγμα, σε επιθέσεις πλημμύρας TCP (TCP flooding attacks) αποστέλλονται συνήθως πακέτα των 120 bytes.

Η συγκεκριμένη διαδικασία, όπως και η εξαγωγή των δικτυακών θυρών διευκολύνεται σε σημαντικό βαθμό από τις δομές δεδομένων που παρέχονται από τη βιβλιοθήκη Scapy.

4.5.3 Δομή Τεχνητού Νευρωνικού Δικτύου

Για τις διαδικασίες της σχεδίασης και της εκπαίδευσης του τεχνητού νευρωνικού δικτύου, πραγματοποιήθηκαν πολλοί πειραματικοί μετασχηματισμοί, μέσω του λογισμικού MATLAB Neural Network Toolbox. Στο Σχήμα 4.8 αποτυπώνεται η αρχιτεκτονική που προτιμήθηκε και απέδωσε τα καλύτερα πειραματικά αποτελέσματα,

στα μέτρα αξιολόγησης που τέθηκαν. Αναλυτικότερα στο επίπεδο εισόδου, ορίζονται τέσσερις νευρώνες, για τα χαρακτηριστικά των δικτυακών ροών, που παρουσιάστηκαν στην παραπάνω υποενότητα. Ακόμη ορίζεται ένα κρυφό επίπεδο, με 85 κρυφούς νευρώνες, οι οποίοι χρησιμοποιούν την εφαπτομενική σιγμοειδή συνάρτηση για να αποδώσουν την έξοδό τους στο επόμενο επίπεδο. Τέλος, το επίπεδο εξόδου περιλαμβάνει ένα τεχνητό νευρώνα, ο οποίος χρησιμοποιεί την λογαριθμική σιγμοειδή συνάρτηση για τον υπολογισμό της τελικής εξόδου του δικτύου. Αν η έξοδος του δικτύου είναι μεγαλύτερη από την τιμή κατωφλίου 0,5 τότε συμπεραίνεται ότι η εκάστοτε δικτυακή ροή παρουσιάζει ύποπτη συμπεριφορά.



Σχήμα 4.8: Δομή τεχνικού νευρωνικού δικτύου εφαρμογής.

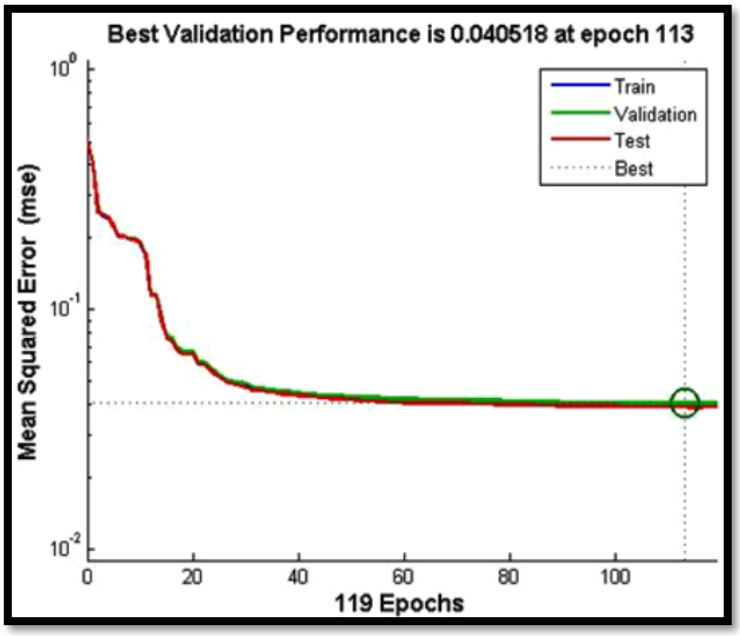
4.5.4 Εκπαίδευση Τεχνητού Νευρωνικού Δικτύου

Κατά τη σχεδίαση ενός IDS, το οποίο στηρίζεται στο μοντέλο ανίχνευσης διαταραχών, απαραίτητη ενέργεια αποτελεί η εκπαίδευση και η αξιολόγηση των μηχανισμών ανίχνευσης με κατηγοριοποιημένα σύνολα δεδομένων [43]. Συγκεκριμένα ορίζονται δύο είδη δεδομένων εκπαίδευσης. Το πρώτο είδος αφορά τα δεδομένα, τα οποία έχουν καταγραφεί από πραγματικές συνθήκες. Οι συγκεκριμένες πληροφορίες αναλύονται και ταξινομούνται, αποκλειστικά από ανθρώπινες ενέργειες. Αντίθετα, το δεύτερο είδος περιλαμβάνει τεχνητά δεδομένα, που έχουν συγκεντρωθεί από πειραματικές ενέργειες, βάσει των οποίων η ταξινόμηση των δεδομένων αποτελεί μία αυτόματη διαδικασία. Αν και τα σύνολα δεδομένων, τα οποία στηρίζονται σε πραγματικές συνθήκες παράγουν καλύτερα αποτελέσματα, η δημιουργία τους αποτελεί δύσκολο έργο, εξαιτίας της ισχύουσας νομοθεσίας για την προστασία της ιδιωτικής ζωής. Αντίθετα έχουν δημιουργηθεί πολλά τεχνητά σύνολα δεδομένων όπως το DARPA 1998 & 1999 [44, 45], το KDD99 [46], το NSL-KDD[47], το σύνολο εκπαίδευσης της Sperotto [49] και το CTU-13 [48].

Για τη διαδικασία της εκπαίδευσης του τεχνητού νευρωνικού δικτύου που ενσωματώνεται από την εφαρμογή «EyeSec» χρησιμοποιήθηκε ο αλγόριθμος εκπαίδευσης Levenberg-Marquardt και υποσύνολο του συνόλου εκπαίδευσης CTU-13 [48]. Αναλυτικότερα στον πίνακα του Σχήματος 4.9 παρουσιάζεται ο συνολικός αριθμός των δικτυακών ροών που χρησιμοποιήθηκε για την εκπαίδευση του δικτύου, καθώς και τα πλήθη των ροών με φυσιολογική και ύποπτη συμπεριφορά. Επίσης, στο Σχήμα 4.10 απεικονίζεται ο ρυθμός μείωσης της συνάρτησης τετραγωνικού σφάλματος, από τις επαναληπτικές διαδικασίες του αλγορίθμου Levenberg-Marquardt.

Σύνολο Δικτυακών Ροών	Φυσιολογική Συμπεριφορά	Ύποπτη Συμπεριφορά
806132	361433	444699

Σχήμα 4.9: Πίνακας δεδομένων του συνόλου εκπαίδευσης.



Σχήμα 4.10: Ρυθμός μείωσης συνάρτηση τετραγωνικού σφάλματος.

