



ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

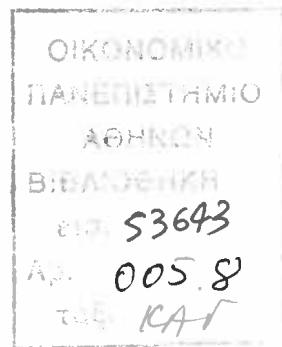
«Ενοποίηση τεχνικών Συμπερασματολογίας μέσω
Υποθέσεων (Case-based Reasoning) σε Συστήματα
Ανίχνευσης Εισβολών»

Καγιαμπάκης Μιχάλης
M3950011

ΑΘΗΝΑ, ΣΕΠΤΕΜΒΡΙΟΣ 1997



**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**«Ενοποίηση τεχνικών συμπερασματολογίας μέσω
υποθέσεων (Case-based Reasoning) σε συστήματα
ανίχνευσης εισβολών»**

Καγιαμπάκης Μιχάλης

M3950011

Επιβλέπων Καθηγητής: Ευάγγελος Κιουντούζης



Στρατηγικός Τομέας: Επιχειρησιακή Κληρονομιά



KATALOGOS

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΕΠΙΧΕΙΡΗΣΗΣ

Επίκουρη Καθηγητής

Επίκουρη Καθηγητής (Επίκουρη Καθηγητής)

Επίκουρη Καθηγητής (Επίκουρη Καθηγητής)

ΕΠΙΧΕΙΡΗΣΗΣ ΚΛΗΡΟΝΟΜΙΑΣ

Επίκουρη Καθηγητής	Επίκουρη Καθηγητής

ΕΠΙΧΕΙΡΗΣΗΣ ΚΛΗΡΟΝΟΜΙΑΣ
ΕΠΙΧΕΙΡΗΣΗΣ ΚΛΗΡΟΝΟΜΙΑΣ



ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον επιβλέπον καθηγητή μου κ. Ευάγγελο Κιουντούζη για την πολύτιμη βοήθειά του. Τον καθηγητή μου κ. Γκρίζαλη για τις χρήσιμες παρατηρήσεις και συμβουλές του για την ολοκλήρωση της εργασίας. Τον υποψήφιο διδάκτορα Σπύρο Κοκολάκη για τις εύστοχες παρατηρήσεις, τις συμβουλές και την καθοδήγησή του σε όλη τη διάρκεια της εργασίας. Επίσης, τον Θωμά Σπύρου από το Πανεπιστήμιο του Αιγαίου για τις συμβουλές του και την παραχώρηση χρήσιμων εγγράφων του SECURENET.

ΛΙΣΤΑ ΕΙΚΟΝΩΝ.....	4
ΛΙΣΤΑ ΠΙΝΑΚΩΝ.....	5
ΠΕΡΙΛΗΨΗ.....	6
ENGLISH ABSTRACT	13
1. ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ.....	18
 1.1 Εισαγωγή	18
1.1.1 Ανίχνευση Εισβολών	18
1.1.1.1 Anomaly detection.....	20
1.1.1.2 Misuse detection.....	21
1.1.2 Ορολογία.....	22
 1.2 Αρχές ασφάλειας σε υπολογιστικά περιβάλλοντα	22
1.2.1 Εκτίμηση Κινδύνων (Risk Assessment)	22
1.2.2 Ανάλυση Κόστους - Οφέλους (Cost Benefit Analysis).....	23
1.2.3 Πολιτική Ασφαλείας (Security Policy).....	23
1.2.4 Γιατί είναι αναγκαία η χρήση συστημάτων ανίχνευσης εισβολών.	24
 1.3 Τεχνικές - μεθοδολογίες ανίχνευσης εισβολών.....	25
1.3.1 Εισαγωγή	25
1.3.2 Χαρακτηριστικά ενός καλού IDS	25
1.3.3 Ένα Μοντέλο ανίχνευσης εισβολών	27
1.3.4 Τρόποι αξιολόγησης της αποτελεσματικότητας ενός IDS	29
1.3.5 Anomaly Intrusion Detection.....	29
1.3.5.1 Τεχνικές στατιστικής ανάλυσης	29
1.3.5.2 Νευρωνικά Δίκτυα	30
1.3.5.3 User Intention Identification	34
1.3.5.4 Χρήση αυτόνομων (autonomous) agents	36
1.3.5.5 Χρήση γράφων (GrIDS - Graph based Intrusion Detection System)	38
1.3.6 Misuse Intrusion Detection	40
1.3.6.1 Εμπειρια συστήματα	40
1.3.6.2 Pattern Matching.....	42
1.3.6.3 Model - based Intrusion Detection.....	44
1.3.7 Επισκόπηση	45
 1.4 Παραδείγματα Συστημάτων Ανίχνευσης Εισβολών.....	46
1.4.1 Εισαγωγή	46
1.4.2 IDES (Intrusion Detection Expert System).....	46
1.4.3 SECURENET	48
1.4.4 Network Security Monitor (NSM)	52
1.4.4.1 Αρχιτεκτονική του NSM	53
1.4.4.2 Ανίχνευση Παρεισφρητικής Συμπεριφοράς στο NSM	53
1.4.5 Επισκόπηση	54
 1.5 Γενική κριτική Συστημάτων Ανίχνευσης εισβολών	54
1.5.1 Συμπεράσματα	59
2. ΣΥΜΠΕΡΑΣΜΑΤΟΛΟΓΙΑ ΜΕΣΩ ΥΠΟΘΕΣΕΩΝ - CASE BASED REASONING	60
 2.1 Εισαγωγή	60
 2.2 Γενικά για CBR.....	60
 2.3 Η ανάγκη για CBR	61
 2.4 Ο Case base Reasoner.....	61
 2.5 Cases.....	62
2.5.1 Τι είναι τα cases	62
2.5.2 Από τι αποτελούνται τα cases	63

2.6 Case Library - Experience	63
2.7 Βασικός τρόπος λειτουργίας του CBR	64
2.8 Ο κύκλος του CBR	65
2.8.1 Retrieve	68
2.8.2 Reuse	69
2.8.3 Revise	70
2.8.4 Retain - Learning	70
2.9 Case Based Συστήματα	71
2.9.1 Εφαρμογές που έχει χρησιμοποιηθεί το CBR	72
2.9.2 Παρατηρήσεις κατά τη διαδικασία ανάπτυξης CBR συστημάτων	73
2.10 Case-Based Reasoning VS Analogical Reasoning	74
2.11 Διαφορές Case Based Reasoning με Expert Systems	74
2.12 Δυνατότητες ενοποίησης στο CBR	77
2.13 Προσδοκίες από τον τομέα των CBR συστημάτων	79
2.14 Συμπεράσματα	80
3. ΕΝΟΠΟΙΗΣΗ CBR ΤΕΧΝΙΚΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ82	
3.1 Εισαγωγή	82
3.2 Περιγραφή του χώρου	82
3.3 Γιατί χρήση CBR?.....	84
3.4 Αρχιτεκτονική του Συστήματος	85
3.5 Περιγραφή υπάρχοντος IDS	87
3.5.1 Περιγραφή Decision Module στο Securenet	87
3.5.2 Παράδειγμα σεναρίου εισβολής.....	90
3.5.3 Δυνατότητες βελτίωσης	92
3.6 Εφαρμογή του προτεινόμενου συστήματος στο SECURENET	94
3.6.1 Οργάνωση της βάσης γνώσης	94
3.6.2 Απόδοση βαρών	96
3.7 Υλοποίηση του Συστήματος	98
3.7.1 Προσδιορισμός των cases που θα αποτελέσουν τη βάση γνώσης	98
3.7.2 Επιλογή CBR Shell.....	100
3.7.3 Στοιχεία απόδοσης του συστήματος	101
4. ΕΡΕΥΝΗΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ	103
5. ΕΠΙΣΚΟΠΗΣΗ	107
6. ΒΙΒΛΙΟΓΡΑΦΙΑ	108
7. ΠΑΡΑΡΤΗΜΑ	113

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

Εικόνα 1. Γενική αναπαράσταση του μοντέλου ανίχνευσης εισβολών	28
Εικόνα 2. Ένα τυπικό νευρώνιο	31
Εικόνα 3. Αρχιτεκτονική πολλών επιπέδων.....	32
Εικόνα 4. Χρήση νευρωνίου για την πρόβλεψη της επόμενης εντολής του χρήστη	33
Εικόνα 5. ΗΠ αρχιτεκτονική.....	35
Εικόνα 6. Γενική Agent - based Αρχιτεκτονική ενός IDS	37
Εικόνα 7. Ο τρόπος εξάπλωσης ενός προγράμματος σκούληκιού σε ένα δίκτυο	39
Εικόνα 8. Αφαιρετική αναπαράσταση που χρησιμοποιεί η GrIDS τεχνική.....	40
Εικόνα 9. Αναπαράσταση γεγονότων που οδηγούν σε αλλαγή καταστάσεων, στην τεχνική pattern matching.	43
Εικόνα 10. Οι δομικές λειτουργικές ενότητες του SECURENET.....	48
Εικόνα 11. Τεχνολογίες που χρησιμοποιούνται στις διάφορες ενότητες του SECURENET.....	49
Εικόνα 12. Γενική αρχιτεκτονική του SECURENET	50
Εικόνα 13. Γενική απεικόνιση του έμπειρου συστήματος στο SECURENET.....	51
Εικόνα 14. Η επικοινωνία των οντοτήτων του SECURENET με το σύστημα λήψης αποφάσεων.....	52
Εικόνα 15. Ο τρόπος οργάνωσης του χώρου προβλημάτων στο CBR	65
Εικόνα 16. Ο κύκλος του CBR	66
Εικόνα 17. Μια άλλη παράσταση του κύκλου του CBR	67
Εικόνα 18. Μια task - oriented περιγραφή του CBR.	68
Εικόνα 19. Μια (sub)task - oriented περιγραφή της Retrieve λειτουργίας.....	68
Εικόνα 20. Μια (sub)task - oriented περιγραφή των Reuse, Revise και Retain λειτουργιών	68
Εικόνα 21. Ταξινόμηση των Συστημάτων σχετικά με την ποσότητα γνώσης του χώρου προβλημάτων που καλούνται να καλύψουν	78
Εικόνα 22. Τρόποι κάλυψης του problem domain και η σχέση τους με τις Knowledge-based τεχνικές.....	79
Εικόνα 23. Παράσταση των σημαντικότερων μονάδων σε ένα σύστημα IDS	83
Εικόνα 24. Αρχιτεκτονική του νέου συστήματος.....	85
Εικόνα 25. Η επικοινωνία των οντοτήτων του SECURENET με το σύστημα λήψης αποφάσεων.....	88
Εικόνα 26. Βήματα εκτέλεσης του CBR κύκλου.	96
Εικόνα 27. Ενοποίηση τεχνικών CBR με συστήματα DBMS	105
Εικόνα 28. Χρήση τεχνικών CBR για Anomaly Detection.....	106
Εικόνα 29. Χρήση τεχνικών CBR για Misuse Detection	107

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΠΕΡΙΛΗΨΗ

Πίνακας 1. Αποτελέσματα χρήσης agents στην ανίχνευση εισβολών.....	38
Πίνακας 2 Συγκριτική παρουσίαση γνωστών συστημάτων ανίχνευσης εισβολών	58
Πίνακας 3. Αντιστοίχηση συστημάτων διαχείρισης γνώσης σε σχέση με την ποσότητα γνώσης και εμπειρίας του χώρου.....	76
Πίνακας 4. Μήνυμα από ES, NN, UII προς το DM.....	88
Πίνακας 5. Μήνυμα από το DM στο CM	89
Πίνακας 6. Attack Classes.	89
Πίνακας 7. Μήνυμα από το ES στο DM.....	90
Πίνακας 8. Μήνυμα από το DM στο CM.	91
Πίνακας 9. Μήνυμα από το CM προς τον SO	91
Πίνακας 10. Κατάλογος αντιμέτρων.....	92
Πίνακας 11. Αντιστοίχηση βαρών στα χαρακτηριστικά του case	97

Δείτε παρακάτω την απότομη διεύθυνση, για την εύρεση μη φυσιολογικής, μη προβλευμένης ανεπιφρούδης των χρηστών. Παραπρέονται οι κυριότερες του χρήστη, προκειμένου να πετύχεισσον στοιχεία με τα οποία μπορεί να χαρακτηριστεί η φυσιολογικότητα των ως μη φυσιολογικής στοιχείων της δρους της ίδιας ανεπιφρούδης των. Με την γνωστική που γνωστοποιούνται μέσω της σύστημα να αντέχει εάν η σύμπεριφορά του χρήστη περιοριστεί ή διακρίνεται από την κανονική του ή όχι από μόνες εντός των είδη ανεπιφρούδης. Εάν κάποιος μαζεύει δημόσια πληροφορία τη συνθηματικό κίνηση χρήστη, οι κτερύγει του χρήστη διαφέρουν από εάν εν γένει ανεπιφρούδη του και το σύστημα διέρκεστερίζει τη συμπελοφόρα με αύξηση ανεπιφρούδης.

Για την απότομη διεύθυνση, οι σημαντικότερες από τις γενικές είναι τα διαδικτικά αποτελέσματα, αποτελητή (μητρική) στατιστικές προβλ. ανεπιφρούδη, γενεντικά δίκτυα (για την εργάζοντας των μελλοντικών κανήσων των χρηστών), μέθοδοι ανεπιφρούδης των προβλημάτων των χρηστών (για την ανακάλυψη σε αυτές κοινόβιων διαθέσιμων), πολύγραμμη προσίσ (για παρακολούθηση της κίνησης των δικτύων για εγγυημένη παρακολούθηση της παραμορφωσής), χρήση γρίφων (για ανίχνευση πιθανών απορροφήσις από μεγάλης κλίμακας διεπιπλώσεις).

Η διεύθυνση βασική λειτουργία των δικτύων είναι η παραγωγή δείγματος. Το σύστημα δικτύων σε αύξηση περιεχομένων προσβαλλές με στούς, έχουν ήδη εμφανιστεί. Είναι από τα πιο διαχειρίσιμα, των για την εποπτεία των χρήστη κάποιο γνωστή περίπτωση απόστρησης και αδυνατεί την διεργασία παραδόσεως για την μεταβολή των αξέλοπτρων. Το περιεχόμενο των ταξυδιών είναι στις διανομές να ανησυχήσουν για την επιβολή, εδώ πάντα κατέβασης σε στούς είναι ήδη καταχωρισμένη από την γενεντική των παραπάνω, η οποία αποτελεί συντριγή αναθεορησης και αποτύπωσης, την να καθίσταση της κακονομέρης, απορροφή.

Για την απότομη διεύθυνση χρητικοποιούνται έπειρα συστήματα δύναμες των συστημάτων πληροφρούρων γνωστής πεντητού επιπλόδου, ταχυτικές βασισμένες σε προσδιόρισμα τεκοντούστη ως αποδινήματα (grasses) γνωστές παραγόντες απεριβάλλοντας μετώπους πολλαπλών απελάσης (όπου βρισκούνται μονάδα με τις γνωστής μεταβολή).

ΠΕΡΙΛΗΨΗ

Τα συστήματα ανίχνευσης εισβολών αποτελούν ένα μέρος από τις στρατηγικές ασφαλείας που μπορεί να εφαρμόσει ένας οργανισμός στα πλαίσια των πολιτικών ασφαλείας θέτει. Η ολοένα αυξανόμενη ανάπτυξη αυτοματοποιημένων συστημάτων επεξεργασίας πληροφοριών από τους οργανισμούς, αυξάνει συνεχώς την ανάγκη για προστασία των πληροφοριών τις οποίες επεξεργάζονται, από τις κακόβουλες διαθέσεις εισβολέων. Η χρήση των δικτύων υπολογιστών αυξάνει συνεχώς. Ο αριθμός των διασυνδεδεμένων πληροφοριακών συστημάτων ολοένα και μεγαλώνει. Αυτό καθιστά την ανάγκη για αποδοτικά IDS ακόμα μεγαλύτερη, προκειμένου να εντοπίζουν έγκαιρα την ύπαρξη εισβολέων και να καταστείλουν τις προσπάθειες παρείσφρησης στο σύστημα και τις πληροφορίες του οργανισμού.

Τα IDS αποτελούν πολύπλοκα συστήματα τα οποία υλοποιούν δύο κύριες λειτουργίες. Την *anomaly detection*, για την εύρεση μη φυσιολογικής, μη προβλέψιμης συμπεριφοράς των χρηστών. Παρατηρούνται οι κινήσεις του χρήστη, προκειμένου να αντληθούν στοιχεία με τα οποία μπορεί να χαρακτηριστεί η συμπεριφορά του ως μη φυσιολογική, σε όρους της εν γένη συμπεριφοράς του. Με τεχνικές που χρησιμοποιούνται μπορεί το σύστημα να αντιληφθεί εάν η συμπεριφορά του χρήστη παρουσιάζει διακυμάνσεις από την κανονική του ή εάν οι επόμενες κινήσεις του είναι αναμενόμενες. Εάν κάποιος εισβολέας έχει «κλέψει» το συνθηματικό κάποιου χρήστη, οι κινήσεις του χρήστη διαφέρουν από την εν γένει συμπεριφορά του και το σύστημα χαρακτηρίζει την συμπεριφορά ως πιθανά παρεισφρητική.

Για την *anomaly detection*, οι σημαντικότερες από τις τεχνικές είναι τεχνικές στατιστικής ανάλυσης (διατήρηση στατιστικών προφίλ συμπεριφοράς), νευρωνικά δίκτυα (για την πρόβλεψη των μελλοντικών κινήσεων των χρηστών), μέθοδοι ανακάλυψης των προδιαθέσεων των χρηστών (για την ανακάλυψη σε αυτές κακόβουλων διαθέσεων), αυτόνομοι agents (για παρακολούθηση της κίνησης του δικτύου για την ανίχνευση παράτυπης συμπεριφοράς), χρήση γράφων (για ανίχνευση εισβολών σε μεγάλης κλίμακας δικτυακά περιβάλλοντα.).

Η δεύτερη βασική λειτουργία των IDS είναι η *misuse detection*. Το σύστημα πρέπει να είναι ικανό να αντιλαμβάνεται εισβολές οι οποίες έχουν ήδη εμφανιστεί. Είναι ενήμερο από τους διαχειριστές του για ήδη γνωστά σενάρια εισβολών. Με τις τεχνικές που ενσωματώνει μπορεί να διαπιστώσει στις κινήσεις του χρήστη κάποιο γνωστό σενάριο εισβολής και ειδοποιεί τον διαχειριστή ασφαλείας για την εισβολή που εξελίσσεται. Το μειονέκτημα των τεχνικών είναι ότι δεν μπορούν να ανακαλύψουν νέες εισβολές, αλλά μόνοι εκείνες οι οποίες είναι ήδη καταχωρημένες στη βάση γνώσης του συστήματος, η οποία απαιτεί συνεχή αναθεώρηση και ανανέωση, για να καλύπτει και τις καινούργιες εισβολές.

Για την *misuse detection* χρησιμοποιούνται έμπειρα συστήματα (στους κανόνες των οποίων περιγράφονται γνωστά σενάρια εισβολών), τεχνικές βασισμένες σε υποδείγματα (όπου κρατούνται σε υποδείγματα (patterns) γνωστές υπογραφές εισβολών) και μοντέλα παλαιότερων απειλών (όπου δημιουργούνται μοντέλα με τις γνωστές εισβολές)

Το μοντέλο της Denning αποτελεί ορόσημο για την γνωστική περιοχή των IDS. Είναι ανεξάρτητο τεχνολογικής πλατφόρμας, περιβάλλοντος εφαρμογής και ευπαθειών, Σε αυτό στηρίχθηκαν πολλά από τα γνωστά συστήματα ανίχνευσης εισβολών. Κάνει διαχωρισμό των στοιχείων του συστήματος σε υποκείμενα, *antikeímena*, *audit records*, *proφíl*, *anomaly records* και *activity rules*. Τα υποκείμενα επενεργούν στα *antikeímena*. Το σύστημα κατακρατεί πληροφορίες για τη δράση αυτή σε εγγραφές (*audit records*). Από την μελέτη των εγγραφών αυτών δημιουργούνται προφίλ συμπεριφοράς για κάθε χρήστη (*anomaly detection*). Η σύγκριση με παλαιότερες τιμές οδηγεί στο συμπέρασμα εάν η συμπεριφορά είναι ανώμαλη σε σχέση με την στατιστικά προβλεπόμενη. Εάν παρουσιαστεί ανωμαλία, αυτή καταγράφεται σε *anomaly records*. Από την άλλη υπάρχουν *activity rules* (*misuse detection*), οι οποίοι εάν ικανοποιηθούν συνθήκες (παρουσιαστεί στις κινήσεις του χρήστη κάποιο γνωστό σενάριο εισβολής) εκτελούνται για την άμεση καταστολή της εισβολής.

Ένα από τα βασικά χαρακτηριστικά που πρέπει ικανοποιεί το IDS είναι η ικανότητά του να ελαχιστοποιεί τα *false negatives* σφάλματα. Η κατηγοριοποίηση μιας συμπεριφοράς ως παρεισφρητικής ενώ αυτή δεν είναι (*false positive*), είναι λιγότερο επικίνδυνη από τον χαρακτηρισμό της συμπεριφοράς ως φυσιολογικής ενώ αυτή είναι παρεισφρητική (*false negative*). Επιπλέον, η απόδοση του IDS στηρίζεται και σε άλλους παράγοντες. Πρέπει να «τρέχει» διαρκώς, με την ελάχιστη δυνατή ανθρώπινη παρακολούθηση. Να είναι ανεκτικό σε παραβιάσεις των στοιχείων που παρακολουθεί, αλλά και των ίδιων των μηχανισμών που ενσωματώνει. Να είναι οικονομικό, σπαταλώντας τους ελάχιστους δυνατόν πόρους από το σύστημα. Πρέπει να εκδίδει συναγερμούς *real time* ή *τάξεως real time*, να μπορεί να λειτουργήσει με λίγες αλλαγές σε διαφορετικά περιβάλλοντα και να χαρακτηρίζεται από την ευκολία στη συντήρηση της βάσης γνώσης του.

Ο τομέας των συστημάτων ανίχνευσης εισβολών είναι αρκετά ζωντανός. Ειδικό βάρος παίζει η γρήγορη ανάπτυξη των δικτυακών υπηρεσιών. Παρόλο που τα IDS έχουν δείξει ενδιαφέροντα στοιχεία στην ανίχνευση εισβολών συγκεκριμένων κατηγοριών, ωστόσο είναι αλληλένδετα με την αρχιτεκτονική στην οποία έχει στηριχθεί η ανάπτυξή τους. Λείπει γενική μεθοδολογία κατασκευής τους, δεν μπορούν να εξαχθούν χρήσιμα στοιχεία για την αποδοτικότητά τους, χαρακτηρίζονται από δυσκολία στη συντήρησή τους.

Επιτακτική εμφανίζεται η ανάγκη για συστήματα ανίχνευσης εισβολών τα οποία θα είναι πιο ευέλικτα, και δυναμικά, θα αναφέρονται σε συστήματα μικρότερης κλίμακας, θα χαρακτηρίζονται από ευκολία εκμάθησης και χειρισμού. Τα έμπειρα συστήματα, οι στατιστικές τεχνικές και οι περισσότερες από τις τεχνικές που χρησιμοποιούνται για τον αρχικό προσδιορισμό της πιθανότητας ύπαρξης απειλής, έχουν ήδη εφαρμοστεί, ενώ αποτελούνται από προκαθορισμένες διαδικασίες και τρόπους ελέγχου των δεδομένων εισόδου τους, που καθιστούν τις λειτουργίες τους λίγο ως πολύ τυποποιημένες. Το έμπειρο σύστημα θα εκφράσει την πιθανότητα ένας χρήστης να ακολουθεί κάποια ήδη γνωστή συμπεριφορά, το νευρωνικό δίκτυο (πιο πολύπλοκα, αλλά και αυτό) θα μπορέσει να εκφράσει κάποιον βαθμό πιθανότητας σχετικά με τη «φυσιολογικότητα» των κινήσεων των χρηστών. Η τελική επιλογή όμως έγκειται στο DM να αποφασίσει εάν όντως πραγματοποιείται μια απειλή και ποια είναι τα κατάλληλα αντίμετρα για την αντιμετώπισή της. Η διεπαφή με το

διαχειριστή ασφαλείας (security officer, SO) είναι σίγουρα απαραίτητη για την λήψη της τελικής απόφασης, αλλά αυτή η επικοινωνία καλό θα ήταν να είναι η λιγότερη δυνατή μιας και εκ των προτέρων είναι δύσκολη σε ένα real time σύστημα. Η ολοένα και περισσότερη απεμπλοκή του SO από την διαδικασία λήψης απόφασης σχετικά με τα αντίμετρα που πρέπει να εφαρμοστούν, είναι επιθυμητή, λόγω του μεγάλου φόρτου εργασίας που γενικά αντιστοιχεί σε αυτόν.

Με αυτή τη διατριβή προτείνουμε την ενσωμάτωση τεχνικών συμπερασματολογίας μέσω υποθέσεων (Case-Based Reasoning, CBR) σε συστήματα ανίχνευσης εισβολών. Τα αποτελέσματα φαίνονται αισιόδοξα για την αποδοτικότερη λειτουργία των μηχανισμών συμπερασματολογίας των συστημάτων αυτών. Η ενσωμάτωση τεχνικών CBR έγινε στο υποσύστημα λήψης αποφάσεων των συστημάτων ανίχνευσης εισβολών, τα οποία στόχο έχουν την επιλογή του καλύτερου συνόλου αντιμέτρων, για την αντιμετώπιση της εμφανιζόμενης απειλής. Καταγράφονται προτάσεις για μελλοντική ενσωμάτωση των CBR τεχνικών και σε άλλα υποσυστήματα των IDS, καθώς και τους τρόπους επικοινωνίας με τα υπόλοιπα υποσυστήματα.

Η συμπερασματολογία μέσω υποθέσεων (CBR), αποτελεί νέο paradigm για την Τεχνητή Νοημοσύνη. Η συμπερασματολογία στο CBR δεν μοντελοποιείται ως μια διαδικασία στην οποία τα συμπεράσματα απορρέουν από την αλυσιδωτή έναρξη κανόνων, όπως συμβαίνει στα συμβατικά rule-based συστήματα. Στο CBR η γνώση δεν είναι αποθηκευμένη σε κανόνες, αλλά σε cases τα οποία είναι οργανωμένα με κατάλληλες δομές στη μνήμη (συνήθως δένδρα). Λύσεις σε προτεινόμενα προβλήματα δίνονται όχι με την αλυσιδωτή εκτέλεση κανόνων, αλλά με την ανάκτηση των περισσότερων σχετικών (relevant) cases και υιοθέτηση μιας λύσης για την αντιμετώπιση της προβληματικής κατάστασης. Στο CBR η συμπερασματολογία βασίζεται στην «ενθύμηση» (remembering).

Το CBR στηρίζεται σε δύο θεμελιώδη αξιώματα. Αρχικά θεωρείται ότι ο κόσμος χαρακτηρίζεται από μια κανονικότητα: σε παρόμοια προβλήματα αντιστοιχούν παρόμοιες λύσεις. Συνεπώς λύσεις σε προβλήματα που έχουν ήδη παρουσιαστεί αποτελούν καλές υποδείξεις για τη χρήση τους σε νέα παρόμοια προβλήματα που παρουσιάζονται. Η δεύτερη θεμελιώδης αρχή αναφέρεται στην πιθανότητα με την οποία συγκεκριμένοι τύποι προβλημάτων τείνουν να ξαναπαρουσιάζονται. Με αυτόν τον τρόπο μελλοντικά προβλήματα ίσως μοιάζουν με τα προβλήματα που ήδη έχουν εμφανιστεί και γνωρίζουμε τις λύσεις τους.

Το βασικό χαρακτηριστικό στο CBR είναι η ικανότητα για μάθηση. Μπορεί να μάθει για την αποτελεσματικότητα συγκεκριμένων λύσεων, τις οποίες να εφαρμόσει σε συγκεκριμένο χώρο προβλημάτων, όσο και για την ανικανότητα κάποιων άλλων προκειμένου να μην ακολουθήσει την ίδια διαδρομή συμπερασματολογίας. Επίσης, έχει τη δυνατότητα να προτείνει γρήγορα λύσεις, και μάλιστα σε περιοχές προβλημάτων τα οποία είναι δύσκολο να μοντελοποιηθούν. Η χρήση των cases αποτελεί γενικά αποτελεσματικότερο τρόπο για την παράσταση της γνώσης σχεδόν σε όλους τους χώρους προβλημάτων.

