ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ ΕΥΕΛΠΙΔΩΝ
Τμήμα Στρατιωτικών Επιστημών

Ε Λ Λ Η Ν Ι Κ Η Δ Η Μ Ο Κ Ρ Α Τ Ι Α
ΔΙΙΔΡΥΜΑΤΙΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΑΚΑΔΗΜΑΪΚΟΥ ΕΤΟΥΣ 2016-17

ΕΦΑΡΜΟΣΜΕΝΗ
ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΕΡΕΥΝΑ & ΑΝΑΛΥΣΗ

(ΠΔ 97 /2015/ΦΕΚ 163Α'/20.08.2014)

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
Σχολή Μηχανικών Παραγωγής & Διοίκησης

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

Ανάλυση Δεδομένων και Εξόρυξη Γνώσης από Μεγάλους Όγκους Δεδομένων Κυβερνοάμυνας

Διατριβή που υπεβλήθη για την μερική ικανοποίηση των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης

Υπό:
Λγος (ΔΒ) Γεώργιος Καραπιλάφης
Α.Μ.: 2015018026

ΟΚΤΩΒΡΙΟΣ 2018

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Η Μεταπτυχιακή Διατριβή του Λγου (ΔΒ) Γεώργιου Καραπιλάφη εγκρίνεται:

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Καθηγητής ΟΝΟΜΑΤΕΠΩΝΥΜΟ (Επιβλέπων)	κος Νικόλαος Ματσατσίνης
Καθηγητής ΟΝΟΜΑΤΕΠΩΝΥΜΟ	κος Νικόλαος Δάρας
Καθηγητής ΟΝΟΜΑΤΕΠΩΝΥΜΟ	κος Στέλιος Τσαφαράκης

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

Έτος 2018

Αφιερώσεις

Στους αγαπημένους μου γονείς και στη Δημητρούλα για την αγάπη τους και την κατανόησή τους.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

ΕΥΧΑΡΙΣΤΙΕΣ

Θερμές ευχαριστίες θα ήθελα να εκφράσω στους καθηγητές του ΔΜΠΣ «Εφαρμοσμένη Επιχειρησιακή Έρευνα και Ανάλυση» που μέσω αυτού μου ανοίχτηκαν εκ νέου νέοι ορίζοντες γνώσης και μάθησης. Ειδικότερα, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή κο. Νικόλαο Ματσατσίνη για τις οδηγίες και κατευθύνσεις του για την εκπόνηση της παρούσας εργασίας και τον Διευθυντή Σπουδών κο. Νικόλαο Δάρα για την έως τώρα υποστήριξή του στα διάφορα επιστημονικά συνέδρια της Στρατιωτικής Σχολής Ευελπίδων.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ

Η παρούσα μεταπτυχιακή διατριβή έχει ως στόχο την κατάδειξη των νέων κατευθύνσεων στο τομέα της κυβερνοάμυνας μέσω της επιστήμης των δεδομένων (data science), προς την δημιουργία ενός ασφαλέστερου περιβάλλοντος στον κυβερνοχώρο. Οι ολοένα και αυξανόμενες σε ιδιοφυία τεχνικές επιθέσεων με την ταυτόχρονη αύξηση της εξάρτησης ακόμα και ολόκληρων οικονομιών στις ψηφιακές λύσεις, καθιστούν την ασφάλεια στον κυβερνοχώρο στρατηγικής σημασίας για κράτη-έθνη, οργανισμούς και τον καθένα προσωπικά. Οι εξελίξεις στο τομέα της μηχανικής μάθησης και της τεχνητής νοημοσύνης, σε συνδυασμό με τις ήδη υπάρχουσες παραδοσιακές λύσεις ασφάλειας, μπορούν να αποκτήσουν τεράστια δυναμική, συμβάλλοντας στη δημιουργία ενός ασφαλέστερου περιβάλλοντος, το οποίο θα μπορούν να εκμεταλλεύονται οι κοινωνίες για την ανάπτυξή τους.

Στη παρούσα διατριβή, θα γίνει ανάλυση ενός συνόλου από δεδομένα που έχουν συλλεχθεί σε περιβάλλον εργαστηρίου και αφορούν συγκεκριμένα σε ροές δεδομένων από αιτήσεις σε περιβάλλον Web μέσω του πρωτοκόλλου HTTP (web requests) προς μελέτη της απόδοσης ενός συστήματος μηχανικής μάθησης για την αναγνώριση και κατηγοριοποίηση αντίστοιχων επιθέσεων ή ανώμαλων ροών δεδομένων.

ΚΕΦΑΛΑΙΟ 1
Εισαγωγή – Παρουσίαση Προβλήματος

§1. Το σύγχρονο ψηφιακό περιβάλλον και οι προκλήσεις της ψηφιακής εποχής

Σε έναν ταχέως εξελισσόμενο κόσμο από πλευράς προόδου, ψηφιακών λύσεων και καινοτομιών, οι διάφορες επιχειρήσεις, οργανισμοί, κράτη αλλά και κάθε άτομο ξεχωριστά, προσπαθεί να ανταποκριθεί μέσα στο περιβάλλον αυτό, να παρακολουθήσει τις εξελίξεις και να τις εκμεταλλευτεί προς όφελός του και κατά περίπτωση. Σε ένα τέτοιο περιβάλλον, τα ψηφιακά δεδομένα, είτε αυτά πρόκειται για προσωπικά δεδομένα είτε για επιχειρηματικά και κυβερνητικά μεγάλης οικονομικής και πολιτικής αξίας (σε ορισμένες περιπτώσεις και στρατηγικής), έχουν αποκτήσει τεράστια σημασία, όπως και η προσπάθεια για την διαφύλαξή τους. Το περιβάλλον του κυβερνοχώρου ως προς τον ορισμό του, είναι ιδιαίτερα πολύπλοκο και ασαφές. Το γεγονός αυτό, καθιστά και τον ορισμό της προστασίας του επίσης δυσχερή και παράλληλα την προστασία των δεδομένων έναν ιδιαίτερα απαιτητικό στόχο. Τα ψηφιακά δεδομένα, έχουν αποκτήσει έναν ρόλο κλειδί που μπορεί να επηρεάσουν τη φήμη, τη λειτουργία ή και πολλές φορές την ίδια την επιβιωσιμότητα διαφόρων οργανισμών. Η προσπάθεια για την προστασία τους απαιτεί αυτοματοποιημένες λύσεις, οι οποίες συνεχώς αναθεωρούνται προσαρμοζόμενες κάθε φορά στις εξελίξεις του τομέα. Η κυβερνοάμυνα και οι λύσεις που τείνουν προς την κατεύθυνση της διαμόρφωσης ενός ασφαλούς ψηφιακού περιβάλλοντος, έχει αποκτήσει τα τελευταία χρόνια από τους πλέον πρωταρχικούς ρόλους και έχει τεθεί σε πολλά επίπεδα ως στρατηγικός στόχος [National Cyber Security Strategy 2016 to 2021 of United Kingdom]. Ταυτόχρονα, οι εξελίξεις στο τομέα της μηχανικής μάθησης και της τεχνητής νοημοσύνης, προσφέρουν μια νέα προσέγγιση, που με τις παραδοσιακές

τεχνικές που ήδη εφαρμόζονται, μπορούν να συμβάλλουν σε ένα ασφαλέστερο ψηφιακό περιβάλλον.

Οι προκλήσεις για τους αμυνόμενους χρόνο με το χρόνο αυξάνονται καθώς η ανακάλυψη και η υιοθέτηση πρωτοεμφανιζόμενων πρακτικών και μεθόδων αποτελεί καθημερινό φαινόμενο, καταδεικνύοντας τη μεγάλη αναγκαιότητα που υπάρχει για ύπαρξη και υλοποίηση πολιτικών ασφαλείας, στρατηγικής αλλά και έρευνας προς την κατεύθυνση αυτή. Χαρακτηριστικά είναι τα όσα αναφέρονται στο [CISCO Cyber Annual Report 2016], όπου οι περισσότεροι υπεύθυνοι ασφαλείας των πληροφοριακών συστημάτων διαφόρων οργανισμών (Chief Security Officers and Security Operations Managers), αναφέρουν πως δεν είναι απόλυτα σίγουροι για την ικανότητά τους να εντοπίσουν και να αντιμετωπίσουν μια κακόβουλη επίθεση εναντίον τους.

Όπως αναφέρεται στο [National Cyber Security Strategy 2016 to 2021 of United Kingdom], η ασφάλεια αλλά και η ευημερία συγκεκριμένα της Αγγλίας, θα στηρίζεται όλο και περισσότερο σε ψηφιακές δομές και για τον λόγο αυτό, αποτελεί πρόκληση για την γενιά μας η δημιουργία μιας ακμάζουσας ψηφιακής κοινωνίας, που θα μπορεί να είναι ελαστική σε επιθέσεις και κατάλληλα εξοπλισμένη με γνώση και δυνατότητες που απαιτούνται για να μεγιστοποιήσουν τις ευκαιρίες και να διευθύνουν τους κινδύνους.

Το διαδίκτυο (internet), έχει μετασχηματίσει τον τρόπο που λειτουργούν ολόκληρες οικονομίες, και πλέον πολλές από αυτές βασίζουν την λειτουργία τους σε αυτό ακριβώς. Η επέκταση της χρήσης του σε συσκευές, πέραν των υπολογιστών και κινητών τηλεφώνων, και σε «έξυπνα συστήματα» (Smart Systems and Cyber-physical Systems and Internet of Things), αυξάνει το επίπεδο της απειλής (Surface of Attack) [Symantec 2016 Internet Security Report]. Από την άλλη είναι ένα πεδίο δράσης και παράνομων παραγόντων (Threat Actors), οι οποίοι εκμεταλλεύονται τις εγγενής αδυναμίες του για την υλοποίηση επιθέσεων. Όπως διαφαίνεται, αυτή η απειλή δεν θα εξαλειφθεί αποτελεσματικά και σε τελειωτικό βαθμό, λόγω της μεγάλης δυναμικής του περιβάλλοντος αυτού και της πολυπλοκότητάς του. Ωστόσο το

ρίσκο μπορεί να μειωθεί σε τέτοια επίπεδα που να επιτρέπουν τις κοινωνίες να αναπτύσσονται και να εκμεταλλεύονται τις τεράστιες δυνατότητες που προσφέρει η ψηφιακή επανάσταση.

Σκοπός της παρούσας εργασίας δεν είναι να αναλύσει σε βάθος και σε έκταση τεχνικές επιθέσεων αλλά και άμυνας που μπορεί να χρησιμοποιηθούν, ωστόσο, μια αναφορά του πλαισίου στρατηγικής και των σκοπών αυτής, κρίνεται σκόπιμη.

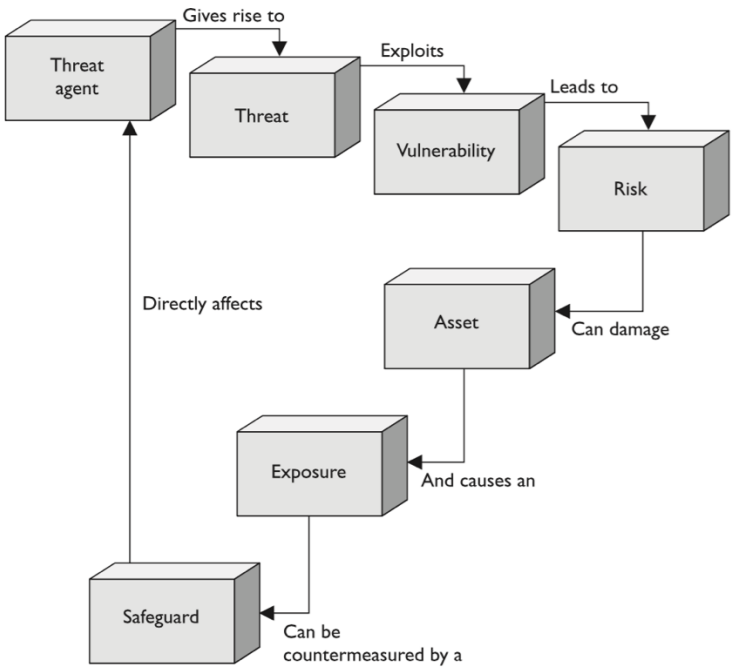
§2. Ορισμός και επιδιώξεις της κυβερνοάμυνας

Υπάρχουν πολλοί ορισμοί που θα μπορούσαν να αποδοθούν στην κυβερνοάμυνα (Cybersecurity). Ως τέτοια, μπορεί να αναφερθεί η προστασία των πληροφοριακών συστημάτων σε επίπεδο υλικο – λογισμικού (Hardware and Software), των δεδομένων τα οποία διακινούνται και αποθηκεύονται μέσω αυτών (Data at Rest, Data in Transit), και των υπηρεσιών που αυτά παρέχουν, από μη εξουσιοδοτημένη πρόσβαση (Unauthorized Access), ζημιά (Harm) και κακή χρήση (Misuse) (CISSP Study Guide, Mike Chapple, Sybex edition). Στα παραπάνω συμπεριλαμβάνεται η ζημιά η οποία προκύπτει εκούσια ή ακούσια από τον διαχειριστή του εκάστοτε συστήματος ή από εξωτερικούς παράγοντες.

Η άμυνα σε βάθος (Defense in Depth), οι καλές πρακτικές χρήσης (Best Business Practices), η εκπαίδευση (Training and Awareness) και ο διαμοιρασμός πληροφοριών (Timely Information Sharing) είναι κάποιες από τις τεχνικές με τις οποίες θα μπορούν ελαχιστοποιηθούν οι επιπτώσεις από πιθανές επιθέσεις. Όλα τα παραπάνω προσβλέπουν στην αντιμετώπιση στο μέγιστο του δυνατού των ευπαθειών που υπάρχουν ή δύναται να υπάρξουν, όπως για παράδειγμα η όλο και αυξανόμενη διασύνδεση στο διαδίκτυο συσκευών με απουσία μηχανισμών ασφαλείας, η μή εφαρμογή πολιτικών ασφαλείας (Cyber Hygiene and Compliance), η παλαιότητα συσκευών δικτύου που δεν ενημερώνονται με τις πιο πρόσφατες εκδόσεις ασφαλείας.

Γενικά, η βασική επιδίωξη της κυβερνοάμυνας είναι η εξασφάλιση της εμπιστευτικότητας (Confidentiality), της ακεραιότητας της πληροφορίας Iintegrity) και της διαθεσιμότητας

(Availability). Όλοι οι μηχανισμοί ασφαλείας που εφαρμόζονται έχουν ως σκοπό την προστασία μίας και παραπάνω από τις προαναφερθείσες αρχές, ενώ η σοβαρότητα των απειλών και των ευπαθειών προσμετρώνται με βάσει τον βαθμό που μπορεί να επηρεάσουν αυτές.



Εικόνα 1 Οι αλληλοσυνδέσεις μεταξύ διαφόρων εννοιών ασφαλείας (πηγή: Harris and Maymi, 2016)

Τα διάφορα μέτρα ασφαλείας που μπορεί να παρθούν σε κάθε περίπτωση, μπορεί να αφορούν μέτρα πρόληψης (Preventive), αποτροπής (Preventive and Deterrent), διορθωτικά (Corrective), επαναφοράς (Recovery) και εντοπισμού (Detective).

§3. Προς μια νέα προσέγγιση για τη λύση του προβλήματος

Η παρούσα μεταπτυχιακή διατριβή έχει ως στόχο, την υλοποίηση μεθόδων εξόρυξης γνώσης με τη χρήση της πλατφόρμας λογισμικού WEKA, πάνω σε δεδομένα τα οποία

έχουν συλλεχθεί από την κίνηση των ψηφιακών πακέτων αιτήσεων WEB (web requests), όπως αυτά καθορίζονται στο [http://www.isi.csic.es/dataset/] και θα αναλυθούν εκτενέστερα παρακάτω. Η προσέγγιση αυτή αποτελεί μια νέα κατεύθυνση και ένα νέο επιστημονικό πεδίο προς την συμβολή της πρόληψης και της δημιουργίας ενός ασφαλέστερου περιβάλλοντος κυβερνοάμυνας γενικότερα.

Η νέα προσέγγιση αφορά στη χρήση στοχευμένων μεθόδων μηχανικής μάθησης και αντίστοιχων αλγορίθμων, οι οποίες εφαρμόζονται σε μεγάλους όγκους δεδομένων κυβερνοάμυνας (Cyber Defense Big Data). Απώτερος σκοπός όλων, είναι η επίτευξη έγκαιρης προειδοποίησης στους εκάστοτε υπεύθυνους ασφαλείας και η πρόληψη ή και καταστολή των επιπτώσεων μιας κυβερνοεπίθεσης, συνεπικουρώντας στις παραδοσιακές μεθόδους προστασίας.

Ο ρόλος των έξυπνων προγραμμάτων (intelligent software) στις επιχειρήσεις κυβερνοπολέμου, έχει αυξηθεί τα τελευταία χρόνια εξαιτίας της ανάγκης επεξεργασίας μεγάλων όγκων δεδομένων. Η ολοένα και αυξανόμενη ευφυία πίσω από τις εφαρμοζόμενες τακτικές με σκοπό την αποφυγή εντοπισμού από τα υπάρχοντα λογισμικά, σηματοδοτεί την ανάγκη εξεύρεσης νέων λύσεων και προσεγγίσεων. Η χρήση της τεχνητής νοημοσύνης και εργαλείων που βασίζονται στην απόκτηση γνώσης, θεωρείται ότι θα συμβάλει προς αυτή την κατεύθυνση. Στο [The Lipman Report, 2010], αναφέρεται ότι «η κυβερνοάμυνα της Αμερικής έχει μείνει βήματα πίσω στις τεχνολογικές δυνατότητες των εν δυνάμει αντιπάλων, τόσο ώστε ο αριθμός των επιθέσεων να είναι τόσο μεγάλος σε αριθμό και ευφυία σχεδιασμού, ώστε πολύ οργανισμοί να μην είναι σε θέση να καθορίσουν ποιες ευπάθειες και απειλές αποτελούν το μεγαλύτερο ρίσκο για αυτές», καταδεικνύοντας και την ανάγκη για την υιοθέτηση νέων μεθόδων στο τομέα αυτό.

§4. Δομή Εργασίας

Στο κεφάλαιο 2 της εργασίας, θα αναφερθούμε γενικά στη δομή του πρωτοκόλλου HTTP, στην υφιστάμενη μεθοδολογία που ακολουθείται για την αναγνώριση κακόβουλων μορφών αιτήσεων σε περιβάλλον WEB, καθώς και στη λειτουργία των παραδοσιακών Web Application Firewalls. Στη συνέχεια στο κεφάλαιο 3 θα αναλυθούν οι έννοιες της τεχνητής νοημοσύνης, ορισμοί της μηχανικής μάθησης και της εξόρυξης γνώσης καθώς και τα κοινά πεδία δράσης και χαρακτηριστικά μεταξύ της μηχανικής μάθησης και της κυβερνοάμυνας όπως και τις μελλοντικές προοπτικές του συγκεκριμένου τομέα. Στο κεφάλαιο 4 θα γίνει μια ανάλυση της υφιστάμενης κατάστασης και τις έως τώρα ερευνητικές προσπάθειες που γίνονται με τη χρήση Τεχνητών Νευρωνικών Δικτύων, Κανόνων Συσχέτισης και Ασαφών Κανόνων, όπως και με Δέντρα Αποφάσεων και Μηχανές Υποστηρικτικού Διανύσματος. Στο Κεφάλαιο 5, παρουσιάζεται και γίνεται μια ανάλυση του εργαλείου WEKA, με το οποίο θα επιχειρήσουμε την ανάλυση ενός συνόλου δεδομένων του πρωτοκόλλου HTTP προς εξέταση της δυνατότητας κατηγοριοποίησης και ανίχνευσης επιθέσεων με τη χρήση διαφόρων αλγορίθμων και μεθόδων του συγκεκριμένου εργαλείου. Η ανάλυση και η μεθοδολογία που θα ακολουθήσουμε, θα παρουσιαστεί στο κεφάλαιο 6.

ΚΕΦΑΛΑΙΟ 2
Το πρωτόκολλο Http

§1. Εισαγωγή

Το πρωτόκολλο http είναι ένα πρωτόκολλο στο επίπεδο των εφαρμογών (application protocol), και αποτελεί τη κύρια δομή πάνω στην οποία στηρίζονται οι επικοινωνίες διαμέσου του World Wide Web. Ο πρώτος ορισμός του πρωτοκόλλου δόθηκε στο RFC 2068 το 1997, ενώ σήμερα περιγράφεται από το RFC 7230 του 2014.

Year	HTTP Version
1991	0.9
1996	1.0
1997	1.1
2015	2.0

Εικόνα 2 Εκδόσεις του πρωτοκόλλου ανά έτη [πηγή: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol]

Είναι το κύριο πρωτόκολλο που χρησιμοποιείται στους σελιδομετρητές του Παγκοσμίου Ιστού για τη μεταφορά δεδομένων μεταξύ ενός πελάτη και ενός διακομιστή. Σήμερα είναι το πλέον καθιερωμένο και διαδεδομένο σε σημείο που σχεδόν όλοι οι σελιδομετρητές να το θεωρούν δεδομένο. Η τόσο μεγάλη χρήση του και αποδοχή του στις επικοινωνίες του Παγκοσμίου Ιστού, σημαίνει μεγάλο ρόλο και στο κομμάτι αναφορικά με την ασφάλεια. Στις μέρες μας το πρωτόκολλο Https, αρχίζει να κυριαρχεί έναντι του "απλού" και μη ασφαλούς Http, πλην όμως, υπάρχει πληθώρα ιστοτόπων που το χρησιμοποιούν ακόμα.