4.5.5 Αξιολόγηση Τεχνητού Νευρωνικού Δικτύου

Για την αξιολόγηση του τεχνητού νευρωνικού δικτύου που ενσωματώνεται από την εφαρμογή «EyeSec» χρησιμοποιήθηκαν τυχαία υποσύνολα δεδομένων ελέγχου, του κατηγοριοποιημένου συνόλου της Sperotto [49] και του CTU-13 [48]. Ο λόγος για τον οποίο επιλέχθηκαν τα συγκεκριμένα σύνολα δεδομένων, είναι ότι οι πληροφορίες που περιέχουν είναι προσαρμοσμένες για συστήματα ανίχνευσης εισβολών, που στηρίζονται στην ανάλυση των δικτυακών ροών. Συγκεκριμένα, δημιουργήθηκαν πέντε υποσύνολα ελέγχου, για κάθε ένα από τα προαναφερθέντα κατηγοριοποιημένα σύνολα.

Οι μετρικές που χρησιμοποιήθηκαν για τη διαδικασία της αξιολόγησης είναι η ακρίβεια και η θετική ανάκληση, των οποίων η περιγραφή αναλύθηκε στο Κεφάλαιο 3. Στα Σχήματα 4.11 και 4.12 παρουσιάζονται πίνακες με τις τιμές των παραπάνω μέτρων αξιολόγησης, για κάθε ένα από τα υποσύνολα ελέγχου. Σύμφωνα με τις τιμές των συγκεκριμένων πινάκων το ποσοστό ακρίβειας ορίζεται κατά προσέγγιση στην τιμή 85,55% ενώ η τιμή της θετικής ανάκλησης, η οποία δηλώνει τον βαθμό ανίχνευσης (detection rate) ορίζεται με σχετική ακρίβεια στην τιμή 81,56%.

Σύνολο	TP	TN	FP	FN	Ακρίβεια	$Ανάκληση_P$
1	5173	209959	31187	785	87,06%	86,82%
2	2913	121667	20851	578	85,32%	83,44%
3	2001	85183	15796	464	84,28%	81,17%
4	1547	65771	12873	363	83,56%	80,99%

5	1267	53542	10817	306	83,12%	80,54%

Σχήμα 4.11: Πίνακας μετρικών αξιολόγησης από υποσύνολα ελέγχου του συνόλου CTU-13.

Σύνολο	**TP**	**TN**	**FP**	**FN**	**Ακρίβεια**	**Ανάκληση$_P$**
1	1070	45241	9258	259	82,95%	80,51%
2	922	40951	6139	223	86,81%	80,52%
3	811	36239	5248	195	87,19%	80,61%
4	726	32550	4587	170	87,49%	81,02%
5	654	29568	4062	163	87,73%	80,04%

Σχήμα 4.12: Πίνακας μετρικών αξιολόγησης από υποσύνολα ελέγχου του συνόλου της Sperotto.

Κεφάλαιο 5

Παρουσίαση Εφαρμογής

Στο συγκεκριμένο κεφάλαιο θα αναφερθούν τα τεχνικά χαρακτηριστικά της εφαρμογής «EyeSec» και θα πραγματοποιηθεί η παρουσίαση των λειτουργιών της. Αναλυτικότερα, θα παρουσιαστούν η διαδικασία εκκίνησης και αρχικοποίησης του λογισμικού, η λειτουργία ανάλυσης της δικτυακής κίνησης και η λειτουργία ανίχνευσης εισβολών. Για την παρουσίαση της εφαρμογής θα χρησιμοποιηθούν εικόνες από τη λειτουργία της, στη συσκευή Sony Xperia P LT22i, η οποία διαθέτει διπύρηνο επεξεργαστή, τύπου ARM Cortex-A9, με ισχύ 1 GHz.

5.1 Τεχνικά Χαρακτηριστικά Εφαρμογής

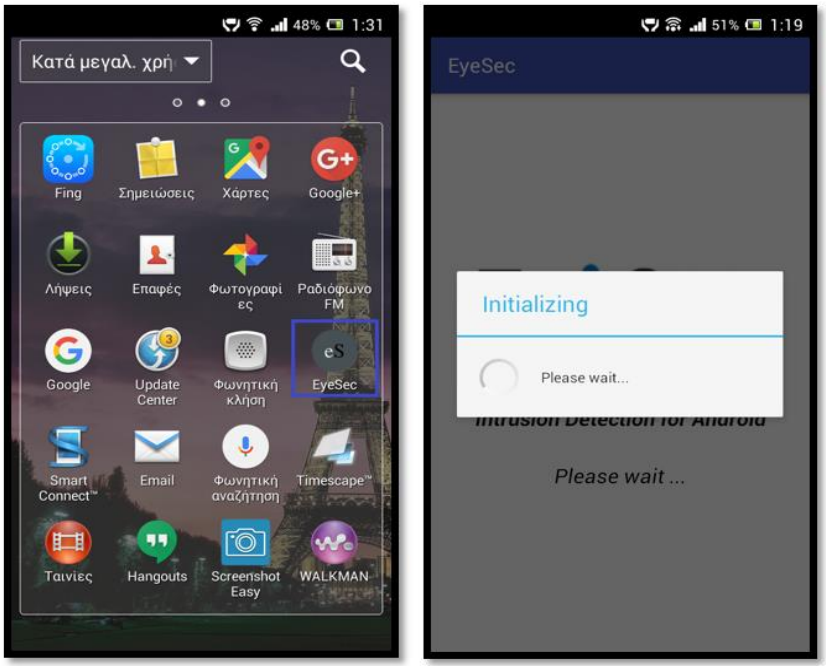
Η εφαρμογή «EyeSec» αποτελείται από 36 αρχεία λειτουργικού κώδικα, από τα οποία τα 34 έχουν δημιουργηθεί χρησιμοποιώντας τη γλώσσα προγραμματισμού Java, ενώ τα υπολειπόμενα δύο, χρησιμοποιώντας τη γλώσσα προγραμματισμού Python. Το σύνολο των συγκεκριμένων αρχείων αποτελείται από 8968 γραμμές κώδικα, εκ των οποίων οι 1095 είναι σχόλια. Η εφαρμογή ανέρχεται στο συγκεκριμένο μέγεθος κώδικα, εξαιτίας της σύνθετης μορφής της και διότι επεξεργάζεται μεγάλο όγκο δεδομένων της ανάλυσης της δικτυακής κίνησης. Τέλος, η διεπαφή χρήστη της εφαρμογής αποτελείται από 32 αρχεία της γλώσσας σήμανσης XML, τα οποία δημιουργήθηκαν με τη βοήθεια του επεξεργαστή Graphical Layout του Android Studio.