Συστατικό στοιχείο στο CBR είναι το case: «ένα κομμάτι γνώσης το οποίο αναπαριστά εμπειρία πάνω σε συγκεκριμένο γνωστικό τομέα, αποτελεί θεμελιώδες στοιχείο εκμάθησης από το *reasoner* για την υλοποίηση των στόχων του». Τα cases αναπαριστούν την εμπειρία του Reasoner για την συγκεκριμένη γνωστική περιοχή. Το σύνολο των cases αποτελούν τη βάση γνώσης (Case Base) για τον συγκεκριμένο χώρο προβλημάτων. Με την εμφάνιση ενός νέου προβλήματος, επιχειρείται η εύρεση παρόμοιων στη βάση γνώσης. Από τα παρόμοια προβλήματα που έχουμε εντοπίσει μπορούμε να αναζητήσουμε τις λύσεις τις οποίες είχαμε υιοθετήσει για αυτά. Η λύση του πιο συναφούς με το νέο πρόβλημα είναι αυτή που θα επιλεγεί και στην οποία θα στηριχθεί η διαδικασία επίλυσης του νέου προβλήματος. Η λύση αυτή μπορεί να είναι εφαρμοστεί αυτούσια αλλά είναι πιθανό να απαιτείται μια διαδικασία αναπροσαρμογής της προκειμένου να ταιριάζει καλύτερα ως λύση στο νέο πρόβλημα. Αν καμία λύση δεν βρεθεί να ταιριάζει, τότε δημιουργείται ένα εξολοκλήρου καινούργιο case, το οποίο αποθηκεύεται στις δομές μνήμης που χρησιμοποιούνται.

Η διαδικασία της ανάκτησης αποτελεί την πρώτη λειτουργία του κύκλου του CBR. Στοχεύει στην εύρεση του πλησιέστερου case της βάσης γνώσης (source case) με εκείνου που έχει εμφανιστεί ως νέο πρόβλημα (target case). Απαιτούνται πολύπλοκες διαδικασίες για το φιλτράρισμα των πληροφοριών, το ξεδιάλεγμα των σημαντικότερων χαρακτηριστικών, την αντιστοίχηση βαρών σε αυτά, ο προσδιορισμός βαθμού διαφοροποίησης (discrimination value), κτλ. Αφού βρεθεί το case το οποίο φαίνεται να αποτελεί την αποτελεσματικότερη λύση, εισάγεται σε μια διαδικασία μετασχηματισμού. Πραγματοποιούνται αλλαγές από τον διαχειριστή της γνώσης, προκειμένου να ταιριάζει ακριβώς στο πρόβλημα που παρουσιάστηκε. Η λύση περνάει από μια διαδικασία αναθεώρησης, πριν εφαρμοστεί, (ιδίως όταν αποτύχει η εφαρμογή της) και αφού ελεγχθεί, δημιουργείται ένα καινούργιο case, το οποίο και αποθηκεύεται από το σύστημα μέσω των μηχανισμών εκμάθησης. Με την αύξηση του αριθμού των cases, αυξάνει και η «εμπειρία» του συστήματος για την έκδοση αποτελεσματικών λύσεων.

Η βασική διαφορά με τα παραδοσιακά συστήματα επεξεργασίας γνώσης, που βασίζονται σε rule-based συστήματα, είναι ότι τα τελευταία δεν χαρακτηρίζονται από την ιδιότητα της εκμάθησης. Οταν το έμπειρο σύστημα πρόκειται να αντιμετωπίσει ένα συγκεκριμένο πρόβλημα, το οποίο έχει ήδη εμφανιστεί σε προηγούμενη στιγμή, πρέπει να εκτελέσει τους ίδιους κανόνες που εκτελέστηκαν και πρωτύτερα, όσο πλήθος και εάν έχουν. Αυτό δεν συμβαίνει με το CBR, όπου και οι λύσεις οργανώνονται σε δομές για την άμεση εύρεσή και ανάκτησή τους.

Το CBR εκδίδει πάντα λύση, ενώ το έμπειρο σύστημα, αν δεν υπάρξουν οι κατάλληλες συνθήκες, μπορεί να μην οδηγηθεί σε λύση. Τα rule-based συστήματα μπορούν να αντεπεξέλθουν αποτελεσματικά σε προβληματικούς χώρους οι οποίοι είναι ακριβώς περιγράψιμοι και σαφώς ορισμένοι, σε αντίθεση με το CBR το οποίο μπορεί να αντεπεξέλθει σε όχι καλά μοντελοποιήσιμους χώρους. Γενικά το CBR ταιριάζει σε χώρους όπου υπάρχει μεγάλο ποσοστό εμπειρίας, ενώ τα rule - based σε χώρους όπου το ποσό της γνώσης είναι πολύ μεγάλο. Το CBR τοποθετείται ανάμεσα στους χώρους που καλύπτουν τα rule based συστήματα (που έχουν ως προϋπόθεση την ύπαρξη μεγάλου όγκου δεδομένων για την συμπερασματολογία τους) και στα «knowledge-limited» συστήματα, όπου η ποσότητα της προϋπάρχουσας γνώσης δεν

παίζει τόσο σημαντικό ρόλο) όπως τα νευρωνικά δίκτυα (neural networks), τα συστήματα αναγνώρισης υποδειγμάτων (pattern recognition), genetic algorithms.

Ενσωματώσαμε τεχνικές CBR σε σύστημα ανίχνευσης εισβολών, συγκεκριμένα στο υποσύστημα λήψης αποφάσεων, το οποίο επιλέγει το καλύτερο σύνολο αντιμέτρων για την καταστολή της εμφανιζόμενης απειλής. Οι τεχνικές CBR προσδίδουν μεγαλύτερη ευελιξία και αποτελεσματικότητα στην επιλογή των κατάλληλων κάθε φορά αντιμέτρων. Η επιλογή CBR τεχνικών κρίθηκε αναγκαία λόγω του εν γένη δύσκολα μοντελοποιήσιμου χώρου που καλύπτουν τα IDS. Σε τέτοιους χώρους συνθήκες επαναλαμβάνονται (παρόμοιες εισβολές παρουσιάζονται), λύσεις σε παρόμοιες τέτοιες εισβολές ξαναεφαρμόζονται. Με τη δυνατότητα εκμάθησης που ενσωματώνει μπορεί να δημιουργήσει νέα cases, τα οποία αποτελούν αντίμετρα για καινούργιες απειλές. Επίσης, το CBR εκδίδει πάντα λύση, ακόμα και αν αυτή φαίνεται ότι δεν είναι η βέλτιστη. Η γνώση δομείται πιο άμεσα με χρήση cases, ενώ τελικά η διεπαφή με τον διαχειριστή μειώνεται αισθητά.

Το νέο σύστημα δέχεται ως είσοδο τα αποτελέσματα που εκδίδονται από τα modules του IDS που πραγματοποιούν το anomaly και misuse detection. Οι έξοδοι από αυτά περνούν από μια διαδικασία φίλτραρίσματος και μετατρέπονται σε μορφή κατανοητή από το επόμενο τμήμα, το CBR Engine.

Το CBR Engine είναι υπεύθυνο για την πραγματοποίηση της συμπερασματολογίας με CBR, σχετικά με το ποια από τα αντίμετρα θα εφαρμοστούν, συγκρίνοντας τα νέα cases, όπως αυτά εισέρχονται από τη διαδικασία φίλτραρίσματος, με εκείνα που βρίσκονται αποθηκευμένα στην Case Base. Αναλαμβάνει τις διαδικασίες αναγνώρισης των σημαντικών χαρακτηριστικών (features) των cases που εισέρχονται για την δεικτοδότησή τους, με βάση κάποιο λεξικό όρων, χρήσιμο για τον προσδιορισμό των πιο σημαντικών χαρακτηριστικών. Μετά τον χαρακτηρισμό του νέου case, αναζητεί από την Case Base, με βάση τεχνικές μέτρησης της ομοιότητας των χαρακτηριστικών των cases, τα πλησιέστερα, τα οποία και θα χρησιμοποιήσει ως λύση για την αντιμετώπιση της απειλής. Τα cases που προκύπτουν από την αναζήτηση αυτή συγκρίνονται με το αρχικό, προκειμένου να προσδιοριστούν ομοιότητες και το περισσότερο όμοιο case κρατείται για χρησιμοποίησή του ως λύση. Ίσως είναι αναγκαία η τροποποίηση του επιλεγμένου case για να ταιριάζει ακριβώς στο νέο. Το ανακτημένο case αλλάζει προκειμένου να ταιριάζει στην νέα απειλή και είναι αυτό που τελικά θα επιλεγεί ως λύση. Προηγείται μια διαδικασία ελέγχου της νέας αυτής λύσης προκειμένου να διαπιστωθεί η αποτελεσματικότητά της στην αντιμετώπιση της απειλής. Ο έλεγχος αυτός μπορεί να αναφέρεται σε προσομοίωση του συστήματος με τη νέα λύση, από την οποία αντλούμε συμπεράσματα για την ορθότητά της, όταν αυτή θα εφαρμοστεί, σε επιθεώρηση από τον διαχειριστή ασφαλείας σχετικά την πιθανότητα επιτυχίας της.

Αν το νέο case εγκριθεί για την εφαρμογή του, μπορεί να δεικτοδοτηθεί και να αποθηκευθεί στην Case Base. Στην περίπτωση που αποτύχει να εφαρμοστεί, αποθηκεύονται στην Case Base οι λόγοι για την αποτυχία της λύσης, προκειμένου να ληφθούν υπόψιν σε μελλοντικές προσπάθειες επίλυσης, για να μην υποπέσει στα ίδια λάθη το σύστημα.

H Case Base , η βάση γνώσης η οποία χρησιμοποιεί το CBR Engine για την επιλογή των κατάλληλων κάθε φορά αντιμέτρων, αποτελείται από cases, που περιέχουν τις λύσεις - αντίμετρα για τις αντίστοιχες εισβολές που περιγράφουν. Τα cases - αντίμετρα είναι δεικτοδοτημένα έτσι ώστε να επιτυγχάνεται γρήγορη εύρεση, τροποποίηση αλλά και τοποθέτηση νέων όταν κρίνεται αναγκαίο.

Σε κάθε ένα από τα πεδία - μεταβλητές του case, αντιστοιχεί ένα βάρος (weight). Με τα βάρη υπολογίζεται η ομοιότητα των cases με το νεοεμφανιζόμενο και επιλέγονται εκείνα που η συνολικός βαθμός ομοιότητας είναι μεγαλύτερος.

Τέλος ο διαχειριστής ασφαλείας παρακολουθεί τη λειτουργία του συστήματος μέσω εύχρηστης διεπαφής, Μπορεί να ελέγχει το περιεχόμενο των αντιμέτρων που εκδίδονται, τις λύσεις πριν αυτές υλοποιηθούν, να δημιουργεί νέα cases, να τροποποιεί γενικά την Case Base, καθώς και να αντλεί στατιστικές πληροφορίες για την λειτουργία του συστήματος.

Περιγράφουμε πως μπορεί να εφαρμοστεί σε ένα υπάρχον σύστημα ανίχνευσης εισβολών. Για το σκοπό αυτό επιλέχθηκε το SECURENET, το οποίο, αφού περιγράφεται, με έμφαση το σύστημα λήψης αποφάσεων και επιλογής αντιμέτρων, διακρίνονται οι αδυναμίες και τα μειονεκτήματά του, περιγράφονται οι δυνατότητες βελτίωσης με το νέο σύστημα που υιοθετούμε. Επιλέγεται ένα CBR εργαλείο για το σκοπό αυτό, και αφού εισαχθούν μερικά cases, γίνεται προσπάθεια αξιολόγησής του σε επίπεδο προσομοίωσης, μιας και είναι δύσκολη η αξιολόγησή του σε πραγματικό περιβάλλον, και σε τάξη πολυπλοκότητας των αλγορίθμων που χρησιμοποιούνται.

Τέλος παρατίθενται ερευνητικές προτάσεις στον τομέα του CBR, αλλά και στον τομέα των συστήματα ανίχνευσης εισβολών με ενσωμάτωση CBR τεχνικών. Καταγράφονται προτάσεις για την χρησιμοποίηση του CBR για misuse και anomaly detection, σε συνδυασμό και με άλλες τεχνικές όπως Νευρωνικά δίκτυα.

Το πρώτο κεφάλαιο αναφέρεται στις γενικές αρχές της ανίχνευσης εισβολών. Περιγράφονται συνοπτικά οι αρχές που πρέπει να διέπουν τα υπολογιστικά συστήματα όσον αφορά την ασφάλεια. Δίνονται οι βασικοί ορισμοί της ανίχνευσης εισβολών, των όρων και βασικών στοιχείων που διέπουν την συγκεκριμένη περιοχή. Αναλύονται οι πιο γνωστές τεχνικές - μεθοδολογίες ανίχνευσης. Γίνεται παράθεση των σημαντικότερων συστημάτων ανίχνευσης εισβολών που έχουν ήδη αναπτυχθεί. Τέλος προχωρούμε σε γενική κριτική των συστημάτων και συμπεράσματα.

Στο δεύτερο κεφάλαιο παρουσιάζονται οι γενικές αρχές της συμπερασματολογίας μέσω υποθέσεων (Case-Based Reasoning). Μετά την περιγραφή των βασικών αρχών, των cases, του τρόπο που λειτουργεί ο reasoner, γίνεται αναλυτική περιγραφή του κύκλου του CBR. Αναφέρονται γνωστά συστήματα που έχουν αναπτυχθεί με χρήση CBR, γίνεται σύγκριση με άλλους τρόπους συμπερασματολογίας και παρουσιάζονται προσδοκίες για την νέο αυτό κλάδο της Τεχνητής Νοημοσύνης.

Στο τρίτο και τελευταίο μέρος γίνεται προσπάθεια εφαρμογής των CBR τεχνικών στον τομέα των συστημάτων ανίχνευσης εισβολών. Προτείνονται ένα γενικευμένο σύστημα, που με τη χρήση CBR τεχνικών επιλέγει το καλύτερο σύνολο

αντιμέτρων που μπορούν να χρησιμοποιηθούν κάθε φορά, για την αντιμετώπιση της εμφανιζόμενης απειλής. Περιγράφουμε την αρχιτεκτονική του συστήματος, τις μονάδες και διαδικασίες που το συνθέτουν τα αποτελέσματα αξιολόγησης και καταγράφονται ερευνητικές προτάσεις για τον χώρο.

We propose a scheme of integrating case-based reasoning (CBR) techniques with intrusion detection systems (IDS). IDS are usually large-scale systems, hard to implement, inflexible, combining a lot of different mechanisms such as expert systems, statistical profiles, neural networks, etc. The integration of CBR, gives IDS more capabilities, flexibility and robustness. We introduce CBR techniques in IDS technology, especially in presenting the appropriate set of countermeasures to the Security Officer, against intrusive behavior.

Keywords

Systems security, Intrusion Detection Systems, Intrusions, Countermeasures, Case-based Reasoning, Case base, Retrieval.

2. INTRODUCTION

Intrusion Detection systems intend to defending security policies the organization applies. The increasing growth of automated transactions, distributed information processing, results in raising the need for protecting these information from the evil purposes of intruders. The use of computer networks, through which sensitive information flows, increases. Also the interconnected information systems. The need for effective intrusion detection systems, is increasing in order to suppress the efforts of stealing the sensitive data from organizations.

3. INTRUSION DETECTION SYSTEMS

Intrusion detection systems are highly complicated systems. The basic operations they are dealing with are *anomaly detection* and *intrusion detection*. With anomaly detection, they aim at finding abnormal activity into every behavior. Their behavior is observed in order to find elements which will characterize specific acts as different from usual. If an intruder performs a password cracking and finally steals the password of a user, the behavior of that user will be different from the usual one. This leads the IDS to raise the suspicious for the specific user as a probable intruder.

The usual techniques for anomaly detection rely on statistical metrics (creating user profiles which are updated with the current user behavior), neural networks (predict the user's future commands), user intention identification techniques (tracing user intentions), autonomic agents (monitoring network traffic for anomalies), graph based techniques (for intrusion detection in large scale networks).

The IDS' second basic operation is *mitigate detection*. IDS must be capable in finding intrusions that have already taken place. It is informed from the administrators about already known intrusive scenarios, looking for evidence of attacks of known vulnerabilities.

Integrating Case-based Reasoning techniques with Intrusion Detection Systems

Abstract

We propose a scheme of integrating case-based reasoning (CBR) techniques with intrusion detection systems (IDS). IDS are usually large scale systems, hard to implement, inflexible, combining a lot of different mechanisms such as expert systems, statistical profiles, neural networks, etc. The integration of CBR, gives IDS more capabilities, flexibility and robustness. We introduce CBR techniques in IDS technology, especially in presenting the appropriate set of countermeasures to the Security Officers, against intrusive behavior.

Keywords

Systems security, Intrusion Detection Systems, Intrusions, Countermeasures, Case-based Reasoning, Case base, Retrieval.

1. INTRODUCTION

Intrusion Detection systems intend in defending security policies the organization applies. The increasing growth of automated transactions, distributed information processing, results in raising the need for protecting these information from the evil purposes of intruders. The use of computer networks, through which sensitive information flows, increases. Also the interconnected information systems. The need for effective intrusion detection systems, is increasing in order to suppress the efforts of stealing the sensitive data from organizations.

2. INTRUSION DETECTION SYSTEMS

Intrusion detection systems are highly complicated systems. The basic operations they are dealing with, are *anomaly detection* and *misuse detection*. With *anomaly detection*, they aim at finding abnormal activity into users behavior. Users behavior is observed in order to find elements which will characterize specific acts as different from usual. If an intruder performs a password cracking and finally «steals» the password of a user, the behavior of that user will be different from the usual one. This leads the IDS to raise the suspicions for the specific user as a probable intrusion.

The usual techniques for anomaly detection rely on statistical metrics (creating user profiles which are updated with the current user behavior), neural networks (predict the user's future commands), user intention identification techniques (tracing user intentions), autonomous agents (monitoring network traffic for anomalies), graph based techniques (for intrusion detection in large scale networks).

The IDS' second basic operation is *misuse detection*. IDS must be capable in finding intrusions that have already taken place. It is informed from the administrators about already known intrusive scenarios, looking for evidence of attacks of known vulnerabilities. The

system is able detect a known attack pattern in users activity and sends an emergency alert to the security officer. The drawback is that the security officer or the knowledge base engineer has to be informed (and train the system) about new intrusions. The Knowledge needs constant updating and replenishment in order to cover both the old and new intrusions.

For misuse detection experts systems are used (their rules describe known intrusive scenarios), pattern matching techniques (patterns keep known intrusion signatures) and models based techniques (where models of known intrusions are created and maintained).

Denning's model is a milestone for the field of IDS. It is independent on technological platforms, the environment of the application and vulnerabilities. Many of the known intrusion detection systems have count on it. It separates the elements of the system to *subjects, objects, audit records, profiles, anomaly records* and *activity rules*. The subjects act on the objects. The system keeps information of these kind of act in records called *audit records*. Studying these records we can create attitude profiles for each user (*anomaly detection*). Comparison with older prices leads to the conclusion whether the attitude is abnormal, compared to the statistical predicted behavior. If abnormality appears it is recorded in *anomaly records*. On the other hand there are *activity rules (misuse detection)*, which under right circumstances are executed, for immediate suppression of the intrusion.

A basic characteristics an IDS must have, is the ability to minimize the false negatives errors. Characterizing an attitude as intrusive, while it is not (*false positive*) is less dangerous than characterizing an attitude as normal while it is intrusive (*false negative*). The performance of an IDS relies on other factors also. It must be able to react in real time basis, constantly, with the minimum possible human supervision. It must be tolerant to preserve its elements but the resources of the computer system it supervises also. It must be economic, wasting the minimum possible resources of the computer system. It is desirable to work with few changes, in different environments and it's knowledge base must be easy to maintain.

The scientific field of intrusion detection systems is "alive". Special role plays the rapid implementations of network installations. IDS however are interlined with their development's architecture. A general methodology for their construction is missing, useful data for their efficiency cannot be exported and they are difficult to maintain.

There is a need for more flexible and effective intrusion detection systems, which will refer to smaller scale systems, easier to be learned and used. Expert systems, statistical profiles and most of the techniques, used to detect the possibility of an intrusion, have already been used. These consist of fixed procedures and ways of controlling their input data, which make their operations less or more standard. The expert system expresses the possibility a user to follow an already known attitude, the neural network (more complicated) but it also shows whether the movements of the user are "normal" or not. The Decision Module is the component which finally decides if there is really a threat and how to confront it. Interfacing with the security officer is necessary, in order to make the final decision, but this communication must be the shortest as possible, taking into account the particular principles that real time systems are governed. The increasing disengagement of the SO from the process of deciding the countermeasures is desirable because generally SO has lots of work to do.

With this thesis we propose the integration of Case-based Reasoning (CBR) techniques with intrusion detection systems. The results seem to be hopefully, as far as the efficient operation of the IDS systems reasoning mechanisms. The integration of CBR techniques attempted in the decision module of intrusion detection systems. Future integration of CBR techniques with other modules of IDS is also proposed and the interconnection between them.

3. CASE BASED REASONING

Case-based Reasoning is a new paradigm in Artificial Intelligence. Reasoning in CBR differs from conventional rule-based reasoning, in which conclusions derive from the serial triggering of rules. In CBR, knowledge is not stored in rules but in cases, organized in appropriate structures in memory (usually trees). Solutions to problems are not proposed through serial execution of rules, but through retrieval of the most relevant cases and the adaptation of previous solutions stored in case base. In CBR the reasoning is based on «remembering» and «experience» of the reasoner.

CBR is based on two fundamental axioms. First we assume that the world has a normality: similar problems have similar solutions. Therefore solutions to old problems may be useful to new similar problems. The second fundamental axiom refers to the possibility that particular types of problems tend to appear again. In that way, future problems may look like problems that have already appeared and we know their solutions.

The basic characteristic of CBR is its ability to learn. It can learn about the efficiency of particular solutions, which can be applied later on similar problems. It has the ability to learn about the inefficiency of some solutions to avoid «bad» reasoning path in the future. It deals effectively with problem domains difficult to model, not typically defined. Generally the use of cases is the most easy way to represent knowledge in almost most types of problem domains.

Cases are the basic elements of CBR. They represent reasoner's experience for the particular problem area. The sum of cases composes the Case Base for that problem domain. When a new problem appears we try to find similar problems in the Case Base. From the similar problems we have found, we can seek the solutions we had adopted for them. We choose the solution of the most relevant problem and on that solution, we base the process of solving the new problem. There is a chance that this solution may be implemented identical as it is, but there is also a possibility to adjust it, to fit better to the new problem. If no solution matches we create an entirely new case, to store the memory structures that are used.

The retrieval process is the first action of the CBR circle. Aims in finding the most similar case (source case) to the new case appeared (target case) from the Case Base. This requires complicated processes for information filtering, selection of the most important features, setting weights for these, discrimination values, etc. The case which seems to be the most efficient solution, is imported into a process of modification. The knowledge administrator makes some changes, so that it fits exactly to the new problem he tries to solve. The solution gets through a revision phase, before it is implemented (especially if it has failed). After the check, a new case is created, which is stored by the system through the mechanisms of



learning. Increasing the number of cases means that the total “experience” of the system increases, so that it can provide more efficient solutions.

The basic difference between traditional rule-based systems and CBR systems is that the first ones do not have the ability to learn. When an expert system has to solve a problem, which has appeared in the past too, it must execute the same path of rules that were executed in the past, no matter how many they are. This does not happen with CBR, where solutions are organized in structures, they can be found and retrieved immediately.

CBR always gives a solution, however the expert system may not give a solution, if the right conditions do not appear. The rule-based systems may work effectively with problems which are well defined and easy to describe, on the other hand CBR can give solutions for problems that are not easily modeled. Generally, CBR suits for problem domains with large amounts of experience, while the rule-based systems suit for problem domains where the amount of knowledge is very big. CBR is placed between rule based systems and “knowledge limited systems” (in these systems the amount of existing knowledge is not so important) such as neural networks, pattern recognition systems, genetic algorithms.

4. INTEGRATING CASE BASED REASONING WITH INTRUSION DETECTION SYSTEMS

We have integrated CBR techniques in intrusion detection systems, specifically in the decision module of these. CBR techniques provide more flexibility and efficiency in choosing the right countermeasures. Choosing CBR techniques was necessary for the difficulty to describe typically the field of IDS. In these kind of problems, conditions are repeated, similar intrusions reappear (and their solutions too). With its ability to learn, new cases will be created, which are the countermeasures for the new threats. CBR always gives solutions, the knowledge is organized more easily with a simpler, understandable way.

Input to the new system is the output from the modules of the IDS, dealing with anomaly and misuse detection. Those outputs get through a filtering process and change into an understood format to the next module, the CBR Engine.

CBR Engine is responsible for the reasoning process. It selects the countermeasures comparing the new cases as they come from the filtering process, to those stored in the Case Base. It is responsible for indexing cases by the most representative features. When a new intrusion is probably taking place it searches the Case Base in order to find the most similar cases (past intrusions with their countermeasure), that will be used to confront the threat. The cases that come up with this search, are compared to the initial one, in order to find similarities. The most similar case is kept to be used as a solution. It may be necessary to modify the selected case to achieve a best fit to the appeared intrusion. The retrieved case is adapted in order to cope with the threat.

If the new case is succeeded to the intrusion, it can be indexed in Case Base. If it fails the reasons of failures are stored, to be taken under consideration in future attempts coping with similar intrusions.



Who Is a Computer Hacker?

Every field of the case holds a weight with which the engine computes a similarity measure. The cases with maximum total weights are selected as probable countermeasures.

Security officer observes the function of the system, through a convenient interface. He can control the contents of the countermeasures, the solutions before their implementation, he can create new cases, modify the Case Base and gather statistical information about systems functionality.

I. ΕΥΘΗΜΑΤΑ ΑΝΤΙΧΕΙΡΗΣ ΕΠΕΒΟΛΩΝ

5. CONCLUSIONS AND FUTURE RESEARCH

We describe how the new system can be applied to an existing IDS (SECURENET). We describe SECURENET, with an emphasis on the decision module, we show the existing drawbacks of the IDS and the benefit from the new approach. We inserted a small amount representative of cases - intrusions into a CBR Shell (CBRWorks). We try a simulation procedure to express some results and an algorithmic estimation cost.

Finally, we propose future research about CBR, the integration with other techniques such as Neural Networks and give insights about using CBR as a misuse detection and anomaly detection component.

5.1. Ανάγνωση Επεβολών

Ο παρόντος ορισμός της γειτονίας δεν υπάρχει ως δομή ακρίβειας, δεδομένου του μετριούς, λέγο να τολμήσεις στην απομάνωση την αντικαυτούσιαν αναπτυξιανή. Παλαιό αριθμητικό είναι, αποτελεί, τοπονόμευτη, αλλά αποτελείται, χωρίς καλύτερη αριθμητική, τη πρώτη σειρά κτιρίων που αποτελείται από μία αριθμητική προσκάδισης για την προστασία της περιοχής στην οποία δέσμευτη είναι η στρατηγική της τον Anderson.

«Η μόνη απόφευκτη μεθοδολογία για αποτέλεσμα της αναπτυξιακής από κίνηση, μη εργαστηριακή γνωστολογία, είναι η σχέση της πληροφορίας μεταξύ των αριθμητικών μέτρων σε κατανομή της περιοχής, σε ότι αποτελείται από μεταβλητές σε μεταβλητές (variables) και γενικότερη (variables) κατανομής» (Anderson, 1980).

Εντούτοις, μάλλον, θα πρέπει να πάρεται με την ορισμό της έννοιας της απομάνωσης, θεωρείται πιο σύντομο.

Κάτια Δημοσία, σπουδαία της στάχτα άριστη, μη καταστητήσαν την απεριόλεπτη διατάξεων και διαπορεύτηκαν πραγματικά την πολιτεία της περιφέρειας.

Εισβολή μπορεί να γραμματίζεται τόνος σε, αποδείξεις παραβίασης της πολιτείας μεταβολής, επίσημη ποστήση.

Who Is a Computer Hacker?

«**HACKER** noun 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities - as opposed to most users of computers, who prefer to learn only the minimum amount necessary. 2. One who programs enthusiastically or enjoys programming rather than just theorizing about programming.»