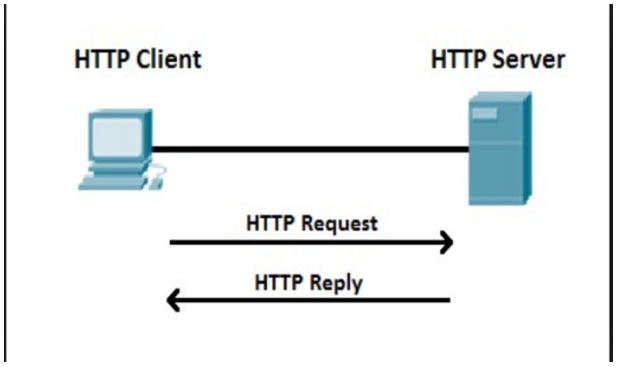
Επιπρόσθετα, η ευρεία του χρήση, δίνει έναυσμα για εκμετάλλευσή του και για κακόβουλες ενέργειες, χρησιμοποιώντας το σαν μέσο, και για τον λόγο αυτό, πολλές λύσεις ασφαλείας που έχουν αναπτυχθεί, όπως για παράδειγμα τοίχοι προστασίας εφαρμογών (Web Application Firewalls), εστιάζουν και στη προστασία των επικοινωνιών με το συγκεκριμένο πρωτόκολλο.

§2. Τεχνική επισκόπηση

Το πρωτόκολλο λειτουργεί στα πλαίσια της δομής της επικοινωνίας μεταξύ ενός εξυπηρετητή (server - client) και ενός πελάτη και είναι πρωτόκολλο αίτησης – απάντησης (request – response). Η διαδικασία που ακολουθούσε το αρχικό πρωτόκολλο ήταν η εξής:

- Σύνδεση στον εξυπηρετητή
- Ερώτηση προς τον εξυπηρετητή
- Απάντηση προς τον εξυπηρετητή

Σήμερα χρησιμοποιεί πολύ περισσότερα χαρακτηριστικά τα οποία παρέχουν ακόμα και τη δυνατότητα στο πρόγραμμα-πελάτης να στέλνει δεδομένα στον εξυπηρετητή, με ότι αυτό μπορεί να συνεπάγεται για την ασφάλειά του.



Εικόνα 3 Διάγραμμα ροής επικοινωνίας του Http [πηγή: http://study-ccna.com]

Αν και το Http πρωτόκολλο σχεδιάστηκε για χρήση στον Ιστό, υποστηρίζει λειτουργίες που είναι πιο γενικές από ότι απαιτείται. Οι λειτουργίες αυτές ονομάζονται μέθοδοι. Κάθε αίτηση αποτελείται από μία ή περισσότερες γραμμές κειμένου ASCII με τη πρώτη λέξη της γραμμής της αίτησης να είναι το όνομα της ζητούμενης μεθόδου.
Παρακάτω παρουσιάζονται συνοπτικά οι ενσωματωμένες μέθοδοι αίτησης του πρωτοκόλλου οι οποίες αναφέρονται και χρησιμοποιούνται στο σύνολο δεδομένων που αθ χρησιμοποιηθεί στη παρούσα διατριβή:

- GET Η μέθοδος αυτή ζητάει από τον διακομιστή να στείλει τη σελίδα με τη πιο συνήθης μορφή να είναι του τύπου GET όνομα_αρχείου HTTP/1.1, όπου το όνομα του αρχείου προσδιορίζει το όνομα του πόρου που πρέπει να προσκομιστεί και το 1.1 είναι η έκδοση του πρωτοκόλλου που χρησιμοποιείται

- POST Η μέθοδος POST κατά την υποβολή των φορμών. Όπως και η μέθοδος GET, έτσι και η POST περιέχει μια διεύθυνση URL αλλά αντί να ανακτά απλώς τη σελίδα μεταφέρει δεδομένα στο διακομιστή, όπως για παράδειγμα τα περιεχόμενα της φόρμας. Έπειτα ο διακομιστής επεξεργάζεται την αίτηση και τελικά η μέθοδος επιστρέφει μια σελίδα που δείχνει το αποτέλεσμα.

Οι παραπάνω μέθοδοι είναι αυτοί που αναφέρονται στο dataset που θα χρησιμοποιηθεί. Για λόγους πληρότητας, παρακάτω αναφέρονται και οι υπόλοιπες του πρωτοκόλλου, όπως οι εξής:

- HEAD
- PUT
- DELETE
- TRACE
- CONNECT
- OPTIONS

```
HTTP/1.1 200 OK
Date: Mon, 23 May 2005 22:38:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 138
Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT
Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)
ETag: "3f80f-1b6-3e1cb03b"
Accept-Ranges: bytes
Connection: close

<html>
<head>
  <title>An Example Page</title>
</head>
<body>
  Hello World, this is a very simple HTML document.
</body>
</html>
```

Εικόνα 4. Ανάλυση της επικοινωνίας του πρωτοκόλλου [πηγή: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol]

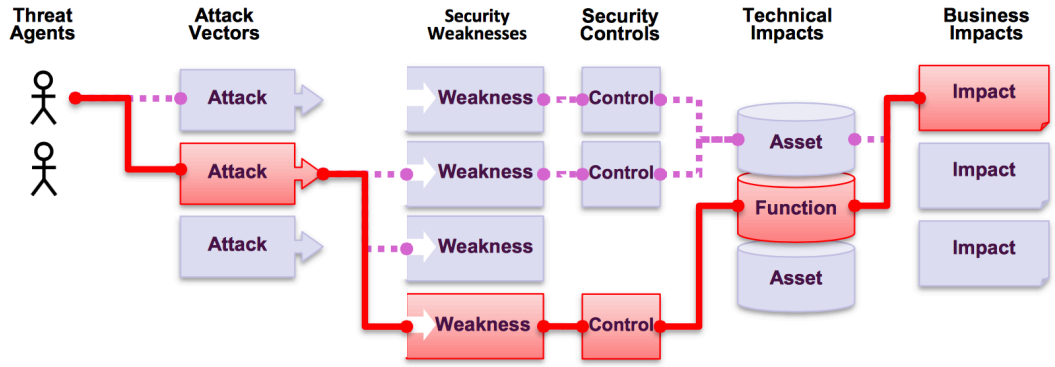
§3. Επιθέσεις εναντίον του HTTP

Στη βιβλιογραφία υπάρχουν πολλές αναφορές σχετικές με τις επιθέσεις που μπορεί να πραγματοποιηθούν εναντίον του πρωτοκόλλου Http. Αξίζει να αναφερθεί ότι το συγκεκριμένο πρωτόκολλο κυριαρχεί στο internet. Καθώς όμως η δημοτικότητα αυξάνεται, το ίδιο συμβαίνει και με το ρίσκο διενέργειας κακόβουλων επιθέσεων μέσω αυτού. Όπως κάθε πρωτόκολλο έτσι και το Http είναι ευπαθές σε διαφόρων τύπων επιθέσεων.

Σκοπός της παρούσας διατριβής δεν είναι η ενδελεχής ανάλυση όλων των δυνατών επιθέσεων. Για λόγους πληρότητας θα γίνει μια αναφορά στις περισσότερο γνωστές επιθέσεις με σκοπό την κατάδειξη του μεγάλου βαθμού της τρωτότητας που υφίσταται στην υλοποίηση του συγκεκριμένου πρωτοκόλλου, στην ποικιλία των επιθέσεων και ταυτόχρονα την ανάγκη για την εφαρμογή επιπλέον μηχανισμών ασφαλείας ή και νέων τεχνικών στους ήδη υπάρχοντες. Έτσι λοιπόν, υπάρχουν επιθέσεις που επικεντρώνονται στην άρνηση υπηρεσίας (Denial of Service) και άλλες που σκοπό έχουν να αναγκάσουν τον διακομιστή σε λειτουργία η οποία δεν είναι η ενδεδειγμένη. Διάφοροι τύποι των επιθέσεων είναι οι εξής:

- SYN FLOOD
- GET FLOOD
- Reverse Bandwidth Floods
- HTTP Fuzzers and misbehaved fields
- Cache Bypassing Attacks
- Cross Site Scripting
- SQL Injection
- Επιθέσεις που περιγράφονται στο OWASP Top 10 [https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf]

Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν πολλές διαφορετικές προσεγγίσεις για να προκαλέσουν κακόβουλα αποτελέσματα σε πληροφοριακά συστήματα διαφόρων οργανισμών και επιχειρήσεων. Μερικές φορές το να αναγνωριστούν τέτοιου είδους κακόβουλες ενέργειες είναι κάτι το τετριμμένο, άλλες φορές όμως μπορεί να αποδειχτεί κάτι το εξαιρετικά δύσκολο. Κατ' επέκταση, οι συνέπειες των κακόβουλων ενεργειών μπορεί να είναι ελάσσονος σημασίας και άλλες να έχουν εξαιρετικά μεγάλο αντίκτυπο. Όπως είναι φυσικό, για να μπορεί να υπολογιστεί το ρίσκο που διατρέχει μια επιχείρηση ή ένας οργανισμός, θα πρέπει να αξιολογηθεί η πιθανότητα η οποία σχετίζεται με τον κάθε παράγοντα απειλής, οι αδυναμίες στα συστήματα που υφίστανται καθώς και εκτιμήσεις αναφορικά με τα υφιστάμενα επίπεδα ασφαλείας.



Εικόνα 5. Διαγραμματική ανάλυση των σταδίων κακόβουλων ενεργειών

[πηγή:www.owasp.org]

Για την αντιμετώπιση των παραπάνω επιθέσεων και όπως έχει ήδη αναφερθεί σε προηγούμενο κεφάλαιο, διάφορες λύσεις ασφάλειας εφαρμόζονται επικουρικά, για την αντιμετώπιση των εκάστοτε ευπαθειών των εκάστοτε πρωτοκόλλων και υπηρεσιών. Απώτερος σκοπός όλων αυτών είναι η εξασφάλιση των αρχών της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των υπηρεσιών (Confidentiality, Integrity, Availability).

Στη παρούσα διατριβή, και όπως θα αναφερθεί στην ανάλυση του συνόλου των δεδομένων που θα χρησιμοποιηθεί, οι κακόβουλες ενέργειες αφορούν κυριότερα επιθέσεις του τύπου SQL

injections, buffer overflows, CRLF injection, Cross Site Scripting. Για λόγους πληρότητας, αξίζει να περιγραφούν αναλυτικότερα οι παραπάνω επιθέσεις.

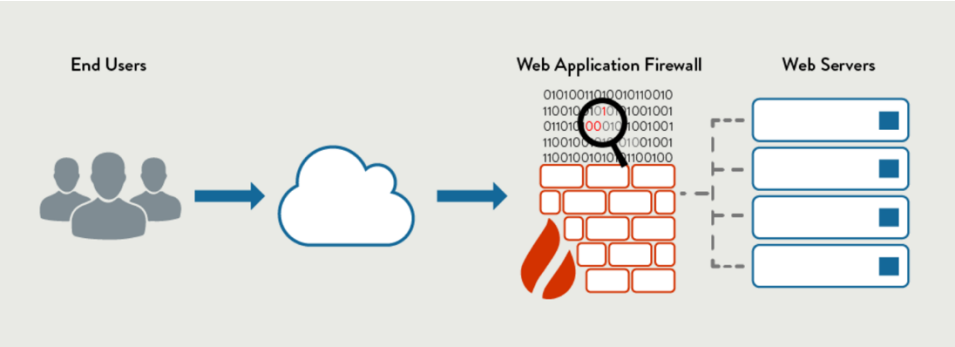
- Injection. Αυτές πραγματοποιούνται όταν μη εμπιστευμένα δεδομένα στέλνονται σε ένα διερμηνέα ως μέρος μιας εντολής ή ερώτησης. Τα δεδομένα του κακόβουλου χρήστη μπορούν να ξεγελάσουν τον διερμηνέα να εκτελέσει μη προβλεπόμενες εντολές ή να έχει πρόσβαση σε δεδομένα που δεν είναι εξουσιοδοτημένος για αυτά.
- Cross Site Scripting. Τέτοιου τύπου επιθέσεις συμβαίνουν όταν μια εφαρμογή περιλαμβάνει μη εμπιστευμένα δεδομένα σε μια νέα ιστοσελίδα χωρίς την κατάλληλη επικύρωση ή ενημερώνει μια ήδη υπάρχουσα ιστοσελίδα με δεδομένα του χρήστη. Τέτοιου τύπου επιθέσεις επιτρέπουν στο κακόβουλο χρήστη να εκτελέσουν αρχεία εντολών (scripts), στον σελιδομετρητή του θύματος και με τον τρόπο αυτόν να ανακατευθύνει τον χρήστη σε άλλες ιστοσελίδες, να αλλάξει την μορφή των ιστοσελίδων και άλλα.
- Buffer Overflow. Τέτοιου τύπου επιθέσεις στόχο έχουν να καταλύσουν τη δομή μιας web εφαρμογής. Αποστέλλοντας κατάλληλα τροποποιημένα δεδομένα, μπορεί να προκληθεί εκτέλεση κακόβουλου κώδικα καταλαμβάνοντας το υπολογιστικό σύστημα που δέχεται την επίθεση.

§4. Υφιστάμενοι τρόποι ανίχνευσης εισβολής και προστασία από επιθέσεις

Είναι παραδεκτό πως στη σημερινή εποχή, καμιά στρατηγική και πολιτική ασφαλείας δεν είναι πανάκεια. Σε πολλούς οργανισμούς, η επιλογή εγκατάστασης ενός IDS (Intrusion Detection System) ή IPS (Intrusion Prevention System), παράλληλα με ένα τείχος

προστασίας (firewall), είναι συνήθης και θεωρείται ως η καλύτερη (best practice), για τον σχεδιασμό ενός δικτυακού περιβάλλοντος.

Τα Web Application Firewalls αποτελούν ένα κύριο εργαλείο για την ασφάλεια μιας Web εφαρμογής και γενικότερα υφίστανται σε ένα τυπικό διάγραμμα δικτύου συνεπικουρώντας στη γενικότερη πολιτική ασφαλείας, όπως φαίνεται στην Εικόνα 6.



Εικόνα 6. Τυπική Διάταξη Web Application Firewall [πηγή: https://avinetworks.com]

Μία επεξήγηση του τρόπου λειτουργίας τους ξεφεύγει από τους σκοπούς της παρούσας διατριβής, ωστόσο δίνεται για λόγους πληρότητας, είναι ότι ένα τέτοιο τείχος προστασίας παρέχει ασφάλεια για online επικοινωνίες από κακόβουλες ενέργειες. Αντίστοιχα τοίχοι προστασίας αναλύουν και φιλτράρουν απειλές οι οποίες μπορούν να υποβαθμίσουν, αποτρέψουν ή παραβιάσουν τις επιτρεπτές επικοινωνίες. Η λειτουργία τους αυτή μπορεί να εφαρμοστεί τόσο σε επίπεδο hardware όσο και σε επίπεδο software, σε ξεχωριστές συσκευές ή ενσωματωμένα σε άλλες δικτυακές συσκευές.

Τα Web Application Firewalls παρεμβάλλονται και έτσι επιθεωρούν τις επικοινωνίες που γίνονται μέσω του πρωτοκόλλου Http, χρησιμοποιώντας κανόνες από μια πολιτική ασφαλείας που έχει οριστεί από τον εκάστοτε διαχειριστή. Παραδοσιακά, η παραμετροποίηση αυτών των κανόνων ασφαλείας είναι μια διεργασία πολύπλοκη και δεν πραγματοποιείται εύκολα χωρίς εξειδικευμένη γνώση. Σε αντίθεση με τα παραδοσιακά τοίχοι προστασίας που προστατεύουν τη ροή των πληροφοριών μεταξύ εξυπηρετητών, τα WAF φιλτράρουν την κίνηση των πακέτων για συγκεκριμένες εφαρμογές.

Τα πρώτα τοίχοι προστασίας εφαρμογών, είχαν ως στόχο τη προστασία σελίδων σχετικών με το ηλεκτρονικό εμπόριο [www.avinetworks.com] και προστάτευαν τους πόρους από επιθέσεις όπως οι παρακάτω:

- Hidden Field Manipulation
- Cookie Poisoning
- Parameter Tampering
- Buffer Overflow
- Cross Site Scripting
- SQL Injection
- Remote Code Execution
- Forced Browsing

Τα πλεονεκτήματα αυτών των συσκευών αφορούν την ικανότητά τους να προστατεύουν από ευπάθειες τις διάφορες εφαρμογές οι οποίες μπορεί να προέρχονται από κακές πρακτικές προγραμματισμού ή και λόγω παλαιότητάς τους. Είναι ικανά να παρέχουν εικόνα για το τί συμβαίνει σε πραγματικό χρόνο παρέχοντας στους διαχειριστές τη δυνατότητα να παρεμβαίνουν σε τυχόν κακόβουλες ενέργειες άμεσα. Ένα WAF αναλύει τους κανόνες ασφαλείας που ταιριάζουν για συγκεκριμένες δικτυακές επικοινωνίες και αναλόγως παρέχει πληροφορίες για το τί πραγματικά μπορεί να συμβαίνει.

Από την άλλη λόγω του ότι τα WAF βρίσκονται ανάμεσα στο χρήστη και την εφαρμογή, αυτό μπορεί να προκαλέσει καθυστερήσεις προκαλώντας μείωση στο δείκτη ευχαρίστησης του χρήστη από τη χρησιμοποίηση της εφαρμογής. Εξ 'ορισμού, η εξέταση των πακέτων κοστίζει σε υπολογιστική ισχύ και έτσι υπεισέρχονται θέματα που αφορούν καθυστέρηση στην κίνηση. Αυτή ακριβώς η κατάσταση είναι που φέρνει τις επιχειρήσεις και τους οργανισμούς μπροστά σε ένα δίλημμα που αφορά είτε τη προσέγγιση αύξησης του κόστους προς αύξηση της αποδοτικότητας του τείχους προστασίας είτε τη μείωση των

απαιτήσεων επιθεώρησης και έτσι την αύξηση του ρίσκου αποδοχής για κακόβουλες ενέργειες. Επιπρόσθετα είναι αρκετά πολύπλοκα ως προς την εγκατάστασή τους απαιτούν συχνές αναθεωρήσεις και επιθεωρήσεις της λειτουργίας τους.

Οι εν λόγω συσκευές, δεν είναι ικανές να προσαρμόζονται αυτόνομα στις ανάγκες ενός δικτυακού περιβάλλοντος και έτσι θα χρειαστεί κάποιος έμπειρος διαχειριστής να τις παραμετροποιήσει κατάλληλα, καθώς δεν μπορεί να θεωρηθούν ως συσκευές 'Plug and Play'. Σήμερα, αποτελεί καλή πρακτική, ο διαχειριστής ενός δικτύου, να αναλύει, εξετάζει και τελικώς να παραμετροποιεί κατάλληλα τα αποτελέσματα από ένα IDS, διαφορετικά θα καταλήγει να δέχεται πολλά 'false positives'.

§5. Η νέα προσέγγιση του προβλήματος με τη χρήση μηχανικής μάθησης και εξόρυξης γνώσης

Παραδοσιακά, όλες οι εφαρμογές πολιτικών ασφαλείας έχουν ως έναν από τους κυρίαρχους στόχους τους, να περιορίσουν στο ελάχιστο τα αποκαλούμενα false positives, δηλαδή όλες εκείνες τις φορές στις οποίες ένα σύστημα ασφαλείας αντέδρασε και επεσήμανε συναγερμό, πλην όμως αυτός ήταν άκυρος. Στη περίπτωση των Web Application Firewalls, παρατηρείται ένας μεγάλος αριθμός false positives (FP), και αυτό έγκειται στο γεγονός του τρόπου λειτουργίας του και του τρόπου ανίχνευσης των απειλών.

Τα σημερινά τείχη προστασίας εφαρμογών βασίζονται αποκλειστικά σε μια μέθοδο παρατηρητικότητας (observational method) για την ανίχνευση απειλών η οποία αποκαλείται Application Learning (AP) [https://www.fortinet.com/blog/business-and-technology/fortiweb-release-6-0--ai-based-machine-learning-for-advanced-thr.html]. Έτσι αυτοματοποιείται η δημιουργία προφίλ χρήσης και δομής της web εφαρμογής. Όταν τα δεδομένα τα οποία έχουν καταγραφεί είναι αρκετά, τότε η παραπάνω μέθοδος χτίζει πολιτικές βασιζόμενη σε ότι έχει συναντήσει έως τότε και οτιδήποτε παρεκκλίνει από αυτό θεωρείται

αιτία περαιτέρω ενεργειών όπως καταγραφής, ειδοποίησης ή και απόρριψης. (logging, alerting, blocking).

Η ακρίβεια που προσφέρεται όμως με αυτή τη μέθοδο δεν είναι η βέλτιστη καθώς προκύπτουν πολλά false positives (www.fortinet.com), και έτσι η πιθανότητα να απορρίπτονται πακέτα εντός των πλαισίων νόμιμης κίνησης είναι υπαρκτός πλην όμως ανεκτός. Το μειονέκτημα αυτό έγκειται στο τρόπο λειτουργίας αυτών των τειχών προστασίας. Εγείρονται ανωμαλίες βασιζόμενες μόνο σε ότι έχει ήδη παρατηρηθεί χωρίς να μπορεί να προσδιοριστεί περαιτέρω αν κάτι πρόκειται για επίθεση ή απλά μια κανονικότητα.

Τα τελευταία χρόνια παρατηρείται μια αύξηση στη χρήση της μηχανικής μάθησης (machine learning) και της εξόρυξης γνώσης (data mining), σε πολλούς τομείς της οικονομίας και τελευταία και στον τομέα της κυβερνοάμυνας. Στην εργασία των Buczak και Guven (2015), γίνεται αναφορά στις μεθόδους που έχουν χρησιμοποιηθεί έως τώρα για την ανάλυση δεδομένων κυβερνοάμυνας με τις παραπάνω μεθόδους. Τα δεδομένα που καταγράφονται αφορούν σε ένα μεγάλο εύρος κατηγοριών ενδιαφέροντος. Χαρακτηριστικά, μπορεί να περιλαμβάνουν δεδομένα από την καταγραφή και ανάλυση της διαδικτυακής κίνησης των ψηφιακών πακέτων μεταξύ διαφόρων δικτυακών συσκευών και δεδομένα καταγραφής από IDSs (Intrusion Detection Systems), τόσο από ενσύρματα όσο και από ασύρματα δίκτυα καθώς και από διαφορετικά επίπεδα του OSI model (Open System Interconnection Model). Αναφορικά με τις μεθόδους καταγραφής και εδώ παρατηρούνται διάφορες προσεγγίσεις, όπως για παράδειγμα με τη χρήση διάφορων εργαλείων καταγραφής όπως είναι το Wireshark, το NetFlow ή logs από IDSs.