Ο απαιτούμενος αποθηκευτικός χώρος για την εγκατάσταση της εφαρμογής είναι 69,07 MB, εκ των οποίων 4,93 MB καταλαμβάνει το πακέτο της εφαρμογής, ενώ 63,83 MB καταλαμβάνουν τα δεδομένα της εφαρμογής. Το μέγεθος των δεδομένων του λογισμικού αιτιολογείται από τα αρχεία που παράγονται κατά την αυτόματη εγκατάσταση μίας στατικής έκδοσης της γλώσσας προγραμματισμού Python. Τέλος, ο

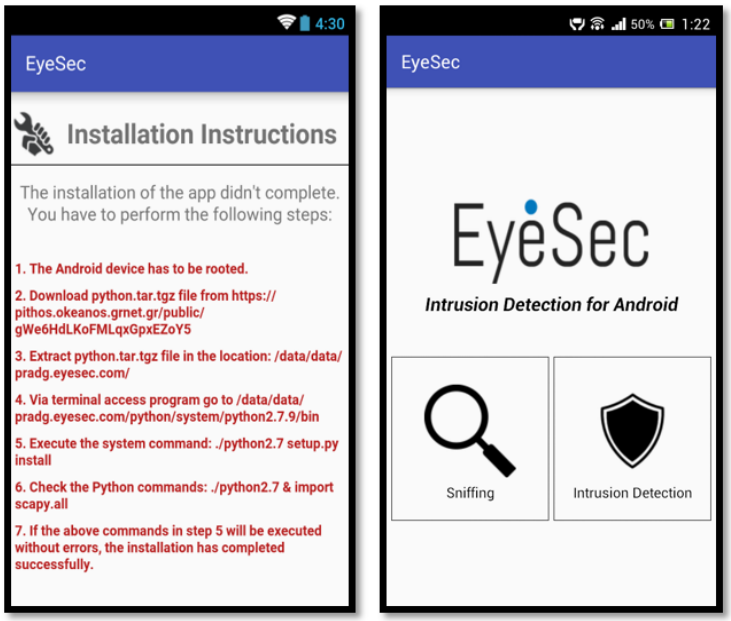
χρόνος εκκίνησης της εφαρμογής κυμαίνεται με σχετική ακρίβεια στα 3 δευτερόλεπτα, ενώ ο χρόνος απόκρισης διατηρείται στα 0,3 δευτερόλεπτα.

5.2 Εκκίνηση και Αρχικοποίηση Εφαρμογής

Ύστερα από την εγκατάσταση του λογισμικού, δημιουργείται στο μενού εφαρμογών του Android, της κινητής συσκευής, ένα νέο εικονίδιο με την ονομασία «EyeSec», όπως απεικονίζεται στην πρώτη οθόνη του Σχήματος 5.1. Κατά την εκτέλεση της εφαρμογής για πρώτη φορά, όπως παρουσιάζεται στη δεύτερη εικόνα του ίδιου σχήματος, εμφανίζεται στον χρήστη ένα αναδυόμενο παράθυρο, που τον ενημερώνει για την αρχικοποίηση της εφαρμογής. Κατά τη συγκεκριμένη διαδικασία, η εφαρμογή εκτελεί αυτόματα την εγκατάσταση μίας στατικής έκδοσης της γλώσσας προγραμματισμού Python. Σε περίπτωση που για κάποιο λόγο η διαδικασία αρχικοποίησης αποτύχει, τότε όπως αποτυπώνεται στην πρώτη εικόνα του Σχήματος 5.2, εμφανίζονται στον χρήστη αναλυτικές οδηγίες, τις οποίες θα πρέπει να εκτελέσει χειροκίνητα, από περιβάλλον γραμμής εντολών του Android. Οι οδηγίες αυτές αναφέρονται σε συνήθεις εντολές του λειτουργικού συστήματος Linux, στο οποίο βασίζεται ο πυρήνας (kernel) του Android και αφορούν τη χειροκίνητη εγκατάσταση της γλώσσας Python. Τα σφάλματα που μπορούν να προκύψουν κατά τη διαδικασία της αρχικοποίησης της εφαρμογής, αφορούν κυρίως την εξαγωγή δυαδικών αρχείων, η οποία πραγματοποιείται από προεγκατεστημένα προγράμματα του πυρήνα του Android, μέσω κλήσεων του λειτουργικού συστήματος. Διαφορετικά, αν δεν προκύψει κάποιο σφάλμα, τότε εμφανίζεται στον χρήστη η δεύτερη οθόνη του Σχήματος 5.2, η οποία αποτελεί το βασικό μενού της εφαρμογής. Στις επόμενες χρήσεις του λογισμικού, αν η διαδικασία αρχικοποίησης έχει ολοκληρωθεί χωρίς σφάλματα, τότε εμφανίζεται άμεσα το βασικό μενού επιλογών.



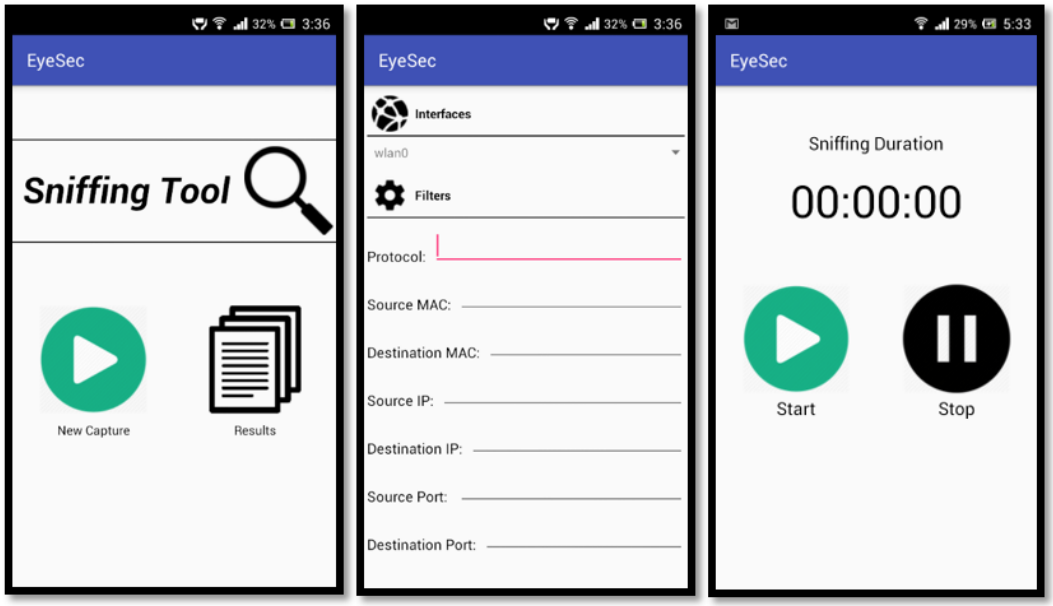
Σχήμα 5.1: (Α) Εικονίδιο εφαρμογής EyeSec, (Β) Διαδικασία αρχικοποίησης εφαρμογής.