-Guy L. Steele, et al.,
The Hacker's Dictionary

1. ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

1.1 Εισαγωγή

Σε αυτήν την εργασία δίνονται οι γενικές αρχές της ανίχνευσης εισβολών. Περιγράφονται οι βασικοί ορισμοί της ανίχνευσης εισβολών, όρων και βασικών στοιχείων απαραίτητων για την κατανόηση των θεμάτων που θίγονται. Περιγράφονται συνοπτικά οι αρχές που πρέπει να διέπουν τα υπολογιστικά συστήματα όσον αφορά την ασφάλεια. Κατόπιν αναλύονται οι πιο γνωστές τεχνικές - μεθοδολογίες ανίχνευσης. Γίνεται παράθεση των σημαντικότερων συστημάτων ανίχνευσης εισβολών που έχουν ήδη αναπτυχθεί. Τέλος προχωρούμε σε γενική κριτική των συστημάτων και συμπεράσματα για την έρευνα που γίνεται στον τομέα ανίχνευσης εισβολών.

1.1.1 Ανίχνευση Εισβολών

Ο ακριβής ορισμός της εισβολής δεν μπορεί να δοθεί ακριβώς, δεδομένου του ασαφούς, λίγο ως πολύ, ορισμού της ασφάλειας των υπολογιστικών συστημάτων. Πολύ περισσότερο της ανυπαρξίας πολιτικής ασφάλειας σε συστήματα, χωρίς καλά ορισμένες τις πράξεις τους και τα χαρακτηριστικά τους. Μια αρχική προσπάθεια για την προσέγγιση του θέματος της εισβολής σε ένα σύστημα δόθηκε από τον Anderson.

«Μια ενέργεια μπορεί να θεωρείται ως απειλή, εάν αυτή μπορεί να χαρακτηριστεί ως πιθανή μη εξουσιοδοτημένη προσπάθεια για προσπέλαση σε πληροφορίες, επηρεασμός των πληροφοριών αυτών ή και εάν το αποτέλεσμα της πράξης έχει ως συνέπεια να μεταβεί το σύστημα σε ασταθής (*unreliable*) και ασυνήθιστη (*unusable*) κατάσταση». (Anderson, 1980)

Ενας άλλος ορισμός (που σχετίζεται άρρηκτα με τον ορισμό της έννοιας της ασφάλειας), θεωρεί ως εισβολή:

«ένα σύνολο ενεργειών που στόχο έχουν να καταστραγήσουν την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των στοιχείων του συστήματος».

Εισβολή μπορεί να χαρακτηριστεί γενικά ως η προσπάθεια παραβίασης της πολιτικής ασφάλειας σε ένα σύστημα.

Οι εισβολές μπορούν να χαρακτηριστούν ως εξωτερικές διεισδύσεις από μη εξουσιοδοτημένους χρήστες, έξω από τα όρια του συστήματος, οι οποίοι προσπαθούν να εισέλθουν σε αυτό για να υλοποιήσουν τις οποιεσδήποτε επιδιώξεις τους. Μια δεύτερη κατηγορία είναι οι εσωτερικές διεισδύσεις, αυτές προκαλούνται από εξουσιοδοτημένους χρήστες του συστήματος στην προσπάθειά τους να προσπελάσουν δεδομένα και πόρους του συστήματος για τα οποία όμως δεν έχουν την κυριότητα. Τέλος υπάρχουν και οι *misfeasors*, οι οποίοι αν και εξουσιοδοτημένοι χρήστες χρησιμοποιούν λανθασμένα και κάνουν κατάχρηση των πόρων του συστήματος.

Μια από τις βασικές επιδιώξεις του επίδοξου εισβολέα είναι η συλλογή πληροφοριών για αυτό. Η χρήση του δάιμονα fingerd αποτελεί κλασικό παράδειγμα σε UNIX περιβάλλοντα (ο οποίος μας ενημερώνει εάν και ποιοι χρήστες είναι συνδεδεμένοι στο σύστημα). Μετέπειτα στόχος είναι να καταλάβει κάποιο λογαριασμό (account) και από κει και έπειτα του υπερχρήστη (root) από τον οποίο θα εξαπολύσει την επίθεσή του. Οι μετέπειτα κινήσεις του (Katzavelou 1995) μπορεί να σχετίζονται με:

- *Masquerade*. Ο εισβολέας συμπεριφέρεται όπως ένας φυσιολογικός χρήστης (του οποίου έχει “κλέψει” το συνθηματικό).
- *Active Wiretrapping*. Ο εισβολέας παρακολουθεί τις κινήσεις των πακέτων που μεταφέρονται σε ένα δίκτυο, ανάμεσα στους διάφορους hosts. Στόχος του είναι η αλλαγή των πληροφοριών που μεταφέρονται.
- *Passive Wiretrapping*. Όπως παραπάνω, με τη διαφορά ότι ο χρήστης δεν αλλάζει το περιεχόμενο των μηνυμάτων που μεταδίδονται. Ενδιαφέρεται μόνο για την παρακολούθηση των πληροφοριών, των διευθύνσεων αποστολής και προορισμού, κτλ.
- *Traffic flow analysis*. Ο εισβολέας παρακολουθεί, αναλύει και καταγράφει στοιχεία για την κίνηση του δικτύου. Παρατηρεί το πλήθος των πακέτων, το μέγεθός τους, τον αριθμό των μηνυμάτων που στέλνονται ανάμεσα στους διάφορους κόμβους του δικτύου.
- *Replay*. Επανάληψη αποστολής ενός μηνύματος (νόμιμου), το οποίο έχει ήδη σταλεί.
- *Message detection*. Ο εισβολέας διαγράφει πληροφορίες, μηνύματα που περνάνε μέσα από ένα κανάλι επικοινωνίας.
- *Denial of service*. Προσπάθεια του εισβολέα όχι να καταστρέψει πληροφορίες, διαγράφοντας ή τροποποιώντας αρχεία, αλλά να θέσει το σύστημα εκτός λειτουργίας ή σε κατάσταση πολύ χαμηλής απόδοσης. Για παράδειγμα αυτό μπορεί να επιτευχθεί μεταφέροντας μεγάλο ποσό δεδομένων διαμέσου ενός καναλιού επικοινωνίας, θέτοντας το κανάλι ανεπαρκές για την μετάδοση άλλων πληροφοριών, μηνυμάτων, για παραλαβή αρχείων και γενικά για εξυπηρέτηση των χρηστών με δικτυακές υπηρεσίες.

Ανεξάρτητα με την κατηγοριοποίηση των εισβολών οι τρόποι για την αναγνώρισή τους είναι είτε μέσω στατιστικής άνάλυσης της συμπεριφοράς του εισβολέα (*anomaly detection*), είτε με την παρακολούθηση και σύγκριση των ενεργειών του με παλαιότερη παρεισφρητική συμπεριφορά (*misuse detection*).

1.1.1.1 Anomaly detection.

Στόχος της είναι η ανακάλυψη και κατηγοριοποίηση της συμπεριφοράς του χρήστη ως αποδεκτής ή πιθανά παρεισφρητικής. Σχετίζεται με την ανακάλυψη κατηγοριών εισβολών οι οποίες χαρακτηρίζονται από ανώμαλη, μη φυσιολογική συμπεριφορά, στα πλαίσια αλληλεπίδρασής του με το σύστημα. Στοχεύει στην ανακάλυψη παράξενης, μη προβλέψιμης συμπεριφοράς, στον τρόπο δράσης του χρήστη, σε σχέση με τον κανονικό τρόπο που κινείται μέσα στο σύστημα. Γίνεται παρατήρηση των κινήσεών του μέσα από πληροφορίες που κατακρατεί το σύστημα σχετικά με τις κινήσεις των χρηστών (audit data), την χρήση των πόρων του συστήματος από τις κινήσεις αυτές (KME, μνήμη, συσκευές εισόδου - εξόδου).

Διατηρείται ένα συγκεκριμένο στατιστικό προφίλ συμπεριφοράς. Το προφίλ αυτό αποτελεί μια αναπαράσταση της συμπεριφοράς του χρήστη, των τάσεων και προτιμήσεών του σχετικά με τον τρόπο που αλληλεπιδρά με το σύστημα. Η τεχνική στηρίζει την λειτουργία της στο γεγονός ότι διαφορετικοί χρήστες χαρακτηρίζονται από διαφορετικά προφίλ δράσης και άρα υπάρχει ένα μέτρο προσδιορισμού τους από το σύστημα. Εάν κάποιος χρήστης εμφανίσει ξαφνικά μια διαφορετικού τύπου συμπεριφορά από αυτή που απεικονίζεται στο στατιστικό του προφίλ, τότε και το σύστημα υποψιάζεται ότι μπορεί να είναι άλλο πρόσωπο το οποίο δραστηριοποιείτε στο σύστημα μέσω του λογαριασμού άλλου χρήστη.

Διαφορετικό είναι, για παράδειγμα, το προφίλ για κάποιον χρήστη που συνδέεται πολλές φορές τη μέρα, εγκαθιδρύει τακτικές, περιορισμένες σε χρονική διάρκεια συνόδους (ώσπου να κοιτάξει τα μηνύματά του από το ηλεκτρονικό ταχυδρομείο) και διαφορετικό εκείνου που εγκαθιδρύει μακρόσυρτες συνόδους και χρησιμοποιεί το σύστημα για να αναπτύσσει και να μεταγλωττίζει εφαρμογές. Εάν αντιληφθούμε τον πρώτο χρήστη να έχει συνδεθεί πολλές ώρες και να ανοίγει ευρετήρια με αρχεία του συστήματος, σίγουρα αποτελεί διαφοροποίηση της συμπεριφοράς του από την "φυσιολογική". Το σύστημα ανίχνευσης εισβολών θα πρέπει, σε αντίστοιχες περιπτώσεις, να εκδώσει κάποιο προειδοποιητικό μήνυμα (*alert*) για πιθανή εισβολή στον υπεύθυνο ασφαλείας του συστήματος.

Πολλές φορές όμως μπορεί μια παρεισφρητική συμπεριφορά να είναι το αποτέλεσμα ενός συνόλου δραστηριοτήτων καμιά από τις οποίες όμως δεν μπορεί να χαρακτηριστεί ξεχωριστά ως ανώμαλη. Το ιδανικό θα ήταν κάθε μη φυσιολογική συμπεριφορά να χαρακτηρίζοταν ως παρεισφρητική. Με αυτόν τον τρόπο θα μειωνόταν ο αριθμός των *false positives* και *false negatives* λαθών.

False negatives παρατηρούμε όταν το σύστημα δεν κατηγοριοποιεί μια συμπεριφορά ως παρεισφρητική ενώ αυτή είναι, ενώ *false positive* όταν την χαρακτηρίζει παρεισφρητική ενώ αυτή δεν είναι. Τα συστήματα που επιδιώκουν την απουσία *false negative* καταστάσεων έχουν πολύ χαμηλά όρια ευαισθησίας (*thresholds*), προκειμένου κάθε παραμικρή έστω διακύμανση από την φυσιολογική συμπεριφορά των χρηστών να την χαρακτηρίζουν ως ύποπτη και να ενημερώνουν τον υπεύθυνο ασφαλείας για αυτό. Αντίθετα, θέτοντας ένα αρκετά υψηλό όριο ευαισθησίας, μπορεί να υπάρξει παρεισφρητική συμπεριφορά αλλά το σύστημα να την αγνοήσει. Ο καθορισμός των ορίων αυτών αποτελεί δύσκολη επιλογή από τους σχεδιαστές των συστημάτων ανίχνευσης εισβολών. Η ύπαρξη πολλών alerts (χαμηλό όριο

ευαισθησίας) παραγκωνίζει το σύστημα λήψης αποφάσεων του συστήματος ανίχνευσης εισβολών από τις ουσιαστικές δραστηριότητες τις οποίες έχει (την αυτοματοποιημένη ανακάλυψη και αντιμετώπιση εισβολών), ενώ ταυτόχρονα δεσμεύει τον υπεύθυνο ασφαλείας στο να ελέγχει ο ίδιος πάρα πολλές περιπτώσεις πιθανών εισβολών. Στην αντίθετη περίπτωση, για να εκδίδονται πολύ λίγα alerts, ένα μεγάλο ποσοστό των οποίων να σχετίζονται με βέβαιες απειλές, υποδηλώνει οτι το σύστημα ανίχνευσης εισβολών έχει σχεδιαστεί πολύ καλά, ενώ υποστηρίζει δυνατότητες αποτελεσματικής κατηγοριοποίησης των απειλών, αναζήτησης μέτρων προστασίας ακόμα και εκμάθησης νέων τρόπων αντιμετώπισης καινούργιων απειλών.

Διακρίνουμε τέσσερις συνδυασμούς μεταξύ παρεισφρητικής και ανώμαλης συμπεριφοράς και ο τρόπος που ένα σύστημα ανίχνευσης μπορεί να τις χαρακτηρίσει.

- **Παρεισφρητική αλλά όχι ανώμαλη:** παρόλο που η συμπεριφορά είναι παρεισφρητική, δεν χαρακτηρίζεται ως ανώμαλη. Σε αυτήν την περίπτωση συναντάμε false negative χαρακτηρισμό, αφού το IDS δεν χαρακτηρίζει θετικά μια παρεισφρητική συμπεριφορά.
- **Μη παρεισφρητική αλλά ανώμαλη:** παρόλο που η συμπεριφορά δεν είναι παρεισφρητική, το IDS την χαρακτηρίζει ανώμαλη. Προξενείτε κυρίως λόγω χαμηλού ορίου ευαισθησίας. Σε αυτήν την περίπτωση συναντάμε false positive χαρακτηρισμό, αφού το IDS χαρακτηρίζει ανώμαλη μη παρεισφρητική συμπεριφορά.
- **Μη παρεισφρητική και ομαλή:** το σύστημα σωστά δεν χαρακτηρίζει την συμπεριφορά του χρήστη ως παρεισφρητική (true negative)
- **Παρεισφρητική και ανώμαλη:** το σύστημα χαρακτηρίζει σωστά την συμπεριφορά ως παρεισφρητική (true positive)

1.1.1.2 Misuse detection

Με την μέθοδο αυτή γίνεται προσπάθεια ανίχνευσης της παρεισφρητικής συμπεριφοράς μέσα από την άμεση παρακολούθηση της συμπεριφοράς του χρήστη. Εστιάζεται στο εάν πραγματοποιούνται κάποιες προϋποθέσεις - κανόνες σχετικά με την αλληλεπίδραση του χρήστη με το σύστημα. Το IDS έχει ενημερωθεί από τους κατασκευαστές τους σχετικά με γνωστά σενάρια παρεισφρήσεων στο σύστημα. Τέτοια μπορούν να είναι γνωστά bugs σε προγράμματα, όπως του fingerd και sendmail του UNIX (που εκμεταλλεύτηκε το σκουλήκι του Internet).

Η πληροφορία που συγκεντρώνει το σύστημα για την συμπεριφορά του χρήστη, την οποία και συγκρίνει με σφραγίδες γνωστών εισβολών προέρχεται από τα audit trails του συστήματος. Αυτό αποτελεί και ένα από τα μεγαλύτερα μειονεκτήματα της μεθόδου, δεδομένου ότι απαιτείται η φύλαξη και παρατήρηση των πληροφοριών αυτών. Επιπλέον από τη φύση της έχει αδυναμίες στην αντιμετώπιση απειλών που σχετίζονται με passive wire-trapping και spoofing.

Παρόλο που η μέθοδος χαρακτηρίζεται από θετικά αποτελέσματα στην εύρεση ήδη γνωστών εισβολών, ωστόσο δεν έχει τη δυνατότητα για ανακάλυψη νέων απειλών. Επίσης η υπερβολική ανάλυση των audit data ανεβάζει το κόστος (κατανάλωση πόρων, χρονικοί περιορισμοί).

1.1.2 Ορολογία

Ακολουθεί η περιγραφή εννοιών - ορισμών που σχετίζονται με την ασφάλεια υπολογιστικών συστημάτων, την ανίχνευση εισβολών και στις οποίες αναφερόμαστε στην παρούσα εργασία. Μερικές από τις έννοιες αυτές έχουν οριστεί επακριβώς από επιστήμονες πληροφορικής ενώ άλλες δεν έχουν ακόμα οριστεί τυπικά.

- **Υποκείμενα (Subjects):** Αποτελούν χρήστες ή διαδικασίες - προγράμματα χρηστών που εκτελούνται.
- **Αντικείμενα (Objects):** Αποτελούν τους πόρους του συστήματος (ΚΜΕ, μνήμη, χρήση συσκευών εισόδου εξόδου, κτλ.).
- **Audit records:** Περιγράφουν τις πράξεις στα αντικείμενα από τα υποκείμενα, καθώς και άλλα συμπληρωματικά στοιχεία όπως ο χρόνος που συνέβηκε η πράξη (timestamp), το ποσοστό πόρων που χρησιμοποιήθηκαν ((resource usage) των αρχείων που ανοίχτηκαν, των γραμμών που εκτυπώθηκαν, κτλ.).
- **Προφίλ (Profiles):** Δομές που χαρακτηρίζουν τη συμπεριφορά των υποκειμένων στα αντικείμενα. Η συμπεριφορά αυτή συνδέεται με στατιστικές μετρικές των μεταβλητών που περιγράφουν το προφίλ του υποκειμένου προκειμένου να χαρακτηρίσουν την συμπεριφορά των αντικειμένων. Η σύγκρισή τους με παλαιότερες τιμές μπορεί να μας οδηγήσει στο συμπέρασμα εάν η συμπεριφορά κάποιου χρήστη ξεφεύγει από την κανονική, εάν είναι ανώμαλη σε σχέση με την στατιστικά προβλεπόμενη.
- **Πολιτική ασφάλειας (Security Policy):** Ορίζεται ως σύνολο αρχών, κανόνων, πρακτικών που καθορίζουν τον τρόπο που ένας οργανισμός διευθύνει, προστατεύει και διανέμει τις ευαίσθητες πληροφορίες.
- **Υπογραφή (Signature), σενάριο (Scenario), υπόδειγμα (Pattern):** Αναφέρετε κυρίως στην αναγνώριση ανώμαλης συμπεριφοράς και συνδέεται με συγκεκριμένα χαρακτηριστικά, συνθήκες, συσχετίσεις στοιχείων στα audit trails και υπογράφουν - προσδιορίζουν μια συγκεκριμένη εισβολή ή προσπάθεια για αυτή.
- **Τρωτότητα (Vulnerability):** Αποτελεί αδυναμία στους αυτοματοποιημένους μηχανισμούς ασφάλειας, στις ελέγχους που κάνει και στους εσωτερικούς μηχανισμούς του, οι οποίοι μπορούν να αξιοποιηθούν από τους εισβολείς στην προσπάθειά τους για απόκτηση πρόσβαση σε πληροφορίες του συστήματος.
- **Ρωγμή (Flaw):** Αποτελεί λάθος είτε σκόπιμο είτε απροσεξίας στη σχεδίαση του συστήματος και επιτρέπει την παράκαμψη των μηχανισμών ασφαλείας. Πολλές φορές είναι συνώνυμο με την έννοια της τρωτότητας.

1.2 Αρχές ασφάλειας σε υπολογιστικά περιβάλλοντα

1.2.1 Εκτίμηση Κινδύνων (Risk Assessment)

Το πρώτο βήμα για την παροχή ασφάλειας σε ένα πληροφοριακό σύστημα είναι η **εκτίμηση των κινδύνων** στους οποίους το σύστημα αυτό είναι υποκείμενο (Κιουντούζης 1994, Garfinkel 1996). Τα τρία στάδια στα οποία διακρίνεται η εκτίμηση κινδύνων είναι:



- **Αναγνώριση αγαθών (Identifying Assets).** Τα αγαθά αυτά μπορούν να είναι υλικά όπως: σκληροί δίσκοι, καλώδια δικτύου, εγχειρίδια, ή άλλα όπως: τα προσωπικά στοιχεία των χρηστών (privacy of users), διαθεσιμότητα του συστήματος, η φήμη του οργανισμού. Ο ορισμός των αγαθών αυτών δεν πρέπει να εξαντλείται στο χώρο του πληροφοριακού συστήματος μόνο. Αντίθετα είναι πολύ σημαντικό να λαμβάνονται υπόψιν και αγαθά που ενώ δεν σχετίζονται άμεσα με το πληροφοριακό σύστημα, είναι δυνατόν να φθαρούν ή να χαθούν έπειτα από μια παραβίαση της ασφάλειας του πληροφοριακού συστήματος.
- **Αναγνώριση απειλών (Identifying Threats).** Η φύση των απειλών μπορεί να είναι τεχνική ή μη. Οι απειλές μπορούν να προέρχονται είτε μέσα από το σύστημα, είτε έξω απ' αυτό. Π.χ μια μη τεχνική απειλή θα μπορούσε να είναι η απουσία ανθρώπων του προσωπικού με σημαντικό πόστο στη γενικότερη οργανωτική δομή του πληροφοριακού συστήματος.
- **Υπολογισμός κινδύνων (Calculating Risks).** Η έννοια του υπολογισμού των κινδύνων υπονοεί μια διαδικασία ποσοτικοποίησης των κινδύνων αυτών κάτι που σε μερικές περιπτώσεις ίσως να μην είναι εύκολο ή να μην οδηγεί σε ασφαλή συμπεράσματα. Σημαντικό στοιχείο είναι ότι τα αποτελέσματα της εκτίμησης κινδύνων δεν είναι στατικά αλλά πρέπει να ενημερώνονται σχετικά συχνά, αφού ούτε το πληροφοριακό σύστημα είναι στατικό, ενώ με την πάροδο του χρόνου αποκτάται εμπειρία σχετική τόσο με τους κινδύνους όσο και με το κόστος που προκαλούν στο σύστημα.

1.2.2 Ανάλυση Κόστους - Οφέλους (Cost Benefit Analysis)

Η ανάλυση κόστους - οφέλους ακολουθεί την εκτίμηση κινδύνων, προσπαθώντας να εκτιμήσει το κόστος κάθε :

- απειλής, όπως αυτή προκύπτει από την εκτίμηση κινδύνων και
- εναλλακτικού τρόπου αντιμετώπισης για την κάθε απειλή.

Η έννοια του κόστους σε αρκετές περιπτώσεις δεν μεταφράζεται σε χρήματα αλλά σε χρόνο. Η διαδικασία υπολογισμού κάθε τέτοιου κόστους είναι ιδιαίτερα δύσκολη εργασία.

Γενικά η αντιμετώπιση μίας απειλής εξετάζονται λύσεις που ενεργούν είτε προληπτικά, είτε κατασταλτικά.

1.2.3 Πολιτική Ασφαλείας (Security Policy)

Η πολιτική ασφαλείας (Kioundouzis 1996, Kokolakis 1995) ορίζει τα αγαθά (assets) που θεωρούνται πολύτιμα και διασαφηνίζει τα βήματα που πρέπει να ακολουθηθούν για την προστασία των αγαθών αυτών. Η πολιτική ασφαλείας πρέπει να

- διευκρινίζει τι προστατεύεται και γιατί,
- περιγράφει σαφώς τις υπευθυνότητες

- παρέχει ένα σταθερό σημείο αναφοράς σε ενδεχόμενα προβλήματα ασφαλείας που μπορούν να προκύψουν στο μέλλον

Από την άλλη μεριά η πολιτική ασφαλείας δεν πρέπει να απαριθμεί εξειδικευμένες απειλές, μηχανές ή ανθρώπους ονομαστικά, αλλά να είναι γενική. Είναι επίσης σημαντικό η πολιτική ασφαλείας να μην αλλάζει συχνά.

Η πολιτική ασφαλείας μπορεί να σχεδιαστεί / διατυπωθεί με πολλούς τρόπους. Π.χ μια απλή και γενική πολιτική που να καλύπτει τα πιο πιθανά ενδεχόμενα, κατηγοριοποίηση των αγαθών και υιοθέτηση πολιτικών για κάθε ένα από τα αγαθά αυτά (e-mail, personal data, accounting information) κ.α.

Μια συνήθης πρακτική είναι η υιοθέτηση μιας μικρής και γενικής πολιτικής ασφαλείας που ορίζει πρότυπα (standards) και οδηγίες (guidelines). Τα πρότυπα στοχεύουν στο να διατυπώσουν ανεξάρτητες από πλατφόρμα γενικές αρχές σχετικές με την ασφάλεια, παρέχοντας ταυτόχρονα κριτήρια με βάση τα οποία αξιολογείται η εφαρμογή τους. Οι οδηγίες διασαφηνίζουν τα πρότυπα σε σχέση με την πλατφόρμα εφαρμογής.

Ένα παράδειγμα προτύπου θα μπορούσε να είναι το παρακάτω:

«Backups shall be made of all on - line and software on a regular basis. In no case will backups be done any less often than once every 72 hours of normal business operation. All backups should be kept for a period of at least six months; the first backup in January and July of each year will be kept indefinitely at an off-site, secured storage location. At least one full backup of the entire system shall be taken every other week. All backup media will meet accepted industry standards for its type, to be readable after a minimum of five years in unattended storage»

Ένα παράδειγμα οδηγίας θα μπορούσε να είναι το παρακάτω:

«Backups on UNIX machines should be done with the “dump” program. Backups should be done nightly, in single-user mode, for systems that are not in 24-hour production use. Backups for systems in 24-hour production mode should be made at the shift change closest to midnight, when the system is less loaded. All backups will be read and verified immediately after being written.»

1.2.4 Γιατί είναι αναγκαία η χρήση συστημάτων ανίχνευσης εισβολών.

Τα συστήματα ανίχνευσης εισβολών στοχεύουν ακριβώς στην υλοποίηση των αρχών και πολιτικών που κάθε σύστημα έχει υιοθετήσει. Μέσα από μηχανισμούς και τεχνικές που ενσωματώνουν, έχουν την δυνατότητα να ελέγχουν τα υπολογιστικά συστήματα που επιβλέπουν από προσπάθειες καταστρατήγησης των πολιτικών ασφαλείας. Βοηθάει στην υλοποίηση των αρχών, που έχουν τεθεί από τους υπεύθυνους ασφαλείας (security officers) του οργανισμού, των πρακτικών και προτύπων. Αφού καταγραφούν τα αγαθά που πρέπει να προστατευθούν, αναγνωριστούν οι κίνδυνοι που απειλούν την καταπάτησή τους και υπολογιστούν οι ζημιές που θα επέλθουν στον οργανισμό από την εμφάνιση των απειλών αυτών, κατηγοριοποιούνται οι τρόποι προστασίας από τις απειλές αυτές. Τα συστήματα ανίχνευσης εισβολών μπορούν να διαδραματίσουν αποτελεσματικό ρόλο στην προσπάθεια αυτή, εάν βέβαια υλοποιηθούν με στόχο την πληρέστερη υλοποίηση των

πολιτικών ασφαλείας, εάν δίνουν σημασία στον ανθρώπινο παράγοντα ως πρωτογενούς στοιχείου του Πληροφοριακού Συστήματος.

1.3 Τεχνικές - μεθόδοι λογισμών ανίχνευσης εισβολών

1.3.1 Εισαγωγή

Τα συστήματα ανίχνευσης εισβολών που έχουν υλοποιηθεί στηρίζουν την λειτουργία τους σε τεχνικές και μεθόδους, άλλες από αυτές σχετίζονται με την ανακάλυψη ανώμαλης συμπεριφοράς (anomaly detection) ενώ άλλες με τον προσδιορισμό misuse detection στις κινήσεις κάποιου χρήστη - πιθανού εισβολέα. Τα IDS δεν χρησιμοποιούν μόνο μια κατηγορία τεχνικών αλλά συνήθως ένα συνδυασμό αυτών για την αποτελεσματική ανακάλυψη παρεισφρητικής συμπεριφοράς. Οι κυριότερες από τις τεχνικές που χρησιμοποιούνται στην περίπτωση της anomaly detection είναι η χρήση στατιστικών τεχνικών, νευρωνικών δικτύων, αλλά και νεότερων όπως, χρήση αυτόνομων agents και γράφων. Στην περίπτωση της misuse detection χρησιμοποιούνται τεχνικές όπως εμπείρων συστημάτων, keystroke monitoring, pattern matching, model-based intrusion detection, για τις οποίες όμως δεν έχουμε ακόμα στοιχεία για την αποδοτικότητά τους. Επίσης παρουσιάζεται ένα μοντέλο ανίχνευσης εισβολών, της Denning, στο οποίο στηρίχθηκαν πολλά από τα σημερινά IDS.