Το σημερινό ψηφιακό περιβάλλον, χρόνο με το χρόνο γίνεται όλο και πιο περίπλοκο και για την ανάλυσή του απαιτούνται πόροι και γνώση που δύσκολα βρίσκονται. Τομείς όπως η ανάλυση αποφάσεων (decision support), η γνώση της υφιστάμενης κατάστασης και η διαχείρισή της (situation awareness and knowledge management), επωφελούνται πλήρως από την εφαρμογή μεθόδων τεχνητής νοημοσύνης και έξυπνων συστημάτων.

Πράγματι, οι νέες προσεγγίσεις στο τομέα της ασφάλειας και ειδικότερα στο τρόπο με τον οποίο οι διαφόρων τύπων συσκευές ασφαλείας προσεγγίζουν το θέμα της ασφάλειας, επιβάλλουν νέες αντιλήψεις και εφαρμογές νέων τεχνικών, όπως της μηχανικής μάθησης και άλλων. Έτσι από την προσέγγιση της σύγκρισης συγκεκριμένων προτύπων με την παρατηρούμενη δραστηριότητα, οδηγούμαστε στο καθορισμό της πιθανότητας μια παρατηρούμενη δικτυακή κίνηση να αποτελεί κίνδυνο ή το αντίθετο.

Στις περισσότερες υλοποιήσεις υπάρχουν πολυεπίπεδα στο τρόπο λειτουργίας των τοίχων προστασίας [https://www.fortinet.com/blog/business-and-technology/fortiweb-release-6-0--ai-based-machine-learning-for-advanced-thr.html]. Έτσι επιτυγχάνεται καλύτερη αντιμετώπιση των περιπτώσεων όπου ένα πακέτο θεωρείται επικίνδυνο, καθώς στο δεύτερο επίπεδο καθορίζεται η πιθανότητα αυτό να είναι σωστό.

Στο επόμενο κεφάλαιο θα γίνει μια ανάλυση των εννοιών της μηχανικής μάθησης και της εξόρυξης γνώσης, των πλεονεκτημάτων αλλά και των αδυναμιών τους γενικότερα. Παράλληλα, θα δοθεί συνοπτικά η χρήση που μπορεί να έχουν στο τομέα της κυβερνοάμυνας.

ΚΕΦΑΛΑΙΟ 3
Η Τεχνητή Νοημοσύνη

§1. Εισαγωγή και ορισμός της Τεχνητής Νοημοσύνης

Η σύγχρονη επιστήμη έχει οδηγήσει στην ανάπτυξη πολλών και διαφορετικών προσεγγίσεων δημιουργίας ευφυών προτύπων, ικανών να αναπαριστούν πολύπλοκες περιπτώσεις φαινομένων και προβλημάτων, με σκοπό τη δημιουργία προγνώσεων ή κατατάξεων και ομαδοποιήσεων. Το αποτέλεσμα είναι ότι με τους μηχανισμούς τους, μπορούν και προσεγγίζουν ικανοποιητικά καταστάσεις σε διάφορα περιβάλλοντα, ένα εκ των οποίων

αποτελεί και αυτό της κυβερνοάμυνας, συμβάλλοντας στο έργο και στις ήδη προσφερόμενες λύσεις για την επίλυση του ζητήματος της ασφάλειας στο κυβερνοχώρο.

Η τεχνητή ευφυία ή αλλιώς τεχνητή νοημοσύνη, είναι ένας όρος για τον οποίο έχουν διατυπωθεί πολλοί ορισμοί (International Dictionary of Artificial Intelligence, Turban) και διαφέρουν αναλόγως της οπτικής γωνίας προσέγγισης του θέματος. Σύμφωνα με τον Turban and Aronson (Decision Support Systems and Intelligent Systems, 1998), «Τεχνητή ευφυία είναι η συμπεριφορά μιας μηχανής, η οποία αν μπορούσε να παρατηρηθεί σε έναν άνθρωπο, θα δικαιολογούσε τον χαρακτηρισμό τους ως ευφυούς», ενώ ο Durkin (Expert Systems Design and Development, 1994), αποδίδει τον ορισμό της τεχνητής νοημοσύνης στον κλάδο της επιστήμης των υπολογιστών που περιλαμβάνει νέες στρατηγικές έρευνας και μεθόδους αναπαράστασης της γνώσης σε προγράμματα ηλεκτρονικών υπολογιστών, στην προσπάθεια να προσομοιωθεί η διαδικασία που ακολουθεί το ανθρώπινο μυαλό για την επίλυση διαφόρων προβλημάτων.

Σήμερα είναι αναγκαία η ανάπτυξη ευφυών πληροφοριακών συστημάτων, ικανών να λειτουργούν σε αβέβαιο περιβάλλον και να συνεκτιμούν αβέβαια, υποκειμενικά, ασαφή και ατελή δεδομένα, παράγοντας εκτιμήσεις αξιόπιστων δεικτών κινδύνου [Ευφυή Πληροφοριακά Συστήματα και Εφαρμογές στην Εκτίμηση Κινδύνου, Λ. Ηλιάδης].

§2. Η τεχνητή έναντι της ανθρώπινης νοημοσύνης

Μια εκ των βασικών κατευθύνσεων και προσπαθειών στον τομέα της ασφάλειας στον κυβερνοχώρο, είναι αυτή της ανάπτυξης ευφυών συστημάτων που να ενσωματώνουν αλγόριθμους και μηχανισμούς μηχανικής μάθησης και εξόρυξης γνώσης, κάτι το οποίο θα αναλυθεί εκτενέστερα παρακάτω. Η βασική προσέγγιση δεν είναι να αντικατασταθεί η ανθρώπινη παρουσία στον καθορισμό και την ανάλυση της λειτουργίας ενός δικτύου, αλλά, να προστεθούν στο οπλοστάσιο των διαχειριστών δικτύων, έμπειρα συστήματα που θα μπορούν

να ανακαλύψουν κρυμμένες πληροφορίες και δομές στην δικτυακή κίνηση, συνεπικουρώντας στις ήδη υπάρχουσες πολιτικές ασφαλείας.

Αξίζει να αναφερθούμε λοιπόν, στις διαφορές μεταξύ της τεχνητής νοημοσύνης και της ανθρώπινης, και να παρουσιαστούν τα βασικά πλεονεκτήματα και μειονεκτήματά τους, έτσι ώστε να καταστεί πιο σαφής η δυναμική που έχει αποκτήσει η χρήση της στο τομέα που εξετάζουμε.

Στο [Συστήματα Υποστήριξης Αποφάσεων, Ν. Ματσατσίνης, 2010], παρατίθεται μια σειρά από τις διαφορές μεταξύ τους. Στη συνέχεια δίνονται τα αποτελέσματα μερικών τέτοιων συγκρίσεων.

- Σε αντίθεση με τον άνθρωπο που έχει μεταβαλλόμενη νοημοσύνη, είτε γιατί αλλάζει άποψη για κάποιο θέμα είτε γιατί ξεχνά, η γνώση της Τ.Ν. παραμένει αναλλοίωτη.
- Η διαδικασία απόσπασης και αποθήκευσης της γνώσης σε ένα σύστημα Τ.Ν. γίνεται μόνο μια φορά, ενώ ακολούθως μπορεί να αναπαραχθεί και να εγκατασταθεί σε όσους υπολογιστές χρειάζεται. Αντιθέτως, η ανθρώπινη γνώση απαιτεί μακροχρόνια εκπαίδευση κάθε φορά που χρειάζεται να μεταφερθεί από ένα άτομο σε ένα άλλο.
- Η χρήση τεχνικών Τ.Ν. κοστίζει τις περισσότερες φορές λιγότερο από το κόστος χρησιμοποίησης ανθρώπων για την διεξαγωγή των ίδιων εργασιών.
- Η ανθρώπινη συμπεριφορά και νοημοσύνη είναι ασταθής και επηρεάζεται από πολλούς παράγοντες, σε αντίθεση με την Τ.Ν. η οποία είναι σταθερή και ανεξάρτητη από εξωτερικές επιδράσεις.
- Η Τ.Ν. μπορεί ανά πάσα στιγμή να τεκμηριώσει το τρόπο σκέψης της. Μπορεί δηλαδή να παραθέσει τα διαδοχικά βήματα που ακολούθησε για να καταλήξει στο συγκεκριμένο συμπέρασμα, σε αντίθεση με τον

άνθρωπο που πολλές φορές δεν μπορεί να αναπαράγει τα διαδοχικά βήματα που ακολούθησε για να φτάσει σε κάποιο συμπέρασμα.

- Ο άνθρωπος έχει τη δυνατότητα να αποκτά και να δημιουργεί γνώση, ενώ αντιθέτως η γνώση στα συστήματα Τ.Ν. έχει αυστηρώς καθορισμένη δομή, η οποία είναι δύσκολο να μετατραπεί.
- Η ανθρώπινη λογική μπορεί να χρησιμοποιεί ένα πολύ ευρύτερο πεδίο γνώσης από αυτό του συγκεκριμένου θέματος απόφασης. Η Τ.Ν. αντιθέτως είναι επικεντρωμένη μόνο σε εξειδικευμένα θέματα, διαθέτοντας γνώση μόνο για την επίλυση συγκεκριμένων προβλημάτων.

Από τα παραπάνω θα μπορούσε να διακρίνει κανείς την δυναμική της εφαρμογής της Τ.Ν. στο τομέα της ασφάλειας. Ένας διαχειριστής ενός δικτύου πληροφοριακών συστημάτων, καλείται να ανταπεξέλθει σε ένα απολύτως δυναμικό περιβάλλον, ασαφές και εχθρικό. Σύμφωνα με το [www.euro2day.gr/specials/topics/article/1533763/aytoi-einai-oi-megalyteroi-kindynoi-gia-epixeirhseis.html], το έγκλημα στον κυβερνοχώρο, έχει πλέον ενταχθεί στον μακρύ κατάλογο παραδοσιακών αιτιών, που μπορούν να προκαλέσουν την δαπανηρή διακοπή των εργασιών ενός οργανισμού ή εταιρείας, ενώ στο [http://www.consilium.europa.eu/el/policies/cyber-security/] αναφέρεται πως μια από τις πέντε κατευθύνσεις της στρατηγικής της Ευρωπαϊκής Ένωσης για την αντιμετώπιση των προκλήσεων στον κυβερνοχώρο, αποτελεί η ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο.

§3. Η μηχανική μάθηση (Machine Learning)

Ως μηχανική μάθηση θα μπορούσε να οριστεί ως το «φαινόμενο κατά το οποίο ένα σύστημα βελτιώνει την απόδοσή του κατά την εκτέλεση μιας συγκεκριμένης εργασίας , χωρίς να υπάρχει ανάγκη να προγραμματιστεί εκ νέου» [https://repository.kallipos.gr/bitstream/11419/3382/1/02_chapter_04.pdf]. Ο Βλαχάβας (Τεχνητή Νοημοσύνη, 2005), αναφέρει πως «μηχανική μάθηση ονομάζεται η

δημιουργία προτύπων από ένα σύνολο δεδομένων, μέσω ενός υπολογιστικού συστήματος» (et al Βλαχάβας, 2005), ενώ υπάρχουν δύο είδη μηχανικής μάθησης, όπως η μάθηση με επίβλεψη ή μάθηση με παραδείγματα (Supervised Machine Learning), ή μάθηση χωρίς επίβλεψη (Unsupervised Learning).

Η μάθηση με επίβλεψη είναι αυτή κατά την οποία, η διαδικασία της δημιουργίας και της αύξησης του πεδίου της βάσης της γνώσης, κατευθύνεται από κάποιους κανόνες και αλγορίθμους. Στην περίπτωση αυτή κατατάσσονται τα προβλήματα ταξινόμησης και παρεμβολής (regression), που αφορά στη δημιουργία μοντέλων πρόβλεψης αριθμητικών τιμών. Τεχνικές μηχανικής μάθησης με επίβλεψη αποτελούν τα δέντρα απόφασης, η μάθηση εννοιών, η μάθηση κανόνων, η μάθηση με πρότυπα Bayes, ορισμένα νευρωνικά δίκτυα και οι μηχανές υποστηρικτικού διανύσματος.

Αντίθετα στη μάθηση χωρίς επίβλεψη, δεν υπάρχουν κανόνες που να ορίζουν τα πλαίσια μέσα στα οποία θα κινείται η νέα προκύπτουσα γνώση.

Στο [Συστήματα Υποστήριξης Αποφάσεων, Ν. Ματσατσίνης, 2010], αναφέρεται ότι τα έμπειρα συστήματα δημιουργήθηκαν για να υποστηρίξουν ή και να αντικαταστήσουν τους εμπειρογνώμονες σε ειδικές περιπτώσεις. Σε γενικές γραμμές και από πραγματικά παραδείγματα, έχει αποδειχθεί ότι σε πολλές περιπτώσεις τα έμπειρα συστήματα αποδίδουν καλύτερα από τους ανθρώπους (Yu et al., 1979, Expert Systems), και ως εκ τούτου μπορούν να αποτελέσουν χρήσιμα εργαλεία στον τομέα της λήψης απόφασης.

§4. Η εξόρυξη γνώσης από δεδομένα (Data Mining)

Ο στόχος της εξόρυξης γνώσης από δεδομένα είναι να δώσει νόημα σε μεγάλους όγκους δεδομένων από κυρίως χωρίς επίβλεψη δεδομένα σε κάποιο πεδίο (Larose, 2006, Cios et al. 2007, Taniar, 2008). Η εξόρυξη γνώσης ξεκίνησε και αναπτύχθηκε στην Αμερική, και σήμερα αποτελεί μια από τις πλέον αναπτυσσόμενες περιοχές της επιστήμης της πληροφορικής. Μερικοί από τους ορισμούς δίνονται στη συνέχεια:

Η εξόρυξη γνώσης ορίζεται ως η αναζήτηση, μέχρι πριν άγνωστων αλλά πολύτιμων, πληροφοριών από μεγάλες βάσεις δεδομένων [Singh, 1998]. Οι πληροφορίες αυτές χρησιμοποιούνται σε περιπτώσεις λήψης αποφάσεων.

Οι [Andriaans και Zantige, 1997], αναφέρουν ότι η εξόρυξη γνώσης ασχολείται με την ανακάλυψη κρυφής γνώσης, νέων κανόνων και απρόβλεπτων δομών και στοιχείων από τεράστιες βάσεις δεδομένων.

Ο [Fong, 1997] την αναφέρει ως την ανακάλυψη κρυφής γνώσης από μεγάλες βάσεις δεδομένων.

Εξόρυξη γνώσης είναι η έρευνα συσχετίσεων και χαρακτηριστικών που υπάρχουν σε μεγάλες βάσεις δεδομένων αλλά είναι κρυμμένες πίσω από τον μεγάλο όγκο τους. Αυτές οι συσχετίσεις αναπαριστούν πολύτιμη πληροφορία για τις οντότητες που αποθηκεύονται στη βάση δεδομένων [Holshemier and Siemes, 1994].

Η εξόρυξη γνώσης από δεδομένα είναι ένα ισχυρό εργαλείο της Τεχνητής Νοημοσύνης η οποία μπορεί να ανακαλύπτει χρήσιμη πληροφορία μέσα σε βάσεις δεδομένων οι οποίες μπορεί να χρησιμοποιηθούν για να βελτιώσουν τις αποφάσεις (http://www.aaai.org/html/mining.html).

Στο [Συστήματα Υποστήριξης Αποφάσεων, Ν. Ματσατσίνης, 2010], αναφέρεται ότι «η εξόρυξη γνώσης από δεδομένα είναι η διαδικασία της ανακάλυψης χρήσιμης πληροφορίες από μεγάλες βάσεις δεδομένων. Η εξόρυξη γνώσης χρησιμοποιεί τη μαθηματική ανάλυση για να αποκτήσει τα πρότυπα και να αποτυπώσει τις τάσεις που υπάρχουν στα δεδομένα. Θα πρέπει να σημειωθεί ότι αυτά τα πρότυπα δεν μπορούν να ανακαλυφθούν μέσω της παραδοσιακής εξερεύνησης δεδομένων είτε επειδή οι σχέσεις τους είναι πολύπλοκες είτε επειδή υπάρχουν πάρα πολλά δεδομένα».

Εξόρυξη γνώσης είναι η αυτοματοποιημένη εξαγωγή χρήσιμων πληροφοριών από μεγάλες βάσεις δεδομένων και οι αλγόριθμοί τους είναι αποτέλεσμα μακροχρόνιας έρευνας σε τομείς όπως η στατιστική, η ανάλυση δεδομένων και η τεχνητή νοημοσύνη. Με δεδομένη την ύπαρξη ικανοποιητικών σε μέγεθος και ποιότητα βάσεων δεδομένων, μπορούμε να

δημιουργήσουμε νέες πρακτικές σε τομείς όπως η αυτοματοποιημένη εύρεση πληροφοριών πρόγνωσης των τάσεων και των συμπεριφορών, εντοπισμός συγκεκριμένων τάσεων, εύρεση σχέσεων ανάμεσα σε συγκεκριμένες δομές.

§5. Η διαδικασία ανακάλυψης γνώσης

Γενικά, η εξόρυξη γνώσης αποτελεί μια επαναληπτική διαδικασία, η οποία δύναται περιλαμβάνει τα ακόλουθα στάδια, χωρίς αυτά να αποτελούν αυστηρό κανόνα ως προς την εφαρμογή τους:

- Καθορισμός του προβλήματος, όπου καθορίζεται συγκεκριμένα ο σκοπός της όλης διαδικασίας. Στο στάδιο αυτό, ειδικοί στην μηχανική μάθηση σε συνεργασία με τους ειδικούς στον εκάστοτε τομέα που εξετάζεται (business experts, domain experts), προσπαθούν να καθορίσουν το αποτέλεσμα της διαδικασίας ώστε να αποκτήσει την επιθυμητή αξία από πλευράς επιχειρησιακής αξιοποίησης (business perspective).

- Επιλογή δεδομένων και κατανόηση αυτών, όπου γίνεται η επιλογή των απολύτως απαραίτητων δεδομένων και γίνεται μια ποιοτική ανάλυση και επιβεβαίωση της ποιότητας αυτών, ενώ μπορεί να χρησιμοποιηθούν και στατιστικά εργαλεία για μια πρώτη αξιολόγησή τους.

- Στο στάδιο της προετοιμασίας των δεδομένων, γίνεται η επιλογή (selecting), ο καθαρισμός (cleaning) και η κωδικοποίηση (formatting) των δεδομένων, χωρίς όμως να επέρχεται κάποια αλλαγή στο νόημα αυτών, με τελικό σκοπό την προετοιμασία τους για την δημιουργία του μοντέλου.

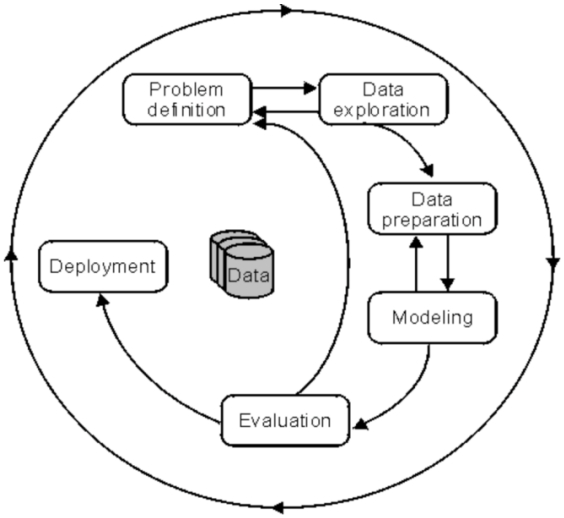
- Στο στάδιο της μοντελοποίησης επιλέγονται και εφαρμόζονται διάφορες μέθοδοι εξόρυξης γνώσης και αξιολογείται το μοντέλο που χρησιμοποιείται, ενώ μπορεί να επαναληφθεί αρκετές φορές με σκοπό την αλλαγή ορισμένων παραμέτρων του μοντέλου έως ότου επιτευχθούν οι βέλτιστες τιμές.

- Στο στάδιο της αξιολόγησης, γίνεται η αξιολόγηση των αποτελεσμάτων του μοντέλου, και εάν αυτό δεν ανταποκρίνεται στις προσδοκίες, τότε επανεξετάζεται η διαδικασία της

σχεδίασης μέχρι να επιτευχθούν τα βέλτιστα αποτελέσματα, ενώ μπορεί να γίνει και μια αξιολόγηση μέσω της απάντησης στις παρακάτω ερωτήσεις:

- Εάν πετυχαίνει το μοντέλο το στόχο της επιχείρησης (business objective)
- Εάν όλοι οι παράμετροι έχουν ληφθεί υπόψη.

- Το τελευταίο στάδιο στην ανάπτυξη του μοντέλου, όπου τα αποτελέσματα μπορούν εξαχθούν σε διάφορα εργαλεία οπτικοποίησης, όπως βάσεις δεδομένων, εφαρμογές ή φύλλα εργασίας.