Σχήμα 5.2: (Α) Χειροκίνητες οδηγίες αρχικοποίησης, (Β) Βασικό μενού επιλογών εφαρμογής.

5.3 Ανάλυση Δικτυακής Κίνησης

Εκτελώντας τη λειτουργία «Sniffing» από το βασικό μενού επιλογών της εφαρμογής (Σχήμα 5.2.Β), εμφανίζεται στον χρήστη η πρώτη εικόνα του Σχήματος 5.3. Στη συγκεκριμένη οθόνη ορίζονται δύο λειτουργίες, είτε να πραγματοποιηθεί μία νέα καταγραφή και ανάλυση της δικτυακής κίνησης, με την επιλογή «New Capture», είτε να εμφανιστούν οι πληροφορίες των δικτυακών πακέτων, της προηγούμενης καταγραφής με την επιλογή «Results».



Σχήμα 5.3: (Α) Επιλογές ανάλυσης δικτυακής κίνησης, (Β) Φίλτρα καταγραφής δικτυακής κίνησης, (Γ) Εκκίνηση καταγραφής δικτυακής κίνησης.

5.3.1 Νέα Ανάλυση της Δικτυακής Κίνησης

Στην περίπτωση που ο χρήστης επιλέξει να εκτελέσει μία νέα ανάλυση της δικτυακής κίνησης, τότε η εφαρμογή μεταβαίνει στη δεύτερη εικόνα του Σχήματος 5.3. Στην οθόνη αυτή, ο χρήστης έχει τη δυνατότητα να ορίσει τη δικτυακή διεπαφή (network interface) και να επιλέξει ορισμένα φίλτρα για την καταγραφή των δικτυακών πακέτων. Αναλυτικότερα διατίθενται οι παρακάτω επιλογές φίλτρων:

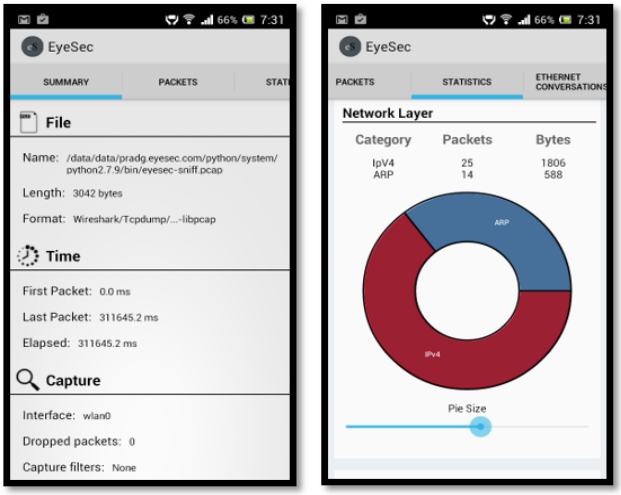
- Protocol: Στο συγκεκριμένο πεδίο δίνεται η δυνατότητα να συμπληρωθεί το πρωτόκολλο των δικτυακών πακέτων, που θα καταγραφούν. Για παράδειγμα, μπορεί να συμπληρωθεί με ονόματα πρωτοκόλλων από το επίπεδο δικτύου, όπως ipv4, ipv6, arp, ή ονόματα πρωτοκόλλων από το επίπεδο μεταφοράς, όπως tcp ή udp.
- Source MAC: Καθορίζει τη φυσική διεύθυνση (διεύθυνση Media Access Control - MAC) της πηγής, των πακέτων που θα καταγραφούν.
- Destination MAC: Αντίστοιχα με την παραπάνω επιλογή, η συγκεκριμένη δηλώνει τη φυσική διεύθυνση του προορισμού, των πακέτων που θα καταγραφούν.
- Source IP: Ορίζει τη διεύθυνση IP της πηγής, των δικτυακών πακέτων.
- Destination IP: Ορίζει τη διεύθυνση IP του προορισμού, των δικτυακών πακέτων.
- Source Port: Ορίζει τη δικτυακή θύρα της πηγής.
- Destination Port: Ορίζει τη δικτυακή θύρα του προορισμού.
- Source or Destination Port: Καθορίζει ταυτόχρονα, είτε τη δικτυακή θύρα της πηγής είτε τη δικτυακή θύρα του προορισμού.
- TCP Flags: Τα συγκεκριμένα φίλτρα καθορίζουν τις σημαίες των πακέτων, του πρωτοκόλλου TCP.

Εφόσον, ο χρήστης επιλέξει τη δικτυακή διεπαφή και τις επιλογές των φίλτρων που επιθυμεί, τότε μπορεί να μεταβεί στην τρίτη οθόνη του Σχήματος 5.3, ώστε να εκκινήσει τη διαδικασία καταγραφής της δικτυακής κίνησης, μέσω της επιλογής «Start». Από τη χρονική στιγμή που θα αρχίσει η συγκεκριμένη ενέργεια, δημιουργείται άμεσα μία Android υπηρεσία (Android service), η οποία καταγράφει στο παρασκήνιο τα δικτυακά πακέτα, βάσει των φίλτρων που επιλέχθηκαν. Ο μοναδικός τρόπος για τη διακοπή της συγκεκριμένης υπηρεσίας, αποτελεί η ενεργοποίηση της επιλογής «Stop» που απεικονίζεται στην τρίτη οθόνη του Σχήματος 5.3. Όταν ενεργοποιηθεί η συγκεκριμένη επιλογή, η εφαρμογή μεταβαίνει αυτόματα στην πρώτη οθόνη του ίδιου σχήματος και δημιουργεί ένα δυαδικό PCAP αρχείο, στο οποίο αποθηκεύονται τα δεδομένα της δικτυακής κίνησης.