1.3.2 Χαρακτηριστικά ενός καλού IDS

Ένα IDS χαρακτηρίζεται ως αποδοτικό εάν:

- “Τρέχει” διαρκώς, χωρίς ανθρώπινη παρακολούθηση. Τα αποδοτικά IDS αναφέρονται σε συστήματα που επεξεργάζονται πληροφορίες από το σύστημα που επιτηρούν ενώ προσφεύγουν προς τον διαχειριστή ασφάλειας του συστήματος μόνο όταν κρίνεται σκόπιμο (ανακάλυψη βέβαιης απειλής, ανακάλυψη νέας απειλής που δεν υπάρχουν ήδη γνωστοί τρόποι αντιμετώπισης). Πρέπει να είναι αρκετά αξιόπιστο ώστε να λειτουργεί στο παρασκήνιο παρέχοντας ένα μόνιμο και συνεχές εμπόδιο στις βλέψεις των κακόβουλων χρηστών.
- Ανεκτικό σε παραβιάσεις του συστήματος που παρακολουθεί. Έπειτα από την προσβολή από κάποιον εισβολέα, η επαναφορά στην προηγούμενη κατάσταση του συστήματος κρίνεται αναγκαία. Η επανάκτηση των συστημάτων αρχείων που μπορεί να χάθηκαν, το σβήσιμο ιομορφών που ενδέχεται να έχουν προσβάλει το σύστημα αποτελεί βασική λειτουργία των αποτελεσματικών IDS. Θα πρέπει να μπορεί να επανέλθει σε κανονική λειτουργία, μετά από μια διακοπή του συστήματος.
- Ανεκτικό σε παραβιάσεις των στοιχείων του. Κοινό χαρακτηριστικό της τακτικής που ακολουθούν πολλοί εισβολείς είναι να διαγράφουν κάθε στοιχείο που μπορεί να υποδηλώνει την παρουσία τους στο σύστημα (από τα audit trails, την πληροφορία από την παρακολούθηση του δικτύου). Αν υποθέσουμε πως τα audit trails αποτελούν βασικά στοιχεία εισόδου για την επεξεργασία του IDS, πρέπει νά φυλάσσονται σε μέρη που δεν μπορούν να τροποποιηθούν (σε άλλη μηχανή, εκτυπώσεις). Το IDS πρέπει να αντιλαμβάνεται τις προσπάθειες αλλαγής των στοιχειών αυτών. Πρέπει να αντιστέκεται σε προσπάθειες παραποίησης της βάσης γνώσης του από

εισβολείς, των κανόνων που χρησιμοποιεί, των στατιστικών προφίλ, μετρικών, ορίων ευαισθησίας που έχουν τεθεί. Ενας από τους δελεαστικούς στόχους ενός εισβολέα μπορεί να είναι το ξεγέλασμα του IDS προκειμένου να κινείτε ανετότερα στο σύστημα, γνωρίζοντας πλέον πως δεν παρακολουθείται.

- **Οικονομικό.** Στόχος πρέπει να είναι η αποδοτικότερη και αδιάλειπτη λειτουργία του υπολογιστικού συστήματος και όχι η παρεμπόδιση και μείωση της αποτελεσματικότητάς του. Πρέπει απασχολεί όσο το δυνατόν λιγότερους από τους πόρους του συστήματος. Φυσικό αποτέλεσμα της αύξησης των χρόνων απόκρισης του συστήματος, είναι, συν τοις άλλοις, η δυσαρέσκεια των χρηστών, η γκρίνια και απογοήτευσή τους για την χαμηλή απόδοσή του. Το IDS θα πρέπει να παρέχει διαφάνεια στις λειτουργίες του συστήματος, δεν πρέπει να είναι αισθητή η παρουσία του, ούτε να κωλυσιεργεί την υλοποίηση των εργασιών των χρηστών.
- **Γρήγορο.** Πρέπει να διακρίνει αμέσως τις διαφορές στην λειτουργία του συστήματος, να καταγράφει στατιστικά στοιχεία της χρήσης των πόρων (KME, μνήμης, I/O), έτσι ώστε ξεχωρίζει την ανώμαλη συμπεριφορά από τις κανονικές, συνηθισμένες τιμές. Ένα IDS το οποίο ανακαλύπτει μεν μια απειλή αλλά έπειτα από την πάροδο μεγάλου χρονικού διαστήματος από τη στιγμή της ανάπτυξής της σίγουρα αποτελεί επιτυχία για την ανακάλυψή της, αλλά μπορεί να αποβεί μοιραία για την ακεραιότητα των πληροφοριών και τη διαθεσιμότητα των πόρων του συστήματος. Πρέπει να εντοπίζει έγκαιρα, σε μια real time βάση τις εισβολές.
- **Προσαρμοστικότητα.** Παρόλο που τα περισσότερα δικτυωμένα υπολογιστικά συστήματα (στο Internet), βασίζονται σε UNIX πλατφόρμες, ωστόσο κάθε ένα από αυτά έχει τις δικές του ξεχωριστές πολιτικές, διαφορετικές ανάγκες σε θέματα ασφάλειας. Συνεπώς ένα αποτελεσματικό IDS πρέπει να μπορεί αν όχι να προσαρμοστεί άμεσα στο νέο περιβάλλον, να έχει τα απαραίτητα εκείνα χαρακτηριστικά ώστε να αναβαθμίζεται και με λίγες τροποποιήσεις να μπορεί να εξυπηρετήσει νέες ανάγκες και στρατηγικές.
- **Αναβαθμισμότητα.** Πρέπει να είναι δυνατή η εισαγωγή νέων τεχνικών ανίχνευσης και αντιμετώπισης απειλών. Οι νέες αυτές τεχνικές θα πρέπει να μπορούν να συνυπάρξουν και να λειτουργήσουν αποδοτικά με τις υπάρχουσες βελτιώνοντας την ικανότητα του IDS για ανίχνευση και αντιμετώπιση νέων απειλών.
- **Συντηρησιμότητα.** Η ανανέωση της βάσης γνώσης των IDS που βασίζονται σε έμπειρα συστήματα για τον έλεγχο αν μια συγκεκριμένη σειρά πράξεων αποτελεί απειλή, δεν είναι και τόσο εύκολη υπόθεση. Απαιτεί γνώσεις διατήρησης και δημιουργίας βάσεων γνώσης, εμπείρων συστημάτων, κανόνων πράγματα που επιβαρύνουν επιπλέον τον διαχειριστή ασφαλείας. Το σύστημα λήψης αποφάσεων του IDS πρέπει να ενημερώνεται εύκολα, χωρίς να απαιτείτε η ανάγκη για ειδικές γνώσεις. Ικανότητες για εκμάθηση από προηγούμενους τρόπους αντιμετώπισης παρόμοιων εισβολών, καλής διαχείρισης - αξιοποίησης της γνώσης που έχει ήδη αποκτηθεί αποτελούν αναγκαία χαρακτηριστικά, αν αναλογιστεί κανείς το μεγάλο μέγεθος που μπορεί να προσεγγίσει η βάση γνώσης, εάν ενημερώνεται τακτικά με νέα σενάρια εισβολών.
- **Ελαχιστοποίηση των *false negatives*.** Ένα IDS πρέπει χαρακτηρίζεται από την ικανότητα να μην κατηγοριοποιεί μια ενέργεια φυσιολογική, ενώ αυτή να είναι απειλητική για την ακεραιότητα, και διαθεσιμότητα των στοιχείων του. Αυτό έχει μεγαλύτερη βαρύτητα από τον χαρακτηρισμό μιας πράξης ως ανώμαλης, ενώ αυτή να μη είναι (*false positive*).

1.3.3 Ένα Μοντέλο ανίχνευσης εισβολών

H Dorothy Denning, το 1987, παρουσίασε ένα μοντέλο ανίχνευσης εισβολών (Denning 1987), το οποίο είναι ανεξάρτητο τεχνολογικής πλατφόρμας, περιβάλλοντος εφαρμογής, ευπαθειών (vulnerabilities) ή είδος εισβολής, παρέχοντας έτσι μια γενική αρχιτεκτονική για την κατασκευή συστημάτων IDS γενικού σκοπού. Ομαδοποιεί τα στοιχεία του συστήματος σε:

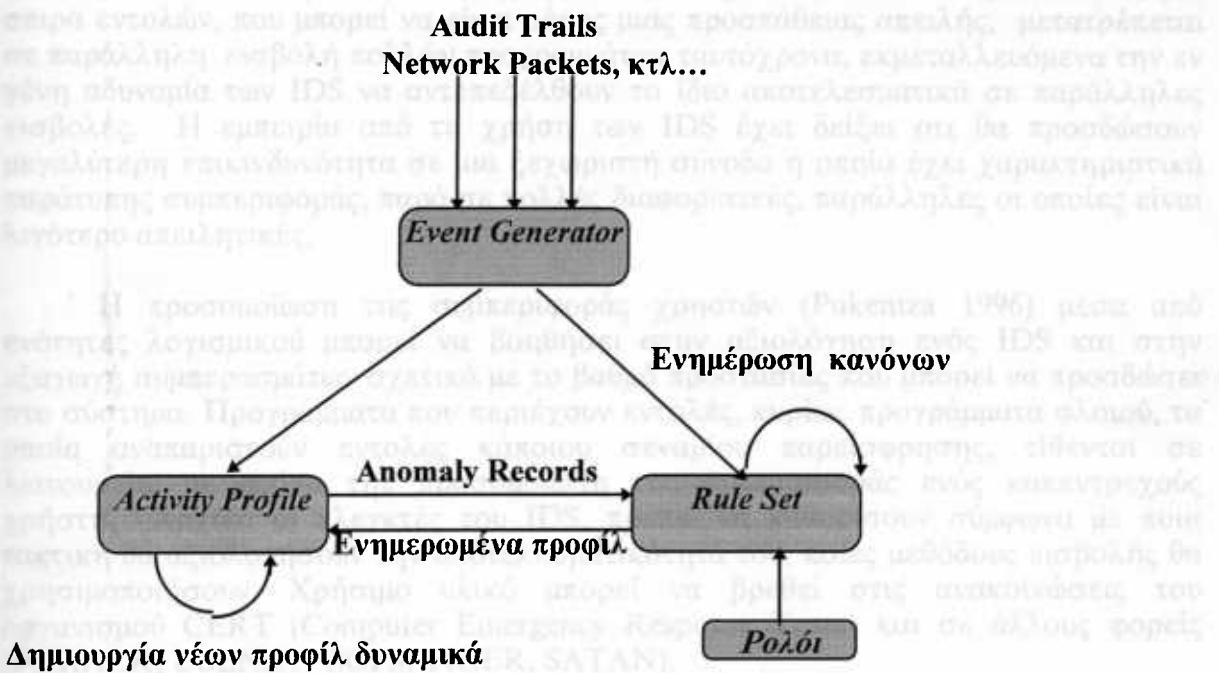
- **Υποκείμενα:** αποτελούν χρήστες ή διαδικασίες - προγράμματα χρηστών που εκτελούνται.
- **Αντικείμενα:** Αποτελούν τους πόρους του συστήματος (ΚΜΕ, μνήμη, χρήση συσκευών εισόδου εξόδου, κτλ.).
- **Audit records:** Περιγράφουν τις πράξεις στα αντικείμενα από τα υποκείμενα, καθώς και άλλα συμπληρωματικά στοιχεία όπως ο χρόνος που συνέβηκε η πράξη (timestamp), το ποσοστό πόρων που χρησιμοποιήθηκαν ((resource usage) των αρχείων που ανοίχτηκαν, των γραμμών που εκτυπώθηκαν, κτλ.).
- **Προφίλ:** Δομές που χαρακτηρίζουν τη συμπεριφορά των υποκειμένων στα αντικείμενα. Η συμπεριφορά αυτή συνδέεται με στατιστικές μετρικές των μεταβλητών που περιγράφουν το προφίλ του υποκειμένου προκειμένου να χαρακτηρίζουν την συμπεριφορά των αντικειμένων. Η σύγκρισή τους με παλαιότερες τιμές μπορεί να μας οδηγήσει στο συμπέρασμα εάν η συμπεριφορά κάποιου χρήστη ξεφεύγει από την κανονική, εάν είναι ανώμαλη σε σχέση με την στατιστικά προβλεπόμενη.
- **Anomaly Records:** Περιγράφουν την παρατυπία στην συμπεριφορά του χρήστη. Εάν η συμπεριφορά αυτή χαρακτηριστεί ανώμαλη και διαφοροποιείται από τις εν γένει νόρμες και κινήσεις του, παράγεται η εγγραφή περιγραφής του γεγονότος που χαρακτηρίζεται από παρατυπία (anomaly record) η οποία αποτελείται από τα εξής στοιχεία: <γεγονός, time-stamp, profile>.
- **Activity Rules:** Αποτελούν τους κανόνες οι οποίοι εάν ικανοποιηθούν οι συνθήκες (παρατηρηθεί κάποια μη αναμενόμενη συμπεριφορά), ενεργοποιούνται, ενημερώνουν τον υπεύθυνο ασφαλείας, για την παρατυπία που εμφανίστηκε και πολλές φορές προτείνουν τρόπους αντιμετώπισης της απειλής

Στο σχήμα που ακολουθεί παρουσιάζεται μια γενική αναπαράσταση του μοντέλου. Ο *Event Generator* είναι η διεπαφή του μοντέλου με το σύστημα που παρακολουθείτε. Δέχεται από αυτό πληροφορίες από τη χρήση του δικτύου, των πόρων του συστήματος, την απασχόληση των συσκευών εισόδου - εξόδου για κάθε χρήστη και γενικά ότι πληροφορία περιγράφεται στα audit trails του συστήματος. Ουσιαστικά φιλτράρονται - εξετάζονται οι πληροφορίες προκειμένου να μπορούν να τύχουν επεξεργασίας από τα υπόλοιπα υποσυστήματα του μοντέλου.

Το *Activity profile* σχετίζεται με την συντήρηση προφίλ συμπεριφοράς για τους χρήστες. Είναι υπεύθυνο για την αναγνώριση κάθε ανωμαλίας στην λειτουργία του συστήματος. Αυτό επιτυγχάνεται με εφαρμογή στατιστικών μεθόδων οι οποίες κρατάνε με έξυπνο τρόπο, με μεταβλητές και στατιστικές μετρικές την συμπεριφορά των χρηστών. Όταν υπάρχουν νέες τιμές στις μετρικές αυτές, γίνεται σύγκριση με τις παλαιότερες προκειμένου να μετρηθεί το ποσοστό παρέκκλισης και να ανανεωθεί το

προφίλ του χρήστη ή και να σημανθεί συναγερμός προς τον υπεύθυνο ασφαλείας για την παρατυπία. Υπάρχει δυνατότητα δημιουργία νέων προφίλ δυναμικά με τη δημιουργία νέων αντικειμένων και υποκειμένων στο σύστημα.

Το υποσύστημα *Rule set* χρησιμοποιεί κανόνες, οι οποίοι έχουν κωδικοποιήσει συγκεκριμένα σενάρια παρεισφρήσεων. Η συμπεριφορά του χρήστη συγκρίνεται με βάση αυτούς τους κανόνες και σε συνδυασμό με τις πληροφορίες για την εν γένει συμπεριφορά του χρήστη από το activity profiles, αυξάνει ή όχι το επίπεδο καχυποψίας για τις κινήσεις του χρήστη. Ταυτόχρονα η παρακολούθηση αυτή της δράσης του χρήστη βοηθάει την αναθεώρηση των προφίλ των χρηστών. Η βάση γνώσης ενημερώνεται όταν γίνουν γνωστοί νέοι τρόποι εισβολών.



Εικόνα 1. Γενική αναπαράσταση του μοντέλου ανίχνευσης εισβολών

Το μοντέλο της Denning έχει βρει μεγάλη απήχηση και σε αυτό στηρίχθηκαν για την κατασκευή τους τα περισσότερα από τα γνωστά συστήματα ανίχνευσης εισβολών. Με τον καιρό όμως εμφανίστηκαν δυσκολίες στην μοντελοποίηση σε αυτό νέων τεχνικών και μεθόδων που χρησιμοποιήθηκαν κυρίως σε νεώτερα IDS. Παράδειγμα αποτελεί η χρήση των νευρωνικών δικτύων τα οποία χρησιμοποιούν διαφορετικούς τρόπους για την κατηγοριοποίηση και εκμάθησης της συμπεριφοράς. Άλλα και τεχνικές όπως οι model - based, η χρήση αυτόνομων agents, η χρήση γράφων (GridIDS), προσδιορισμού προδιαθέσεων χρηστών, δυσκολεύονται να ενσωματωθούν άμεσα σε αυτή τη δομή.

Επίσης και στο θέμα της συντήρησης, ανανέωσης της βάσης γνώσης, παρουσιάζονται καινούργιες μέθοδοι για προσαρμογή της βάσης με νέα στοιχεία (knowledge adaptation, knowledge acquisition, learning), για τεχνικές εκμάθησης, όπου ο ρόλος του διαχειριστή μειώνεται αισθητά αφήνοντας το αυτοματοποιημένο σύστημα

μόνο του να εκτελεί τις περισσότερες από τις προηγούμενα προγραμματιστικές - χειρωνακτικές εργασίες.

1.3.4 Τρόποι αξιολόγησης της αποτελεσματικότητας ενός IDS

Η προσπάθεια εισβολής σε κάποιο σύστημα από πολλούς χρήστες ταυτόχρονα (tiger teams) ή από ένα χρήστη μέσα από πολλές διαφορετικές συνόδους ταυτόχρονα, είναι πολύ πιο επικίνδυνη, από έναν μεμονωμένο χρήστη. Έχουν αναπτυχθεί αλγόριθμοι οι οποίοι μετατρέπουν μια σειρά εντολών ή ένα πρόγραμμα φλοιού σε πολλά παράλληλα προγράμματα (Chung 1994). Με τον τρόπο αυτό, μια σειρά εντολών, που μπορεί να είναι μέρος μιας προσπάθειας απειλής, μετατρέπεται σε παράλληλη εισβολή πολλών προγραμμάτων ταυτόχρονα, εκμεταλλευόμενα την εν γένη αδυναμία των IDS να αντεπεξέλθουν το ίδιο αποτελεσματικά σε παράλληλες εισβολές. Η εμπειρία από τη χρήση των IDS έχει δείξει ότι θα προσδώσουν μεγαλύτερη επικινδυνότητα σε μια ζεχωριστή σύνοδο η οποία έχει χαρακτηριστικά παράτυπης συμπεριφοράς, παρά σε πολλές διαφορετικές, παράλληλες οι οποίες είναι λιγότερο απειλητικές.

Η προσομοίωση της συμπεριφοράς χρηστών (Pukentza 1996) μέσα από ενότητες λογισμικού μπορεί να βοηθήσει στην αξιολόγηση ενός IDS και στην εξαγωγή συμπερασμάτων σχετικά με το βαθμό προστασίας που μπορεί να προσδώσει στο σύστημα. Προγράμματα που περιέχουν εντολές, κυρίως προγράμματα φλοιού, τα οποία αναπαριστούν εντολές κάποιου σεναρίου παρείσφρησης, τίθενται σε λειτουργία, με στόχο την προσομοίωση της συμπεριφοράς ενός κακεντρεχούς χρήστη. Αρχικά οι ελεγκτές του IDS, πρέπει να καθορίσουν σύμφωνα με ποια τακτική θα αξιολογήσουν την αποτελεσματικότητά του, ποιες μεθόδους εισβολής θα χρησιμοποιήσουν. Χρήσιμο υλικό μπορεί να βρεθεί στις ανακοινώσεις του οργανισμού CERT (Computer Emergency Response Team) και σε άλλους φορείς (PHRACK, USENET, COPS, TIGER, SATAN).

1.3.5 Anomaly Intrusion Detection

1.3.5.1 Τεχνικές στατιστικής ανάλυσης

Στα συστήματα που χρησιμοποιούνται αυτές οι τεχνικές (Lunt 1989, Lunt 1992) χαρακτηριστική είναι η έννοια του προφίλ του χρήστη. Το προφίλ δημιουργείτε από τον τρόπο που ένα υποκείμενο δρά σε ένα αντικείμενο του συστήματος. Τα στατιστικά αυτά προφίλ σχεδιάζονται με τρόπο ώστε να χρησιμοποιούν με τον οικονομικότερο δυνατό τρόπο την μνήμη του συστήματος. Επιπλέον χαρακτηριστικό τους είναι η ευκολία αναπροσαρμογής τους δεδομένου ότι ίσως να είναι αναγκαία να γίνεται πολύ συχνά.

Το προφίλ του χρήστη απαρτίζεται από ένα σύνολο μετρικών - παραμέτρων οι οποίες ενημερώνονται ανάλογα με τη συμπεριφορά του. Η πληροφορία αυτή βασίζεται στην πληροφορία που κρατάει το σύστημα για αυτόν στα audit trails. Με βάση αυτά προσδιορίζονται τιμές σε συγκεκριμένες μετρικές από το σύνολο των

οποίων διατηρείται το συγκεκριμένο προφίλ συμπεριφοράς. Με τη συλλογή νέων πληροφοριών γίνεται σύγκριση με τις ήδη αποθηκευμένες τιμές και προσδιορίζεται το ποσοστό παρέκκλισης στην συμπεριφορά του χρήστη από την προβλεπόμενη. Εάν η τιμή περάσει κάποιο ανώτατο όριο απορρέει το συμπέρασμα ότι πρόκειται για ανώμαλη συμπεριφορά και πιθανά εισβολή. Μερικές από τις μετρικές αυτές περιλαμβάνουν:

- **Συχνότητα χρήσης πόρων.** Σχετίζεται με τη συχνότητα της χρήσης πόρων του συστήματος. Παραδείγματα είναι η συχνότητα εισόδου του χρήστη στο σύστημα, χρήσης των μεταγλωττιστών, του φλοιού, των εκδοτών, κτλ.
- **Τυπικές μετρήσεις.** Ενώ η παραπάνω μετρικές σχετίζονται με την συχνότητα που προσπελάζονται συγκεκριμένα στοιχεία του συστήματος, οι μετρικές αυτές προχωρούν στον στατιστικό υπολογισμό τιμών σχετικές με την χρήση των πόρων αυτών.
- **Καθολικές μετρικές.** Σχετίζονται με την καταγραφή τιμών σχετικά με την συνολική δραστηριοποίηση του χρήστη στο σύστημα. Τέτοιες είναι οι τιμές της χρήσης των συσκευών εισόδου - εξόδου ή προσπέλασης αρχείων σε ολόκληρο το σύστημα για τον συγκεκριμένο χρήστη.

Πλεονεκτήματα

- Μπορούν εύκολα να χρησιμοποιηθούν τεχνικές προερχόμενες από την στατιστική επιστήμη. Μια συμπεριφορά χαρακτηρίζεται ως ανώμαλη εάν στον χρόνο παρουσιάζει μεγάλη διακύμανση τιμών από την προβλεπόμενη.

Μειονεκτήματα

- Εάν ένας χρήστης γνωρίζει ότι παρακολουθείται, μπορεί να παρεκκλίνει σταδιακά από την εν γένη συμπεριφορά του, έτσι ώστε μετά το πέρασμα κάποιου χρονικού διαστήματος, η (νέα) συμπεριφορά να τείνει να είναι παράτυπη. Το σύστημα έχει δημιουργήσει ένα νέο προφίλ, το οποίο όμως είναι αποδεκτό, γιατί έχει προκύψει από την σταδιακή - αργή παρέκκλιση από τις συνηθισμένες νόρμες και συνήθειες. Παρόλαυτά όμως η νέα αυτή δραστηριότητα ίσως είναι απειλητική για την ακεραιότητα του συστήματος. Αυτός είναι και ο λόγος που τα περισσότερα IDS που χρησιμοποιούν στατιστικές τεχνικές για ανακάλυψη ανώμαλης συμπεριφοράς, έχουν και ένα έμπειρο σύστημα με για προσδιορισμό misuse συμπεριφοράς, όταν προκύψει άμεσα παρεισφρητική δραστηριότητα.
- Είναι δύσκολος ο καθορισμός ορίων ευαισθησίας (thresholds), πάνω από τα οποία μια συμπεριφορά θεωρείται απειλητική ενώ χαμηλότερα όχι. Θέτοντας χαμηλά όρια αυξάνουμε την πιθανότητα για false positives λάθη, ενώ με μεγάλα όρια έχουμε την περίπτωση για false negative λάθη.

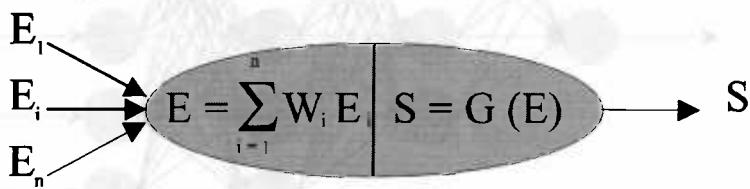
1.3.5.2 Νευρωνικά Δίκτυα

Τα IDS που στηρίζονται στις τεχνικές των εμπείρων συστημάτων, έχουν σοβαρό μειονέκτημα την δυσκολία καθορισμού ενός ανώτατου ορίου (threshold) πέρα από το οποίο πρόκειται να σημανθεί alert προς τον υπεύθυνο ασφαλείας (γιατί μάλλον πραγματοποιείται εισβολή). Δίνοντας ένα αρκετά χαμηλό όριο, θα παράγονται πολλοί συναγερμοί προς τον υπεύθυνο, τα περισσότερα από τα οποία δεν είναι παρεισφρήσεις. Αντίστοιχα, ένα αρκετά υψηλό όριο δεν θα δώσει στον υπεύθυνο

ειδοποίηση για κάποια σίγουρη απειλή. Η ανάγκη για αποτελεσματικό φιλτράρισμα των audit πληροφοριών καθίσταται αναγκαία μέσα από την εφαρμογή έξυπνων μηχανισμών, ειδικά σε συστήματα όπου ο ρυθμός παραγωγής πληροφορίας από την δράση των χρηστών είναι μεγάλος (τα audit trails μπορεί να φτάνουν σε πολλά Mbytes ανά ώρα).

Τα νευρωνικά δίκτυα, σε συνδυασμό με ένα έμπειρο σύστημα με το οποίο θα συνεργάζονται, μπορεί να δώσουν αξιόλογα αποτελέσματα στην αποδοτική λειτουργία ενός IDS.

Ο ορισμός των νευρωνικών δικτύων (Rumelhart 1994) προέρχεται από πολύ παλιά (1940), όπου δόθηκε ο ορισμός του τυπικού νευρώνιου:



Εικόνα 2. Ένα τυπικό νευρώνιο.

Τα νευρώνια αποτελούν τα συστατικά στοιχεία των νευρωνικών δικτύων. Αποτελούν γραμμικά αυτόματα τα οποία οργανώνονται σε επίπεδα. Κάθε νευρώνιο δέχεται ως είσοδο ένα ερέθισμα, τις τιμές κάποιας μεταβλητής ή ενός διανύσματος μεταβλητών E_i . Υπολογίζεται το άθροισμα των βαρών των δεδομένων εισόδου και στη συνέχεια με βάση αυτό το άθροισμα εξάγεται το τελικό αποτέλεσμα από το νευρώνιο με βάση μια άλλη συνάρτηση G .

Τα συστατικά στοιχεία του νευρώνιου είναι:

Τα στοιχεία εισόδου (E_1, E_2, \dots, E_n) αποτελούν την πληροφορία που εισάγεται στο νευρώνιο και μπορεί να προέρχεται από κάποιο άλλο νευρώνιο, από το ίδιο το νευρώνιο ή από εξωτερικές πηγές.

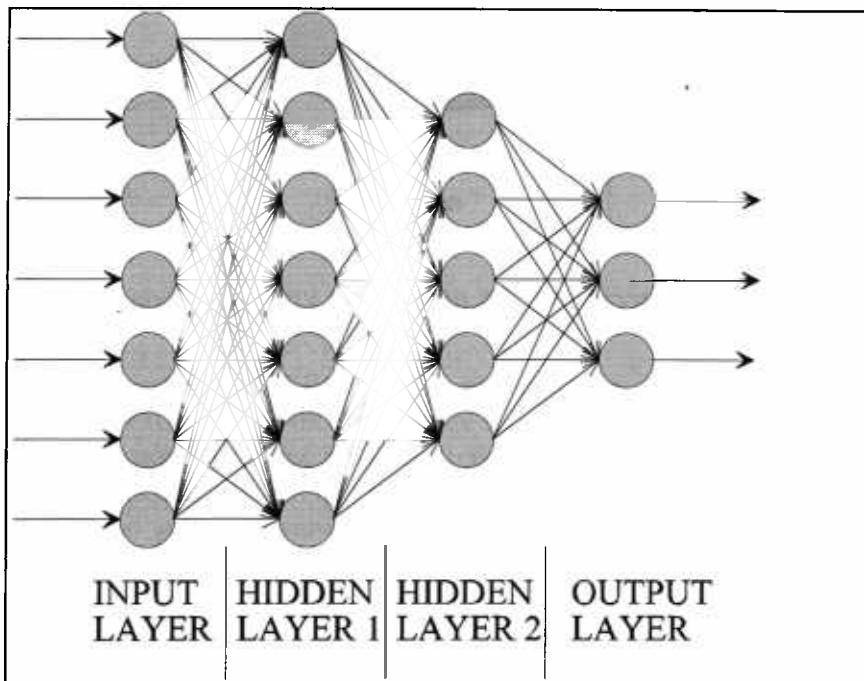
Τα βάρη (W_1, W_2, \dots, W_n) υποδηλώνουν την σημασία που κάθε στοιχείο εισόδου E_i έχει στον υπολογισμό του αποτελέσματος από το νευρώνιο.