Εικόνα 4. Το μοντέλο CRISP-DM (Cross-Industry Standard Process for Data Mining)[https://www.ibm.com/support/knowledgecenter/en/SSEPGG_9.5.0/com.ibm.im.easy.doc/c_dm_process.html]

Μια ταξινόμηση των διαφόρων μεθόδων εξόρυξης γνώσης είναι η παρακάτω:

- Κατηγοριοποίηση δεδομένων (classification) – Μάθηση με επίβλεψη (Supervised Learning)
  - Μέθοδοι κατηγοριοποίησης
    - Δέντρα Απόφασης (decision trees)
    - Κανόνες (Rule – based Methods)
    - Μηχανές Διανυσμάτων Υποστήριξης (Support Vector Machines)
    - Bayes μέθοδοι κατηγοριοποίησης

- Νευρωνικά Δίκτυα
- Αλγόριθμοι Κοντινότερου Γείτονα
- Γενετικοί Αλγόριθμοι
- Προσέγγιση Rough Sets
- Προσέγγιση Ασαφούς Λογικής

- Συσταδοποίηση (clustering) – Μάθηση χωρίς επίβλεψη (Unsupervised Learning)
  - Μέθοδοι διαμερισμού
    - k – means
    - k – methods
  - Ιεραρχικές μέθοδοι (hierarchical methods)
  - Μέθοδοι βασιζόμενοι στην πυκνότητα (density – based methods)
  - Μέθοδοι βασιζόμενοι σε πλέγματα (grid – based methods)
  - Ανίχνευση Ανωμαλιών (Anomaly detection)
  - Νευρωνικά Δίκτυα

§6. Κοινά πεδία δράσης και χαρακτηριστικά μεταξύ της Μηχανικής Μάθησης και της Κυβερνοάμυνας και μελλοντικές προοπτικές

Μέχρι τώρα έχει γίνει μια εισαγωγή στη χρήση του πρωτοκόλλου Http, της κυβερνοάμυνας σαν έννοια γενικότερα και τους σκοπούς αυτής, και στους τομείς της τεχνητής νοημοσύνης και της μηχανικής μάθησης. Αξίζει να αναφερθούμε στα σημεία εκείνα τα οποία ως ορισμοί ή απλές αναφορές συναντώνται από κοινού στους παραπάνω τομείς, με σκοπό να αναγνωριστεί η αξία της επιλογής του συνδυασμού των πεδίων αυτών και της δυναμικής των αποτελεσμάτων που μπορεί αυτό να έχει.

Ο μεγάλος ρυθμός δημιουργίας δεδομένων τα τελευταία χρόνια, έχει δημιουργήσει ένα νέο ορισμό για την περιγραφή τους, τα «big data». Αυτά τα δεδομένα αποτέλεσαν έναν από

τους κύριους πυλώνες ανάπτυξης της μηχανικής μάθησης, σε συνδυασμό με την ολοένα και μεγαλύτερη δυνατότητα επεξεργασίας αυτών, λόγω της ανάπτυξης και της μείωσης του κόστους της υπολογιστικής ισχύος. Στον τομέα της κυβερνοάμυνας, η συλλογή και αποθήκευση μεγάλων όγκων δεδομένων, τα οποία φιλτράρονται και αξιολογούνται, είναι μια συνήθης και επιβαλλόμενη πρακτική. Ένας διαχειριστής ενός δικτύου ή ο υπεύθυνος ασφαλείας του συστήματος, έρχεται αντιμέτωπος καθημερινά με την εξέταση μεγάλων όγκων δεδομένων, υποβοηθούμενος από διάφορα εργαλεία που έχουν αναπτυχθεί για την απλούστευση της παρουσίασης της πληροφορίας προς αυτόν.

Είναι κοινά παραδεκτό ότι η διασφάλιση ενός ψηφιακού περιβάλλοντος από κακόβουλες ενέργειες αποτελεί ένα επίπονο και απαιτητικό έργο. Με τις ολοένα αυξανόμενες ανησυχίες αναφορικά με την ασφάλεια που παρέχεται στο cloud, του Internet of Things (IoT), και άλλων αναπτυσσόμενων τεχνολογιών και την ολοένα και μεγαλύτερη εφευρετικότητα από την πλευρά των κακόβουλων πλευρών, η εύρεση νέων μεθόδων και εργαλείων που θα συμβάλλουν στο αποτελεσματικότερο περιορισμό των απειλών, θα συνεχίσει να αποτελεί έναν από τους πρωταρχικούς στόχους για τον τομέα της ασφάλειας. Οι εμπειρογνώμονες συναντούν δυσκολίες στο να αποτυπώσουν την γνώση τους μέσα σε ένα ασαφές ως προς τον προσδιορισμό του περιβάλλοντος του κυβερνοχώρου και της ασφάλειάς του. Οι αποφάσεις ενός διαχειριστή, συχνά λαμβάνονται υπό αβεβαιότητα (uncertainty), δηλαδή έλλειψη ακριβούς πληροφορίας, με τις κυριότερες πηγές να είναι οι παρακάτω :

- Ανακριβή δεδομένα (imprecise data)
- Ελλιπή δεδομένα (incomplete data)
- Υποκειμενικότητα ή/και ελλείψεις στην περιγραφή της γνώσης
- Κάθε είδους περιορισμοί που κάνουν το όλο πλαίσιο λήψης απόφασης ατελές.

Έτσι λοιπόν, ο χειρισμός της ασάφειας και η ίδια η ασάφεια ως έννοια, αλλά και η εξαγωγή πολύτιμης γνώσης, αποτελεί ένα κοινό πεδίο δράσης των δύο τομέων, με την ασαφή

λογική να παρέχει μια διαφορετική προσέγγιση σε προβλήματα ελέγχου και ταξινόμησης, αποβαίνοντας χρήσιμη στις παρακάτω περιπτώσεις που:

- δεν υπάρχει μαθηματικό μοντέλο του προβλήματος, όπως αυτό της κυβερνοάμυνας
- εμπλέκονται υψηλά μη γραμμικές διαδικασίες
- υπάρχει διαθέσιμη εμπειρική γνώση λειτουργίας του περιβάλλοντος

Αυτή τη στιγμή, πολλές πρακτικές μηχανικής μάθησης εφαρμόζονται στο τομέα της κυβερνοάμυνας [http://www.cybersecurity-review.com/industry-perspective/applying-machine-learning-to-advance-cyber-security-analytics], περισσότερο ως ένα εργαλείο προειδοποίησης ενός διαχειριστή, ο οποίος θα λάβει και την τελική απόφαση για την αντιμετώπιση ενός γεγονότος ή μη. Οι μελλοντικές προοπτικές φανερώνουν μια δυναμική εισαγωγή παρόμοιων μεθόδων στον τομέα, χωρίς όμως ακόμα να γίνεται φανερή η πλήρης αντικατάσταση των διαχειριστών ασφαλείας. Οι μεγάλες ποσότητες δεδομένων που παράγονται, σε συνδυασμό με τα προβλήματα που παρουσιάζονται σε περιπτώσεις ανάλυσης μεγάλης κλίμακας δεδομένων, προσφέρουν μια μεγάλη δυναμική χρήσης τεχνικών μηχανικής μάθησης, καθώς η ικανότητα ανίχνευσης και διαχείρισης ενός περιστατικού ασφαλείας αποτελεί πρωταρχική διαδικασία για τον τομέα της ασφάλειας.

ΚΕΦΑΛΑΙΟ 4

Υφιστάμενη κατάσταση

§1. Εισαγωγή

Στο κεφάλαιο αυτό θα επιχειρήσουμε να αναπτύξουμε τις έως τώρα ερευνητικές προσπάθειες που έχουν γίνει και αφορούν την μηχανική μάθηση (machine learning) και την εξόρυξη γνώσης (data mining) από δεδομένα που αφορούν την κυβερνοάμυνα και σκοπεύουν στην ανακάλυψη πρωτοεμφανιζόμενων και μη επιθέσεων και τον βαθμό ικανότητάς τους να το επιτύχουν. Στην προσπάθεια αυτή θα γίνουν αναφορές στην πολυπλοκότητα της χρήσης

αλγορίθμων που αφορούν αυτό το σκοπό, τα σύνολο των δεδομένων που χρησιμοποιήθηκαν (data sets), και τις προοπτικές και προκλήσεις που έχουν αναγνωριστεί.

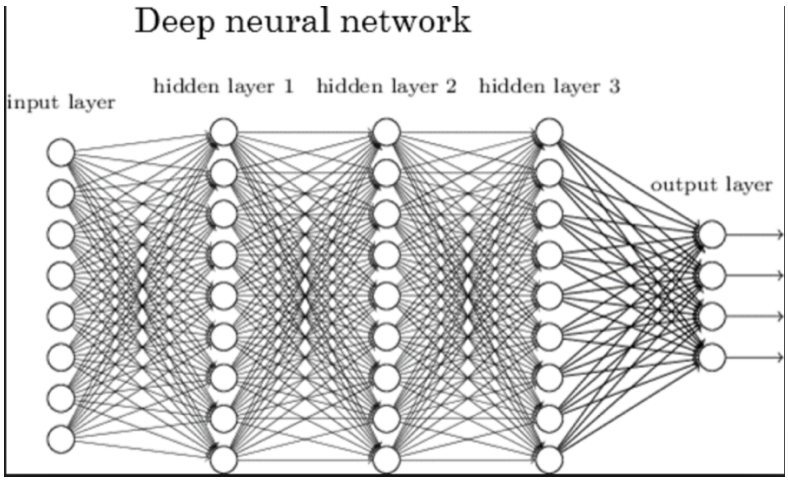
Η κυβερνοάμυνα σαν χώρος είναι ιδιαίτερα δυναμικός και πολυδιάστατος και για αυτό το λόγο πολλές από τις βιβλιογραφικές αναφορές που σχετίζονται με τις τεχνικές που εξετάζει και η παρούσα διατριβή, επικεντρώνονται σε συγκεκριμένους τομείς, όπως για παράδειγμα στην ανίχνευση επιθέσεων σε ασύρματα δίκτυα, ανίχνευση επιθέσεων προερχόμενες από το εσωτερικό ενός δικτύου ή από το εξωτερικό και άλλα. Για παράδειγμα στο άρθρο των Nguyen, Nguyen and Armitage (2008), περιγράφονται τεχνικές για την κατηγοριοποίηση της διαδικτυακής κίνησης, λαμβάνοντας υπόψη όμως μόνο ένα συγκεκριμένο πρωτόκολλο αυτό του IP (Internet Protocol) και βασίζεται σε στατιστική ανάλυση της κίνησης των πακέτων. Μια άλλη προσέγγιση στο θέμα γίνεται στο [Anomaly based network intrusion detection: Techniques, systems and challenges, P.Garci-Teodoro, J.Diaz-Verdejo, 2009], όπου εξετάζεται η ανίχνευση επιθέσεων μέσω ανωμαλιών που παρατηρούνται σε ένα δίκτυο (anomaly based network intrusion), ενώ υπάρχει και η τεχνική της σύγκρισης των υπογραφών των κινήσεων των πακέτων (signature based anomaly detection).

Μεγάλες διαφοροποιήσεις στη βιβλιογραφία, αφορούν επίσης στην επιλογή των διαφόρων αλγορίθμων μηχανικής μάθησης και εξόρυξης δεδομένων που χρησιμοποιούνται. Έτσι, παρατηρείται ανά περίπτωση η εξέταση του προβλήματος με τη χρήση υπολογιστικών μεθόδων όπως Τεχνητών Νευρωνικών Δικτύων (Artificial Neural Networks), Ασαφή Συστήματα (Fuzzy Systems), εξελεκτικούς αλγόριθμους (Evolutionary Algorithms), Artificial Immune Systems, Swarm Intelligence αλλά και μεθόδων ομαδοποίησης (clustering) και δέντρων αποφάσεων (decision trees). Τέλος, διαφοροποιήσεις μπορεί να παρατηρούνται σε ότι έχει να κάνει με το περιβάλλον που αυτές εφαρμόζονται, δηλαδή αν εξετάζεται ένα δικτυακό περιβάλλον ενσύρματο, ή ένα ασύρματο κλπ.

§2. Τα Τεχνητά Νευρωνικά Δίκτυα

Τα τεχνητά νευρωνικά δίκτυα έχουν εμπνευστεί από τη δομή του ανθρώπινου εγκέφαλου και αποτελούνται από πολλούς αλληλοσυνδεδεμένους νευρώνες, όπου ο καθένας αναλαμβάνει μια συγκεκριμένη υπολογιστική πράξη. Τα TNN, χρησιμοποιούνται ως εργαλείο για κατηγοριοποίηση δεδομένων (classification) και υπήρξαν πολύ διαδεδομένα έως το 1990, οπότε και ανακαλύφθηκαν οι μηχανές υποστηρικτικού διανύσματος (support vector machines) [Λάζαρος Σ. Ηλιάδης (Ευφυή Πληροφοριακά Συστήματα και Εφαρμογές στην Εκτίμηση Κινδύνου)]. Τα TNN συχνά απαιτούν μεγάλους χρόνους εκπαίδευσης όσο αυξάνονται τα εισαγόμενα στοιχεία και υποφέρουν από τοπικά ελάχιστα, ενώ με τη χρήση ανάστροφης οπισθοδρόμησης (back propagation) μπορούν να μοντελοποιήσουν τις λογικές EX-OR. Τα TNN με τις βελτιώσεις που πραγματοποιούνται (recurrent, feed-forward, convolutional ANNs), κερδίζουν ξανά σε δημοτικότητα και χρησιμοποιούνται ευρέως σε προβλήματα κατηγοριοποίησης και αναγνώρισης προτύπων (pattern recognition) [N. Ματσατσίνης, 'Συστήματα Υποστήριξης Αποφάσεων', 2010, Εκδόσεις Νέων Τεχνολογιών].

Στο [Artificial neural networks for misuse detection, J.Cannady, 1998] ο Cannady χρησιμοποίησε TNN ως ένα κατηγοριοποιητή (classifier) για την ανίχνευση μή ορθής χρήσης ενός συστήματος (misuse detection), χρησιμοποιώντας δεδομένα από την παρακολούθηση ενός δικτύου το οποίο δεχόταν προσομοιωμένες δικτυακές επιθέσεις.



Εικόνα 5 Η δομή ενός Τεχνητού Νευρωνικού Δικτύου (www.quora.com)

Στο [Improving intrusion detection performance using keyword selection and neural networks, Lipmann και Cunningham, 2000], στα πλαίσια της ανίχνευσης ανωμαλίας και της υβριδικής ανίχνευσης (anomaly detection and hybrid detection), οι Lipmann και Cunningham πρότειναν ένα σύστημα το οποίο χρησιμοποιεί στατιστικές επιλογές συγκεκριμένων λέξεων από συνδέσεις telnet, οι οποίες και εισάγονται σε ένα TNN για τον υπολογισμό της πιθανότητας μιας επίθεσης. Ένα δεύτερο TNN χρησιμοποιήθηκε για την κατηγοριοποίηση των περιπτώσεων που σηματοδοτήθηκαν ως επιθέσεις, ενώ η ακρίβεια αναφέρθηκε στο 80%.

Ο Bivens στο [Network based intrusion detection using neural networks, 2002], περιγράφει ένα Intrusion Detection System, που εφαρμόζει ένα στάδιο προ-επεξεργασίας, ομαδοποίησης, κανονικοποίησης και εκπαίδευσης ενός TNN και απόφασης ενός δεύτερου. Στο πρώτο στάδιο χρησιμοποιήθηκε ένα Self-Organizing Map (SOM), ένας τύπος TNN χωρίς επίβλεψη, για την εκμάθηση των προτύπων της κανονικής δικτυακής κίνησης, όπως οι συχνά χρησιμοποιούμενες πόρτες του TCP-IP και στο δεύτερο στάδιο ένα δεύτερο TNN για τις προβλέψεις.

§3. Κανόνες Συσχέτισης και Ασαφείς Κανόνες Συσχέτισης

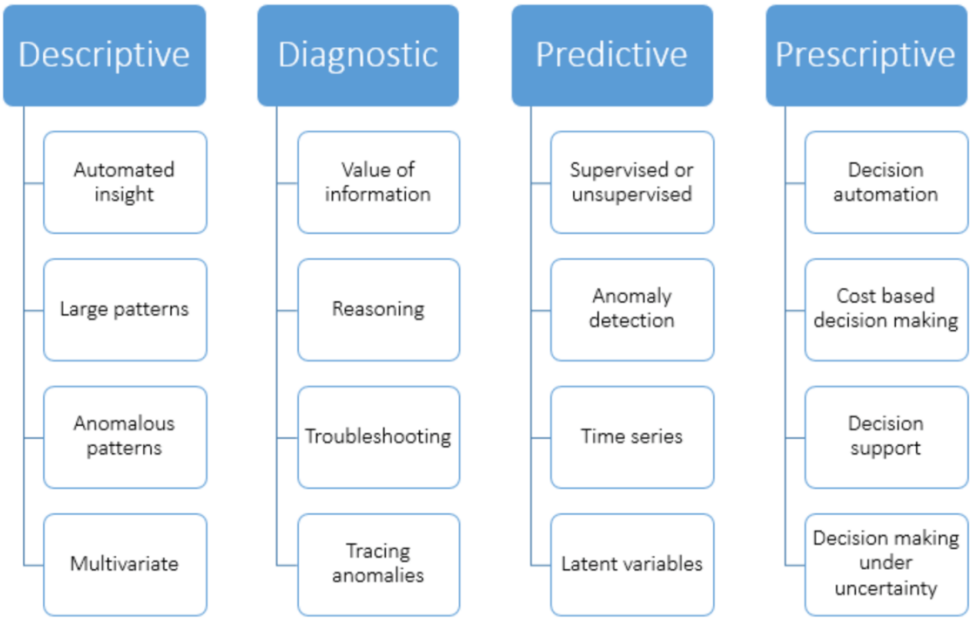
Ο στόχος των κανόνων συσχέτισης είναι η ανακάλυψη νέων κανόνων από ένα σύνολο δεδομένων που προηγουμένως δεν είχαν αναγνωριστεί. Ένας τέτοιος κανόνας περιγράφει τη σχέση μεταξύ διαφορετικών στοιχείων από μια βάση δεδομένων όπως για παράδειγμα : εάν (Α και Β), τότε Γ. Ο παραπάνω κανόνας περιγράφει τη σχέση όπου εάν τα Α και Β είναι παρόντα, τότε είναι και η τιμή του Γ. Οι κανόνες συσχέτισης παρουσιάστηκαν από τον Agrawal et.al. [Mining association rules between sets of items in large databases, 1993], σαν ένας τρόπο να περιγράψει ταυτόχρονα περιστατικά, σε δεδομένα που προέρχονταν από super market. Στη παραπάνω λογική υπάρχει ένας περιορισμός που αφορά τον δυαδικό χαρακτήρα

των δεδομένων όπου έρχεται σε αντίθεση με δεδομένα τα οποία μπορεί να είναι κατηγορικά ή και ποσοτικά. Μια επέκταση του παραπάνω κανόνα που αφορά και τις τελευταίες κατηγορίες δεδομένων, είναι οι ασαφείς κανόνες συσχέτισης που έχουν την μορφή: ΕΑΝ (Χ είναι Α)→ (Υ είναι Β), όπου τα Χ και Υ είναι μεταβλητές και τα Α και Β είναι ασαφείς κανόνες συσχέτισης που χαρακτηρίζουν τα Χ και Υ. Μια αναλυτικότερη περιγραφή τους, γίνεται στο [Fuzzy Sets, Zadeh, 1965].

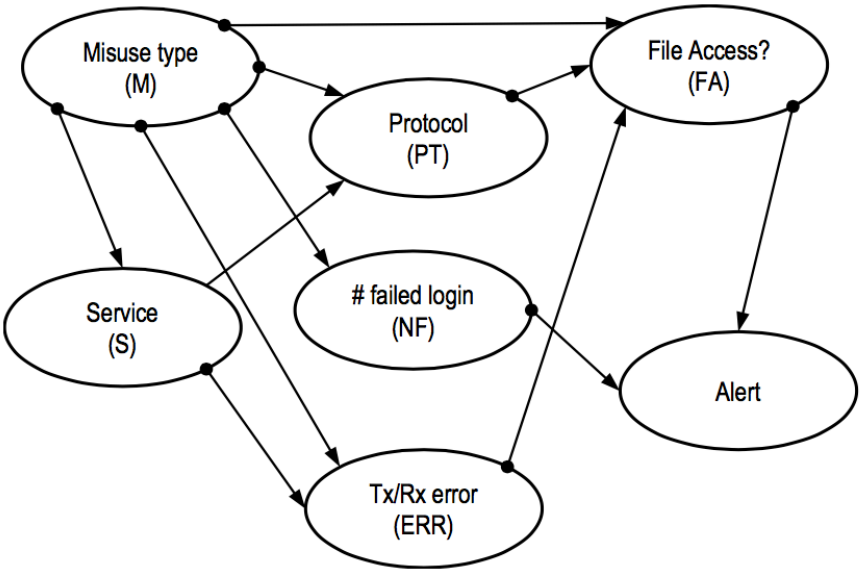
Με βάσει τους κανόνες συσχέτισης, και στην κατεύθυνση του misuse detection, κινήθηκε ο Brahmi [OMC-IDS: at the cross-roads of OLAP mining and intrusion detection, 2012], ο οποίος χρησιμοποίησε το σύνολο δεδομένων του DAPRA 1998 και προσπάθησε να αναγνωρίσει συσχετίσεις που μπορεί να υπήρχαν μεταξύ παραμέτρων που αφορούσαν το TCP-IP πρωτόκολλο και διαφόρων τύπων επιθέσεων, χρησιμοποιώντας πολυδιάστατους κανόνες συσχετίσεων. Ένα από τα πλεονεκτήματα αυτής της τεχνικής είναι ότι οι κανόνες που τυχόν ανακαλύπτονται, περιγράφουν τις συσχετίσεις που υπάρχουν ξεκάθαρα και για αυτό και είναι μια υποσχόμενη κατηγορία για την δημιουργία υπογραφών επιθέσεων (attack signatures).