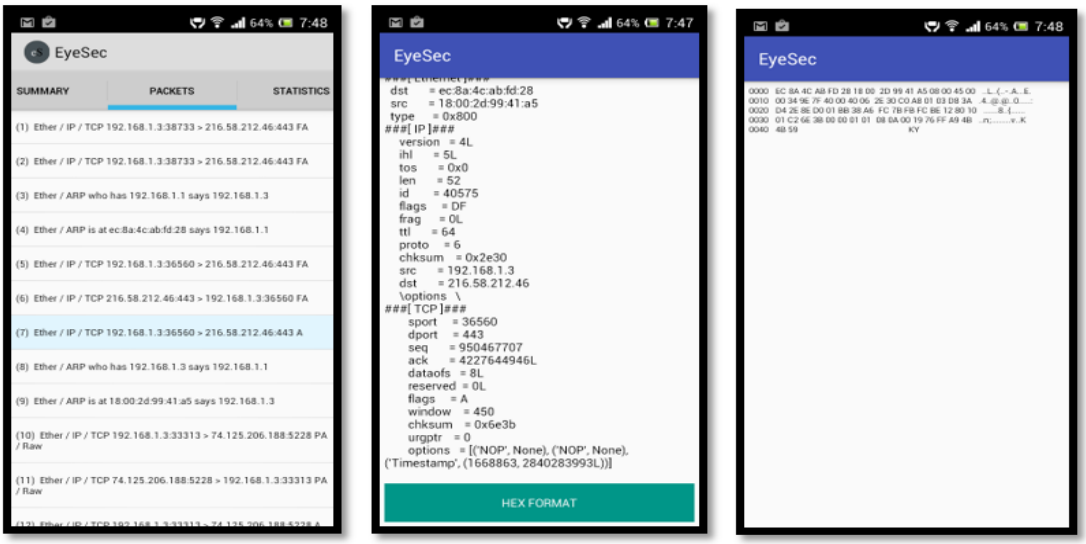
5.3.2 Πληροφορίες Δικτυακής Κίνησης

Με την ενεργοποίηση της επιλογής «Results» από την πρώτη εικόνα του Σχήματος 5.3, ο χρήστης έχει τη δυνατότητα να εξετάσει αποκλειστικά τις πληροφορίες της δικτυακής κίνησης, της προηγούμενης καταγραφής. Ακριβέστερα, οι συγκεκριμένες πληροφορίες διαιρούνται σε έντεκα κύριες οθόνες λειτουργίας, οι οποίες εμπεριέχονται σε ένα γραφικό στοιχείο Android Action Bar. Ορισμένα δεδομένα πληροφοριών, όπως τα δικτυακά πακέτα, μπορεί να οδηγούν σε δευτερεύουσες οθόνες για την εμφάνιση επιπλέον λεπτομερειών.

Συγκεκριμένα, στην πρώτη οθόνη του Σχήματος 5.4 παρουσιάζονται συνοπτικές πληροφορίες, σχετικά με τη χρονική διάρκεια καταγραφής των δικτυακών πακέτων, των φίλτρων που χρησιμοποιήθηκαν, καθώς και του PCAP αρχείου καταγραφής. Στη δεύτερη οθόνη του ίδιου σχήματος παρουσιάζονται στατιστικά διαγράμματα, για τα δικτυακά πακέτα που καταγράφηκαν, ανά επίπεδο της στοίβας TCP/IP.



Σχήμα 5.4: (Α) Συνοπτικές πληροφορίες ανάλυσης της δικτυακής κίνησης, (Β) Στατιστικά στοιχεία της δικτυακής κίνησης.

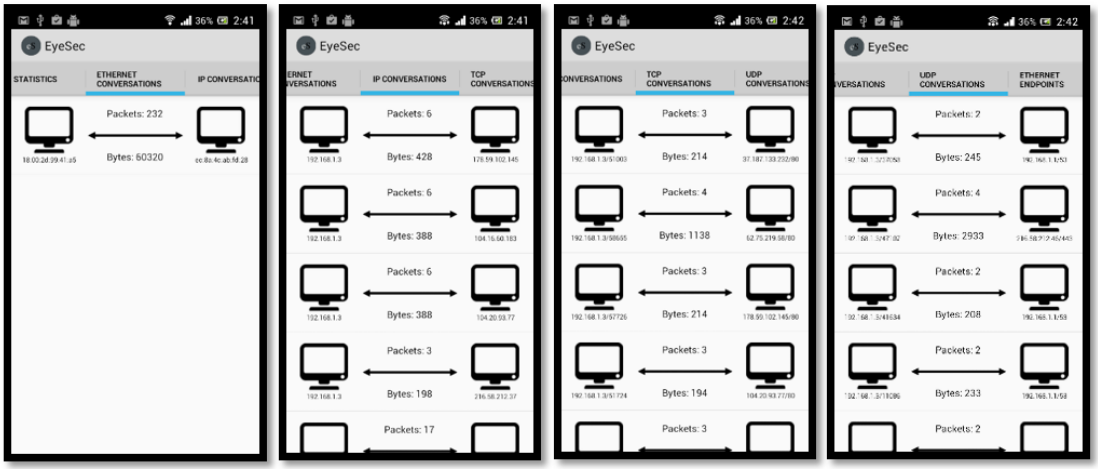


Σχήμα 5.5: (Α) Τα δικτυακά πακέτα που καταγράφηκαν, (Β) Λεπτομέρειες πακέτου, (Γ) Δεκαεξαδική αναπαράσταση πακέτου.

Επίσης, στην πρώτη οθόνη του Σχήματος 5.5 παρουσιάζεται μία λίστα με τα δικτυακά πακέτα που καταγράφηκαν. Σε περίπτωση που επιλεγεί κάποιο από αυτά, η εφαρμογή μεταβαίνει στη δεύτερη οθόνη του Σχήματος 5.5, η οποία παρουσιάζει λεπτομερέστερα τις πληροφορίες του εκάστοτε πακέτου, αναλύοντας ιεραρχικά τα επίπεδα που το διακρίνουν. Τέλος στη συγκεκριμένη οθόνη ορίζεται η επιλογή «HEX FORMAT» η οποία αν ενεργοποιηθεί, εμφανίζει τις πληροφορίες του εκάστοτε πακέτου σε δεκαεξαδική μορφή, όπως απεικονίζεται στην τρίτη εικόνα του ίδιου σχήματος.

Επιπλέον, στις οθόνες του Σχήματος 5.6 εμφανίζονται για κάθε σημείο τερματισμού (endpoint), των πρωτοκόλλων Ethernet, IP, TCP και UDP, τα πλήθη των πακέτων, καθώς και τα μεγέθη αυτών σε bytes. Αντίστοιχα στις εικόνες του Σχήματος 5.7, απεικονίζονται οι επικοινωνίες που πραγματοποιήθηκαν ανά πρωτόκολλο.

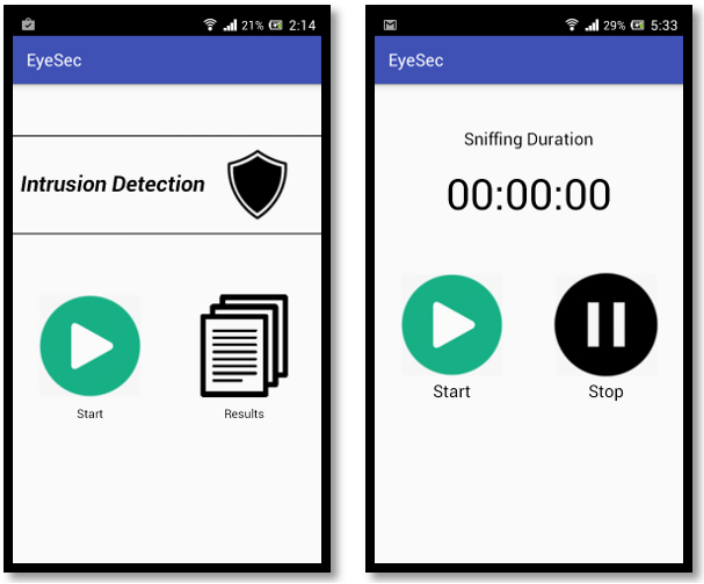
Σχήμα 5.6: (Α) Πλήθος και μέγεθος πακέτων Ethernet σημείων τερματισμού, (Β) Πλήθος και μέγεθος πακέτων IP σημείων τερματισμού, (Γ) Πλήθος και μέγεθος πακέτων TCP σημείων τερματισμού, (Δ) Πλήθος και μέγεθος πακέτων UDP σημείων τερματισμού.