Ο υπολογισμός μιας τιμής σχετικά με τις εισόδους και τη σημασία κάθε μιας στο νευρώνιο. Συνήθως το αποτέλεσμα είναι το άθροισμα $\sum W_i E_i$.

Η συνάρτηση G , η οποία με βάση το προηγούμενο εξαγόμενο, υπολογίζει την τελική απόφαση του νευρώνιου.

Η απόφαση του νευρώνιου S αποτελεί την τελική κρίση του και η τιμή της διαδίδεται σε άλλα νευρώνια ως είσοδος σε αυτά ή σε εξωτερικές πηγές.

Τα αποτελέσματα αυτά με τη σειρά τους, αποτελούν εισόδους σε άλλα νευρώνια ή σε ένα σύνολο νευρώνιων και παράγεται το τελικό εξαγόμενο από τα νευρώνια που βρίσκονται στο τελευταίο επίπεδο.

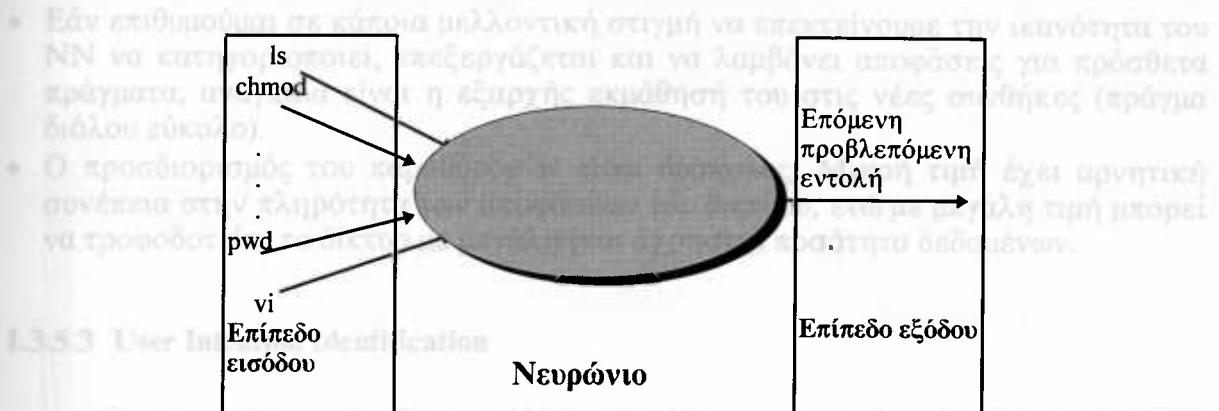


Εικόνα 3. Αρχιτεκτονική πολλών επιπέδων.

Μια από τις χαρακτηριστικές ιδιότητες των NN είναι η ικανότητά τους για μάθηση. Έχοντας υλοποιήσει ένα NN, το πρώτο πράγμα που πρέπει να γίνει είναι η εκμάθησή του σε συγκεκριμένους τύπους συμπεριφοράς. Δίνοντας ένα συγκεκριμένο input και το αναμενόμενο output, το NN μαθαίνει ένα τρόπο δράσης. Η ύπαρξη ενός αλγόριθμου, ο οποίος θα διορθώνει τα αποτελέσματα του NN είναι αναγκαίος, προκειμένου αυτό να μάθει σωστά να αντιστοιχίζει ορισμένα input σε αντίστοιχα output. Το output που παράγεται από τα νευρώνια, λειτουργεί ως input, ανατροφοδοτώντας το δίκτυο ξανά με στοιχεία, για την καλύτερη συμπεριφορά του.

Στο πεδίο των IDS (Debar 1992a, Debar 1992b, Guiner 1991, Doumas 1992, Σπύρου 1993, Κοκολάκης 1994), το NN δέχεται ως είσοδο πληροφορίες από τα audit trails του συστήματος που παρακολουθείται. Αφού τις επεξεργαστεί, τις φιλτράρει και διατηρεί προφίλ για τον κάθε χρήστη. Οι είσοδοι στα νευρώνια είναι η εντολή και οι προηγούμενες w εντολές (το w είναι το μέγεθος του παραθύρου των παρελθόντων εντολών που έχει εκτελέσει ο χρήστης) τις οποίες λαμβάνει υπόψιν του το NN προκειμένου να προβλέψει την επόμενη εντολή του. Από τη στιγμή που το NN εκπαιδευτεί με ένα σύνολο αντιπροσωπευτικών εντολών του χρήστη, δημιουργεί ένα προφίλ συμπεριφοράς για αυτόν.

Στο σχήμα που ακολουθεί αναπαριστάνονται οι προηγούμενες w εντολές του χρήστη και το νευρώνιο προσπαθεί να προβλέψει την επόμενη εντολή.



Εικόνα 4. Χρήση νευρωνίου για την πρόβλεψη της επόμενης εντολής του χρήστη

Τα NN έχουν χρησιμοποιηθεί και σε συνεργασία με άλλες τεχνικές όπως τα έμπειρα συστήματα. Μπορούν να αποτελέσουν ιδανικά φίλτρα πληροφοριών δίνοντας στο έμπειρο σύστημα μόνο εκείνες που είναι χρήσιμες και ικανές για την παραγωγή συμπερασμάτων σχετικά με πιθανή παρείσφρηση. Έχουν δείξει ότι μπορούν να μειώνουν κατά 80% το μέγεθος των εισερχόμενων προς εξέταση πληροφοριών. Το καλό φιλτράρισμα των δεδομένων είναι απόρροια της καλής εκπαίδευσης του δικτύου, του τρόπου εκμάθησης που χρησιμοποιήθηκε (των αλγορίθμων), της επανατροφοδότησης των αποτελεσμάτων ξανά στο σύστημα.

Πλεονεκτήματα

- Έχουν την δυνατότητα να κατηγοριοποιούν τύπους και προφίλ συμπεριφοράς χρηστών ή ομάδες αυτών, με λιγότερο ακριβής διαδικασίες (fuzziness), δίνοντας ένα σοβαρό πλεονέκτημα σε σχέση με τις στατιστικές μεθόδους.
- Εάν εκπαιδευτεί το δίκτυο πάνω σε συγκεκριμένους τρόπους συμπερασματολογίας, είναι πολύ δύσκολο να “ξεχάσει” πως οδηγήθηκε σε μια συγκεκριμένη απόφαση. Λόγω της μακροχρόνιας μνήμης τους, μπορούν να διατηρούν τους γενικούς κανόνες συμπεριφοράς, ενώ στη βραχυχρόνια μνήμη, διατηρούν λεπτομερή στοιχεία για την εκάστοτε περίπτωση λήψης αποφάσεων που εξετάζεται.
- Μπορούν να αποτελέσουν άριστα φίλτρα των audit πληροφοριών, (απορρίπτουν έως και 80% των πληροφοριών) εξαιτίας της fuzziness που τα διακρίνει.
- Λόγω της γενικής αρχιτεκτονικής τους, ένα NN μπορεί εύκολα να προσαρμοστεί για να λειτουργήσει σε διαφορετικά περιβάλλοντα.

Μειονεκτήματα

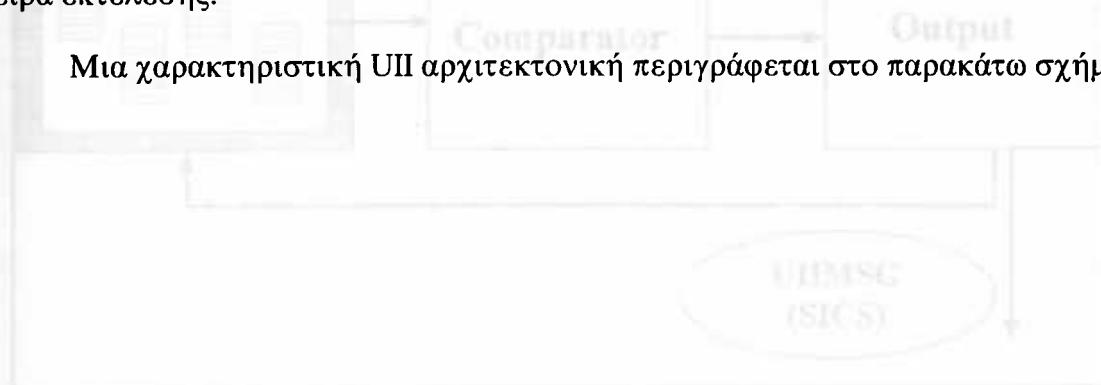
- Η διαδικασία εκπαίδευσης του δικτύου είναι αρκετά δύσκολη υπόθεση. Μπορεί να καταναλώσει πολύ από τον χρόνο των σχεδιαστών και του υπεύθυνου ασφαλείας. Όσο καλά και να ισχυριζόμαστε πως είναι εκπαιδευμένο, μπορεί επίμονα να δίνει λάθος αποτελέσματα σε συγκεκριμένα input, χωρίς να διαφαίνεται ξεκάθαρα η αιτία. Απαιτείται ιδιαίτερη προσοχή κατά τη διάρκεια εκμάθησης του δικτύου. Απροσεξίες και παραλήψεις μπορεί να οδηγούν σε τελείως διαφορετικά συμπεράσματα από αυτά που θα έπρεπε.
- Η χρήση των NN είναι ακόμα σε πειραματικό στάδιο. Αυτό εξηγεί την ανικανότητα εκμάθησης συγκεκριμένων τρόπων λήψης αποφάσεων, την δυσκολία καθορισμού του επαρκούς μεγέθους για κάθε περίπτωση.

- Εάν επιθυμούμαι σε κάποια μελλοντική στιγμή να επεκτείνουμε την ικανότητα του NN να κατηγοριοποιεί, επεξεργάζεται και να λαμβάνει αποφάσεις για πρόσθετα πράγματα, αναγκαία είναι η εξαρχής εκμάθησή του στις νέες συνθήκες (πράγμα διόλου εύκολο).
- Ο προσδιορισμός του παραθύρου w είναι δύσκολος. Μικρή τιμή έχει αρνητική συνέπεια στην πληρότητα των αποφάσεων του δικτύου, ενώ με μεγάλη τιμή μπορεί να τροφοδοτείτε το δίκτυο με μεγάλη (και άχρηστη) ποσότητα δεδομένων.

1.3.5.3 User Intention Identification

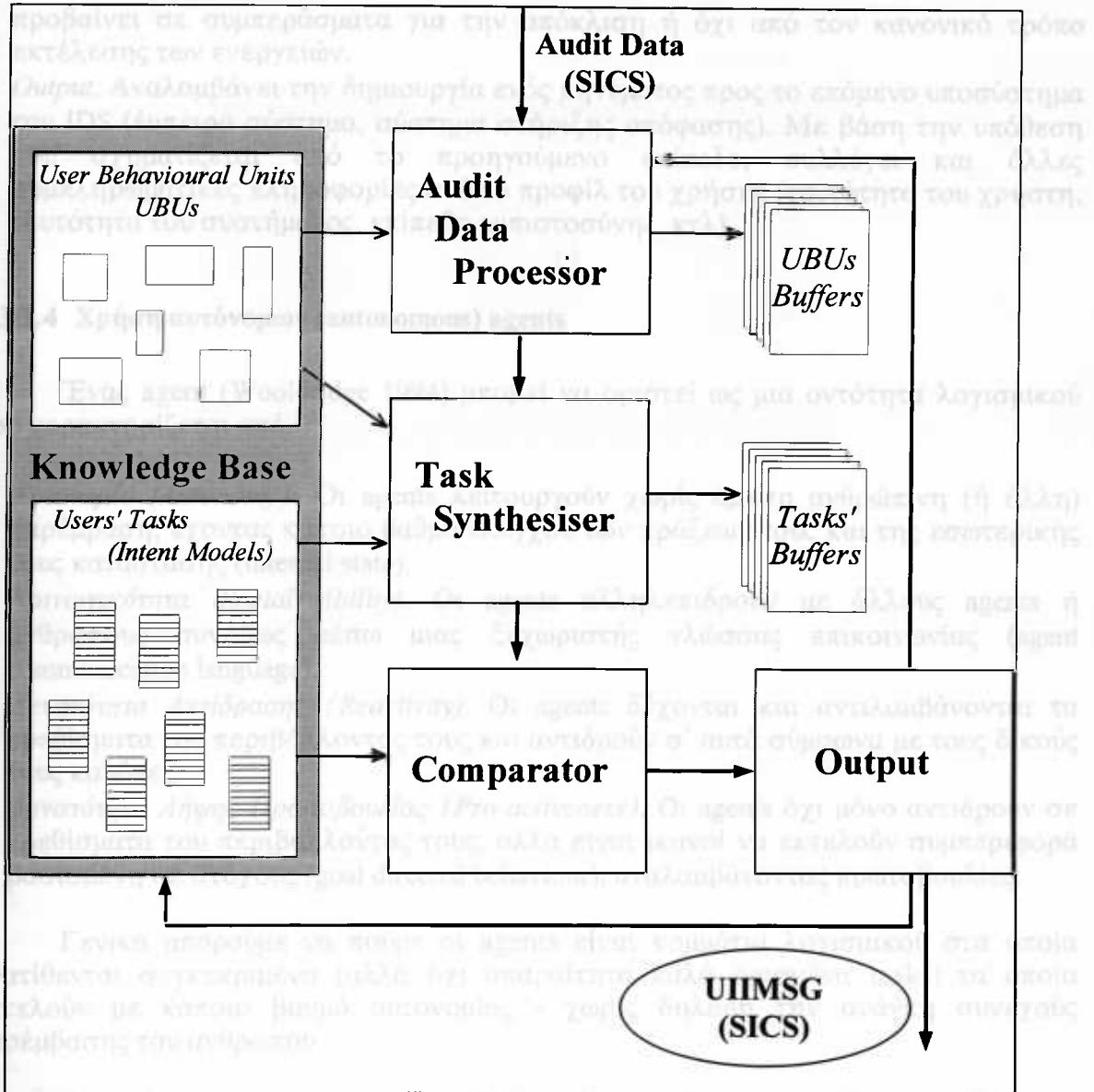
Οι τεχνικές αυτές (Spyrou 1995) στηρίζονται στην θεωρία ότι ο χρήστης χρησιμοποιεί το σύστημα προκειμένου να υλοποιήσει συγκεκριμένους στόχους (goals) που έχει θέσει, τους οποίους πραγματώνει με την ολοκλήρωση επιμέρους ενεργειών (tasks). Βασικός στόχος των τεχνικών αυτών είναι να βρεθούν εκείνες οι πράξεις οι οποίες είναι απειλητικές για την ασφάλεια του συστήματος, αλλά οι επιμέρους ενέργειες από τις οποίες αποτελούνται δεν μπορούν να χαρακτηριστούν ως απειλητικές. Αυτό που απαιτείται είναι η μελέτη της αιτιολογίας (rationality) των επιμέρους αυτών ενεργειών, σε σχέση βέβαια και με τον καθολικό στόχο που έχει θέσει ο χρήστης. Μια συμπεριφορά χαρακτηρίζεται ως ύποπτη εάν η εκτέλεση των πράξεων που ολοκληρώνουν τις tasks παρεκκλίνει από την ομαλή, προκαθορισμένη σειρά εκτέλεσης.

Μια χαρακτηριστική UII αρχιτεκτονική περιγράφεται στο παρακάτω σχήμα



Εικόνα 5. Τελικό πατρικό

- Άλλη μια γνωστή διάταξη που τα δεδομένα πάρεται, και τα μεταφέρεται σε μερική κατανόηση πριν από το SICS ήταν Knowledge management. Σήδιος είναι το υποστημένο τρόπο της λήψης των δεδομένων.
- Ταύτιση του παραπάνω παραδοσιακού με την βασική διαδικασία των παραπομπών, των ορισμένων βασιζόμενων στην αλληλεπίδραση των λειτίνων των ADP. Η παραπομπή στο ΓΕΣ, τη οποία, επομένως θα γίνεται καθένας αντιστοιχείος με την ίδια.
- Comparison. Ο αναδιπλός γνωστός είναι βασικότερο μηχανισμό συγχρονιστικής της τεχνολογίας. Είναι παλιότερο για τη διάταξη των παραπομπών, των ορισμένων από την επιχείρηση με την προηγούμενη επίκειδα, και περιήλθε περίπλοκα πριν από την πρόσφατη όλη αύξηση εισήλατη ή όχι. Συγκρινεί τη φασή λειτίνων που παρέρχονται στην παραπομπική κλήση με στόχο την απόδοση της, από την παραπομπή μετά την επιχείρηση του χρήστη.



Εικόνα 5. UII αρχιτεκτονική.

- **Audit data processor.** Επεξεργάζεται τις audit πληροφορίες και τις μετατρέπει σε μορφή κατανοητή προς τις TKS (Task Knowledge structures). Στόχος είναι το αποδοτικό και γρήγορο φίλτραρισμα των πληροφοριών.
- **Task Synthesizer.** Το επόμενο επίπεδο προχωρεί σε μια βασική διερμηνεία της συμπεριφοράς των χρηστών βασιζόμενο στην πληροφορία που λαμβάνει από τον ADP. Προσδιορίζονται οι TKS, οι tasks, ενώ με τη χρήση κανόνων γίνονται αντιστοιχίσεις μεταξύ τους.
- **Comparator.** Ο comparator αποτελεί τον βασικότερο μηχανισμό συμπερασματολογίας της τεχνικής. Είναι υπεύθυνος για την διερμηνεία της συμπεριφοράς του χρήστη όπως αυτή περιγράφεται από τα προηγούμενα επίπεδα, και παράγει υποθέσεις σχετικά με το αν πρόκειται για πιθανή εισβολή ή όχι. Συγκρίνει τις δομές γνώσεις που υπάρχουν για την πραγματοποίηση κάποιου στόχου με αυτές που έχουν παρατηρηθεί από την συμπεριφορά του χρήστη και

προβαίνει σε συμπεράσματα για την απόκλιση ή όχι από τον κανονικό τρόπο εκτέλεσης των ενεργειών.

- *Output*. Αναλαμβάνει την δημιουργία ενός μηνύματος προς το επόμενο υποσύστημα του IDS (έμπειρο σύστημα, σύστημα στήριξης απόφασης). Με βάση την υπόθεση που σχηματίζεται από το προηγούμενο επίπεδο, συλλέγει και άλλες συμπληρωματικές πληροφορίες από το προφίλ του χρήστη (ταυτότητα του χρήστη, ταυτότητα του συστήματος, επίπεδο εμπιστοσύνης, κτλ)

1.3.5.4 Χρήση αυτόνομων (autonomous) agents

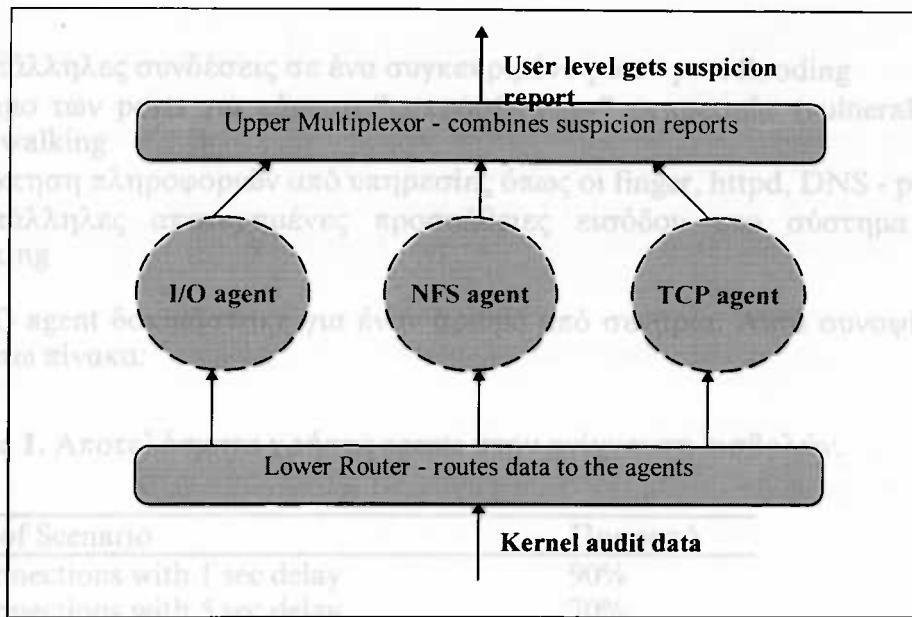
Ένας agent (Wooldridge 1994) μπορεί να οριστεί ως μια οντότητα λογισμικού που χαρακτηρίζεται από:

- *Αυτονομία (Autonomy)*. Οι agents λειτουργούν χωρίς άμεση ανθρώπινη (ή άλλη) παρέμβαση, έχοντας κάποιο βαθμό ελέγχου των πράξεων τους και της εσωτερικής τους κατάστασης (internal state).
- *Κοινωνικότητα (Social Ability)*. Οι agents αλληλεπιδρούν με άλλους agents ή ανθρώπους συνήθως μέσω μιας ξεχωριστής γλώσσας επικοινωνίας (agent communication language).
- *Δυνατότητα Αντίδρασης (Reactivity)*. Οι agents δέχονται και αντιλαμβάνονται τα ερεθίσματα του περιβάλλοντος τους και αντιδρούν σ' αυτά σύμφωνα με τους δικούς τους κανόνες.
- *Δυνατότητα Λήψης Πρωτοβουλίας (Pro-activeness)*. Οι agents όχι μόνο αντιδρούν σε ερεθίσματα του περιβάλλοντος τους, αλλά είναι ικανοί να εκτελούν συμπεριφορά βασισμένη σε στόχους (goal directed behaviour), αναλαμβάνοντας πρωτοβουλίες.

Γενικά μπορούμε να πούμε οι agents είναι κομμάτια λογισμικού στα οποία ανατίθενται συγκεκριμένα (αλλά όχι απαραίτητα καλά ορισμένα tasks) τα οποία εκτελούν με κάποιο βαθμό αυτονομίας - χωρίς δηλαδή την ανάγκη συνεχούς παρέμβασης του ανθρώπου

Στο χώρο της ανίχνευσης εισβολών έχουν γίνει προσπάθειες υιοθέτησης αυτόνομων agents (Crosbie 1995a, Crosbie 1995b) προκειμένου να ανιχνευθεί παρεισφρητική συμπεριφορά.

Οι πιο τολμηρές από τις προσπάθειες αυτές αναφέρονται στη χρήση multi-agent συστημάτων όπου ο κάθε agent αναλαμβάνει ένα task και συνεργάζεται με τους άλλους agents ή με μια προϊστάμενη αρχή (agency) προκειμένου να φέρει σε πέρας το task αυτό.



Εικόνα 6. Γενική Agent - based Αρχιτεκτονική ενός IDS.

Μία τέτοια προσέγγιση προϋποθέτει τα εξής:

- Κάθε agent έχει το δικό του μηχανισμό συμπερασματολογίας σχετικά με την αξιολόγηση των γεγονότων που συμβαίνουν στο σύστημα.
- Κάθε agent διαχειρίζεται δικές του βάσεις γνώσης και γνωρίζει ποια audit trails τον αφορούν,
- Κάθε agent μπορεί να επικοινωνήσει με τα άλλα συστατικά του συστήματος μέσα από συγκεκριμένα Application Program Interfaces (APIs).

Μια προσπάθεια χρήσης agents σε ένα IDS έγινε από το COAST Laboratory. Από τη στιγμή που οι agents ενεργούν σχετικά αυτόνομα, οι κατασκευαστές του συστήματος αποφάσισταν να χρησιμοποιήσουν agents, προκειμένου αυτοί να αντιμετωπίζουν σχετικά απλές εισβολές.

Ένας από τους agents που κατασκευάστηκε παρακολουθούσε τις συνδέσεις που υπήρχαν σε ένα δίκτυο, χρησιμοποιώντας πληροφορία από τα audit trails του συστήματος (σχετικά με τις κλήσεις connect() και accept()). Οι μετρικές που χρησιμοποιήθηκαν ήταν:

1. Συνολικός αριθμός των socket connections,
2. Μέσος χρόνος μεταξύ δύο διαδοχικών socket connections
3. Ελάχιστος χρόνος μεταδύο δύο socket connections
4. Μέγιστος χρόνος μεταδύο δύο socket connections
5. client port
6. server port

Πιθανές εισβολές που θα μπορούσαν να αντιμετωπιστούν από έναν τέτοιο agent θα ήταν:

- Ανεπάλληλες συνδέσεις σε ένα συγκεκριμένο port - port flooding
- Ψάξιμο των ports για εύρεση “ευπρόσβλητων” υπηρεσιών (vulnerable services) - port walking
- Απόκτηση πληροφοριών από υπηρεσίες όπως οι finger, httpd, DNS - probing
- Ανεπάλληλες αποτυχημένες προσπάθειες εισόδου στο σύστημα - password cracking

Ο agent δοκιμάστηκε για έναν αριθμό από σενάρια. Αυτά συνοψίζονται στον παρακάτω πίνακα:

Πίνακας 1. Αποτελέσματα χρήσης agents στην ανίχνευση εισβολών.

Type of Scenario	Ποσοστό
10 connections with 1 sec delay	90%
10 connections with 5 sec delay	70%
10 connections with 30 sec delay	40%
10 connections with 1 min delay	30%
Rapid connections, then random pauses	80%
Intermittent connections	10%
Connections to privileged ports	90%
Connections to any port	70%

1.3.5.5 Χρήση γράφων (GrIDS - Graph based Intrusion Detection System)

Πολλές από τις μεθόδους ανίχνευσης εισβολών, έχουν την ικανότητα για αναγνώριση εισβολέων σε ένα υπολογιστή (host) ή σε ένα δίκτυο ενός οργανισμού. Ένα βασικό χαρακτηριστικό που έχει η μέθοδος GrIDS (Staniford-Chen 1996), είναι η δυνατότητα για ανακάλυψη εισβολών σε δίκτυα μεγάλης κλίμακας. Η εμφάνιση του σκουληκιού (worm) του Internet, στα τέλη της δεκαετίας του '80, παρέλυσε σε λίγες ώρες ένα μεγάλο κομμάτι του διαδικτύου. Εάν παρόμοια απειλή εμφανιζόταν σήμερα, τα αποτελέσματα θα ήταν σίγουρα πολύ χειρότερα, δεδομένης της τεράστιας αύξησης του δικτύου καθημερινά. Σε τέτοιες περιπτώσεις εισβολών, ενθαρρυντικά αποτελέσματα μπορεί να δώσει η μέθοδος GrIDS.

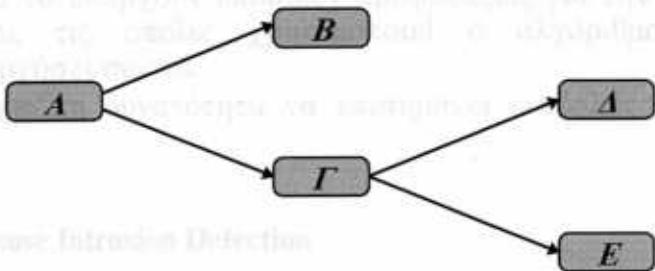
Στόχος είναι η ανάλυση της δραστηριότητας των κόμβων που συνεργούν σε ένα δίκτυο, η παράσταση της συμπεριφοράς σε μορφή γράφων (activity graphs), οι οποίοι με τη σειρά τους εξετάζονται. Από την ανάλυση που προκύπτει απορρέουν συμπεράσματα σχετικά με τυχόν παράτυπη δραστηριότητα στο δίκτυο. Εάν σε ένα δίκτυο εξαπολυθεί ένα σκουλήκι (worm), από τον υπολογιστή Α και αυτός μολύνει με τη σειρά του τους Β και Γ, τότε θα φτιαχτεί ένα γράφημα της μορφής 1. Εάν παρέλθει αρκετό χρονικό διάστημα χωρίς την συνέχιση αντίστοιχης δραστηριότητας, ο γράφος διαγράφεται και η συμπεριφορά δεν θεωρείται επικίνδυνη. Εάν όμως παρατηρηθεί η μόλυνση και σε άλλους υπολογιστές του δικτύου, τότε ο γράφος συνεχώς μεγαλώνει. Ο γράφος που δημιουργείται έχει τη μορφή δένδρου, μορφή που χαρακτηρίζει τη δράση των σκουληκιών. Εάν το μέγεθος του δένδρου ξεπεράσει ένα συγκεκριμένο όριο, ανακοινώνεται η ύπαρξη σκουληκιού.