§4. Τα Bayesian δίκτυα

Ένα δίκτυο Bayesian είναι ένα πιθανολογικό γραφικό μοντέλο που παρουσιάζει τις μεταβλητές και τις σχέσεις μεταξύ τους. Μπορούν να χρησιμοποιηθούν σε ένα μεγάλο εύρος περιπτώσεων όπως για πρόβλεψη, ανίχνευση ανωμαλίας, διαγνωστικούς σκοπούς, λήψη αποφάσεων υπό αβεβαιότητα κλπ. Στην εικόνα, δίδονται οι δυνατότητες που προσφέρονται υπό τις τέσσερις μεγάλες κατηγορίες αναλύσεων (analytics).



Εικόνα 6. Οι δυνατότητες των Bayesian δικτύων σε επίπεδο analytics (https://www.bayesserver.com)



Εικόνα 6. Παράδειγμα Bayesian δικτύου για ανίχνευση υπογραφής (Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection')

Το δίκτυο αποτελείται από κόμβους που μπορεί να παίρνουν διακριτές και συνεχείς τιμές, και από κατευθυνόμενες σχέσεις μεταξύ των κόμβων που καταδεικνύουν την μεταξύ του ή όχι, εξάρτηση. Ανάλογα με την περίπτωση, το δίκτυο μπορεί να χρησιμοποιηθεί για να

εξηγήσει την αλληλοσύνδεση που μπορεί να υπάρχει μεταξύ των κόμβων και ενός δεδομένου αποτελέσματος, ή και να υπολογίσει την πιθανότητα ενός αποτελέσματος, δεδομένων των τιμών στους κόμβους.

Στην κατεύθυνση του misuse detection ο Λιβαδάς στο [Using machine learning techniques to identify botnet traffic, 2006], προσπάθησε να διαχωρίσει την διαδικτυακή κίνηση που προερχόταν από botnets και της κίνησης που προερχόταν από πακέτα του Internet Relay Chat (IRC) και έτσι να διαπιστώσει την ύπαρξη ή όχι ενός botnet στο δίκτυο. Η μελέτη χρησιμοποίησε δεδομένα τα οποία προήλθαν από το ασύρματο δίκτυο 18 περιοχών του πανεπιστημίου του Dartmouth, περιόδου 4 μηνών και αφορούσαν στο επίπεδο του TCP-IP πρωτοκόλλου, ύστερα από κατάλληλη επεξεργασία και χρήση προσομοίωσης. Η επίδοση του Bayesian δικτύου αναφέρεται σε ποσοστό 93% ακρίβειας, με ένα ποσοστό False Positive (FP) της τάξεως του 1.39%.

Στην κατεύθυνση της ανίχνευσης ανωμαλίας και της υβριδικής ανίχνευσης (anomaly detection and hybrid detection), ο Kruegel et.al. [Bayesian event classification for intrusion detection, 2003], χρησιμοποίησε ένα δίκτυο Bayesian για να κατηγοριοποιήσει τα γεγονότα που συμβαίνουν όταν ένα λειτουργικό σύστημα καλεί τον πυρήνα (kernel) του συστήματος, όταν δέχεται ροές πακέτων TCP-IP. Ο Kruegel χρησιμοποίησε το σύνολο των δεδομένων του DARPA 1999 για να μελετήσει την παραπάνω διαδικασία, και εξάγοντας συγκεκριμένα χαρακτηριστικά από τις ροές των δεδομένων όπως το συντακτικό στις εντολές (command syntax) και σημεία (tokens) στις παραμέτρους των κλήσεων του συστήματος, τροφοδότησε ένα δίκτυο Bayesian για να υπολογίσει την πιθανότητα της κανονικής ή μη κίνησης. Για τον καθορισμό πολύπλοκων επιθέσεων απαιτείται να υπάρξει μια συσχέτιση μεταξύ των παρατηρούμενων ανωμαλιών και για τον σκοπό αυτό μελετήθηκε η συσχέτιση μεταξύ των καταστάσεων συναγερμού, χρησιμοποιώντας μεθόδους ομαδοποίησης (clustering).

§5. Η ομαδοποίηση (clustering)

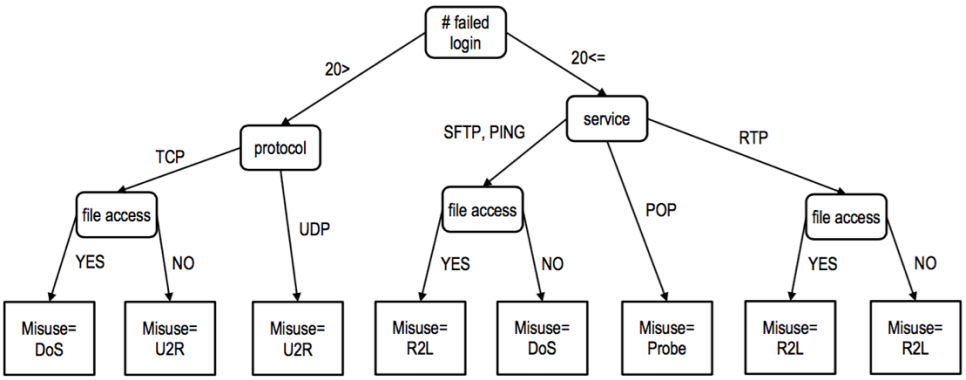
Η ομαδοποίηση [Algorithms for Clustering Data, K. Jain and R. C. Dubes, 1998] είναι ένα σύνολο τεχνικών για την αναγνώριση προτύπων από ένα σύνολο πολυδιάστατων μη προσδιορισμένων δεδομένων (unlabeled data). Τα δεδομένα κατηγοριοποιούνται χωρίς επίβλεψη (unsupervised learning), με βάση κάποιο χαρακτηριστικό ομοιότητας. Το κύριο πλεονέκτημα αυτής της τεχνικής αναφορικά με την ανίχνευση επιθέσεων, είναι ότι είναι μέσω αυτής εξάγεται γνώση χωρίς την παρέμβαση κάποιου ειδικού που θα χρειάζεται να περιγράψει και να καθορίσει λεπτομέρειες αναφορικά με τις κλάσεις των επιθέσεων. Υπάρχουν διάφορες προσεγγίσεις ομαδοποίησης δεδομένων που έχουν προταθεί ο καθένας με την δική του φιλοσοφία, όπως για παράδειγμα ο K- means, οι ιεραρχικοί αλγόριθμοι συσταδοποίησης, οι αλγόριθμοι ανταγωνιστικής μάθησης και άλλοι.

Στη βιβλιογραφία υπάρχουν αναφορές όπως στο [Intrusion signature creation via clustering anomalies, M. Blowers and J. Williams, 2014], [Machine Learning Applied to Cyber Operations, M. Blowers and J. Williams, 2014], [ADMIT: anomaly-based data mining for intrusions, K. Sequeira and M. Zaki, 2002], όπου ο καθένας από τους εκδότες χρησιμοποιώντας διαφορετικές τακτικές και σύνολα δεδομένων, αναφέρουν μεγάλα ποσοστά σωστής ανίχνευσης επιθέσεων.

§6. Τα δέντρα αποφάσεων (decision trees)

Τα δέντρα αποφάσεων είναι μια δομή για καθοδηγούμενη μάθηση με μια αναπαράσταση ανάλογη με αυτή ενός δέντρου αποτελώντας έναν ειδικό τύπο μοντέλου ταξινόμησης. Το δέντρο απόφασης είναι ένα γράφος με την κλασσική δεντρική δομή (Νανόπουλος και Μανωλόπουλος, 2008) όπου διακρίνουμε έναν αρχικό κόμβο, εσωτερικούς κόμβους, και εξωτερικούς. Σε κάθε κόμβο εισέρχεται μια κατευθυνόμενη ακμή από κάποιον άλλο κόμβο, ενώ σε κάθε εσωτερικό κόμβο αντιστοιχεί ένα χαρακτηριστικό που χρησιμοποιείται για τον περαιτέρω διαχωρισμό του δέντρου. Στις ακμές που εξέρχονται από

κάθε εσωτερικό κόμβο, αντιστοιχούν συνθήκες ελέγχου με βάση το διαχωριστικό χαρακτηριστικό. Οι πιο γνωστές μέθοδοι για την δημιουργία δέντρων αποφάσεων είναι με την χρησιμοποίηση των αλγορίθμων ID3 [Induction of decision trees, R. Quinlan, 1986] και C4.5 [C4.5: Programs for Machine Learning, Quinlan, 1993]. Τα πλεονεκτήματα των δέντρων αποφάσεων είναι ότι μπορούν να εκφράσουν μια ευκολονόητη αναπαράσταση γνώσης, υψηλά ποσοστά ακρίβειας και απλότητα στην υλοποίησή τους. Μεγάλα δέντρα αποφάσεων παρουσιάζουν συνήθως υψηλά ποσοστά ακρίβειας, χωρίς όμως να μπορούν να γενικεύσουν, ενώ τα μικρά δέντρα αποφάσεων μπορούν να αναπαριστούν με απλό τρόπο την γνώση και είναι απλούστεροι σε σύγκριση με τους αλγόριθμους που χρησιμοποιούνται σε μηχανές υποστηρικτικού διανύσματος (support vector machines).



Εικόνα 7. Παράδειγμα δέντρου απόφασης (Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection')

Οι Kruegel και Toth στο [Using decision trees to improve signature- based intrusion detection, Kruegel and Toth, 2003], αντικατέστησαν την μηχανή ανίχνευσης κακής χρήσης (misuse detection engine) του δημοφιλούς εργαλείου για τον σκοπό αυτό, του Snort [Snort 2.0, Sourcefire, 2014], με δέντρα αποφάσεων. Αρχικά ομαδοποίησαν τους κανόνες που χρησιμοποιεί το Snort και έπειτα δημιούργησαν ένα δέντρο απόφασης με τον ID3 αλγόριθμο. Έτσι κατάφεραν να μειώσουν τον απαιτούμενο χρόνο σύγκρισης που χρειάζεται, βελτιώνοντας την απόδοση και καταδεικνύοντας πως ο συνδυασμός μεθόδων ομαδοποίησης με δέντρα

αποφάσεων μπορεί να οδηγήσει σε μείωση του απαιτούμενου χρόνου για ένα σύστημα ανίχνευσης κακής χρήσης.

§7. Οι μηχανές υποστηρικτικού διανύσματος (support vector machines)

Οι μηχανές υποστηρικτικού διανύσματος (ΜΥΔ) πραγματοποιούν μια κατηγοριοποίηση κατασκευάζοντας ένα υπερεπίπεδο ν διαστάσεων, το οποίο χωρίζει τα δεδομένα σε κατηγορίες. Οι μηχανές υποστηρικτικού διανύσματος με τα νευρωνικά δίκτυα ανήκουν στην κατηγορία μεθόδων της ήπιας υπολογιστικής και ανταποκρίνονται πολύ καλά ακόμα και αν έχουμε ένα σύνολο δεδομένων με πολλά χαρακτηριστικά αλλά με λίγες τιμές, κάτι το οποίο δεν καθίσταται εφικτό με τα νευρωνικά δίκτυα (Vapnik, 1998). Πρόκειται για κατηγοριοποιητή που βασίζεται στο να χωρίζει τα δεδομένα με ένα υπερεπίπεδο, με τέτοιο τρόπο ώστε η απόσταση μεταξύ των υπερεπιπέδων και του κοντινότερου σημείου της κάθε κλάσης να μεγιστοποιείται. Οι ΜΥΔ είναι γνωστές για την ικανότητά τους να γενικεύουν.
Προς την κατεύθυνση της ανακάλυψης μη ορθής χρήσης ενός συστήματος (misuse detection) με ΜΥΔ κινήθηκε ο Li et al. [An efficient intrusion detection system based on support vector machines and gradually feature removal method, Y. Li, 2012], όπου χρησιμοποιήθηκε ο πυρήνας Radial Basis Function (RBF) για να κατηγοριοποιήσει το σύνολο δεδομένων KDD 1999 σε προκαθορισμένες τιμές. Από τα συνολικά 41 χαρακτηριστικά του συνόλου των δεδομένων επιλέχθηκαν τελικά 19 εφαρμόζοντας μια αφαιρετική πολιτική. Επίσης ο Amiri et al. [Mutual information-based feature selection for IDSs, F. Amiri, 2011] χρησιμοποίησε τη μέθοδο των ελαχίστων τετραγώνων για να πετύχει μια γρηγορότερη εκπαίδευση στο σύνολο των δεδομένων, ενώ και αυτός προχώρησε στη μείωση των χαρακτηριστικών χρησιμοποιώντας τρεις αλγορίθμους επιλογής χαρακτηριστικών (feature selection algorithms).

§8. Σύνοψη – Μερικά Συμπεράσματα

Από την μέχρι τώρα σύνοψη, παρατηρούμε ότι υπάρχει πληθώρα προσεγγίσεων για το πρόβλημα στο οποίο επικεντρωνόμαστε. Η πληθώρα αυτή αφορά το είδος του μηχανισμού που μπορεί να χρησιμοποιηθεί για την επίλυσή του, αλλά και το τρόπο με τον οποίο αυτοί εφαρμόζονται, και συγκεκριμένα, αν αυτές εφαρμόζονται σε πραγματικό χρόνο ή όχι. Όπως αναφέρεται και στο (Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection'), το μεγαλύτερο ποσοστό της υπό μελέτη βιβλιογραφίας αφορούσε σε προσεγγίσεις σε μη πραγματικό χρόνο (offline). Τα δεδομένα είχαν περάσει από το στάδιο της επεξεργασίας και στη συνέχεια γίνονταν εισερχόμενα στο σύστημα. Στην περίπτωση όπου η επεξεργασία των δεδομένων θέλουμε να γίνεται σε πραγματικό χρόνο, τότε, θα πρέπει να ληφθούν υπόψη και επιπλέον παράμετροι, όπως είναι οι ροές των δεδομένων (streaming data), η μνήμη του συστήματος (buffering) και η προβολή των αποτελεσμάτων με χρονικές πληροφορίες. Γενικότερα, αναφέρεται ότι όταν είναι επιθυμητή η υλοποίηση ενός συστήματος σε πραγματικό χρόνο, θα πρέπει να λαμβάνονται υπόψη οι παράγοντες της πολυπλοκότητας του χρόνου (time complexity), της ικανότητας γενίκευσης (generalization capacity) και της δυνατότητας της ενημέρωσης (incremental update capability). Στον πίνακα 3, παρουσιάζεται η πολυπλοκότητα του χρόνου για διάφορες κατηγορίες αλγορίθμων.

Algorithm	Typical Time Complexity	Streaming Capable	Comments
ANN	O(emnk)	low	Jain et al. [107] e: number of epochs k: number of neurons
Association Rules	>> $O(n^3)$	low	Agrawal et al. [108]
Bayesian Network	>> O(mn)	high	Jensen [41]
Clustering, k-means	O(kmni)	high	Jain and Dubes [46] i: number of iterations until threshold is reached k: number of clusters
Clustering, hierarchical	$O(n^3)$	low	Jain and Dubes [46]
Clustering, DBSCAN	O(n log n)	high	Ester et al. [109]
Decision Trees	$O(mn^2)$	medium	Quinlan [54]
GA	O(gkmn)	medium	Oliveto et al. [110] g: number of generations k: population size
Naïve Bayes	O(mn)	high	Witten and Frank [89]
Nearest Neighbor k-NN	O(n log k)	high	Witten and Frank [89] k: number of neighbors
HMM	$O(nc^2)$	medium	Forney [111] c: number of states (categories)
Random Forest	O(Mmn log n)	medium	Witten and Frank [89] M: number of trees
Sequence Mining	>> $O(n^3)$	low	Agrawal and Srikant [92]
SVMs	$O(n^2)$	medium	Burges [112]

Πίνακας 3. Η πολυπλοκότητα αλγορίθμων σε σχέση με το χρόνο [A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, Anna Buczak]

Το ερευνητικό πεδίο της χρήσης αλγορίθμων εξόρυξης δεδομένων και μηχανικής μάθησης στο τομέα της κυβερνοάμυνας, παρουσιάζει μεγάλο ενδιαφέρον και ήδη υπάρχει αρκετή βιβλιογραφία που πραγματεύεται τις δυνατότητες χρήσης. Το ερώτημα όμως το οποίο κυριαρχεί, είναι ποιες από αυτές τις μεθόδους είναι η καταλληλότερη για εφαρμογή, κάτι το οποίο όμως, όπως διαφαίνεται και στο [A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, Anna Buczak], δεν είναι δυνατό να απαντηθεί στην παρούσα φάση.

Μεγάλες είναι και οι αποκλίσεις που παρουσιάζονται ως προς το σύνολο των δεδομένων που χρησιμοποιεί η κάθε μια μελέτη. Οι περισσότερες, χρησιμοποιούν το σύνολο των δεδομένων του DAPRA 1998, 1999, 2000 και KDD 1999 κατά περίπτωση, όμως όπως έχει ήδη αναφερθεί και στη παρούσα εργασία, υπήρξαν και μελέτες που χρησιμοποίησαν δεδομένα τα οποία προέρχονταν από άλλες πηγές και από διαφορετικά πρωτόκολλα όπως DNS και SSH. Χαρακτηριστικό είναι επίσης το γεγονός της δυσκολίας που υπάρχει στο να δημιουργηθεί ένα κατάλληλο σύνολο δεδομένων για μελέτη. Για το λόγο αυτό παρατηρείται η τάση, το ίδιο σύνολο δεδομένων να χρησιμοποιείται επαναληπτικά, κάτι το οποίο προσφέρει

όμως τη δυνατότητα της σύγκρισης της απόδοσης μεταξύ των διαφορετικών προσεγγίσεων στο πρόβλημα.

Η μηχανική μάθηση και η εξόρυξη δεδομένων έχει αποτελέσει εξαιρετικό εργαλείο για πολλές εφαρμογές. Στο τομέας της κυβερνοάμυνας, παραμένει μια δυσχέρεια απόλυτης εφαρμογής τους, λόγω του δυναμικού περιβάλλοντος και των ιδιαιτεροτήτων του, που αφορούν κυρίως το πόσο συχνά πρέπει να εκπαιδεύεται το μοντέλο αλλά και τη διαθεσιμότητα των δεδομένων. Στις περισσότερες των εφαρμογών, το μοντέλο εκπαιδεύεται και χρησιμοποιείται για ένα μεγάλο χρονικό διάστημα χωρίς αλλαγές. Στο περιβάλλον της κυβερνοάμυνας, τα μοντέλα θα πρέπει να εκπαιδεύονται καθημερινά και όποτε το κρίνει ο αναλυτής ή όποτε ένα νέο πρότυπο επίθεσης γίνεται γνωστό. Έτσι, το κριτήριο του απαιτούμενου χρόνου εκπαίδευσης, αποκτά ιδιαίτερη αξία. Σύμφωνα με την [Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection'], ένα ενδιαφέρον πεδίο έρευνας θα αποτελούσε η μελέτη των μεθόδων εκπαίδευσης με 'γρήγορη αυξητική μάθηση' (fast incremental learning), που θα χρησιμοποιείτο για καθημερινές ενημερώσεις του εκπαιδευμένου μοντέλου.

ML/DM Method	Paper	No. of Times Cited (as of 7/28/2015)	Cyber Approach	Data Used
ANN	Cannady [24]	463	misuse	Network packet-level data
ANN	Lippmann & Cunningham [27]	235	anomaly	DARPA 1998
ANN	Bivens et al. [28]	135	anomaly	DARPA 1999
Association rules	Brahmi et al. [32]	3	misuse	DARPA 1998
Association rules	Zhengbing et al. [33]	33	misuse	Attack signatures (10 to 0 MB)
Association rules	Apiletti et al. [35]	14	anomaly	NetFlow
Association rules – Fuzzy	Luo and Bridges [39]	192	anomaly	tcpdump
Association rules – Fuzzy	Tajbakhsh et al. [38]	124	hybrid	KDD 1999 (corrected)
Bayesian network	Livadas et al. [42]	208	misuse	tcpdump – botnet traffic
Bayesian network	Jemili et al. [43]	31	misuse	KDD 1999
Bayesian network	Kruegel et al. [44]	260	anomaly	DARPA 1999
Clustering – density based	Hendry and Yang [50]	6	misuse	KDD 1999
Clustering – density based	Blowers and Williams [51]	2	anomaly	KDD 1999
Clustering – sequence	Sequeira and Zaki [52]	214	anomaly	shell commands
Decision tree	Kruegel and Toth [55]	155	misuse	DARPA 1999
Decision tree	Bilge et al. [56]	187	anomaly	DNS data
Ensemble learning	Mukkamala et al. [65]	255	misuse	DARPA 1998
Ensemble – Random Forest	Gharibian and Ghorbani [63]	19	misuse	KDD 1999
Ensemble – Random Forest	Bilge et al.[66]	49	anomaly	NetFlow
Ensemble – Random Forest	Zhang et al. [62]	92	hybrid	KDD 1999
Evolutionary Comp - GA	Li [73]	235	misuse	DARPA 2000
Evolutionary Comp - GP	Abraham et al. [74]	83	misuse	DARPA 1998
Evolutionary Comp - GP	Hansen et al. [75]	52	misuse	KDD 1999 – subset
Evolutionary Comp - GA	Khan [76]	15	anomaly	KDD 1999
Evolutionary Comp - GP	Lu and Traore [78]	124	anomaly	DARPA 1999
HMM	Ariu et al. [82]	25	misuse	HTTP payload
HMM	Joshi and Phoha [83]	61	anomaly	KDD 1999
Inductive learning	Lee et al. [87]	1358	misuse	DARPA 1998
Inductive learning	Fan et al. [88]	195	anomaly	DARPA 1998
Naïve Bayes	Benferhat et al. [45]	17	anomaly	DARPA 2000
Naïve Bayes	Panda and Patra [90]	90	misuse	KDD 1999
Naïve Bayes	Amor et al. [91]	277	anomaly	KDD 1999
Sequence mining	Hu and Panda [93]	151	misuse	Database logs
Sequence mining	Li et al. [94]	18	anomaly	DARPA 2000
SVM	Li et al. [96]	56	misuse	KDD 1999
SVM	Amiri et al. [97]	84	misuse	KDD 1999
SVM – Robust	Hu et al. [98]	114	anomaly	DARPA 1998
SVM	Wagner et al. [99]	1	anomaly	NetFlow
One-class SVM and GA	Shon and Moon [101]	166	hybrid	DARPA 1999

Πίνακας 4. Μέθοδοι μηχανικής μάθησης και εξόρυξης γνώσης και σύνολα δεδομένων που χρησιμοποιήθηκαν στην υπάρχουσα βιβλιογραφία (Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection')

Τα κριτήρια σύγκρισης των μεθόδων μηχανικής μάθησης και εξόρυξης γνώσης από μεγάλα σύνολα δεδομένων, αφορούν στην ακρίβεια που έχουν, τον απαιτούμενο χρόνο εκπαίδευσης ενός μοντέλου, του χρόνου που απαιτείται για την κατηγοριοποίηση μιας πρωτοεμφανιζόμενης κατάστασης και την ευκολία κατανόησης της λύσης που παρουσιάζουν [Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection']. Η σύγκριση της ακρίβειας μεταξύ διαφόρων μεθόδων μηχανικής μάθησης, θα πρέπει να γίνεται λαμβάνοντας υπόψη τα ίδια δεδομένα εκπαίδευσης (training

data) και τα ίδια ακριβώς δεδομένα ελέγχου (test data). Σύμφωνα με την [Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection'], στην υπάρχουσα βιβλιογραφία, αν και οι μελέτες χρησιμοποιούσαν τα ίδια σύνολα δεδομένων, η μετέπειτα αναμεταξύ τους σύγκριση, γινόταν με έναν ημιτελή τρόπο, καθώς χρησιμοποιούσαν ένα υποσύνολο των δεδομένων και επομένως η ακρίβεια των αποτελεσμάτων παραμένει ανακριβής.