Σχήμα 5.7: (Α)Πλήθος και μέγεθος πακέτων Ethernet επικοινωνιών, (Β) Πλήθος και μέγεθος πακέτων IP επικοινωνιών, (Γ) Πλήθος και μέγεθος πακέτων TCP επικοινωνιών, (Δ) Πλήθος και μέγεθος πακέτων UDP επικοινωνιών.

5.4 Ανίχνευση Εισβολών

Εκτελώντας τη λειτουργία «Intrusion Detection» από το βασικό μενού επιλογών της εφαρμογής (Σχήμα 5.2.B), εμφανίζεται στον χρήστη η πρώτη εικόνα του Σχήματος 5.8. Στη συγκεκριμένη οθόνη ορίζονται δύο λειτουργίες, είτε να πραγματοποιηθεί μία νέα διαδικασία ανίχνευσης εισβολών, με την επιλογή «Start», είτε να εμφανιστούν οι πληροφορίες της προηγούμενης διαδικασίας ελέγχου, μέσω της επιλογής «Results».



Σχήμα 5.8: (A) Επιλογές ανίχνευσης εισβολών,
(B) Εκκίνηση ανίχνευσης εισβολών.

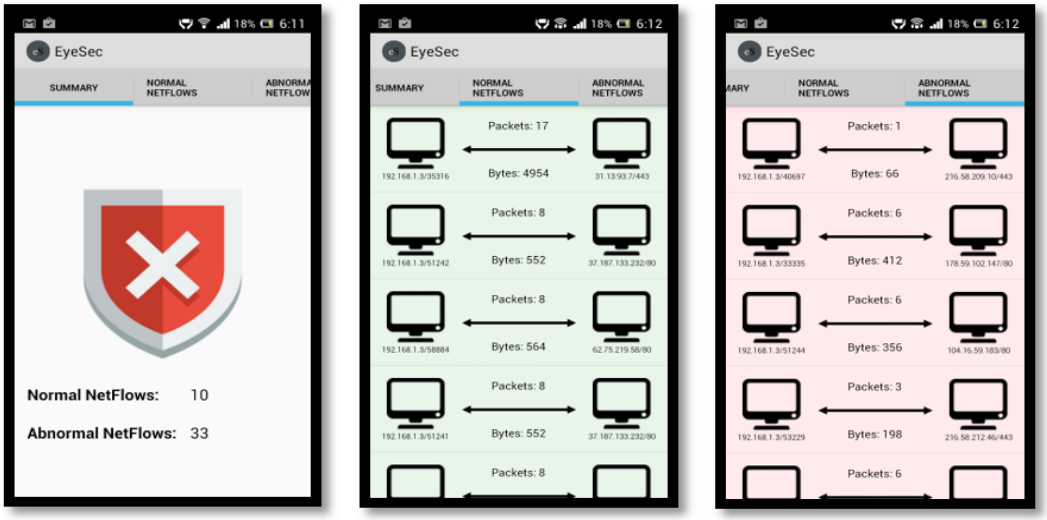
5.4.1 Νέα Ανίχνευση Εισβολών

Στην περίπτωση που ο χρήστης επιλέξει να εκτελέσει μία νέα διαδικασία ανίχνευσης εισβολών, τότε η εφαρμογή μεταβαίνει στη δεύτερη εικόνα του Σχήματος 5.8. Στη συγκεκριμένη οθόνη, από τη χρονική στιγμή, που ο χρήστης ενεργοποιήσει την επιλογή «Start», δημιουργείται άμεσα μία Android υπηρεσία, η οποία καταγράφει στο παρασκήνιο τις αμφίδρομες δικτυακές ροές από όλες τις δικτυακές διεπαφές. Ο μοναδικός τρόπος για τη διακοπή της συγκεκριμένης υπηρεσίας, αποτελεί η ενεργοποίηση της επιλογής «Stop» που απεικονίζεται στην ίδια οθόνη. Όταν ενεργοποιηθεί η συγκεκριμένη επιλογή, η εφαρμογή μεταβαίνει αυτόματα στην πρώτη οθόνη του ίδιου σχήματος και δημιουργεί ένα αρχείο κειμένου με τις δικτυακές ροές που καταγράφηκαν και ένα δυαδικό PCAP αρχείο με το περιεχόμενο της δικτυακής κίνησης που παρακολουθήθηκε.

5.4.2 Πληροφορίες Ανίχνευσης Εισβολών

Με την ενεργοποίηση της επιλογής «Results» από την πρώτη εικόνα του Σχήματος 5.8, ο χρήστης έχει τη δυνατότητα να εξετάσει αποκλειστικά τις πληροφορίες της προηγούμενης διαδικασίας ανίχνευσης εισβολών. Όπως αποτυπώνεται στο Σχήμα 5.9, οι συγκεκριμένες πληροφορίες διαιρούνται σε τρεις οθόνες λειτουργίας, οι οποίες

εμπεριέχονται σε ένα γραφικό στοιχείο Android Action Bar. Αναλυτικότερα στην πρώτη οθόνη του Σχήματος 5.9, εμφανίζονται τα πλήθη των δικτυακών ροών με φυσιολογική και ύποπτη συμπεριφορά, ενώ οι επόμενες οθόνες απεικονίζουν δύο λίστες με τις ακίνδυνες και ύποπτες δικτυακές ροές.



Σχήμα 5.9: (Α) Πλήθη ακίνδυνων και ύποπτων δικτυακών ροών, (Β) Ακίνδυνες δικτυακές ροές, (Γ) Ύποπτες δικτυακές ροές.

Κεφάλαιο 6

Επίλογος

Αντικείμενο της παρούσας διπλωματικής εργασίας αποτέλεσε η μελέτη του τρόπου λειτουργίας των συστημάτων ανίχνευσης εισβολών και η δημιουργία μίας πρωτότυπης εφαρμογής, αναγνώρισης εισβολών για κινητές συσκευές με λειτουργικό σύστημα Android. Στο συγκεκριμένο κεφάλαιο θα πραγματοποιηθεί η καταγραφή των συμπερασμάτων της μελέτης που πραγματοποιήθηκε και θα αναφερθούν πιθανές μελλοντικές επεκτάσεις για την εξέλιξη της εφαρμογής.