Το λογισμικό του GrIDS, πρέπει να βρίσκεται εγκατεστημένο σε κάθε υπολογιστή του δικτύου. Περιέχει ένα κομμάτι που συλλέγει πληροφορίες για τη συμπεριφορά κάθε κόμβου, ενώ ένα άλλο στέλνει αναφορές (reports) στην διεργασία παραγωγής γράφων. Η διεργασία αυτή, αφού δημιουργήσει τους γράφους, στέλνει πληροφορίες στην αντίστοιχη διεργασία του πατέρα - κόμβου, ο οποίος βρίσκεται σε υψηλότερο επίπεδο, ακολουθώντας την φυσική τοπολογία του δικτύου. Υπάρχει ένας κεντρικός σταθμός ο οποίος συλλέγει πληροφορίες για τους υπο-γράφους που δημιουργούνται, έχοντας πάντα υπόψιν την φυσική διάρθρωση του δικτύου, εξετάζοντας την εμφάνιση δενδρικών σχηματισμών (στην περίπτωση εξέτασης σκουληκιών).

Κάθε γράφος περιέχει καθολικές μεταβλητές - χαρακτηριστικά σχετικά με το είδος των δικτυακών προσβολών που εξετάζει. Υπάρχουν κανόνες με τους οποίους καθορίζονται εάν πρέπει να ενωθούν δύο γράφοι, υπολογίζοντας τις τιμές των μεταβλητών κάθε γράφου, κτλ. Νέοι γράφοι μπορούν να δημιουργηθούν, σε υψηλότερο ιεραρχικό επίπεδο, λαμβάνοντας πάντα υπόψιν τη φυσική τοπολογία του δικτύου, αποκρύπτοντας λεπτομέρειες σχετικά με τις συνδέσεις των κόμβων και την ιεραρχία τους. Ένα δίκτυο μπορεί να παρασταθεί με την κορυφή ενός γράφου, εάν πρώτα εξεταστεί οτι δεν παρατηρείται σε αυτόν παράτυπη συμπεριφορά. Με αυτόν τον τρόπο μειώνονται τα δεδομένα για εξέταση, ο αλγόριθμος λειτουργεί σε ένα αφαιρετικό επίπεδο, φιλτράρονται οι πληροφορίες και παραμένουν λιγότερες για εξέταση στα υψηλότερα επίπεδα.

Μηχανισμοί εξέτασης

- Πήραν την απόφαση πώς θα αποτελέσει την πρώτη παραγάγοντας μια διάταξη για την παραγωγή της σε αυτόν τον κόμβο.
- Διέπιπτε σε αυτόν τον κόμβο για να επιλέγει την πρώτη παραγάγοντας μια γράφη πάροι.

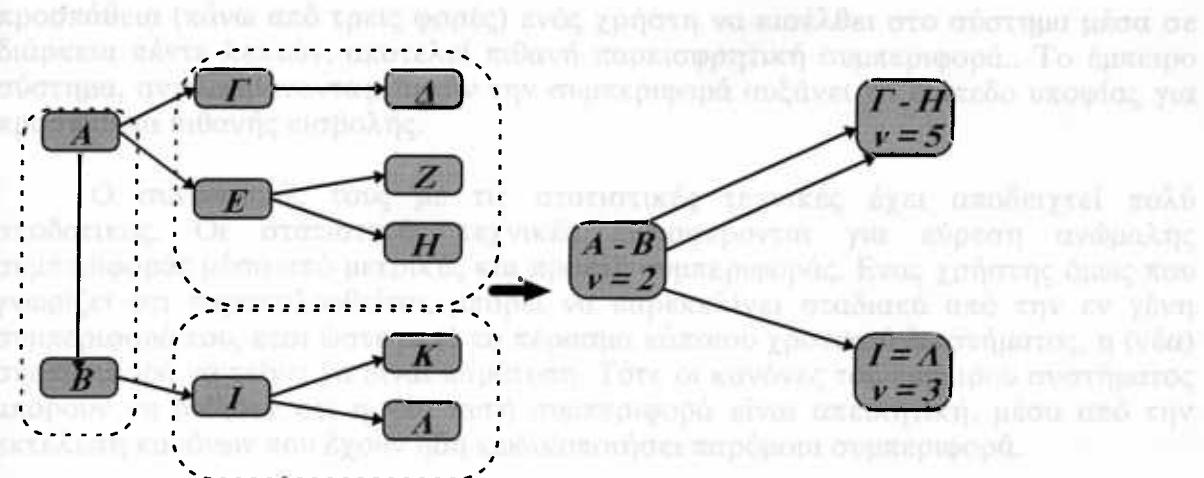


13.5. Minor Intrusion Detection

Εικόνα 7. Ο τρόπος εξάπλωσης ενός προγράμματος σκουληκιού σε ένα δίκτυο

Το πρότυπο πλευράς εργού διέβει την προστασία υποτελέσματα στην χώρα του, σε IDS (van 1988; Linn 1992; Hilder 1992). Μπορεί να συντηρούν μια βασική γνώσης με την προηγούμενη για «μέτρηση» και να διέργαν λεπτά, συμβολίζοντας την αντεπίθετη προστασία, με την προηγούμενη για «μέτρηση» στην πατέρα. Οι λεπτούς περιγράφουν έπειτα συμπεριφορές η οποία πουλήγεται από συνάδαις πληθύσματος. Στο παρόν μεσονετηρίου μέλεκτε την πεθόντη έναν ακόρετη, η στήμαση την πατέρας την μόστις γνώση, με από το οποίον παραπέμπει περπάν και είναι πιο σύρραγος, επιπλέον, την νεοτερή πρόσωπος παρέμβαση, όπως την παραπέμπει την πατέρα στην πατέρα του.

Τα ρευματικά δέρχονται με διαδρομή τη μεσή της των συστήματος. Επομένως, κανέναν που μετέβει τη περίπτωση λέγεται να έχει διανομή συστήματος.



Εικόνα 8. Αφαιρετική αναπαράσταση που χρησιμοποιεί η GrIDS τεχνική.

Πλεονεκτήματα

- Παρέχει πιο ακριβή έλεγχο της δραστηριότητας του δικτύου από άλλες τεχνικές (πχ Firewalls).
- Φαίνεται αποδοτικός στην προστασία δικτύων μεγάλης κλίμακας, δεδομένης της καταστροφής που επιφέρει η δράση κακόβουλων προγραμμάτων (πχ. σκουληκιών) σε μεγάλα δίκτυα (Internet).

Μειονεκτήματα

- Πρέπει να υπάρχουν επιπλέον προφυλάξεις για την προστασία των γραμμών του δικτύου, τις οποίες χρησιμοποιεί ο αλγόριθμος, προκειμένου αυτός να λειτουργήσει σωστά.
- Δεν έχει τη δυνατότητα να επισημάνει εισβολές που αναπαράγονται με αργό ρυθμό.

1.3.6 Misuse Intrusion Detection

1.3.6.1 Έμπειρα συστήματα

Τα έμπειρα συστήματα έχουν δείξει ικανοποιητικά αποτελέσματα στην χρήση τους σε IDS (Lunt 1988, Lunt 1992, Holder 1992). Μπορούν να συντηρούν μια βάση γνώσης με τη μορφή κανόνων (if - then εντολών), και να δίνουν λύσεις, συμβουλές στον υπεύθυνο ασφαλείας εάν αντιληφθούν πιθανή εισβολή στο σύστημα. Οι κανόνες περιγράφουν ύποπτη συμπεριφορά, η οποία προέρχεται από σενάρια παλαιότερων εισβολών, γνωστών σφαλμάτων σε προγράμματα. Ένα βασικό μειονέκτημα άλλωστε της μεθόδου είναι ακριβώς η ενημέρωση και συντήρησης της βάσης γνώσης, μιας και ο υπεύθυνος ασφαλείας πρέπει να είναι συνεχώς ενήμερος για νέους τρόπους εισβολών και να μπορεί να τους μεταφράζει σε κανόνες προκειμένου το IDS να τους ανακαλύψει αυτόματα όταν παρουσιαστούν στο σύστημά του.

Τα έμπειρα συστήματα δέχονται ως είσοδο τα audit trails του συστήματος. Παράδειγμα κανόνων που μπορεί να περιέχουν είναι οτι η συνεχής ανεπιτυχής

προσπάθεια (πάνω από τρεις φορές) ενός χρήστη να εισέλθει στο σύστημα μέσα σε διάρκεια πέντε λεπτών, αποτελεί πιθανή παρεισφρητική συμπεριφορά.. Το έμπειρο σύστημα, αντιλαμβάνοντας, αυτήν την συμπεριφορά αυξάνει το επίπεδο υποψίας για προσπάθεια πιθανής εισβολής.

Ο συνδυασμός τους με τις στατιστικές τεχνικές έχει αποδειχτεί πολύ αποδοτικός. Οι στατιστικές τεχνικές ενδιαφέρονται για εύρεση ανώμαλης συμπεριφοράς μέσα από μετρικές και προφίλ συμπεριφοράς. Ενας χρήστης όμως που γνωρίζει οτι παρακολουθείται, μπορεί να παρεκκλίνει σταδιακά από την εν γένη συμπεριφορά του, έτσι ώστε μετά το πέρασμα κάποιου χρονικού διαστήματος, η (νέα) συμπεριφορά να τείνει να είναι παράτυπη. Τότε οι κανόνες του έμπειρου συστήματος μπορούν να δείξουν οτι η νέα αυτή συμπεριφορά είναι απειλητική, μέσα από την εκτέλεση κανόνων που έχουν ήδη κωδικοποιήσει παρόμοια συμπεριφορά.

Πλεονεκτήματα

- Έχουν δείξει οτι μπορούν αποτελεσματικά να εντοπίσουν παραβιάσεις σε ένα σύστημα, να προσδιορίσουν σημεία στη συμπεριφορά που είναι απειλητικά και να δώσουν έγκαιρα alerts προς τον υπεύθυνο ασφαλείας σε περιπτώσεις παράτυπης δράσης χρηστών στο σύστημα. Αποτελεί συστατικό κομμάτι σε όλα σχεδόν τα συστήματα ανίχνευσης εισβολών.
- Είναι ανεξάρτητα τεχνολογικής πλατφόρμας. Μπορούν να λειτουργήσουν σε οποιοδήποτε περιβάλλον. Αυτό βέβαια προϋποθέτει αλλαγές στον τρόπο που επεξεργάζεται την audit πληροφορία, δεδομένου οτι διαφορετικές εκδόσεις του UNIX έχουν διαφορετικό τρόπο δόμησης των πληροφοριών που κατακρατούν για τη δράση των χρηστών. Μπορούν να χρησιμοποιηθούν ως συστατικά στοιχεία IDS γενικού σκοπού.
- Όταν “τρέχει” σε ξεχωριστό περιβάλλον (σε ξεχωριστή μηχανή) είναι αρκετά ανεκτικό σε παραβιάσεις των στοιχείων του ίδιου του IDS, της βάσης γνώσης, των στατιστικών στοιχείων που διατηρεί, του λογισμικού του, κτλ

Μειονεκτήματα

- Δυσκολία διατήρησης και συνεχούς ανανέωσης της βάσης γνώσης με νέα παραδείγματα, σενάρια εισβολών. Ο μεγαλύτερος κίνδυνος παρουσιάζεται από την έλλειψη ενημέρωσης του συστήματος για νέες υπογραφές. Απαιτείται αρκετά μεγάλο φόρτο εργασίας από τον υπεύθυνο ασφαλείας για την αναδιοργάνωση των κανόνων της βάσης γνώσης. Αυτό γίνεται ολοένα και δυσκολότερο εάν οι εισβολείς φροντίζουν να διαγράφουν κάθε ίχνος της παρουσίας τους από τα audit trails και από κάθε αρχείο (log file) που καταγράφει την δράση και την παρουσία τους στο σύστημα προορισμού (target system). Έτσι καθίσταται πολύ δύσκολη η καταγραφή του σεναρίου εισβολής και η σύγκρισή του με τα γνωστά σενάρια της βάσης γνώσης.
- Είναι πιθανό να μην ανακαλύψει παρεισφρήσεις, εάν ο επίδοξος εισβολέας κινηθεί σε χαμηλό επίπεδο δράση και δεν είναι δυνατή η καταγραφή των κινήσεών του από τους μηχανισμούς παρακολούθησης του συστήματος.
- Για να είναι αποτελεσματικό ένα έμπειρο σύστημα πρέπει να περιέχει ένα αρκετά μεγάλο σύνολο κανόνων, μια μεγάλη βάση γνώσης η οποία θα ανανεώνεται συνεχώς. Κάτι τέτοιο όμως σημαίνει κατανάλωση πόρων, πράγμα που τείνει να οδηγήσει, σε μικρά κυρίως συστήματα, σε δυσλειτουργία, μείωση των χρόνων απόκρισης του συστήματος και αργή ανάδραση στις εντολές των χρηστών. Φυσική

συνέπεια αποτελεί η γκρίνια αυτών για την αναποτελεσματικότητα που παρουσιάζεται, η έλλειψη εμπιστοσύνης προς το σύστημα (εάν γνωρίζουν πως κάθε κίνησή τους καταγράφεται και αναλύεται μήπως βρεθεί ως ύποπτη).

1.3.6.2 Pattern Matching

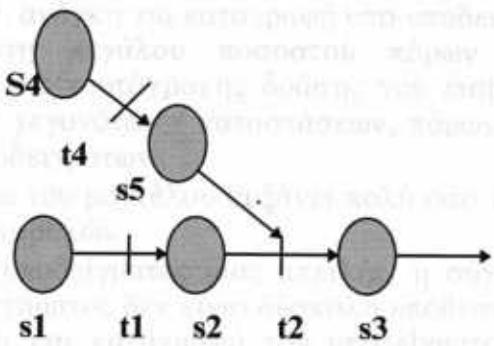
Η πλειοψηφία των περιπτώσεων ανίχνευσης παρεισφρήσεων στηρίζεται στην εύρεση τροποποιημένων στοιχείων των συστημάτων, (διαγραμμένα αρχεία, αλλαγμένα δικαιώματα προσπέλασης, κτλ) ή στην καταγραφή των πράξεων του χρήστη, την μετέπειτα επεξεργασία τους και την απόδοση του συμπεράσματος οτι είναι ή όχι εισβολέας, συγκρινόμενες με παρόμοια σενάρια παρεισφρήσεων. Ο τρόπος αυτός (pattern matching) (Kumar 1995, Spafford 1995), στηρίζεται στην έννοια του γεγονότος (event) και στις μεταβάσεις (transitions) του συστήματος από τη μια κατάσταση σε κάποια άλλη, έπειτα από την μεσολάβηση κάποιου γεγονότος. Ένα γεγονός μπορεί από μόνο του να οδηγήσει σε μια νέα περιγράψιμη κατάσταση, όσο και ένα σύνολο από γεγονότα με τις αντίστοιχες μεταβάσεις που δημιουργούνται στις καταστάσεις του συστήματος. Τα γεγονότα αυτά καταγράφονται και συσχετίζονται με μια μεταβλητή, το χρόνο που συνέβηκε το κάθε γεγονός. Το ζεύγος (e,t), δηλώνει πως το γεγονός e συνέβηκε το χρόνο t. Η καταγραφή της χρονικής στιγμής που συνέβηκε το γεγονός (όπως καταγράφεται στα audit trails), έχει μεγάλη σημασία για την αναγνώριση εισβολών.

Βασικής σημασία για την τεχνική pattern matching, αποτελεί το γεγονός πως η ακολουθία δυο γεγονότων a και b (a, b), δεν σημαίνει οτι το γεγονός b καταγράφηκε αμέσως μετά το γεγονός a, αλλά σε κάποιο χρονικό διάστημα (ίσως μηδαμινό αλλά) μεταγενέστερο του a. Αυτός ο συλλογισμός είναι κατάλληλος για αναπαράσταση της συμπεριφοράς σε ένα σύστημα, στο οποίο οι χρήστες χρησιμοποιούν παραθυρικά περιβάλλοντα ή συνδέονται σε ένα σύστημα από διαφορετικές συνόδους ταυτόχρονα.

Ενας από τους τρόπους αναπαράστασης του γίνεται με χρήση των Petri Nets. Κάθε σενάριο αντιστοιχίζεται με ένα CPA (Colored Petri Automaton). Κάθε CPA, περιγράφει την εναλλαγή καταστάσεων με γεγονότα που μεσολαβούν, έως ότου οδηγηθούμε σε μια νέα κατάσταση. Ουσιαστικά η γνώση για συγκεκριμένα υποδείγματα (patterns) συμπεριφοράς αποθηκεύονται σε κάθε CPA. Το ταίριασμα (matching) της τρέχουσας συμπεριφοράς του πιθανού εισβολέα με κάποιο γνωστό υπόδειγμα (pattern), πραγματοποιείται σταδιακά, αρχίζοντας από το αρχικό τμήμα των CPA και συνεχίζεται για κάθε τμήμα ως το τέλος.

Η δραστηριότητα του χρήστη αναπαριστάνεται με καταστάσεις και γεγονότα, τα οποία οδηγούν στην αλλαγή της κατάστασης του συστήματος. Για να πραγματοποιηθεί μια αλλαγή σε μια δεδομένη κατάσταση, πρέπει να υπάρχουν τα κατάλληλα input, έτσι ώστε να προκαλέσει την αντίδραση (trigger) για ένα γεγονός και να μετακινηθούμε σε μια νέα κατάσταση. Κάθε τμήμα του δικτύου (Petri Net) περιγράφει την κατάστασή του με συγκεκριμένες (εσωτερικές) μεταβλητές, που αφορούν το συγκεκριμένο κομμάτι (token). Για να γίνει αναφορά παρεισφρησης στον υπεύθυνο ασφαλείας, πρέπει το τελευταίο κομμάτι του δικτύου να γίνει triggered. Αυτό σημαίνει πως έχουν συμβεί όλα τα προηγούμενα γεγονότα, έχουν αλλάξει οι καταστάσεις και το σύστημα έχει οδηγηθεί σε μια παράτυπη κατάσταση.





Κατάσταση συστήματος

Μετάβαση σε νέα κατάσταση

Εικόνα 9. Αναπαράσταση γεγονότων που οδηγούν σε αλλαγή καταστάσεων, στην τεχνική pattern matching.

Στο παραπάνω σχήμα αναπαριστάνεται μια παρεισφρητική συμπεριφορά. Στο διαγώνιο κομμάτι αντιστοιχεί ένα μέρος αυτής (πχ. η χρήση της εντολής DEBUG στο sendmail) και στο οριζόντιο το υπόλοιπο (πχ. η χρησιμοποίηση του fingerd στόχο την αξιοποίηση των bugs που κρύβει (Internet Worm)). Η μετάβαση t2 αποτελεί σημείο συγχρονισμού, των δύο αλυσίδων. Για την λειτουργία του μοντέλου, πρέπει να υπάρχουν τουλάχιστον δύο σημεία αφετηρίας (δύο αλυσίδες) και μόνο μία τελική κατάσταση. Για να πραγματοποιηθεί η μετάβαση t2, πρέπει να υπάρχουν οι προϋποθέσεις ή στην κατάσταση s2 ή στην s5.

Πλεονεκτήματα

- Το μοντέλο χαρακτηρίζεται από μεταφερσιμότητα και λειτουργία σε ετερογενή περιβάλλοντα, με πολύ μικρές αλλαγές. Οι περιγραφές των γνωστών σεναρίων παρείσφρησης μπορούν εύκολα να μεταφερθούν ενώ η ασαφής περιγραφή των audit trails επαρκούν για να αναπαραστήσουν σε γεγονότα και καταστάσεις την συμπεριφορά του συστήματος.
- Νέες “υπογραφές” εισβολών μπορούν να προστεθούν στο μοντέλο, ενώ αυτό μπορεί να βρίσκεται ήδη σε λειτουργία, αναπροσαρμόζοντας την στρατηγική του συστήματος.
- Μπορούν εύκολα να τεθούν προτεραιότητες, σχετικά με τη σημασία εμφάνισης κάποιων χαρακτηριστικών στη συμπεριφορά του συστήματος. Ορισμένα γεγονότα μπορεί να οδηγήσουν σε καταστάσεις, που ίσως να μπορούμε να τις χαρακτηρίσουμε αμεσότερα ως πιθανές εισβολές.

Μειονεκτήματα

- Στην περίπτωση που ένας εισβολέας προσπαθεί να προσβάλλει το σύστημα, έχοντας εγκαθιδρύσει διαφορετικές συνόδους, μέσα από διαφορετικούς λογαριασμούς (accounts), έχει ως συνέπεια την δημιουργία μεγάλου αριθμού

γεγονότων και καταστάσεων. Άμεσο αποτέλεσμα είναι η δημιουργία μεγάλου όγκου δεδομένων, ανάγκη για καταγραφή υπο-υποδειγμάτων (sub - patterns), και εν γένει κατανάλωση μεγάλου ποσοστού πόρων του συστήματος, για την παρακολούθηση της ταυτόχρονης δράσης του εισβολέα, χώρος μνήμης για την αποθήκευση των γεγονότων / καταστάσεων, πόρων KME για την σύγκριση των διαφορετικών υποδειγμάτων.

- Η πολυπλοκότητα του μοντέλου αυξάνει πολύ όσο αυξάνει η πολυπλοκότητα των υπογραφών των εισβολών.
- Δεδομένου ενός υποδείγματος μιας απειλής, η σύγκρισή της με την δράση των χρηστών του συστήματος δεν είναι δύσκολη υπόθεση. Η δυσκολία όμως βρίσκεται στην αναγνώριση και καταγραφή του υποδείγματος της απειλής, μέσα από τα κείμενα που περιγράφουν την απειλή. Αναγκαία είναι υψηλή εξειδίκευση και γνώσεις για την εξαγωγή των υποδειγμάτων.

1.3.6.3 Model - based Intrusion Detection

Οι οπαδοί της τεχνικής αυτής (Garvey 1991, Lunt 1993) στηρίζονται στο ότι οι εισβολείς συχνά χρησιμοποιούν γνωστούς τρόπους για να παραβιάσουν την ασφάλεια των συστημάτων. Τέτοιοι τρόποι αναφέρονται σε προγραμματισμένες επιθέσεις για κλοπή του αρχείου συνθηματικών, πρόσβαση σε συγκεκριμένα αρχεία, εκμετάλλευση γνωστών αδυναμιών του συστήματος. Οι τρόποι αυτοί δράσης των εισβολέων μοντελοποιούνται και αποθηκεύονται. Η συμπεριφορά του χρήστη εξετάζεται προκειμένου να εντοπιστεί συγγένεια με τα υπάρχουσα μοντέλα παρεισφρήσεων που ήδη είναι γνωστά.

Εάν εντοπιστεί συγγένεια, η επόμενη κίνηση του χρήστη μπορεί να προβλεφτεί, εάν εξακριβωθεί ότι ακολουθεί ένα συγκεκριμένο σενάριο. Αυτό καθοδηγεί το σύστημα στην εξέταση των audit trails για την εύρεση συγκεκριμένων «αποδεικτικών στοιχείων» για την επιβεβαίωση της συγκεκριμένης απειλής. Εάν δεν βρεθούν στοιχεία από εκείνα που αναμένονται να βρεθούν (εάν εκτυλίσσετε η συγκεκριμένη απειλή), τότε δεν επιχειρείται η εισβολή. Εάν όμως αντιληφθεί την ύπαρξη των πληροφοριών που ψάχνει στα audit trails, τότε μπορεί να προβλέψει την επόμενη κίνηση του εισβολέα και εξετάζει πολύ λιγότερα δεδομένα, όσα είναι απαραίτητα για την τελική επιβεβαίωση της συγκεκριμένης εισβολής.

Η τεχνική διατηρεί μια βάση γνώσης, που περιέχει προδιαγραφές διάφορων σεναρίων παρεισφρήσεων και μοντέλων παράτυπης συμπεριφοράς. Ένα μοντέλο, για παράδειγμα, μπορεί να αποτελεί εκείνο της προγραμματισμένης επίθεσης για την κλοπή του αρχείου των συνθηματικών ενός συστήματος. Το αντίστοιχο μοντέλο περιγράφει λεπτομερώς τις κινήσεις, τα βήματα του εισβολέα στην προσπάθειά του να «κλέψει» το αρχείο, εκφρασμένο με όρους της συμπεριφοράς του κακεντρεχούς χρήστη (και όχι με όρους των πληροφοριών που κατακρατούνται στα audit trails). Εάν ο χρήστης Α παρατηρηθεί ότι εξετάζει τους καταλόγους του συστήματος και συγκεκριμένα εκείνου όπου περιέχει το αρχείο συνθηματικών, τότε μετατρέπει το αντίστοιχο μοντέλο που έχει στη βάσει γνώσης σε «ενεργό». Ενεργά είναι τα μοντέλα, τα οποία το σύστημα έχει εξακριβώσει στοιχεία ύπαρξής τους στην συμπεριφορά των χρηστών. Έχοντας την «υπόνοια» πως κάποιος χρήστης συμπεριφέρεται με τρόπο ανάλογο κάποιου γνωστού σεναρίου, προσπαθεί να



αντλήσει όσο το δυνατόν περισσότερες πληροφορίες σχετικά με αυτόν και τη δράση του. Έπειτα προσπαθεί να προβλέψει την επόμενη κίνηση του εισβολέα, στην περίπτωσή μας δημιουργείτε η υπόθεση πως ο εισβολέας θα προσπαθήσει να αντιγράψει το αρχείο συνθηματικών του συστήματος. Σύμφωνα με το μοντέλο δράσης είναι γνωστό ποια είναι η πληροφορία που πρέπει να βρεθεί στα audit trails του συστήματος προκειμένου να επιβεβαιώσει το ενεργό σενάριο. Εάν βρεθούν τα ίχνη που αναμενόταν, τότε εκδίδεται alert για εισβολή.

Πλεονεκτήματα

- Μπορούν να επεξεργαστούν περισσότερα δεδομένα, αφού για τον προσδιορισμό μιας συμπεριφοράς ως παρεισφρητικής (intrusive), απαιτείται η σύγκριση ορισμένων (λίγων) στοιχείων.
- Βασίζονται στην “μαθηματικοποιημένη” συμπερασματολογία με την παρουσία αβεβαιότητας - διαίσθησης, προσφέροντας θετικά αποτελέσματα στην δύσκολη απόφαση εάν κάποιος αποτελεί εισβολέα ή όχι.
- Μπορούν να εφαρμοστούν σε πολλές πλατφόρμες, αφού είναι ανεξάρτητα από την audit πληροφορία.
- Το σύστημα μπορεί να προβλέψει την επόμενη κίνηση κάποιου εισβολέα, αφού βασίζεται σε υπάρχοντα σενάρια - μοντέλα intrusive συμπεριφοράς. Με δεδομένη τη δυνατότητα αυτή, ο υπεύθυνος ασφαλείας μπορεί να αναλάβει πρώιμη φροντίδα και μέτρα προφύλαξης πριν ολοκληρωθεί η απειλή, υποδεικνύονται σε αυτόν στοιχεία του συστήματος που κινδυνεύουν κάθε στιγμή και την ανάγκη για την προφύλαξή τους (τονίζοντας τα ευπαθή σε κάθε σενάριο απειλής).
- Ευκολία τροποποίησης του από τον υπεύθυνο ασφαλείας, για την λειτουργία του σε κάποιο άλλο περιβάλλον.
- Παρέχουν ακριβέστερη παράσταση της intrusive συμπεριφοράς, από τον τρόπο που αυτή παρουσιάζεται στα audit trails.

Μειονεκτήματα

- Δεν είναι ξεκάθαρο πως οδηγείται στο συμπέρασμα εάν μια συμπεριφορά είναι ύποπτη για εισβολή, έχοντας ήδη παρατηρήσει μόνο ένα μέρος της.
- Περιορίζει τον υπεύθυνο που δημιουργεί τα μοντέλα παρεισφρησης στο να καθορίσει συγκεκριμένα και ακριβή όρια που περιγράφουν το μοντέλο εισβολής. Δυσκολία περιγραφής νέων μοντέλων στη βάση γνώσης.