Ο χρόνος εκπαίδευσης ενός μοντέλου είναι σημαντικός διότι το περιβάλλον του κυβερνοχώρου όπως έχει αναφερθεί είναι ιδιαίτερα δυναμικό και ταχέως εξελισσόμενο, ενώ ο χρόνος της κατηγοριοποίησης μιας νέας κατάστασης, θα προσφέρει στους ειδικούς τον απαιτούμενο χρόνο αντίδρασης δίνοντας τη δυνατότητα εξασφάλισης της προστασίας των συστημάτων τους (system patch).

Αναφορικά με τον τρόπο απόκτησης των δεδομένων, συγκριτικά με άλλους τομείς (π.χ. παρακολούθηση της καλής κατάστασης των συστημάτων ενός αεροσκάφους), ο τομέας της κυβερνοάμυνας παρουσιάζεται πρόσφορος ως προς την απόκτησή τους, καθότι μπορούν να συλλέγονται δεδομένα, σε μικρό χρονικό διάστημα, τοποθετώντας αισθητήρες παρακολούθησης και καταγραφής των χαρακτηριστικών ενός δικτύου για παράδειγμα. Ωστόσο, πρόκληση παραμένει το γεγονός της αποθήκευσης αυτών, καθότι παράγονται τεράστιες ποσότητες δεδομένων της τάξης των terabyte ανά ημέρα, όπως και της κατηγοριοποίησης αυτών για να αποτελούν χρήσιμη πληροφορία, κάτι το οποίο μπορεί να αποτελέσει μια επίπονη διαδικασία.

ΚΕΦΑΛΑΙΟ 5
Το εργαλείο WEKA

§1. Εισαγωγή

Το Πανεπιστήμιο Waikato της Νέας Ζηλανδίας, ανέπτυξε μια πλατφόρμα εργαλείων και αλγορίθμων μηχανικής μάθησης, ονομάζοντάς το WEKA από τα αρχικά Waikato Environment for Knowledge Analysis. Πρόκειται για λογισμικό ανοιχτού κώδικα το οποίο εκχωρείται σύμφωνα με τους όρους χρήσης της άδειας GNU General Public License. Με το συγκεκριμένο πρόγραμμα (software), ένας ειδικός μπορεί με τη χρήση τεχνικών μηχανικής μάθησης, να αποκτήσει - εξάγει γνώση από βάσεις δεδομένων οι οποίες είναι πολύ μεγάλες για να τις αναλύσει με άλλο τρόπο (48). Περιλαμβάνει εκτεταμένη υποστήριξη για όλη τη διαδικασία της εξόρυξης δεδομένων, συμπεριλαμβανομένου της προετοιμασίας των δεδομένων εισαγωγής, στατιστική αξιολόγηση των σχεδίων μάθησης και οπτικοποίησης αυτών και των αποτελεσμάτων. Παρέχονται υλοποιήσεις όλων των κύριων μεθόδων κατηγοριοποίησης, όπως Δέντρα Αποφάσεων, Νευρωνικά δίκτυα, Μηχανές Διανυσμάτων Υποστήριξης, Μπαυεσιανοί κατηγοριοποιητές, Λογιστική Παλινδρόμηση, k-πλησιέστεροι γείτονες κλπ [https://repository.kallipos.gr/bitstream/11419/1239/2/Kef._13.pdf].

§2. Γραφικό Περιβάλλον του WEKA

Ο ευκολότερος τρόπος να χρησιμοποιήσει κανείς το WEKA είναι μέσω του ενός από τα τέσσερα γραφικά περιβάλλοντα που υποστηρίζει και που ονομάζεται Explorer. Αυτό δίνει πρόσβαση σε όλες τις δυνατότητες που προσφέρει το λογισμικό διαμέσου επιλογών από μενού και συμπλήρωσης φορμών. Ο χρήστης μπορεί να εκτελέσει όλες τις κύριες εργασίες εξόρυξης δεδομένων όπως κατηγοριοποίηση, παλινδρόμηση, ανάλυση συστάδων, ανακάλυψη κανόνων συσχέτισης, οπτικοποίηση.

Υπάρχουν άλλα τρία γραφικά περιβάλλοντα στο WEKA. Ένα εξ αυτών είναι και η διεπαφή με το όνομα Knowledge Flow, το οποίο σου επιτρέπει να σχεδιάσεις παραμετροποιήσεις για ροές δεδομένων (streamed data processing), με ένα κύριο μειονέκτημα να εντοπίζεται στο γεγονός ότι τα δεδομένα φορτώνονται από τη μνήμη, πράγμα που σημαίνει ότι δεν κρίνεται κατάλληλο για επεξεργασία δεδομένων μεγάλου όγκου. Παρόλα αυτά το WEKA παρέχει εργαλεία επεξεργασίας μεγάλων όγκων δεδομένων με τη χρήση των επαυξητικών αλγορίθμων (incremental algorithms).

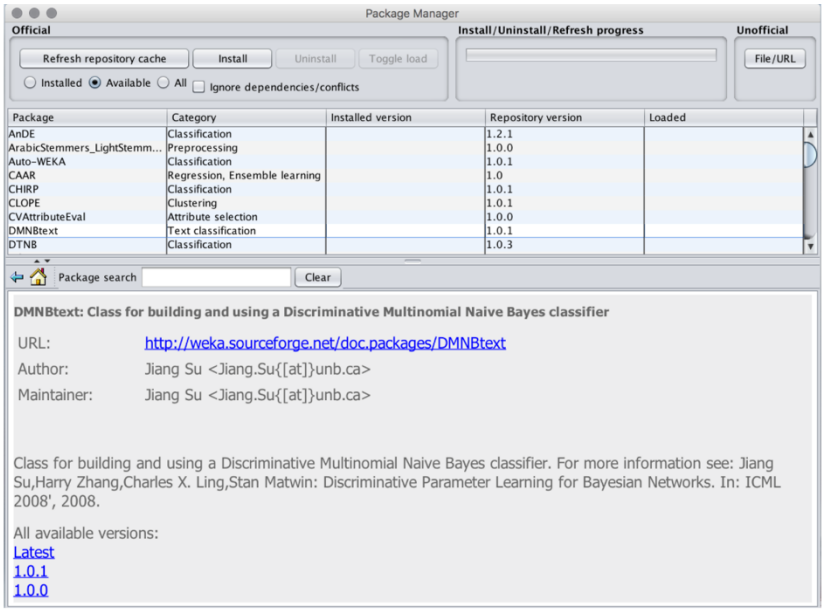
Εικόνα 8. Το γραφικό περιβάλλον χρήστη του WEKA

Η τρίτη διεπαφή ονομάζεται Experimenter και είναι σχεδιασμένη για να δίνει απάντηση σε μια βασική ερώτηση όταν εφαρμόζονται τεχνικές ταξινόμησης και παλινδρόμησης, του ποιες μέθοδοι και παράμετροι είναι αποτελεσματικότεροι για το δεδομένο πρόβλημα. Το παραπάνω μπορεί να πραγματοποιηθεί και με τη χρήση του explorer αλλά με το experimenter δίνεται η δυνατότητα αυτοματοποίησης της όλης διαδικασίας και κάνοντας ευκολότερη τη χρήση ταξινομητών και φίλτρων και χρήσης στατιστικών απόδοσης, διευκολύνοντας τη σύγκριση της επίδοσης διάφορων μοντέλων παρουσιάζοντας αυτά σε μορφή πίνακα.

Η τέταρτη διεπαφή ονομάζεται Workbench και περιλαμβάνει ένα συνδυασμό των παραπάνω τριών σε μια εφαρμογή. Είναι πλήρως παραμετροποιήσιμη και επιτρέπει στο

χρήστη να επιλέγει ποιες εφαρμογές και πρόσθετα θα εμφανίζονται όπως και με ποιες ρυθμίσεις.

Εξαιτίας της μεγάλης ανάπτυξης και αναγνωρισιμότητας που γνώρισε το WEKA, πολλοί από τους αλγόριθμους που προστίθεντο στη πλατφόρμα, κατηγοριοποιήθηκαν εντός συγκεκριμένων «πακέτων» (packages) και έτσι δημιουργήθηκε το Package Management System, το οποίο επιτρέπει στο χρήστη να ανατρέξει, επιλέξει και εγκαταστήσει τα πακέτα αλγορίθμων του ενδιαφέροντός του (Εικόνα 9).



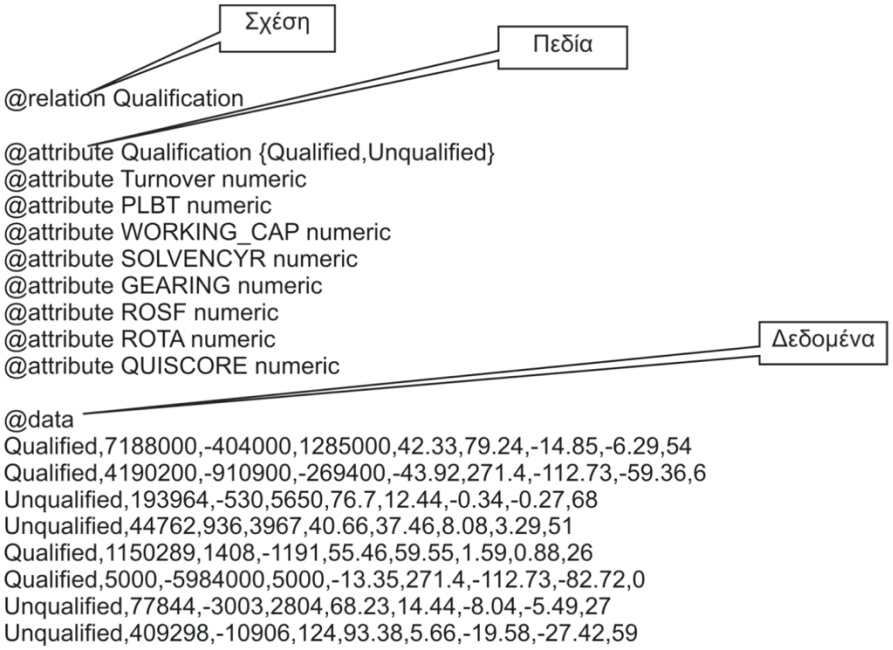
Εικόνα 9. The Package Manager

§3. Μέθοδος χρησιμοποίησης του WEKA

Καθότι η παρούσα εργασία έχει ως κύριο στόχο την επεξεργασία ενός συνόλου δεδομένων σχετικά με την ασφάλεια του κυβερνοχώρου, κρίνεται σκόπιμο να παρουσιαστεί συνοπτικά, η μεθοδολογία που χρησιμοποιείται κατά την επεξεργασία δεδομένων στο WEKA.

Έτσι, κατά τη χρήση του WEKA Explorer, το πρώτο βήμα είναι η εισαγωγή των δεδομένων. Δεδομένα μπορούν να εισάγονται από μια βάση δεδομένων, είτε και απευθείας

στη μορφή ARFF η οποία υποστηρίζεται από το λογισμικό και που αναλύεται παρακάτω. Τα αρχεία ARFF είναι απλά αρχεία κειμένου με τις τιμές τους να διαχωρίζονται με κόμμα (Comma Separated Values). Το αρχείο πρέπει να περιέχει μια επικεφαλίδα, στην οποία ορίζονται το όνομα της σχέσης, και τα πεδία, όπως φαίνεται και στην εικόνα 10.



Εικόνα 14. Αρχείο τύπου ARFF

Μετά την εισαγωγή των δεδομένων, το παράθυρο της προ επεξεργασίας παρουσιάζονται διάφορες πληροφορίες για τα δεδομένα, και παρέχεται η δυνατότητα στο χρήστη να εκτελέσει εργασίες διερευνητικής ανάλυσης και προ επεξεργασίας. Επιλέγοντας τα πεδία ο χρήστης μπορεί να παρατηρήσει την κατανομή των τιμών και αναλόγως αν θεωρήσει ότι είναι μερικώς προβληματικές, όπως για παράδειγμα εάν τις θεωρεί θόρυβο, μπορεί να τις τροποποιήσει αναλόγως. Εκτός τούτου, δίνεται η δυνατότητα να εφαρμοστούν δυνατότητες αυτοματοποιημένης προ επεξεργασίας των δεδομένων, με τις συνηθέστερες που μπορούν να εφαρμοστούν να είναι οι παρακάτω:

- Η κανονικοποίησης αριθμητικών τιμών
- Η διακριτοποίηση αριθμητικών τιμών

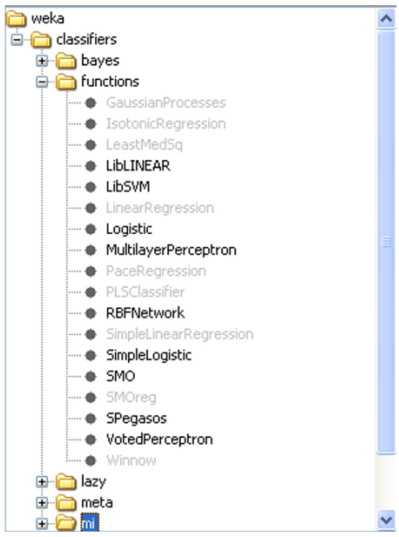
- Η μετατροπή αριθμητικών και ονομαστικών τιμών σε δυαδικά
- Η συγχώνευση δύο ονομαστικών πεδίων
- Η δημιουργία νέων συνόλων δεδομένων με εφαρμογή δειγματοληψίας

Το WEKA προσφέρει μια μεγάλη ποικιλία εργαλείων κατηγοριοποίησης, όπως φαίνεται στην εικόνα 15. Ορισμένες από τις κυριότερους μεθόδους κατηγοριοποίησης όπως έχει ήδη αναφερθεί είναι οι Μηχανές Διανυσμάτων Υποστήριξης, η Λογιστική Παλινδρόμηση, Νευρωνικά Δίκτυα και Δέντρα Αποφάσεων.

Ο χρήστης αφού ορίσει τη μέθοδο κατηγοριοποίησης, έπειτα ορίζει το πεδίο της κλάσης και τη μέθοδο αξιολόγησης του κατηγοριοποιητή, ανάμεσα από τις τέσσερις εναλλακτικές που προσφέρονται όπως παρακάτω:

- "Use Training Set", όπου υπολογίζονται οι επιδόσεις του μοντέλου, χρησιμοποιώντας το σύνολο εκπαίδευσης
- "Supplied Test Set", όπου χρησιμοποιείται ένα διαφορετικό σύνολο δεδομένων
- "Cross Validation", όπου ο χρήστης μπορεί να ορίσει το πλήθος των τμημάτων
- "Percentage Spit", όπου διασπάται το σύνολο των δεδομένων σε υποσύνολο εκπαίδευσης και υποσύνολο επικύρωσης, σύμφωνα με ποσοστά που ορίζονται από το χρήστη.

Με την ολοκλήρωση των προηγούμενων σταδίων, μπορεί να η εκπαίδευση και η αξιολόγηση του μοντέλου.



Εικόνα 15. Μέθοδοι κατηγοριοποίησης

ΚΕΦΑΛΑΙΟ 6
Το HTTP Dataset CSIC 2010

§1. Εισαγωγή

Το συγκεκριμένο σύνολο δεδομένων περιέχει αυτοματοποιημένες αιτήσεις περιεχομένου στο Web, με σκοπό την μελέτη και ανάλυση του τρόπου λειτουργίας και μελλοντικού σχεδιασμού συστημάτων προστασίας επιθέσεων μέσω αντίστοιχων αιτήσεων (Web Attack Protection Systems). Το συγκεκριμένο σύνολο αναπτύχθηκε από το Information Security Institute of CSIC (Spanish Research National Council) [http://www.isi.csic.es/dataset/], και είναι ελεύθερα προσβάσιμο και αξιοποιήσιμο για ερευνητικούς σκοπούς με την προϋπόθεση αναφοράς του.

Σκοπός της δημιουργίας του παραπάνω dataset, αποτέλεσε το πρόβλημα στην έλλειψη συνόλων δεδομένων που είναι δημόσια διαθέσιμα με σκοπό την αναγνώριση επιθέσεων WEB αλλά και ελέγχου της απόδοσης των αντίστοιχων τοίχων προστασίας (Web Application Firewalls). Επιπρόσθετα, εξαιτίας του γεγονότος ότι για την καταγραφή αντίστοιχων datasets

θα πρέπει να λαμβάνεται σοβαρά υπόψη η προστασία των προσωπικών δεδομένων, ένας παραπάνω λόγος ήταν η δημιουργία του συγκεκριμένου.

Ο σκοπός της παρούσας εργασίας είναι να χρησιμοποιήσει το παραπάνω σύνολο δεδομένων και να αναζητήσει λύσεις στο πρόβλημα τις αναγνώρισης κακόβουλων επιθέσεων και ενεργειών μέσω του πρωτοκόλλου Http όπως έχει αναφερθεί, χρησιμοποιώντας αλγορίθμους μηχανικής μάθησης. Ειδικότερα θα χρησιμοποιηθεί το εργαλείο WEKA με συγκεκριμένους αλγόριθμους που, στο μέτρο που μπορούμε να γνωρίζουμε, δεν έχει εφαρμοστεί στο παρελθόν σε κάποια εργασία στο συγκεκριμένο σύνολο δεδομένων

§2. Περιγραφή του συνόλου δεδομένων

Το σύνολο δεδομένων περιέχει την κίνηση των δικτυακών πακέτων που παράγονται στοχεύοντας σε μια εφαρμογή ηλεκτρονικού εμπορίου (e-commerce web application), η οποία αναπτύχθηκε για τους σκοπούς αυτούς. Μέσω της συγκεκριμένης εφαρμογής, οι χρήστες μπορούν να αγοράζουν προϊόντα χρησιμοποιώντας μια τραπεζική κάρτα, και να κατοχυρώνουν τα προσωπικά τους στοιχεία.

Η παραγωγή του συνόλου γίνεται αυτόματα και περιέχει 36000 κανονικές – επιτρεπόμενες αιτήσεις, και περισσότερες από 25000 μη επιτρεπτές. Οι αιτήσεις του πρωτοκόλλου Http, χαρακτηρίζονται ως ‘normal’ ή ‘anomalous’ και περιέχονται επιθέσεις που έχουν αναλυθεί παραπάνω και μπορεί να αφορούν SQL injections, buffer overflow, information gathering, files disclosure, CRLF injection, XSS, server side include, parameter tampering και άλλες.

Η κίνηση των πακέτων πραγματοποιείται αρχικά συλλέγοντας όλα τα στοιχεία των παραμέτρων της εφαρμογής. Όλα τα δεδομένα (ονόματα, επίθετα, διευθύνσεις κλπ) αποσπώνται από πραγματικές βάσεις δεδομένων, και μετέπειτα αποθηκεύονται σε δύο βάσεις, μία για τις κανονικές καταχωρήσεις και μια δεύτερη για τις μη κανονικές. Επιπρόσθετα, όλες οι δημόσιες σελίδες της εφαρμογής καταγράφονται. Στο επόμενο στάδιο δημιουργούνται κανονικές και μη αιτήσεις για κάθε σελίδα.

Για τη δημιουργία των αιτήσεων, τρεις τύποι ανώμαλων αιτήσεων χρησιμοποιήθηκαν:

- Static Attacks, όπου προσπαθούν να αιτηθούν κρυμμένες ή ανύπαρκτες πηγές, και περιλαμβάνουν session IDs, configuration files, default files κλπ
- Dynamic Attacks, όπου τροποποιούνται έγκυρες αιτήσεις, SQL Injection, XSS, buffer overflows κλπ.
- Unintentional illegal requests, όπου πρόκειται για αιτήσεις που δεν αφορούν σκόπιμες κακόβουλες ενέργειες, παρόλα αυτά δεν ακολουθούν την κανονικότητα των μεθόδων των αιτήσεων και δεν έχουν την κανονική δομή όπως οι τιμές των κανονικών παραμέτρων.