6.1 Συμπεράσματα

Τα τελευταία χρόνια τα υπολογιστικά συστήματα και ιδιαίτερα η κινητή τεχνολογία έχει αναπτυχθεί σε σημαντικό επίπεδο. Συγκεκριμένα, οι κινητές συσκευές αποτελούν αναπόσπαστο μέρος της ανθρώπινης καθημερινότητας, εξαιτίας του συνδυασμού των πολλαπλών τρόπων διασύνδεσης που παρέχουν και της εύκολης μεταφερσιμότητάς τους. Ωστόσο ταυτόχρονα με τις νέες δυνατότητες που προσφέρουν, ο όγκος των δεδομένων που περιλαμβάνουν, αποτελεί ελκυστικό στόχο ενός ολοένα αυξανόμενου πλήθους απειλών κατά της ασφάλειάς τους. Αν και η ερευνητική κοινότητα έχει δημιουργήσει αρκετούς μηχανισμούς ασφάλειας που αφορούν τα συνήθη συστήματα υπολογιστών, το σύνολο των βιβλιογραφικών αναφορών, που ερευνούν τεχνικές ενίσχυσης της ασφάλειας, των συσκευών κινητής υπολογιστικής, είναι ιδιαίτερα περιορισμένο. Επίσης, αν και έχουν δημιουργηθεί αρκετοί μέθοδοι αυτοματοποιημένης αντιμετώπισης γνωστών τύπου επιθέσεων, μεγάλο ενδιαφέρον παρουσιάζει η πρόβλεψη και η αντιμετώπιση άγνωστων τύπου εισβολών.

Κατά τη χρονική διάρκεια της υλοποίησης της παρούσας διπλωματικής εργασίας μελετήθηκαν οι τύποι και οι μηχανισμοί των συστημάτων ανίχνευσης εισβολών, με στόχο την κατασκευή μίας εφαρμογής αναγνώρισης, άγνωστων επιθέσεων, για κινητές

συσκευές με λειτουργικό σύστημα Android. Η εφαρμογή υλοποιήθηκε βασιζόμενη στο μοντέλο ανίχνευσης διαταραχών και συγκεκριμένα στις υπολογιστικές διαδικασίες ενός τεχνητού νευρωνικού δικτύου, για τον έλεγχο των αμφίδρομων δικτυακών ροών. Ακόμη, η κατασκευή της εφαρμογής πραγματοποιήθηκε με συγκεκριμένο τρόπο, ώστε κατά την εκτέλεσή της να μην επηρεάζονται σε σημαντικό βαθμό τα χαρακτηριστικά της λειτουργίας, της κινητής συσκευής. Τέλος, τα πειραματικά αποτελέσματα που λήφθηκαν είναι ιδιαίτερα ενθαρρυντικά. Συγκεκριμένα το ποσοστό ακρίβειας της αναγνώρισης των δικτυακών ροών με ύποπτη συμπεριφορά, αγγίζει την τιμή 85,55%, ενώ ο βαθμός ανίχνευσης εισβολών αγγίζει την τιμή 81,56%.

6.2 Μελλοντικές Επεκτάσεις

Η εφαρμογή που υλοποιήθηκε μπορεί να αποτελέσει αφετηρία για την επέκταση της έρευνας της ανάπτυξης των συστημάτων ανίχνευσης εισβολών σε κινητές συσκευές. Κάποιες κατευθύνσεις με βάση τις οποίες θα μπορούσε να επεκταθεί η συγκεκριμένη εργασία είναι οι εξής:

- Περαιτέρω βελτίωση των τιμών της ακρίβειας και του βαθμού ανίχνευσης που επιτυγχάνεται από την αρχιτεκτονική του συγκεκριμένου τεχνητού νευρωνικού δικτύου, με την προσθήκη επιπλέον κρυφών επιπέδων ή τη χρησιμοποίηση διαφορετικών τεχνικών ταξινόμησης.

- Δημιουργία ενός δεύτερου τεχνητού νευρωνικού δικτύου, σκοπός του οποίου θα αποτελεί η ταξινόμηση της ύποπτης δικτυακής ροής σε συγκεκριμένους τύπους επιθέσεων.

- Ανίχνευση περισσότερων μορφών εισβολών, χρησιμοποιώντας πληροφορίες από τα χαρακτηριστικά λειτουργίας των κινητών συσκευών, όπως το ποσοστό κατανάλωσης της ενέργειας της μπαταρίας, το ποσοστό χρήσης της CPU, το πλήθος των μηνυμάτων SMS ή MMS (Short/Multimedia Message Service) που έχουν αποσταλεί, τις κλήσεις του λειτουργικού συστήματος, κτλ.

- Ανίχνευση περισσότερων μορφών εισβολών, χρησιμοποιώντας πληροφορίες από το προφίλ του χρήστη, όπως τα πρότυπα αφής που παράγονται, όταν ο χρήστης αλληλοεπιδρά με την οθόνη της συσκευής ή ο τρόπος με τον οποίο χρησιμοποιεί δημοφιλείς εφαρμογές ή υπηρεσίες.

Βιβλιογραφία

[1] Kruegel, C., Valeur, F., & Vigna, G. (2005). Intrusion detection and correlation. Advances in information security, vol. 14.

[2] Jones, A. K., & Sielken, R. S. (2000). Computer system intrusion detection: A survey. Computer Science Technical Report, 1-25.

[3] Anderson, J. P. (1980). Computer security threat monitoring and surveillance (Vol. 17). Technical report, James P. Anderson Company, Fort Washington, Pennsylvania.

[4] Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. IEEE network, 8(3), 26-41.

[5] Denning, D. E. (1987). An intrusion-detection model. IEEE Transactions on software engineering, (2), 222-232.

[6] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). NIST special publication, 800(2007), 94.

[7] Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In Wireless Network Security (pp. 103-135). Springer US.

[8] Chow, G. W., & Jones, A. (2008, January). Framework for anomaly detection in OKL4-Linux based smartphones. In Australian Information Security Management Conference (p. 49).

[9] Damopoulos, D., Kambourakis, G., & Gritzalis, S. (2011, June). iSAM: an iPhone stealth airborne malware. In IFIP International Information Security Conference (pp. 17-28). Springer Berlin Heidelberg.

[10] La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices. IEEE communications surveys & tutorials, 15(1), 446-471.

[11] Teraoka, T. (2012). Organization and exploration of heterogeneous personal data collected in daily life. Human-Centric Computing and Information Sciences, 2(1), 1.

[12] Lookout, 2012. State of mobile security 2012.