1.3.7 Επισκόπηση

Παρουσιάστηκαν οι περισσότερες από τις τεχνικές που χρησιμοποιούνται σε συστήματα ανίχνευσης εισβολών. Πολλές από τις τεχνικές αυτές είναι αρκετά παλιές, εμφανίστηκαν με την παρουσίαση του μοντέλου της Denning, στο οποίο πολλά IDS έχουν στηριχθεί. Μερικές όμως, όπως η χρήση agents, γράφων (GrIDS) pattern matching, model - based reasoning, δεν έχουν εφαρμοστεί σε πραγματικά περιβάλλοντα για να μπορέσουμε να παραθέσουμε στοιχεία για την αποδοτικότητά τους. Ειδικά να αναφέρουμε ότι οι τεχνική model - based intrusion detection μάλλον έχει αποτύχει να εφαρμοστεί σε πραγματικά συστήματα λόγω ακριβώς των σοβαρών μειονεκτημάτων που την χαρακτηρίζουν. Γενική παρατήρηση πάντως αποτελεί οτι η χρήση μόνο μιας

τεχνικής δεν είναι ικανή για την αποτελεσματική λειτουργία ενός IDS, ενώ όλες οι τεχνικές παρουσιάζουν μειονεκτήματα, άλλες σε θέματα κατανάλωσης πόρων του συστήματος, άλλες σε χρονικούς περιορισμούς, στη συντήρηση της βάσης γνώσης, κ.α.

1.4 Παραδείγματα Συστημάτων Ανίχνευσης Εισβολών

1.4.1 Εισαγωγή

Στην προηγούμενη ενότητα έγινε μια παρουσίαση των τεχνικών οι οποίες μπορούν να χρησιμοποιηθούν σε συστήματα ανίχνευσης εισβολών. Πολλές από αυτές δεν έχουν ακόμα δείξει αποτελέσματα ή δεν έχουν ενσωματωθεί σε συστήματα. Παρακάτω αναφέρονται τα κυριότερα συστήματα IDS τα οποία έχουν αναπτυχθεί και έχουν χρησιμοποιηθεί σε πραγματικές συνθήκες. Τα περισσότερα στηρίζονται στο μοντέλο της Denning. Ενσωματώνουν τεχνικές εμπείρων συστημάτων και στατιστικών προφίλ συμπεριφοράς των χρηστών, ενώ τα νεότερα κάνουν χρήση και άλλων τεχνικών. Χαρακτηριστικό είναι το παραδειγμα του SECURENET (η ευρωπαϊκή πρόταση στα συστήματα ανίχνευσης εισβολών), που ενσωματώνει τεχνικές εμπείρων συστημάτων, νευρωνικών δικτύων και γλωσσών προσδιορισμού προδιαθέσεων των χρηστών. Ένα σύστημα που δεν στηρίζεται τόσο στην εξέταση των audit trails των υπολογιστών που παρακολουθεί αποτελεί το NSM (Network Security Monitor), το οποίο παρακολουθεί παθητικά το δίκτυο και τις υπηρεσίες του για ανεύρεση παράτυπης συμπεριφοράς.

1.4.2 IDES (Intrusion Detection Expert System)

Το IDES (Lunt 1988, Lunt 1992) αναπτύχθηκε στο τέλος της δεκαετίας του '80 από μια ομάδα του SRI. Στόχος ήταν η ανίχνευση παρεισφρήσεων είτε από εξωτερικούς παράγοντες (άτομα που δεν είχαν λογαριασμό), είτε από εσωτερικούς χρήστες, οι οποίοι προσπαθούν να προξενήσουν ζημιά, εκμεταλλευόμενοι τα δικαιώματα που τους έχουν δοθεί.

Λειτουργεί σε ξεχωριστό υπολογιστικό σύστημα, "τρέχει" στο δικό του hardware, και προσπαθεί να ανακαλύψει εισβολές σε κάποιο σύστημα (target system). Η πληροφορία από τα audit trails του target system, μετατρέπεται σε μορφή κατανοητή και επεξεργάσιμη από το IDES. Ήπειτα από την ανάλυση των στοιχείων αυτών, προσπαθεί να ανακαλύψει ίχνη παράνομης συμπεριφοράς χρηστών στο σύστημα, εάν ναι, εκδίδει επείγοντα μηνύματα (alerts) στον υπεύθυνο ασφαλείας.

Στηρίζεται στο μοντέλο της Denning, το οποίο είναι ανεξάρτητο τεχνολογικής πλατφόρμας και είδος παρεισφρήσεων. Αποτελεί ένα αρκετά αποτελεσματικό σύστημα στην ανίχνευση εισβολών, όταν αυτές συμβαίνουν (real-time). Το γεγονός οτι το IDES είναι εγκατεστημένο και λειτουργεί σε δικό του περιβάλλον, του προσδίδει μεγάλη ανθεκτικότητα και ανοχή σε προσπάθειες αλλοίωσης των χαρακτηριστικών και του τρόπου λειτουργίας του. Πολλά διαφορετικά υπολογιστικά συστήματα μπορούν να παρακολουθηθούν από το IDES.

Τα στοιχεία των audit πληροφοριών που τυγχάνουν επεξεργασία, είναι πότε συνδέθηκε (login) και πότε αποσυνδέθηκε (logout) ο χρήστης, τις τροποποιήσεις καταλόγων που πραγματοποίησε, την πρόσβαση σε αρχεία, κλήση πυρήνα, δραστηριότητα δικτύου και αλλαγή περιοχής από την οποία γίνεται η σύνδεση (session location change).

Η απόφαση σχετικά με το εάν μια συμπεριφορά οδηγεί σε εισβολή γίνεται με δύο τρόπους. Την αναγνώριση εισβολέων σύμφωνα με στατιστικά προφίλ δράσης τους και με τη χρήση εμπείρου συστήματος με κανόνες οι οποίοι εκτελούνται εάν παρατηρηθούν προϋποθέσεις ανίχνευσης γνωστών προσπαθειών εισβολής. Στην πρώτη περίπτωση γίνεται ο διαχωρισμός σε ομάδες χρηστών, υπολογιστών (hosts) και target systems. Για κάθε χρήστη διατηρείται ένα προφίλ, που τον χαρακτηρίζει. Το προφίλ αυτό περιέχει στατιστικά στοιχεία της συμπεριφοράς του, τις συνήθειές του, τις νόρμες του (έπειτα από τη διαχρονική παρακολούθηση της δράσης του στο σύστημα). Το προφίλ χαρακτηρίζει την φυσιολογική συμπεριφορά του χρήστη, κάθε παρέκκλιση από αυτήν θεωρείται ύποπτη για εισβολή. Από την εγκαθίδρυση μιας συνόδου, μεταφέρονται πληροφορίες για τις ενέργειές του με τη μορφή διανύσματος, N στοιχείων (μεταβλητών), οι τιμές των οποίων σχετίζονται με το τι κάνει ο χρήστης, πως συμπεριφέρεται με το σύστημα κάθε στιγμή. Έπειτα ανακαλούνται από τη βάση γνώσης αντίστοιχες μετρήσεις που σχετίζονται με παλαιότερη δραστηριότητα του χρήστη. Αλλαγή στις τιμές, σημαίνει πως ο χρήστης συμπεριφέρεται διαφορετικά σε σχέση με την φυσιολογική συμπεριφορά του πράγμα που ίσως υποδηλώνει πιθανή εισβολή. Η στατιστική αυτή βάση γνώσης ανανεώνεται συνεχώς, σύμφωνα με την εκάστοτε συμπεριφορά του χρήστη.

Η διατήρηση στατιστικών προφίλ και η εκμάθηση για νέους τρόπους συμπεριφοράς αποτελεί σημαντικό στοιχείο στην εύρεση εισβολών, έχει όμως και σοβαρά μειονεκτήματα. Κάποιος έμπειρος εισβολέας που γνωρίζει πως παρακολουθείται, μπορεί σταδιακά να αλλάξει την συμπεριφορά του, έτσι ώστε μετά από ένα χρονικό διάστημα, να έχει δημιουργηθεί ένα νέο προφίλ για αυτόν, αλλά ικανό για να εξαπολύσει ένα καίριο χτύπημα στο σύστημα, ενώ το IDES να μην μπορεί να χαρακτηρίσει τη νέα συμπεριφορά ως επικίνδυνη.

Για να ανταποκριθεί το IDES σε αυτό το πρόβλημα, υπάρχει το δεύτερο κομμάτι, το έμπειρο σύστημα, το οποίο βασίζεται σε κανόνες. Οι κανόνες περιγράφουν ύποπτη συμπεριφορά, όπως έχει καταγραφεί από παλαιότερες, γνωστές προσπάθειες εισβολών. Εάν η δράση κάποιου χρήστη είναι τέτοια ώστε να ισχύσουν οι συνθήκες στο αριστερό μέρος του κανόνα, εκτελείται η πράξη που περιγράφεται στο δεξί μέρος. Το μειονέκτημα του τρόπου αυτού είναι ότι απαιτείται συνεχή ανανέωση των κανόνων με νέες μεθόδους παρεισφρήσεων, αναδιοργάνωση των κανόνων και καταβολή προσπάθειας από τον διαχειριστή ασφαλείας για την καταγραφή των νέων.

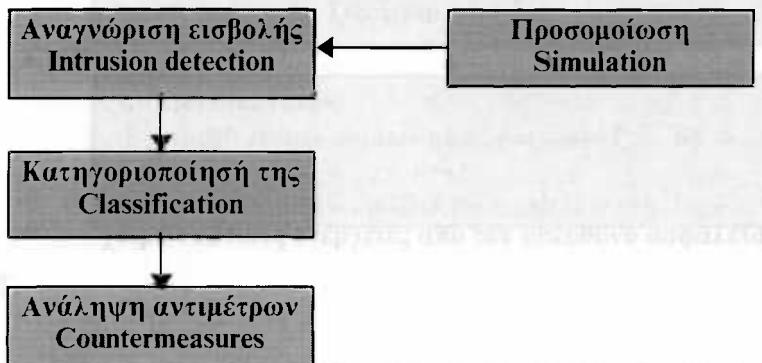
Τέλος το IDES δείχνει στον υπεύθυνο ασφαλείας σε μορφή γραφικής παράστασης την κατάσταση του target system, τον ρυθμό δημιουργίας των audit records, την επεξεργασία τους, κτλ. Παρουσιάζει την ανώμαλη συμπεριφορά όταν αυτή παρατηρείται (real time) και δίνει τη δυνατότητα αναζήτησης στοιχείων στη βάση γνώσης του IDES με προκατασκευασμένες επερωτήσεις (queries).

1.4.3 SECURENET

Το SECURENET (Denault 1992, Theodoropoulos 1996, Spirakis 1995) αποτελεί ένα έξυπνο σύστημα για την παρακολούθηση και προστασία δικτύων υπολογιστών (IBC). Ενοποιεί πολλές από τις γνωστές τεχνικές μαζί, προκειμένου στην αποδοτικότερη προστασία ενός δικτυακού περιβάλλοντος από προσπάθειες εισβολών και προγραμμάτων ιών. Το κύριο χαρακτηριστικό του οτι αναφέρεται σε προστασία δικτύων ευρείας ζώνης και η ενσωμάτωση τεχνικών νευρωνικών δικτύων με έμπειρα συστήματα, καθώς και τεχνικές προσδιορισμού προδιαθέσεων (ISL, Intent Specification Languages).

Οι κύριες ενέργειές του είναι η αναγνώριση (detection) μιας απειλής, η κατηγοριοποίησή της (classification) σε συνθήκες πραγματικού χρόνου και η επιλογή και εφαρμογή κατάλληλων αντιμέτρων (countermeasures) για την πάταξή της. Επιπλέον λειτουργία αποτελεί η προσομοίωση, η οποία αναλαμβάνει να προσομοιώνει τις δικτυακές λειτουργίες, να εκπαιδεύει το νευρωνικό δίκτυο και να ελέγχει την ικανότητα των μηχανισμών ασφαλείας του δικτύου, εξαπολύοντας εικονικές επιθέσεις.

Αυτές οι λειτουργίες αποτελούν τις δομικές ενότητες του συστήματος και παρουσιάζονται συνοπτικά στο παρακάτω σχήμα.



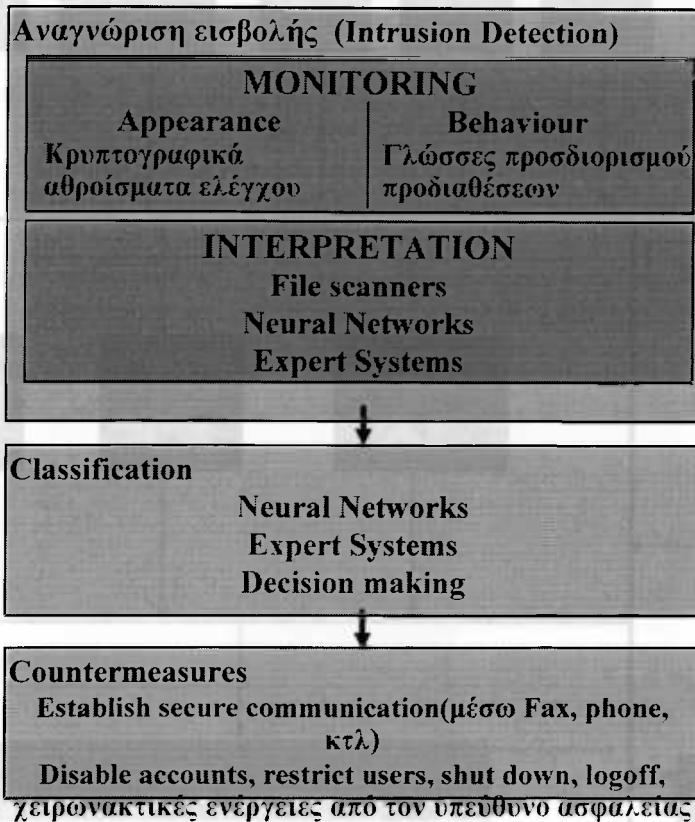
Εικόνα 10. Οι δομικές λειτουργικές ενότητες του SECURENET.

Κάθε μια από τις λειτουργίες αυτές υλοποιεί επιμέρους τεχνικές και μηχανισμούς. Συγκεκριμένα η αναγνώρισης μιας απειλής πραγματοποιείται από την λειτουργία της παρακολούθησης (monitoring). Είναι υπεύθυνη για την αναγνώριση από την εμφάνισή της (by appearance), είτε από τη συμπεριφορά (by behavior) μιας απειλής. Η ανίχνευση με βάση τη συμπεριφορά στοχεύει στην ανίχνευση στη συμπεριφορά των χρηστών στοιχεία παρατυπίας και παρέκκλισης από τους εν γένει τρόπους δράσης τους. Η διερμηνεία (interpretation) της συμπεριφοράς προσπαθεί να προσδιορίσει εάν αυτή η συμπεριφορά είναι απειλητική για το σύστημα.

Για την αναγνώριση με βάση την εμφάνιση χρησιμοποιούνται κρυπτογραφικά αθροίσματα ελέγχου. Ο λόγος είναι οτι αποτελούν πιο γρήγορο, ασφαλή και αποτελεσματικό τρόπο σε σχέση με άλλες μεθόδους εξακρίβωσης της ακεραιότητας στοιχείων με ελάχιστα πιθανότητα σφάλματος. Άλλες τεχνικές που χρησιμοποιούνται

είναι οι file scanners, τα νευρωνικά δίκτυα, τα έμπειρα συστήματα και γλώσσες προσδιορισμού προδιαθέσεων.

Εικόνα 11. Τεχνολογίες που χρησιμοποιούνται στις διάφορες ενότητες του



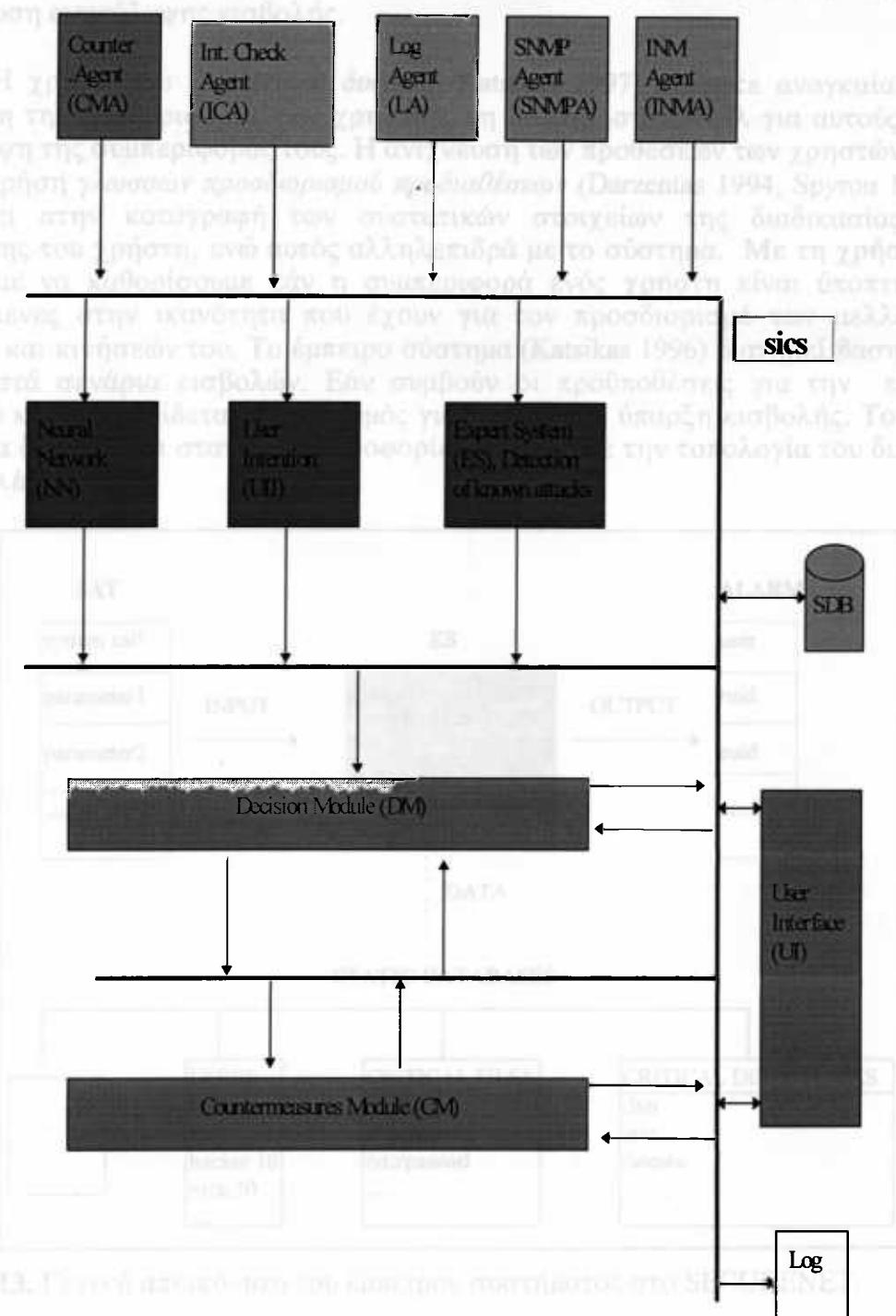
SECURENET.

Ενώ οι προηγούμενες λειτουργίες απλά ενημερώνουν την ύπαρξη πιθανής απειλής, η λειτουργία της κατηγοριοποίησης (classification) στοχεύει στο φιλτράρισμα της γνώσης που υπάρχει στο SECURENET για προηγούμενες απειλές. Επεξεργάζονται οι πληροφορίες του προηγούμενου επιπέδου για πιθανή απειλή προκειμένου στο επόμενο στάδιο να επιλεγούν τα απαραίτητα μέτρα προστασίας για την αντιμετώπισή της.

Η λειτουργία της ανάληψης αντιμέτρων (counteraction), αφού έχει λάβει από το προηγούμενο επίπεδο όλες τις απαραίτητες πληροφορίες για την συγκεκριμένη απειλή, επιλέγει τα απαραίτητα μέτρα προστασίας. Ενημερώνει τον υπεύθυνο ασφαλείας του συστήματος για την εμφάνιση της απειλής, ενώ μπορεί και αυτόματα να ενεργοποιήσει μηχανισμούς καταστολής αυτής.

Όπως περιγράφεται στο παρακάτω σχήμα οι οντότητες του συστήματος επικοινωνούν μεταξύ τους με μέσω του εσωτερικού συστήματος επικοινωνίας (SECURENET Internal Communication System, SICS). Μερικές από τις κύριες λειτουργίες του SICS αποτελούν η μεταφορά μηνυμάτων μεταξύ των οντοτήτων, η

συντήρηση των συνδέσεων μεταξύ των οντοτήτων, ο καθορισμός της γενικής συμπεριφοράς του συστήματος σε real time βάση.

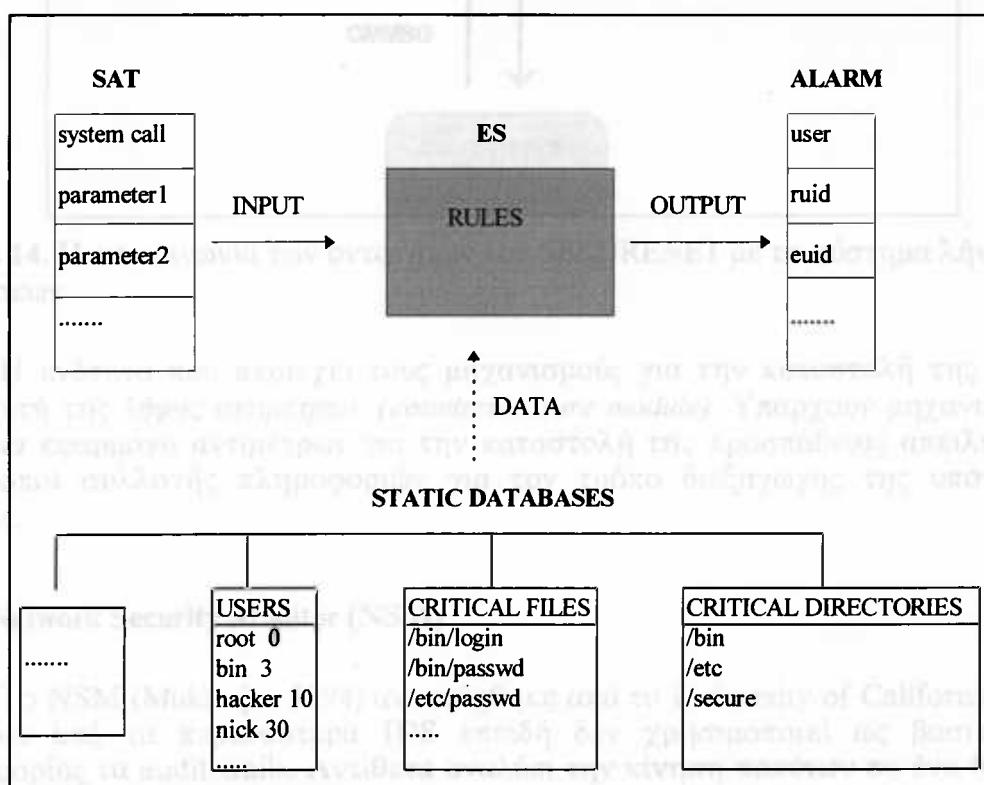


Εικόνα 12. Γενική αρχιτεκτονική του SECURENET.

Οι agents αποτελούν οντότητες προγράμματος οι οποίες διαμένουν σε κάθε σε κάθε κόμβο (host) ο οποίος παρακολουθείται και είναι υπεύθυνοι για τη συλλογή στοιχείων για τη λειτουργία του. Κύριες εργασίες τους είναι η συλλογή πληροφοριών

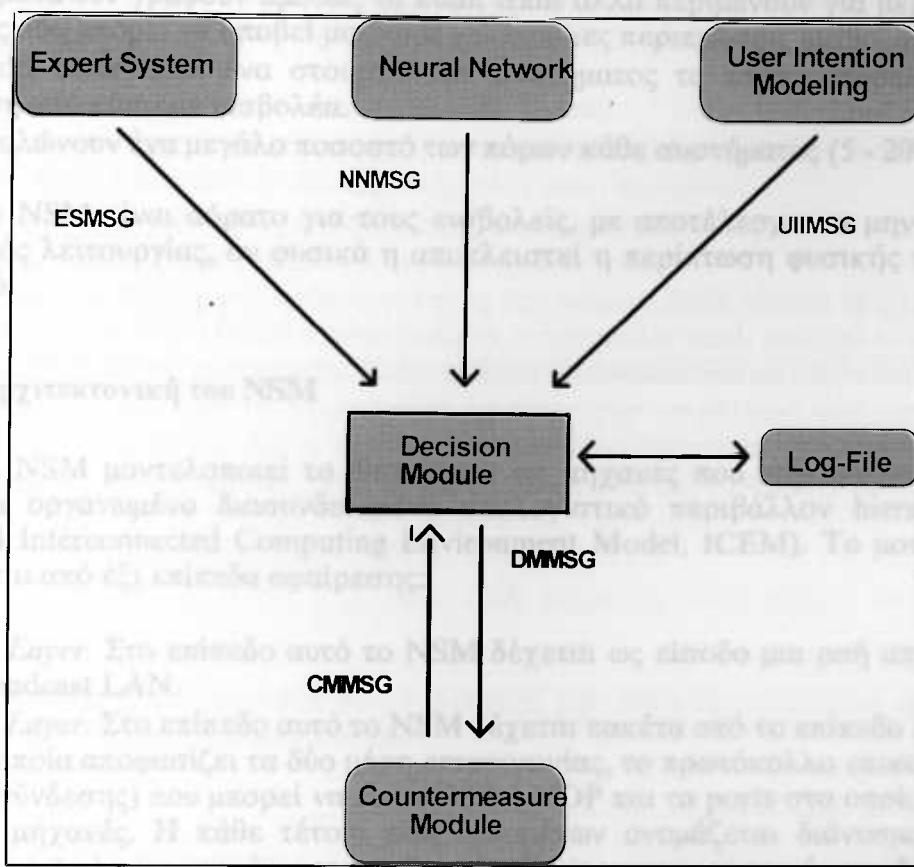
για τον κόμβο, για τις δραστηριότητές του, για τις εφαρμογές που «τρέχουν» σε αυτόν, για τους χρήστες, η αποστολή των πληροφοριών αυτών στις άλλες οντότητες του SECURENET και η λήψη από αυτές πληροφοριών για τον τρόπο δράσης τους σε περίπτωση ανακάλυψης εισβολής.

Η χρήση του νευρωνικού δικτύου (Katsikas 1997) κρίθηκε αναγκαία για την ανάλυση της συμπεριφοράς των χρηστών, τη διατήρηση προφίλ για αυτούς και την πρόβλεψη της συμπεριφοράς τους. Η ανίχνευση των προθέσεων των χρηστών γίνεται με τη χρήση γλωσσών προσδιορισμού προδιαθέσεων (Darzentas 1994, Spyrou 1995) και στοχεύει στην καταγραφή των συστατικών στοιχείων της διαδικασίας λήψης απόφασης του χρήστη, ενώ αυτός αλληλεπιδρά με το σύστημα. Με τη χρήση αυτών μπορούμε να καθορίσουμε εάν η συμπεριφορά ενός χρήστη είναι ύποπτη ή όχι, βασιζόμενες στην ικανότητα που έχουν για τον προσδιορισμό των μελλοντικούς στόχων και κινήσεών του. Το έμπειρο σύστημα (Katsikas 1996) διατηρεί βάση γνώσης με γνωστά σενάρια εισβολών. Εάν συμβούν οι προϋποθέσεις για την εκτέλεση κάποιου κανόνα εκδίδεται συναγερμός για την πιθανή ύπαρξη εισβολής. Το έμπειρο σύστημα δέχεται και στατικές πληροφορίες σχετικά με την τοπολογία του δικτύου το οποίο ελέγχεται.



Εικόνα 13. Γενική απεικόνιση του έμπειρου συστήματος στο SECURENET.

Όλες οι παραπάνω τεχνικές εάν αντιληφθούν την ύπαρξη παράτυπης συμπεριφοράς, εκδίδουν κάποιο συναγερμό (alarm) προς το σύστημα λήψης αποφάσεων (decision module) (Spyrou 1995). Αυτό με τη σειρά του λαμβάνει την τελική απόφαση σχετικά με το αν πραγματοποιείτε ή όχι εισβολή. Το decision module ενεργοποιείται εάν τουλάχιστον μια από τις προηγούμενες ενότητες εκδώσουν alarm.