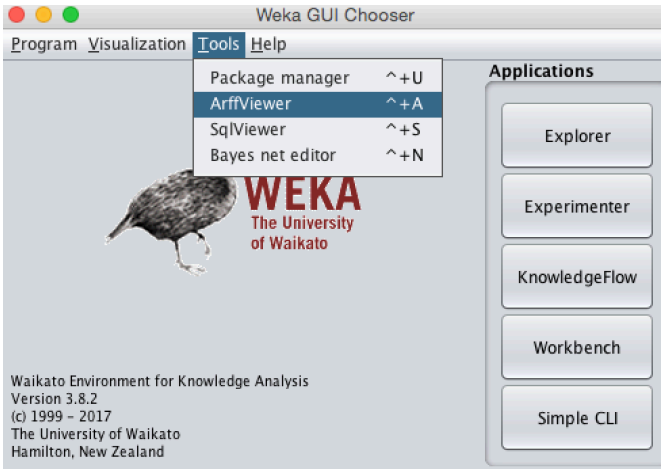
Οι επιθέσεις δημιουργήθηκαν με τη χρήση των εργαλείων PAROS [Chinotec Technologies Company: Paros - for web application security assessment. http://www.parosproxy.org/index.shtml (2004)] και W3AF [Andrıs Riancho: Web Application Attack and Audit Framework. http://w3af.sourceforge.net (2007)].

Το σύνολο δεδομένων χωρίζεται σε τρία υποσύνολα, ένα για το training phase, όπου περιέχονται μόνο κανονικές αιτήσεις, και δύο υποσύνολα για το test phase, ένα με κανονικές αιτήσεις και ένα δεύτερο με μη κανονικές. Ο λόγος που για το training phase χρησιμοποιούνται μόνο δεδομένα με κανονικές αιτήσεις είναι ότι ακολουθείται συγκεκριμένη προσέγγιση του ορισμού του τί θεωρείται ανώμαλο και τί όχι, δηλαδή, προσδιορίζεται η κανονική συμπεριφορά και οτιδήποτε άλλο εκτός τούτου θεωρείται μη κανονικό.

Εικόνα 16. Μέρος του συνόλου των δεδομένων σε αρχείο csv

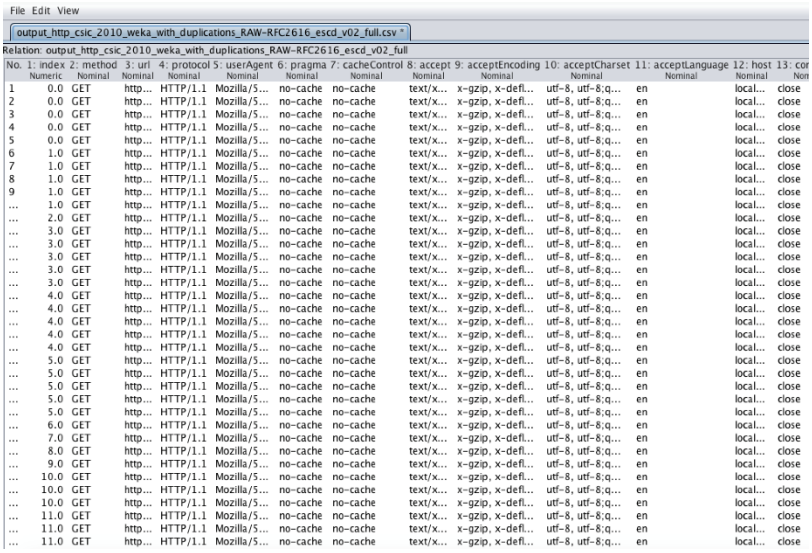
§3. Επεξεργασία των δεδομένων με το WEKA

Όπως φαίνεται και στην εικόνα 16, το σύνολο των δεδομένων που θα χρησιμοποιηθεί είναι σε μορφή CSV (comma separated value). Μέσω του WEKA μας δίνεται η δυνατότητα επεξεργασίας αντίστοιχων αρχείων και μετατροπή τους στην κατάλληλη μορφή για το συγκεκριμένο λογισμικό, δηλαδή τη μορφή ARFF (Attribute Relation File Format) (https://www.cs.waikato.ac.nz/ml/weka/arff.html). Μέσω της επιλογής ArffViewer από το μενού όπως φαίνεται και στην εικόνα 17, τελικώς μετατρέπουμε το αρχείο μας σε μορφή Arff (εικόνα 18).

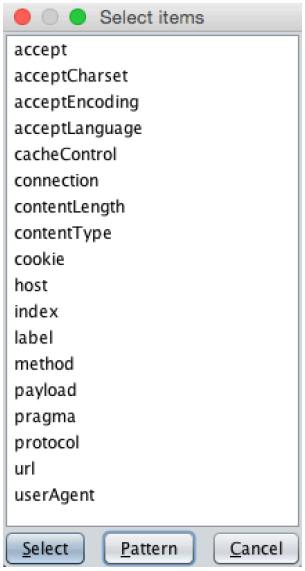


Εικόνα 17. Επιλογή για τη μετατροπή του συνόλου δεδομένων σε αρχείο ARFF.

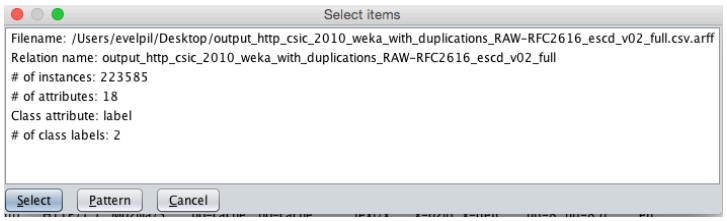
Το σύνολο των δεδομένων αποτελείται από 18 μεταβλητές (εικόνα 19) με 223585 δείγματα τα οποία μπορεί να παίρνουν ονομαστικές και αριθμητικές τιμές, ενώ υπάρχουν δύο κατηγορίες προς κατηγοριοποίηση (normal, anomaly). Από την εφαρμογή του Explorer και ανοίγοντας το αρχείο μας, οδηγούμαστε στην επιλογή «Preprocess», από όπου αντλούμαι ορισμένα ενδιαφέροντα στοιχεία για το σύνολο των δεδομένων μας όπως φαίνεται στην εικόνα 21.



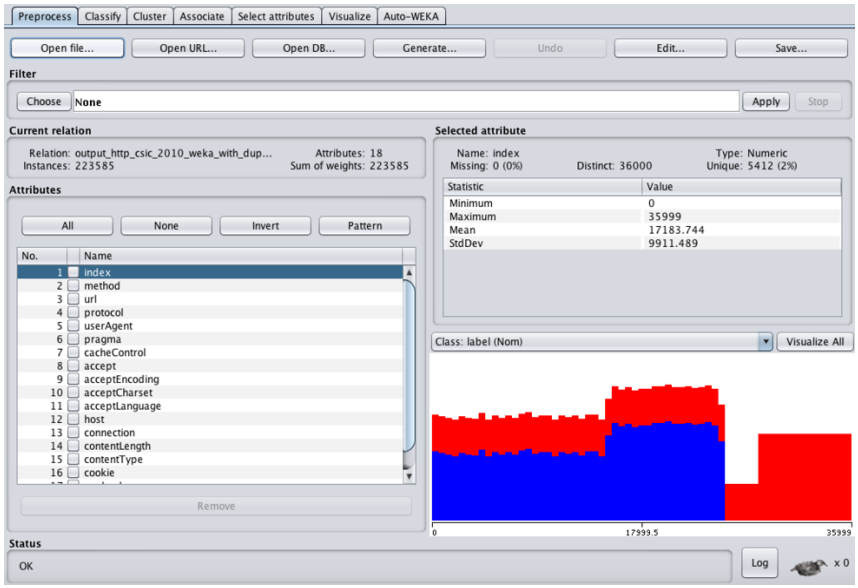
Εικόνα 18. Το σύνολο δεδομένων σε μορφή ARFF



Εικόνα 19. Οι μεταβλητές του συνόλου δεδομένων



Εικόνα 20. Οι ιδιότητες του συνόλου δεδομένων



Εικόνα 21. Το στάδιο «Preprocess»

Ειδικότερα, επιλέγοντας την κάθε μια μεταβλητή, μπορούμε να αντλήσουμε στατιστικά στοιχεία όπως τις ελάχιστες και μέγιστες τιμές της μεταβλητής υπό εξέταση, το τύπο της, το μέσο όρο και την τυπική απόκλιση.

§4. Knoledge Flow

§4.1 Εισαγωγή

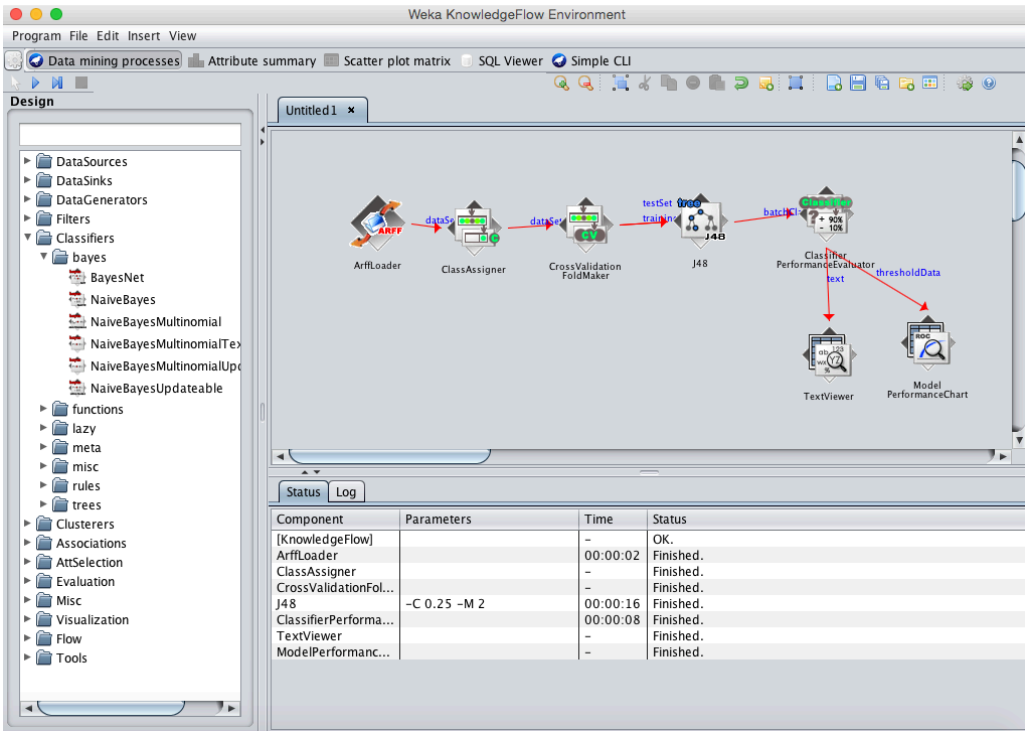
Στη παρούσα εργασία, η επεξεργασία των δεδομένων και η παρουσίαση των αποτελεσμάτων θα πραγματοποιηθούν εναλλακτικά μέσω του μενού Knowledge Flow, καθώς αυτό μας δίνει τη δυνατότητα για τη δημιουργία ενός γραφικού περιβάλλοντος και γραφικής αποτύπωσης της διαδικασίας, κάτι το οποίο μπορεί να είναι πιο προσιτό για τον αναγνώστη.

Ο χρήστης μπορεί να επιλέγει στοιχεία του WEKA από ένα μενού επιλογής, να τα τοποθετεί στην επιφάνεια εργασίας και να ενώνει τα μεταξύ τους στοιχεία δημιουργώντας έτσι μια διαδικασίας ροής δεδομένων και γνώσης (knowledge flow). Τα στοιχεία τα οποία μπορεί κάποιος να χρησιμοποιήσει μέσω της επιλογής του Explorer, τα βρίσκει και σε αυτό το μενού, με κάποια επιπλέον στοιχεία.

Το πρόβλημα το οποίο καλούμαστε να αντιμετωπίσουμε είναι ένα πρόβλημα κατηγοριοποίησης. Το WEKA προσφέρει μια μεγάλη ποικιλία εργαλείων για κατηγοριοποίηση, από τις οποίες ορισμένες από τις κυριότερες αποτελούν τα Μπαυεσιανά Δίκτυα, οι Μηχανές Υποστηρικτικού Διανύσματος, η Λογιστική Παλινδρόμηση, τα Νευρωνικά Δίκτυα και τα Δέντρα Αποφάσεων.

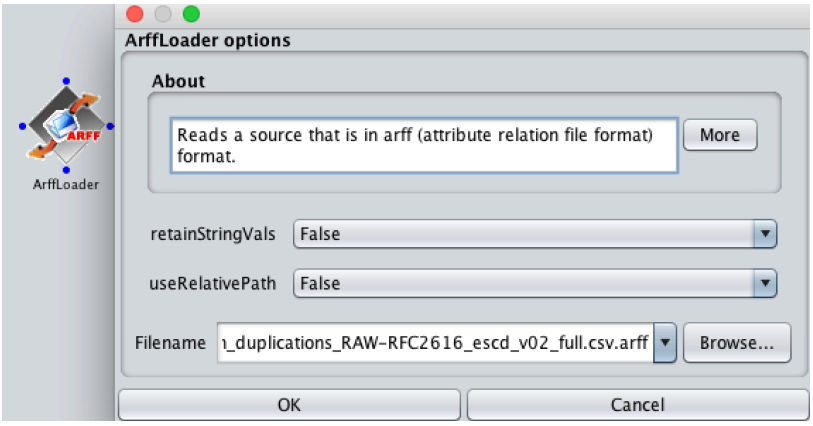
§4.2 Το περιβάλλον του WEKA Knowledge

Όπως φαίνεται και στην εικόνα 22, μας δίνεται η δυνατότητα δημιουργίας μιας ροής δεδομένων και γνώσης, με εικονική αποτύπωση. Στο αριστερό μέρος και διαδοχικά δίνεται η δυνατότητα της επιλογής διαφόρων στοιχείων, όπως για παράδειγμα του αλγόριθμου κατηγοριοποίησης που θα χρησιμοποιηθεί, και επιπλέον μενού παραμετροποίησης των εν λόγω στοιχείων.

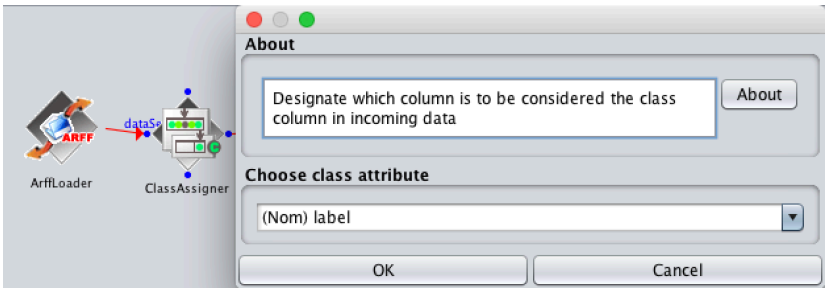


Εικόνα 22. Το περιβάλλον του WEKA Knowledge

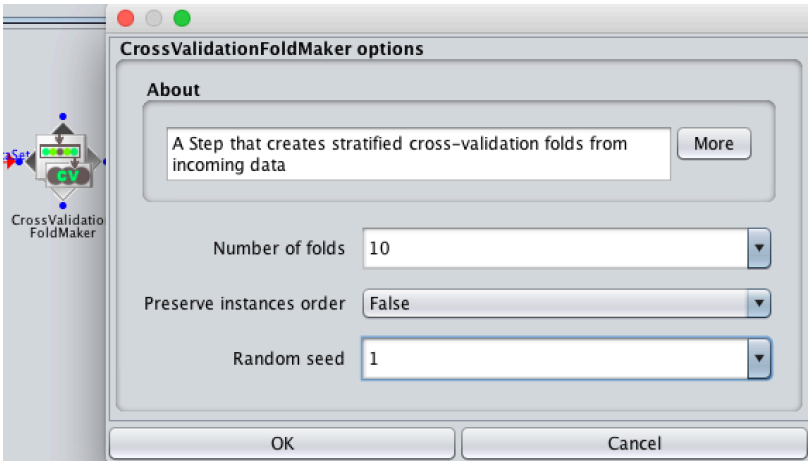
Αρχικά επιλέγουμε από το μενού DataSources, τη πηγή των δεδομένων μας και τοποθετούμε το εικονίδιο στην επιφάνεια εργασίας (εικόνα 23). Μέσω του ClassAssigner, προσδιορίζουμε ποια θα είναι η κλάση από το σύνολο των δεδομένων μας (Εικόνα 24) και στη συνέχεια προσδιορίζουμε τον αριθμό των πτυχών με τον οποίο θέλουμε να χωριστεί το σύνολο των δεδομένων μας για τον προσδιορισμό της ποιότητάς του.



Εικόνα 23. Η επιλογή του ArffLoader



Εικόνα 24. Η επιλογή του ClassAssigner



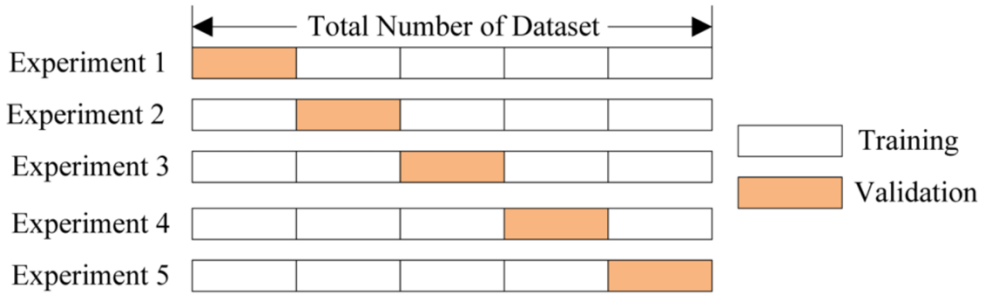
Εικονα 25. Η επιλογή του CrossValidationFoldMaker

§4.3 Η διαδικασία της μεθόδου Cross – Validation

Για το σύνολο των δεδομένων που θα χρησιμοποιήσουμε, θα επιλέξουμε την μέθοδο του cross validation, η οποία χρησιμοποιείται κυρίως σε περιπτώσεις όπου σκοπός είναι η πρόβλεψη και η εκτίμηση του πόσο καλά μπορεί ένα μοντέλο να αποδώσει. Συγκρινόμενη με την μέθοδο του χωρισμού του συνόλου δεδομένων σε δεδομένα εκπαίδευσης και δεδομένα test – validation, η μέθοδος του cross-validation μας δίνει πιο αξιόπιστες μετρήσεις για την ποιότητα του εξεταζόμενου μοντέλου, αν και απαιτεί περισσότερο χρόνο.

Στη μέθοδο αυτή, τρέχουμε τη διαδικασία στο μοντέλο μας, σε πολλαπλά υποσύνολα του συνόλου των δεδομένων μας, έχοντας έτσι πολλαπλές μετρήσεις της ποιότητας αυτών, όπως φαίνεται και στην εικόνα 22 (https://www.kaggle.com/dansbecker/cross-validation). Για παράδειγμα μπορούμε να τρέξουμε ένα πρώτο πείραμα, έχοντας επιλέξει το 20% αυτού να αποτελεί το σύνολο για το test ενώ το υπόλοιπο παραμένει το training set. Αυτό μας δίνει

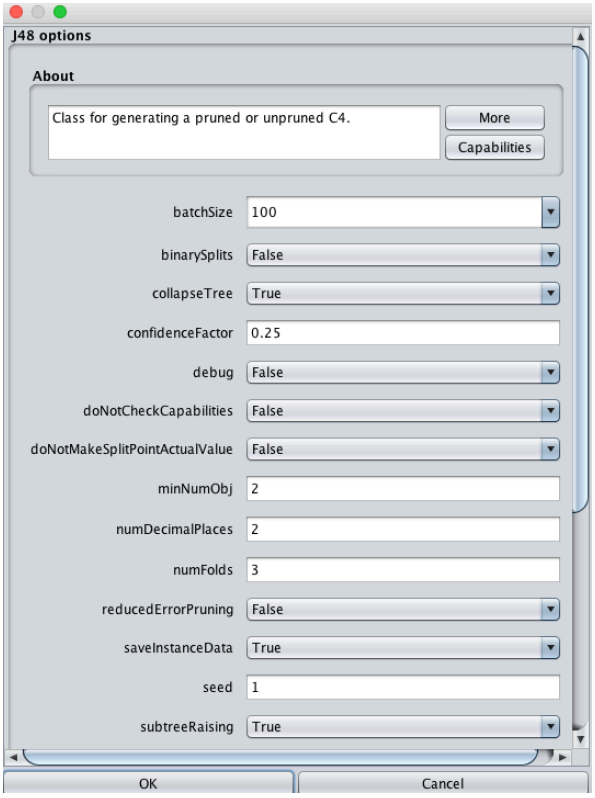
μια εικόνα της ποιότητας του συνόλου δεδομένων μας. Η ίδια διαδικασία επαναλαμβάνεται για όσες φορές έχουμε επιλέξει ως παράγοντα διαχωρισμού. Το μειονέκτημα της μεθόδου είναι ότι απαιτείται περισσότερος χρόνος για την επεξεργασία. Η επιλογή μεταξύ των δύο μεθόδων εξαρτάται κάποιες φορές από το μέγεθος του συνόλου των δεδομένων μας, όπου σε σχετικά μικρότερα σύνολα η cross – validation προτιμάται έναντι του διαχωρισμού σε δεδομένα εκπαίδευσης και δεδομένα validation.



Εικόνα 22. Η μέθοδος του Cross - Validation

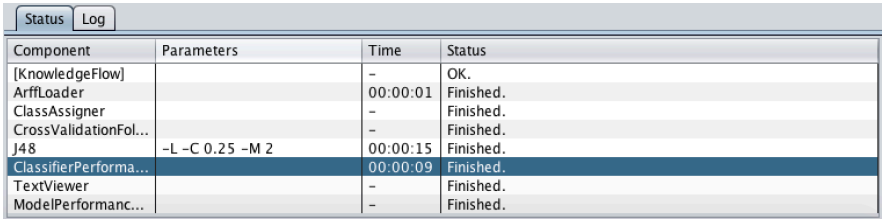
§4.4 Ο αλγόριθμος J48

Αρχικά, έχουμε επιλέξει να χρησιμοποιήσουμε για τις δοκιμές τον αλγόριθμο J48 με τις επιλογές παραμετροποίησης όπως αυτές φαίνονται στην εικόνα 23. Ο συγκεκριμένος αλγόριθμος ανήκει στην κατηγορία των δέντρων απόφασης (decision trees) και αποτελεί ένα μοντέλο μηχανικής μάθησης για πρόβλεψη. Η μεταβλητή η οποία είναι να προβλεφθεί αποτελεί την εξαρτημένη μεταβλητή ενώ όλες οι υπόλοιπες αποτελούν τις ανεξάρτητες.