[13] El Kettani, M. D. E. C., & En-Nasry, B. (2011). MIdM: an open architecture for mobile identity management. JoC, 2(2), 25-32.

[14] Lee, M., Shon, T., Cho, K., Chung, M., Seo, J., & Moon, J. (2007, August). An approach for classifying internet worms based on temporal behaviors and packet flows. In International Conference on Intelligent Computing (pp. 646-655). Springer Berlin Heidelberg.

[15] Cisco.com: Cisco ios netflow configuration guide, release 12.4. (September 2010), http://www.cisco.com.

[16] Claise, B. (2008). Specification of the IP flow information export (IPFIX) protocol for the exchange of IP traffic flow information (No. RFC 5101).

[17] Trammell, Brian, and Elisa Boschi. Bidirectional Flow Export Using IP Flow Information Export (IPFIX). No. RFC 5103. 2008.

[18] Fioreze, T., Wolbers, M. O., van de Meent, R., & Pras, A. (2007, May). Finding elephant flows for optical networks. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 627-640). IEEE.

[19] Joo, D., Hong, T., & Han, I. (2003). The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors. Expert Systems with Applications, 25(1), 69-75.

[20] Γκρίτζαλης, Σ., Κάτσικας, Σ., & Γκρίτζαλης, Δ. (2003). Ασφάλεια δικτύων υπολογιστών. Εκδόσεις Παπασωτηρίου.

[21] Lankewicz, L., & Benard, M. (1991, December). Real-time anomaly detection using a nonparametric pattern recognition approach. In Computer Security Applications Conference, 1991. Proceedings., Seventh Annual (pp. 80-89). IEEE.

[22] Jumes, J. G., Cooper, N. F., Chamoun, P., & Feinman, T. M. (1998). Microsoft Windows NT 4.0 Security, Audit, and Control. Microsoft Press.

[23] Teng, H. S., Chen, K., & Lu, S. C. (1990, May). Adaptive real-time anomaly detection using inductively generated sequential patterns. In Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on (pp. 278-284). IEEE.

[24] Heberlein, L. T., Dias, G. V., Levitt, K. N., Mukherjee, B., Wood, J., & Wolber, D. (1990, May). A network security monitor. In Research in Security and Privacy, 1990. Proceedings., 1990 IEEE Computer Society Symposium on (pp. 296-304). IEEE.

[25] Snapp, S. R., Brentano, J., Dias, G. V., Goan, T. L., Heberlein, L. T., Ho, C. L., ... & Teal, D. M. (1991, October). DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype. In Proceedings of the 14th national computer security conference (Vol. 1, pp. 167-176).

[26] Crosbie, M., & Spafford, E. H. (1995). Defending a computer system using autonomous agents.

[27] Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. IBM Journal of research and development, 3(3), 210-229.

[28] Mitchell, T. M. (1997). Machine learning. New York.

[29] Duda, R. O., Hart, P. E., & Stork, D. G. (2012). Pattern classification. John Wiley & Sons.

[30] Theodoridis, S., & Koutroumbas, K. (1999). Pattern Recognition, Academic Press. New York.

[31] Λυκοθανάσης Σπυρίδων, Μαυρούδη Σεφερίνα, Σκάρλας Λάμπρος, Εισαγωγή στις Ευρετικές Μεθόδους, Πανεπιστημιακές σημειώσεις, Πάτρα Δεκέμβριος 2007.

[32] Hornik, K., Stinchcombe, M., & White, H. (1989). Multilayer feedforward networks are universal approximators. Neural networks, 2(5), 359-366.

[33] Hornik, K. (1991). Approximation capabilities of multilayer feedforward networks. Neural networks, 4(2), 251-257.

[34] Ryan, J., Lin, M. J., & Miikkulainen, R. (1998). Intrusion detection with neural networks. Advances in neural information processing systems, 943-949.

[35] Ghosh, A. K., & Schwartzbard, A. (1999, August). A Study in Using Neural Networks for Anomaly and Misuse Detection. In USENIX Security.

[36] Cannady, J. (1998, October). Artificial neural networks for misuse detection. In National information systems security conference (pp. 368-81).

[37] Tan, K. (1995, November). The application of neural networks to UNIX computer security. In Neural Networks, 1995. Proceedings., IEEE International Conference on (Vol. 1, pp. 476-481). IEEE.

[38] Zhang, Z., Li, J., Manikopoulos, C. N., Jorgenson, J., & Ucles, J. (2001, June). HIDE: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification. In Proc. IEEE Workshop on Information Assurance and Security (pp. 85-90).

[39] Hoglund, A. J., Hatonen, K., & Sorvari, A. S. (2000). A computer host-based user anomaly detection system using the self-organizing map. In Neural Networks, 2000. IJCNN 2000, Proceedings of the IEEE-INNS-ENNS International Joint Conference on (Vol. 5, pp. 411-416). IEEE.

[40] Lichodzijewski, P., Zincir-Heywood, A. N., & Heywood, M. I. (2002, May). Host-based intrusion detection using self-organizing maps. In IEEE international joint conference on neural networks (pp. 1714-1719).

[41] Γιακουμάκης, Ε. (2009). Τεχνολογία λογισμικού.

[42] Panagiotis, R. G., Evdoxia, M., & Minas, D. (2016, May). Parallelization of the hierarchical search in Python for high performance embedded systems. In Modern Circuits and Systems Technologies (MOCAST), 2016 5th International Conference on (pp. 1-4). IEEE.

[43] Mell, P., Hu, V., Lippmann, R., Haines, J., & Zissman, M. (2003). An overview of issues in testing intrusion detection systems.

[44] Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., Weber, D., Webster, S.E., Wyschogrod, D., Cunningham, R.K., Zissman, M. A. (2000). Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. In DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings (Vol. 2, pp. 12-26). IEEE.

[45] Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). The 1999 DARPA off-line intrusion detection evaluation. Computer networks, 34(4), 579-595.

[46] Stolfo, S. J., Fan, W., Lee, W., Prodromidis, A., & Chan, P. K. (2000). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. In DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings (Vol. 2, pp. 130-144). IEEE.

[47] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009.

[48] Garcia, S., Grill, M., Stiborek, J., & Zunino, A. (2014). An empirical comparison of botnet detection methods. computers & security, 45, 100-123.

[49] Sperotto, A., Sadre, R., Van Vliet, F., & Pras, A. (2009, October). A labeled data set for flow-based intrusion detection. In International Workshop on IP Operations and Management (pp. 39-50). Springer Berlin Heidelberg.

[50] Hagan, M. T., & Menhaj, M. B. (1994). Training feedforward networks with the Marquardt algorithm. IEEE transactions on Neural Networks, 5(6), 989-993.

[51] Jacobson, V., Leres, C., & McCanne, S. (1989). The tcpdump manual page. Lawrence Berkeley Laboratory, Berkeley, CA.