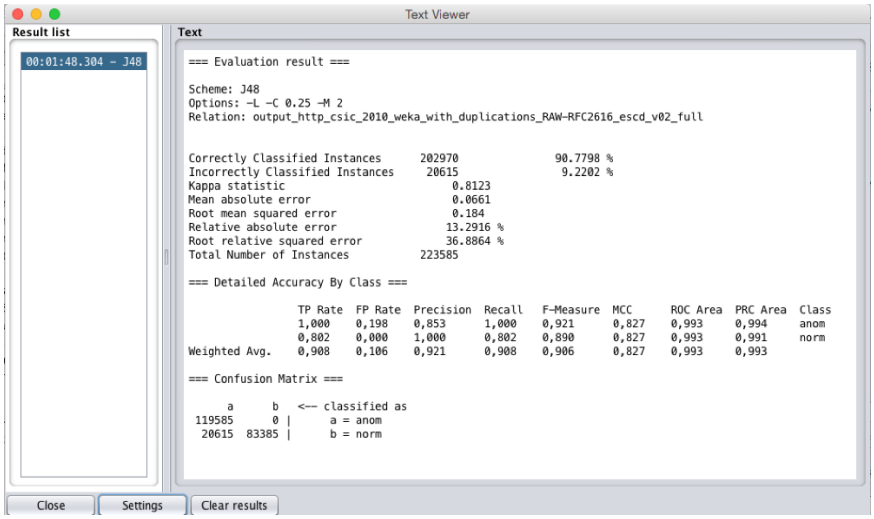


Εικόνα 23. Οι επιλογές για τον αλγόριθμο J-48

Έχοντας προσθέσει στο διάγραμμα ροής και το πρόσθετο ClassifierPerformanceEvaluator για την εξαγωγή συμπερασμάτων αναφορικά με τις μεθόδους προσδιορισμού της απόδοσης του εκάστοτε αλγορίθμου, μπορούμε να προχωρήσουμε στην εκτέλεση των ενεργειών του αλγορίθμου. Όταν αυτό πραγματοποιηθεί παρατηρούμε αλλαγές στο παράθυρο της κατάστασης με διάφορες καταχωρήσεις, όπως φαίνεται στην εικόνα 24.



Εικόνα 24. Το παράθυρο status

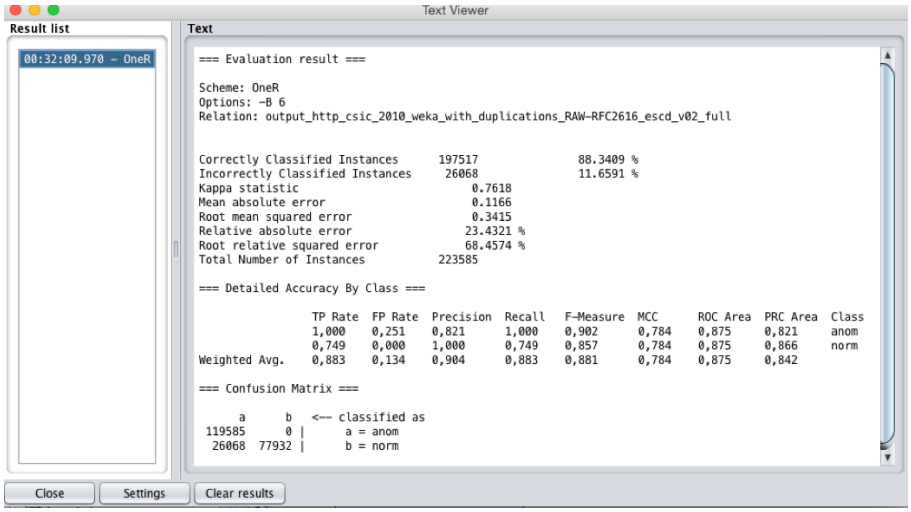


Εικόνα 25. Εξαγωγή των αποτελεσμάτων του αλγόριθμου J48

Η εξαγωγή των αποτελεσμάτων γίνεται μέσω του TextViewer και την επιλογή ShowResults. Τα αποτελέσματα από την εκτέλεση του αλγορίθμου φαίνονται στην εικόνα 25. Παρατηρούμε ότι ένα ποσοστό 90.7797% του συνόλου των δεδομένων έχει κατηγοριοποιηθεί σωστά, ενώ λανθασμένα έχει κατηγοριοποιηθεί ποσοστό 9.2202%.

§4.5 Ο αλγόριθμος OneR

Για τη σύγκριση των αποτελεσμάτων της κατηγοριοποίησης, θα προχωρήσουμε και στη χρήση και άλλων μεθόδων όπως ο αλγόριθμος OneR. Ο συγκεκριμένος αλγόριθμος είναι ο πιο απλός αλγόριθμος παραγωγής κανόνων ταξινόμησης μιας και δημιουργεί μόνο έναν κανόνα και σε αυτόν βασίζει τις αποφάσεις του (Holte. 1993). Όπως παρατηρούμε και στην εικόνα 26, ο αλγόριθμος καταφέρνει να κατηγοριοποιήσει σωστά ένα ποσοστό 88.3409% έναντι 11.6591% λάθους.



Εικόνα 26. Εξαγωγή των αποτελεσμάτων του αλγόριθμου OneR

§4.6 Ο αλγόριθμος BayesNet

Η μάθηση που προκύπτει από τα δίκτυα Bayes οφείλεται σε διάφορους αλγόριθμους αναζήτησης και ποιοτικά κριτήρια, δίνοντας εξαιρετικά αποτελέσματα στον καθορισμό των επιδράσεων διαφόρων παραγόντων σε ένα αποτέλεσμα, αναζητώντας αλληλεξαρτήσεις μεταξύ των δεδομένων. Όπως φαίνεται και στην εικόνα 27, η απόδοση του αλγορίθμου στο σύνολο των δεδομένων μας ανέρχεται σε 99,6332% σωστής κατηγοριοποίησης.

```
=== Evaluation result ===

Scheme: BayesNet
Options: -D -Q weka.classifiers.bayes.net.search.local.K2 -- -P 1 -S BAYES -E weka.classifiers.bayes.net.estimate.SimpleEstimator -- -A 0.5
Relation: output_http_csic_2010_weka_with_duplications_RAW-RFC2616_escd_v02_full


Correctly Classified Instances      222765               99.6332 %
Incorrectly Classified Instances       820                0.3668 %
Kappa statistic                          0.9926
Mean absolute error                      0.0294
Root mean squared error                  0.0786
Relative absolute error                  5.9155 %
Root relative squared error             15.7489 %
Total Number of Instances           223585

=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
               0,993    0,000    1,000      0,993    0,997      0,993    1,000     1,000     anom
               1,000    0,007    0,992      1,000    0,996      0,993    1,000     1,000     norm
Weighted Avg.  0,996    0,003    0,996      0,996    0,996      0,993    1,000     1,000

=== Confusion Matrix ===

      a      b   <-- classified as
 118790    795 |      a = anom
     25 103975 |      b = norm
```

Εικόνα 27. Εξαγωγή των αποτελεσμάτων του αλγόριθμου BayesNet

§4.7 Άλλες μέθοδοι που έχουν εφαρμοστεί στο παρελθόν και τα αποτελέσματά τους

Η ενίσχυση της ανίχνευσης ανωμαλιών και της κατηγοριοποίησης επιθέσεων ή μη κανονικής κίνησης στο web, έχει γίνει και στο παρελθόν με τη χρήση διαφόρων τεχνικών. Για παράδειγμα ο Pham (2016), πραγματοποίησε μια επισκόπηση διάφορων μεθόδων μηχανικής μάθησης όπως random forest, logistic regression, decision tree, AdaBoost, για την εύρεση μηχανισμών ανίχνευσης επιθέσεων σε περιβάλλον Web. Αλλά και πιο συγκεκριμένα, έκανε μια επισκόπηση τενχικής μάθησης με logistic regression στο ίδιο σύνολο δεδομένων με τη παρούσα εργασία, όπου επικαλείται η καλή εφαρμογή της με καλή απόδοση.

Άλλες εργασίες που έχουν πραγματοποιηθεί, είναι μεταξύ άλλων αυτές των Nguyenet (2011) και Gallagher (2009), όπου προσεγγίζουν το πρόβλημα κάνοντας χρήση τεχνικών επιλογής χαρακτηριστικών (feature selection), μέσω μεθόδων όπως correlation feature selection (CFS) και minimal-redundancy-maximal-relevance (mRMR), όπου αναφέρονται πολύ καλά αποτελέσματα.

Επιπρόσθετα, η Althubiti (2017), χρησιμοποίησε μεθόδους αξιολόγησης χαρακτηριστικών (attribute evaluator methods) στο ίδιο σύνολο δεδομένων με αυτό της εργασίας μας, βασιζόμενη πάνω στα αποτελέσματα της μελέτης του Nguyenet, και τα οποία σύμφωνα με την εργασία παρουσίασαν καλύτερα αποτελέσματα συγκρινόμενα με αυτά του τελευταίου, κάνοντας χρήση μόλις πέντε χαρακτηριστικών με σκοπό την μείωση του χρόνου εκπαίδευσης αλλά και την βελτίωση της ακρίβειας. Άλλη μια διαφοροποίηση ως προς την προσέγγιση επίλυσης του προβλήματος είναι τα ποσοστά διαχωρισμού των δεδομένων σε δεδομένα εκπαίδευσης και δεδομένα ελέγχου, όπου αντίστοιχα ήταν 60% και 40%.

Μια σύγκριση που μπορεί να γίνει μεταξύ των αποτελεσμάτων της παραπάνω εργασίας και της δικής μας είναι στις περιπτώσεις όπου γίνεται χρήση των αλγορίθμων J48 και των Μπαεσυανών Δικτύων, με τα αποτελέσματα της σύγκρισης να φαίνονται στο παρακάτω πίνακα, η οποία όμως δεν είναι τόσο ενδεικτική καθόσον δεν συγκρίνονται αποτελέσματα τα οποία

προκύπτουν από την ίδια μέθοδο, ωστόσο παρουσιάζονται για την κατάδειξη των καλών αποτελεσμάτων που δίνουν σχετικά με την κατηγοριοποίηση των δεδομένων.

	Althubiti	Παρούσα Εργασία	Althubiti	Παρούσα Εργασία
Μέθοδοι	J48		Native Bayes	
TP Rate	99.6	90.8	88.8	99.6
FP Rate	0.1	10.6	88.8	0.3
Precision	99.9	92.1	89.0	99.6
Recall	99.6	90.8	88.8	99.6
F-Measure	99.8	90.6	88.9	99.6

§4.8 Συμπεράσματα

Από τα ως άνω αποτελέσματα, προκύπτει ότι με τη χρήση αλγορίθμων μηχανικής μάθησης και συγκεκριμένα στο εργαλείο WEKA, προκύπτουν συμπεράσματα τα οποία προσδίδουν αποτελεσματικότητα στην ανίχνευση ανωμαλιών ή και κακόβουλων ενεργειών σε ένα δίκτυο. Ο χώρος του κυβερνοπολέμου αποτελεί μια πολύ ευρεία έννοια, πολλές φορές ιδιαίτερα πολύπλοκη και για την ασφάλειά του επενδύονται, ή πρέπει να επενδύονται πολλές φορές, μεγάλα χρηματικά ποσά. Οι αποδόσεις αλγορίθμων, όπως παραπάνω έχει περιγραφεί, στην εύρεση προτύπων που παρεκκλίνουν από τα συνηθισμένα ή «υγιή» όρια της κανονικής λειτουργίας ενός δικτύου και εφαρμογών που τρέχουν πάνω σε αυτό, μαρτυρά τη δυναμική που υπάρχει προς αυτή την κατεύθυνση για τη χρήση τέτοιων τεχνικών στο τομέα της ασφάλειας.

ΚΕΦΑΛΑΙΟ 7

Επίλογος

Το σημερινό ψηφιακό περιβάλλον παρουσιάζει σημαντικές προκλήσεις για την διασφάλιση της προστασίας του και των χρηστών του. Η πολυπλοκότητα, οι υψηλής ευφυίας και τεχνικής κατάρτισης επιθέσεις που παρατηρούνται και οι κίνδυνοι που εμφανίζονται από

την εισαγωγή νέων ευπαθειών, είτε από αμέλεια είτε από βιασύνη, οδηγούν στη δημιουργία ενός περιβάλλοντος του οποίου η διασφάλιση με τα παραδοσιακά μέσα, τείνει να γίνει ανεπαρκής. Η ανάπτυξη νέων προσεγγίσεων και μεθόδων προστασίας του ψηφιακού πεδίου, δείχνει να αποτελεί μια νέα απαίτηση. Η χρήση νέων ευφυών συστημάτων με τη χρήση της τεχνητής νοημοσύνης και της μηχανικής μάθησης αποτελούν μια υπόσχεση προς αυτή την κατεύθυνση. Πεδία όπως η υποστήριξη αποφάσεων (decision support), η αποτίμηση και γνώσης της κατάστασης (situation awareness) και η διαχείριση γνώσης (knowledge management) είναι μερικά από τα οποία μπορούν να βρουν εφαρμογή οι νέες αυτές τεχνικές. Αυτές οι νέες πρακτικές σε συνδυασμό με τις έως τώρα παραδοσιακές πρακτικές ασφαλείας, μπορούν να παρέχουν τα κατάλληλα εργαλεία στην κοινότητα της ασφάλειας των επικοινωνιών με σκοπό την συνέχιση της προάσπισης και διασφάλισης της ασφάλειάς του προς όφελος όλων.

Βιβλιογραφία

(1) National Cyber Security Strategy 2016 to 2021 of United Kingdom

(2) CISCO Cyber Annual Report 2016

(3) Symantec 2016 Internet Security Report

(4) Kolias C., Kampourakis G., Stavrou A., Gritzalis S., Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset, IEEE Communication Surveys and tutorials

(5) The Lipman Report , "Threats to the Information Highway: CyberWarfare, CyberTerrorism and CyberCrime, October 15, 2010"

(6) Harris, S., F. Maymi (2016), CISSP All-in-One Exam Guide (7th Edition), McGraw-Hill Education.

(7) IEEE. 802.11-1997 IEEE Standard for Information Technology, Telecommunications and Information Exchange Between System Local and Metropolitan Area Networks. Nov 2014 URL: http://ieeexplrore.ieee.org/xpl/articleDetails.jsp?arnumber=654749

(8) Md Sohail Ahmad and Shashank Tadakamadla. "Short paper: security evaluation of IEEE 802.11 w specification " in : Proceedings of the fourth ACM conference on Wireless Network Security. AMC. 2011, pp 53-58.

(9) Scott Fluhrer, Itsik Mantin, and Adi Shamir. "Weak- nesses in the key scheduling algorithm of RC4". In: *Selected areas in cryptography*. Springer. 2001, pp. 1– 24.

(10) Andrea Bittau. "Additional weak IV classes for the FMS attack". In: *Department of Computer Science, University College London* (2003).

(11) Hal Berghel and Jacob Uecker. "WiFi attack vectors". In: *Communications of the ACM* 48.8 (2005), pp. 21–28.

(12) Rafik Chaabouni. *Break wep faster with statistical analysis Tech. Rep. 2006*

(13) Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. "Breaking 104 bit WEP in less than 60 sec onds". In: *Information Security Applications*. Springer, 2007, pp. 188–202.

(14) Andreas Klein. "Attacks on the RC4 stream cipher". In: *Designs, Codes and Cryptography* 48.3 (2008), pp. 269–286.

(15) KoreK. *ChopChop (Experimental WEP attacks)*. Nov. 2014. URL: http://www.netstumbler.org/showthread. php?t=12489.

(16) Andrea Bittau. "The Fragmentation Attack in Practice". In: *IEEE Symposium on Security and Privacy, IEEE Computer Society*. 2005.

(17) Kemal Bicakci and Bulent Tavli. "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks". In: *Computer Standards & Interfaces* 31.5 (2009), pp. 931–941.

(18)http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp

(19)https://www.alienvault.com/blogs/security-essentials/intrusion-detection-techniques-methods-best-practices

(20) Anna Buczak, 'A survey of data Mining and Machine Learning Methods for Cyber Security Intrusion Detection', DOI 10.1109/COMST.2015.2494502, IEEE Communications Surveys and Tutorials

(21) Λάζαρος Σ. Ηλιάδης (2008), Ευφυή Πληροφοριακά Συστήματα και Εφαρμογές στην Εκτίμηση Κινδύνου, Εκδοτικός Οίκος Ηρόδοτος

(22) Ν. Ματσατσίνης, 'Συστήματα Υποστήριξης Αποφάσεων', 2010, Εκδόσεις Νέων Τεχνολογιών

(23)http://www.euro2day.gr/specials/topics/article/1533763/aytoi-einai-oi-megalyteroi-kindynoi-gia-epiheirhse.html

(24) http://www.consilium.europa.eu/el/policies/cyber-security/

(25) https://repository.kallipos.gr/bitstream/11419/3382/1/02_chapter_04.pdf

(26)https://www.ibm.com/support/knowledgecenter/en/SSEPGG_9.5.0/com.ibm.im.easy.doc/c_dm_process.html

(27)http://www.cybersecurity-review.com/industry-perspective/applying-machine-learning-to-advance-cyber-security-analytics/

(28) T.T.T Nguyen, and G.Armitage, "A survey of techniques for internet traffic classification using machine learning", IEEE Communications Surveys and Tutorials, no 4, 2008 pp 56-76

(29) P.Garci-Teodoro, J.Diaz-Verdejo, "Anomaly based network intrusion detection: Techniques, systems and challenges", Computers & security 28, no. 1, 2009, pp. 18-28

(30) J.Cannady "Artificial neural networks for misuse detection". Procceedings of the

1998 National Information System Security Conference, Arlinghton VA, 1998 pp 443-456

(31) Richard P.Lippman, Robert Cunningham, "Improving intrusion detection performance using keyword selection and neural networks", Computer Networks 34 (2000) 597-603

(32) Bivens, C.Palagiri "Network based intrusion detection using neural networks", Intelligent Engineering Systems Through Artificial Neural Networks 12 (1), 2002, pp. 579-584

(33) R.Agrawal, T.Imielinski, and A.Swami, "Mining association rules between sets of items in large databases", Procceedings of the International Conference on Management of Data, Association for Computing Machinery, 1993, pp. 207-216

(34) L.Zadeh, "Fuzzy Sets", Information and Control, 8 (3), 1965, pp.335-35

(35) H.Brahmi, B.Imen and B.Sadok, "OMC-IDS: at the cross-roads of OLAP mining and intrusion detection", Advances in Knowledge Discovery and Data Mining, Springer Berlin Heidelberg, 2012

(36) C. Livadas, R. Walsh, D. Lapsley, and W. Strayer, "Using machine learning techniques to identify botnet traffic," Proceedings of the 31st IEEE Conference on Local Computer Networks, IEEE, 2006

(37) C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. "Bayesian event classification for intrusion detection," Proceedings of Computer Security Applications Conference. 19th Annual. IEEE, 2003

(38) K. Jain and R. C. Dubes, Algorithms for Clustering Data, Prentice- Hall, 1988

(39) R. Hendry and S. J. Yang, "Intrusion signature creation via clustering anomalies," SPIE Defense and Security Symposium, International Society for Optics and Photonics, 2008

(40) M. Blowers and J. Williams, "Machine Learning Applied to Cyber Operations," Network Science and Cybersecurity, Springer New York, 2014, pp. 55–175

(41) K. Sequeira and M. Zaki, "ADMIT: anomaly-based data mining for intrusions," Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2002

(42) R. Quinlan, "Induction of decision trees," Machine Learning, 1 (1), 1986, pp. 81–106

(43) R. Quinlan, C4.5: Programs for Machine Learning, Morgan Kaufmann Publishers, 1993

(44) C. Kruegel and T. Toth, "Using decision trees to improve signature- based intrusion detection," Proceedings of the 6th International Workshop on the Recent Advances in Intrusion Detection, West Lafayette, IN, 2003, pp. 173–191

(45) Snort 2.0, Sourcefire (http://www.sourcefire.com/technology/whitepapers.htm) [accessed June 2014]

(46) Y. Li, J. Xia, S. Zhang, J. Yan, X. Ai, and K. Dai, "An efficient intrusion detection system based on support vector machines and gradually feature removal method," Expert Systems with Applications, 39 (1), 2012, pp. 424–430

(47) F. Amiri, M. Mahdi, R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual information-based feature selection for IDSs," Journal of Network and Computer Applications, 34 (4), 2011, pp. 1184–1199

(48) https://www.cs.waikato.ac.nz/ml/weka/Witten_et_al_2016_appendix.pdf

(49) Chinotec Technologies Company: Paros - for web application security assessment. http://www.parosproxy.org/index.shtml (2004)

(50) Andrıs Riancho: Web Application Attack and Audit Framework. http://w3af.sourceforge.net (2007)

(51) https://www.cs.waikato.ac.nz/ml/weka/arff.html

(52) Sara Althubiti "Analysing HTTP Requests for web intrusion detection", 2017

(53) Nguyen, "Application of the generic feature selection measure in detection of web attacks", 2011

(54) Gallagher, "Classification of HTTP attacks, study on the ECML/PKDD 2007 discovery challenge", 2009

(55) Pham, "Machine learning techniques or web intrusion detection", 2016