Εικόνα 14. Η επικοινωνία των οντοτήτων του SECURENET με το σύστημα λήψης αποφάσεων

Η ενότητα που περιέχει τους μηχανισμούς για την καταστολή της απειλής είναι αυτή της λήψης αντιμέτρων (*countermeasure module*). Υπάρχουν μηχανισμοί όχι μόνο για εφαρμογή αντιμέτρων για την καταστολή της προσπάθειας απειλής, αλλά και τρόποι συλλογής πληροφοριών για τον τρόπο διεξαγωγής της υποτιθέμενη απειλής.

1.4.4 Network Security Monitor (NSM)

Το NSM (Mukherjee 1994) αναπτύχθηκε από το University of California, Davis. Διαφέρει από τα περισσότερα IDS επειδή δεν χρησιμοποιεί ως βασική πηγή πληροφορίας τα audit trails. Αντίθετα αναλύει την κίνηση πακέτων σε ένα broadcast LAN για να ανιχνεύσει ύποπτη συμπεριφορά. Το NSM έχει υλοποιηθεί για TCP/IP δίκτυα.

Οι κατασκευαστές του NSM δεν προτίμησαν τη συνήθη πρακτική ανάλυσης audit trails προκειμένου να ανιχνεύσουν εισβολές, για τους εξής λόγους:

- Η μορφή των audit trails δεν παρουσιάζει ομοιογένεια για κάθε πλατφόρμα,
- Τα audit trails δεν είναι πάντοτε διαθέσιμα σε real-time (κάποια IDS τρέχουν σε ξεχωριστές μηχανές όπου μεταφέρονται και τα audit tails - κάποια λειτουργικά

συστήματα δεν γράφουν αμέσως τα audit trails αλλά περιμένουν για μερικά λεπτά, χρόνος που μπορεί να αποβεί μοιραίος για κάποιες περιπτώσεις εισβολών),

- Τα audit trails είναι ένα στοιχείο του συστήματος το οποίο μπορεί να δεχτεί επίθεση από κάποιον εισβολέα.
- Καταναλώνουν ένα μεγάλο ποσοστό των πόρων κάθε συστήματος (5 - 20%).

Το NSM είναι αόρατο για τους εισβολείς, με αποτέλεσμα να μην μπορεί να τεθεί εκτός λειτουργίας, αν φυσικά η αποκλειστεί η περίπτωση φυσικής πρόσβασης προς αυτό.

1.4.4.1 Αρχιτεκτονική του NSM

Το NSM μοντελοποιεί το δίκτυο και τις μηχανές που παρακολουθεί σε ένα ιεραρχικά οργανωμένο διασυνδεδεμένο υπολογιστικό περιβάλλον hierarchically - structured Interconnected Computing Environment Model, ICEM). Το μοντέλο αυτό αποτελείται από έξι επίπεδα αφαίρεσης:

- *Packet Layer.* Στο επίπεδο αυτό το NSM δέχεται ως είσοδο μια ροή από bits, από ένα broadcast LAN.
- *Thread Layer.* Στο επίπεδο αυτό το NSM δέχεται πακέτα από το επίπεδο 2 κατά OSI για τα οποία αποφασίζει τα δύο μέρη επικοινωνίας, το πρωτόκολλο επικοινωνίας (ή τρόπο σύνδεσης) που μπορεί να είναι TCP ή UDP και τα ports στα οποία “ακούνε” οι δύο μηχανές. Η κάθε τέτοια ροή δεδομένων ονομάζεται διάνυσμα κλωστής (thread vector) και μεταφέρεται στο 3ο επίπεδο της αρχιτεκτονικής του NSM.
- *Connection Layer.* Στο επίπεδο αυτό τα διανύσματα κλωστών συσχετίζονται ανά δύο με σκοπό να αποκαλυφθούν οι συνδέσεις μεταξύ μηχανών που υπάρχουν ανά πάσα στιγμή στο δίκτυο. Τα ζευγάρια τέτοιων δυανισμάτων ονομάζονται διανύσματα συνδέσεων (connection vectors) και μεταφερονται στο 4ο επίπεδο του NSM.
- *Host Layer.* Στο επίπεδο αυτό τα διανύσματα συνδέσεων μετατρέπονται σε διανύσματα μηχανών (host vectors). Τα διανύσματα μηχανών αντανακλούν τις επικοινωνίες στις οποίες αναλώνεται η κάθε μηχανή. Τα διανύσματα μηχανών μεταφερονται στο 5ο επίπεδο του NSM.
- *Connected Network Layer.* Τα διανύσματα μηχανών χρησιμοποιούνται στο connected network layer προκειμένου να σχηματιστούν συνδεδεμένα γραφήματα που θα περιγράφουν τις επικοινωνίες στο σύνολο των μηχανών που αποτελούν το δίκτυο. Για κάθε ακμή του γραφήματος κρατείται πληροφορία σχετικά με τα δύο επικοινωνούντα μέρη και την υπηρεσία που χρησιμοποιείται (host 1, host 2, service). Το επίπεδο αυτό μπορεί να απαντά ερωτήσεις του χρήστη σχετικά με τις επικοινωνίες που υπάρχουν στο δίκτυο. Το γράφημα αυτό μεταφέρεται στο 6ο επίπεδο του NSM.
- *System Layer.* Στο επίπεδο αυτό παράγεται ένα γράφημα που μοντελοποιεί το σύνολο του δικτύου όσον αφορά στις επικοινωνίες που υπάρχουν στη ζητούμενη χρονική στιγμή.

1.4.4.2 Ανίχνευση Παρεισφρητικής Συμπεριφοράς στο NSM

Για την ανίχνευση παρεισφρητικής συμπεριφοράς χρησιμοποιείται ένα έμπειρο σύστημα. Οι είσοδοι του έμπειρου συστήματος είναι:

- Η τρέχουσα επικοινωνιακή κατάσταση στο δίκτυο.
- Αναμενόμενα προφίλ επικοινωνιακής συμπεριφοράς του δικτύου όσον αφορά τις μηχανές που επικοινωνούν και τις υπηρεσίες που εκτελούν.
- Γνώση σχετική με τις υπηρεσίες που εκτελούνται -ποιες οι δυνατότητες των χρηστών, γνωστά bugs για κάθε τέτοια υπηρεσία κ.α..
- Το επίπεδο πιστοποίησης αυθεντικότητας που απαιτεί κάθε τέτοια υπηρεσία -π.χ. η υπηρεσία finger δεν άπαιτει authentication, η υπηρεσία mail απαιτεί authentication χωρίς επιβεβαίωση, η υπηρεσία telnet απαιτεί authentication με επιβεβαίωση.
- Το επίπεδο ασφαλείας (ή αξιοπιστίας ως προς την ασφάλεια) των μηχανών που επικοινωνούν είναι μια άλλη είσοδος στο έμπειρο σύστημα. Η παράμετρος αυτή βασίζεται σε στοιχεία όπως: την αναφορά του National Computer Security Center για κάθε μηχανή, τα αποτελέσματα εκτελεσης λογισμικού αξιολόγησης μηχανών όπως το Security Profile Inspector (SPI), το COPS, κ.α.,
- Η τελευταία είσοδος είναι η ιστορία κάθε μηχανής όσον αφορά προηγούμενες επιθέσεις.

Το έμπειρο σύστημα προσπαθεί να υπολογίσει την πιθανότητα κάποια σύνδεση να αποτελεί παρεισφρητική συμπεριφορά.

1.4.5 Επισκόπηση

Παρουσιάστηκε μια, όσο το δυνατόν πληρέστερη αναφορά σε ήδη υλοποιημένα συστημάτων ανίχνευσης εισβολών. Τα IDS αποτελούν μια νέα σχετικά ερευνητική περιοχή, κλείνει μόλις περίπου δέκα χρόνια έρευνας, από την πρώτη εμφάνιση προτάσεων, μοντέλων και συστημάτων που ικανοποιητικά να μπορούν να προστατεύουν σε κάποιο βαθμό ένα σύστημα από απειλές. Τα περισσότερα IDS στηρίζονται κυρίως στο φιλτράρισμα των audit trails, μέσα από την ενσωμάτωση σε αυτά έξυπνων εργαλείων. Νεότερα συστήματα χρησιμοποιούν ιδέες προερχόμενες από την επιστήμη της τεχνητής νοημοσύνης (Frank 1994), των συστημάτων στήριξης αποφάσεων στην προσπάθεια κατασκευής αποδοτικότερων συστημάτων. Η ενσωμάτωση τεχνικών όπως νευρωνικά δίκτυα, γλωσσών προσδιορισμού προδιαθέσεων αλλά και αυτόνομων agents και γράφων (τα οποία βρίσκονται ακόμα σε πειραματικό στάδιο) έχουν χρησιμοποιηθεί, για να πετύχουν την αποδοτικότηρη, ταχύτερη, εύρωστη και με λιγότερο κόστος λειτουργία των συστημάτων αυτών.

1.5 Γενική κριτική Συστημάτων Ανίχνευσης εισβολών

Τα συστήματα ανίχνευσης εισβολών που έχουν υλοποιηθεί, παρόλο που εμφανίζουν ελπιδοφόρα αποτελέσματα στην αντιμετώπιση εισβολέων και των εχθρικών τάσεων αυτών προς τα συστήματα στα οποία προσπαθούν να παρεισφέρουν, ωστόσο χαρακτηρίζονται από αρκετά μειονεκτήματα. Συγκεκριμένα αναφέρονται σε:



- **Απουσία γενικής μεθοδολογίας για την υλοποίησή τους.** Η ανίχνευση εισβολών είναι μια νέα ερευνητική περιοχή, τα πρώτα συστήματα εμφανίστηκαν στα τέλη της δεκαετίας του '80. Αποτέλεσμα είναι η αδυναμία εύρεσης κοινής συναίνεσης σχετικά με το ποιες είναι οι αποδοτικότερες τεχνικές που μπορούν να χρησιμοποιηθούν, ενώ ακόμα εμφανίζονται νέες ιδέες και μηχανισμοί ανίχνευσης εισβολών. Η έλλειψη από κοινού αναγνωρισμένης μεθοδολογίας καθιστά δύσκολη την υλοποίηση τέτοιων συστημάτων καθώς και αύξηση του κόστους ανάπτυξής τους.
- **Αποδοτικότητα.** Τα περισσότερα από τα IDS που εμφανίζονται προσπαθούν να πετύχουν την ανακάλυψη εισβολέων όταν και την στιγμή που αυτές εμφανίζονται. Πολύ λίγα (και συνήθως τα παλαιότερα συστήματα) ελέγχουν ανά τακτά χρονικά διαστήματα τις πληροφορίες που συλλέγονται από το σύστημα για να ανακαλύψουν παρεισφρήσεις ενώ όλα τα όλα προσπαθούν σε real-time βάση να προσφέρουν υπηρεσίες στον διαχειριστή ασφαλείας. Η επεξεργασία όμως των πληροφοριών αυτών, ειδικά όταν γίνεται real-time και σε μεγάλα συστήματα που το μέγεθος των audit πληροφοριών φτάνει αρκετά megabytes, καταναλώνει πολλούς από τους πόρους του συστήματος βγάζοντας ουσιαστικά και το IDS εκτός λειτουργίας. Για την ανακάλυψη ανώμαλης συμπεριφοράς απαιτείται συνεχείς παρακολούθηση και ανανέωση των στατιστικών προφίλ συμπεριφοράς για την έγκαιρη πρόληψη πιθανής εισβολής. Για την ανακάλυψη misuse detection από την άλλη χρησιμοποιούνται έμπειρα συστήματα με την εν γένη αδυναμία τους στην συντήρηση και αξιοποίηση της βάσης γνώσης.
- **Μεταφερσιμότητα.** Τα περισσότερα από τα συστήματα που έχουν υλοποιηθεί είναι προσανατολισμένα σε συγκεκριμένη πλατφόρμα, λειτουργικό σύστημα, περιβάλλον. Υλοποιήθηκαν για συστήματα με συγκεκριμένες αρχές ασφαλείας και περιορισμούς. Είναι πολύ δύσκολη η μεταφορά ενός IDS σε διαφορετικό υπολογιστικό περιβάλλον, παρόλο που οι πολιτικές ασφαλείας μπορεί να μην διαφέρουν ριζικά μεταξύ τους.
- **Δυνατότητα αναβάθμισης.** Από τη στιγμή της κατασκευής του συστήματος είναι δύσκολη η ανατροφοδότησή του με νέες τεχνικές και μεθόδους αντιμετώπισης νέων απειλών. Η δυσκαμψία συνίσταται με την αδυναμία εύρεσης τρόπου επικοινωνίας των νέων με τις υπάρχουσες τεχνικές και τον τρόπο που θα λειτουργούν από κοινού ενιαία ως ένα σύστημα.
- **Συντήρηση.** Η συντήρηση ενός IDS αποτελεί δύσκολη εργασία. Ο λόγος είναι οτι δεν απαιτούνται μόνο γνώσης ασφάλειας υπολογιστών αλλά και βαθύτερες γνώσεις εμπείρων συστημάτων και διαχείρισης βάσεων γνώσης. Η αναπροσαρμογή των κανόνων, η προσθαφαίρεσή τους, σίγουρα δεν είναι εύκολη υπόθεση για κάποιον που δεν είναι γνώστης θεμάτων σχετικά με έμπειρα συστήματα. Αντίστοιχες είναι και οι παρατηρήσεις για αναθεώρηση των στατιστικών μετρικών του ανιχνευτή της ανώμαλης συμπεριφοράς για την διατήρηση στατιστικών προφίλ.
- **Απόδοση.** Το ιδανικό θα ήταν να υπάρχουν δεδομένα και αποτελέσματα μετρήσεων σχετικά με το ποσοστό των εισβολών που ένα IDS μπορεί να εντοπίσει. Δυστυχώς τέτοια δεδομένα δεν έχουν δει ποτέ το φως της δημοσιότητας. Ο λόγος είναι πιθανόν η αδυναμία να καταγράψεις τέτοια θέματα σε μεγάλα περιβάλλοντα, με την διαδικτύωση που παρατηρείται σήμερα με την ιλιγγιώδη ανάπτυξη του Internet. Επιπλέον αιτία μπορεί να θεωρηθεί η άρνηση των εταιρειών να εκδώσουν

αποτελέσματα σχετικά με τις ικανότητες των συστημάτων IDS που χρησιμοποιούν στην ανίχνευση εισβολών.

- **Αδυναμία τρόπου ελέγχου τους.** Η αδυναμία προσομοίωσης παρεισφρητικής συμπεριφοράς καθώς και ο συνεχώς αυξανόμενος αριθμός των εισβολών και των μεθόδων που εμφανίζονται για την παραβίαση των συστημάτων ασφαλείας καθιστούν δύσκολη την αξιολόγηση της αποτελεσματικότητας των συστημάτων IDS. Επιπλέον, η διαφορετικοί τρόποι που κάθε σύστημα χρησιμοποιεί για τη καταγραφή της συμπεριφοράς των χρηστών μέσω audit trails, καθιστούν ακόμα δυσκολότερη την σύγκριση των IDS.

Στον πίνακα που ακολουθεί γίνεται μια συγκριτική παράθεση γνωστών συστημάτων ανίχνευσης εισβολών, με έμφαση στις τεχνικές που ενσωματώνουν (για anomaly και misuse detection) και μερικά επιπλέον χρήσιμα χαρακτηριστικά τους (αν λειτουργούν σε real time πλατφόρμα, αν παρακολουθούν την κίνηση μεμονωμένων υπολογιστών (hosts) ή δικτύων υπολογιστών.

Πίνακας 2 Συγκριτική παρουσίαση γνωστών συστημάτων ανίχνευσης εισβολών

Συστήματα	IDES/NIDES	SECURENET	NSM	HAYSTACK ¹	MIDAS ¹	WISDOM & SENSE ¹	NADIR ¹
<i>Kριτήρια</i>							
<i>Misuse Detection</i>							
Εμπειρα Συστήματα	✓	✓	✓	✓	✓	✓	✓
Pattern Matching							
Model based							
<i>Anomaly Detection</i>							
Στατιστικές τεχνικές	✓		✓	✓	✓		✓
Νευρωνικά Δίκτυα		✓					
Αυτόνομοι Agents							
User Intention Identification		✓					
Χρήση Γράφων							
<i>Άλλα Χαρ/κά</i>							
Real Time λειτουργία	✓	✓	✓	✓	✓	✓	
Host based				✓	✓	✓	
Network based	✓	✓	✓				✓

¹ : Περισσότερες πληροφορίες για τα συστήματα αυτά, καθώς και για άλλα, μπορεί να αναζητήσει ο αναγνώστης στο Παράρτημα που ακολουθεί στο τέλος της εργασίας

1.5.1 Συμπεράσματα

Με βεβαιότητα μπορούμε να πούμε αναφέρουμε ότι ο ερευνητικός αυτός τομέας της ασφάλειας των υπολογιστών είναι αρκετά ζωντανός. Ιδιαίτερο βάρος δίνει η εξάπλωση, με ταχύ ρυθμό, της χρήσης των δικτυακών υπηρεσιών, τηλε-εργασία, τηλε-εκπαίδευση, νέοι τρόποι ψυχαγωγίας και ενημέρωσης, τα πολυμέσα. Η διεθνοποίηση των πληροφοριακών συστημάτων των οργανισμών, αλλά και των εταιρικών δικτύων με τις κρίσιμες πληροφορίες που αυτά περιέχουν, οδηγεί τις επιχειρήσεις στην αναζήτηση ασφαλών λύσεων για την μεταφορά των πληροφοριών, προστασία των δικτύων και των υπολογιστών, στους οποίους έχουν επενδύσει και που περιέχουν ευαίσθητες πληροφορίες.

Παρόλο που τα συστήματα ανίχνευσης εισβολών έχουν δείξει ικανοποιητικά αποτελέσματα στην ανίχνευση εισβολών συγκεκριμένων κατηγοριών και συγκεκριμένων αρχιτεκτονικών, στις οποίες βασίστηκε η υλοποίησή τους, είναι συνδεδεμένα με συγκεκριμένο περιβάλλον και τρόπους ανίχνευσης. Θέματα αποδοτικότητας τίθενται συνεχώς μιας και η εμφάνιση νέων τεχνολογιών και τεχνικών κλονίζει την κυριαρχία παλαιότερων και ήδη χρησιμοποιούμενων. Στα σύγχρονα IDS παρατηρείται μια ενοποίηση εμπείρων συστημάτων με νευρωνικά δίκτυα, αυτόνομων agents με χρήση γνωσιακών δομών για πρόβλεψη της συμπεριφοράς.

Έντονη είναι επίσης η ανάγκη για δημιουργία IDS τα οποία θα αναφέρονται σε συστήματα μικρότερης κλίμακας, μεσαίου μεγέθους, θα είναι πιο ευέλικτα και δυναμικά ενώ θα χαρακτηρίζονται από ευκολία αναβάθμισης και χειρισμού. Απαιτείται η ενσωμάτωση και άλλων τεχνικών, με τελικό στόχο την ολοένα και αποδοτικότερη διαφύλαξη των πολιτικών ασφαλείας, των αρχών και μηχανισμών που προστατεύουν την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των στοιχείων των

2. ΣΥΜΠΕΡΑΣΜΑΤΟΛΟΓΙΑ ΜΕΣΩ ΥΠΟΘΕΣΕΩΝ - CASE BASED REASONING

2.1 Εισαγωγή

Η συμπερασματολογία μέσω υποθέσεων (Case based Reasoning, CBR), αποτελεί ώριμο πλέον μέρος της Τεχνητής Νοημοσύνης. Παρόλη τη μικρή διάρκεια εμφάνισης της μεθοδολογίας του CBR, έχουν οριστεί οι βασικές αρχές του και πολλά συστήματα έχουν κάνει την εμφάνισή τους, στηρίζοντας τη συμπερασματολογία τους στην προηγούμενη - ήδη αποκτηθείσα εμπειρία. Στο κεφάλαιο αυτό παρουσιάζονται οι γενικές αρχές του νέου αυτού κλάδου, ο οποίος έχει δείξει πολλά θετικά αποτελέσματα και οι υποστηριχτές του, προβλέπουν πολλά περισσότερα για το μέλλον. Μετά την περιγραφή των βασικών αρχών, των cases, του τρόπο που λειτουργεί ο reasoner, γίνεται αναλυτική περιγραφή του κύκλου του CBR, παρουσιάζεται ένας τρόπος - αλγόριθμος εκμάθησης που χρησιμοποιείται ήδη σε υπάρχοντα CBR συστήματα, και, τέλος, καταγράφονται συμπεράσματα για την ευοίωνη πορεία του.

2.2 Γενικά για CBR

Η συμπερασματολογία μέσω υποθέσεων (Case based Reasoning, CBR), αποτελεί νέο paradigm (Kuhn 1970) για την Τεχνητή Νοημοσύνη. Η συμπερασματολογία δεν μοντελοποιείται ως μια διαδικασία στην οποία τα συμπεράσματα απορρέουν από την αλυσιδωτή έναρξη κανόνων, πράγμα που αποτελεί και την βασική ειδοποιό διαφορά με στο CBR. Σε αυτό η γνώση δεν είναι αποθηκευμένη σε κανόνες, αλλά σε cases τα οποία είναι οργανωμένα στη μνήμη. Λύσεις σε προτεινόμενα προβλήματα δίνονται όχι με την αλυσιδωτή εκτέλεση κανόνων, αλλά με την ανάκτηση των περισσότερων σχετικών (relevant) cases από την μνήμη και υιοθέτηση μιας λύσης για την αντιμετώπιση της προβληματικής κατάστασης. Στο CBR η συμπερασματολογία βασίζεται στην «ενθύμηση» (remembering).

Το CBR στηρίζεται σε δύο θεμελιώδη αξιώματα. Αρχικά θεωρείται ότι ο κόσμος χαρακτηρίζεται από μια κανονικότητα: σε παρόμοια προβλήματα αντιστοιχούν παρόμοιες λύσεις. Συνεπώς λύσεις σε προβλήματα που έχουν ήδη παρουσιαστεί αποτελούν καλές υποδείξεις για τη χρήση τους σε νέα παρόμοια προβλήματα που παρουσιάζονται. Η δεύτερη θεμελιώδης αρχή αναφέρεται στην πιθανότητα με την οποία συγκεκριμένοι τύποι προβλημάτων τείνουν να ξαναπαρουσιάζονται. Με αυτόν τον τρόπο μελλοντικά προβλήματα ίσως μοιάζουν με τα προβλήματα που ήδη έχουν εμφανιστεί και γνωρίζουμε τις λύσεις τους.

Η συμπερασματολογία που χρησιμοποιεί το CBR δεν είναι όμως μόνο ικανοποιητική για επίλυση παρόμοιων προβλημάτων με αυτά που έχουν ήδη εμφανιστεί. Όσο περισσότερο αυξάνεται τη δυνατότητα του reasoner για επίλυση νέων προβλημάτων, τόσο μετακινείται από τη διαδικασία της επαναχρησιμοποίησης παλιότερων λύσεων (reuse) σε εκείνη της δημιουργικής και αυτόνομης λύσης

προβλημάτων (problem solving). Ένα βασικό χαρακτηριστικό της μεθόδου είναι η ικανότητά της να χρησιμοποιεί την πρότερη εμπειρία, εκείνη που έχει ήδη αποκτηθεί από τη λύση παλαιότερων προβλημάτων, για την αντιμετώπιση νέων καταστάσεων.

2.3 Η ανάγκη για CBR

Η θεμελίωση και εφαρμογή του CBR προήλθε από τον τομέα της Γνωστικής Επιστήμης (Cognitive Science) και από την Τεχνητή Νοημοσύνη. Η Γνωστική Επιστήμη ενδιαφέρεται να μοντελοποιήσει την ανθρώπινη συμπερασματολογία και μάθηση, ενώ η τεχνητή νοημοσύνη προσβλέπει στην ανάπτυξη συστημάτων που θα ενσωματώνουν τεχνολογία η οποία θα υλοποιεί «έξυπνες» λειτουργίες.

Οι άνθρωποι έχουν τη δυνατότητα να αντιμετωπίζουν αποτελεσματικά δύσκολα προβλήματα παρότι έχουν περιορισμένη γνώση πολλές φορές για αυτά και στηριζόμενοι σε αβέβαιες πληροφορίες. Η ικανότητά τους για επίλυση των προβλημάτων αυτών μεγαλώνει με την απόκτηση όσο το δυνατό μεγαλύτερης εμπειρίας πάνω σε προβληματικές καταστάσεις. Τέτοια ζητήματα δεν είναι νέα για την επιστήμη της τεχνητής νοημοσύνης και το CBR μπορεί να θεωρηθεί ότι προσεγγίζει τις αρχές της ανθρώπινης μάθησης και νιοθέτησης λύσεων σε προβλήματα. Η χρήση του εξάλλου σε πολλές εφαρμογές παρά την πρώιμη εμφάνιση αυτού του είδους της συμπερασματολογίας αποτελεί καλή ένδειξη για την πορεία που πρόκειται να ακολουθήσει και στο μέλλον.

2.4 Ο Case base Reasoner

Ο Case base Reasoner στηρίζεται σε προηγούμενα cases προκειμένου να εξάγει αποτελέσματα για νέα προβλήματα. Με τα cases τα οποία «ενθυμάται» (remembering), προτείνει τρόπους για εύρεση λύσεων σε νεοεμφανιζόμενα, προτείνει τρόπους για νιοθέτηση λύσεων οι οποίες δεν είναι οι βέλτιστες, προειδοποιεί για πιθανές αποτυχίες, προσανατολίζεται σε συγκεκριμένες παραμέτρους και καταστάσεις στη διαδικασία λύσης μιας προβληματικής κατάστασης.

Ο τρόπος που λειτουργούν οι άνθρωποι για την επίλυση προβληματικών καταστάσεων μιας θυμίζει πάρα πολύ τον τρόπο που το CBR επεξεργάζεται την γνώση και τη χρησιμοποιεί. Οι δικηγόροι έχουν μάθει να βασίζονται σε παλαιότερες υποθέσεις (cases) προκειμένου να δημιουργήσουν και να καταστρώσουν επιχειρηματολογία για καινούργιες υποθέσεις που εμφανίζονται. Ένας γιατρός στην προσπάθειά του να θεραπεύσει έναν ασθενή με παράξενη εμφάνιση συμπτωμάτων, μπορεί να χρησιμοποιήσει μια παλαιότερη διάγνωση (εάν προϋπήρχε αντίστοιχη περίπτωση ασθενούς) για την θεραπεία του καινούργιου. Βέβαια δεν σημαίνει ότι η παλαιότερη διάγνωση είναι και η βέλτιστη δυνατή. Μπορεί να αποτελέσει όμως μέτρο, μια πρώτη προσέγγιση και αφού κριθεί να χρησιμοποιηθεί. Παρόμοιος είναι και ο τρόπος με τον οποίο αντιμετωπίζει τα θέματα και ένας μηχανικός αυτοκινήτου. Αν βρεθεί αντιμέτωπος με μια παράξενη βλάβη, η ενθύμηση μιας παρελθούσης αντίστοιχης μπορεί να τον βοηθήσει να προσεγγίσει τη λύση στο πρόβλημα που αντιμετωπίζει ευκολότερα αν όχι και άμεσα (με την επαναχρησιμοποίηση της ίδιας ακριβώς λύσης). Σίγουρα πάντως θα είναι περισσότερος αποδοτικός δεδομένου ότι θα

προσπαθήσει να αποφύγει τα προγενέστερα λάθη που διέπραξε ή τις πιθανές αδυναμίες παλαιοτέρων λύσεων με στόχο την επιλογή της βέλτιστης.

Ένα από τα βασικότερα στοιχεία που προσδιορίζει τον CB Reasoner είναι η ικανότητα για μάθηση στηριζόμενος σε παλαιότερη εμπειρία. Επιπλέον έχει τη δυνατότητα να:

- Προτείνει γρήγορα λύσεις σε προβλήματα, παρακάμπτοντας χρόνο και προσπάθεια για αναπαραγωγή της λύσης από την αρχή.
- Προτείνει λύσεις σε περιοχές προβλημάτων (problem domains) τα οποία είναι δύσκολο να αποσαφηνιστούν και μοντελοποιηθούν.
- Παρέχει τρόπο για αξιολόγηση των λύσεων που έχουν ήδη προταθεί, παρά την δυσκολία εύρεσης αλγορίθμικών τρόπων για την υλοποίηση αυτού του στόχου.
- Γενικότερα με τη χρήση υποθέσεων (cases), μπορούμε να διερμηνεύσουμε έννοιες που είναι δύσκολο να αποσαφηνιστούν.
- Με τη χρήση cases μπορούμε να συγκεντρωθούμε σε συγκεκριμένα στιγμιότυπα, παραμέτρους του προβλήματος με το να μας επιδεικνύουν τα πιο σημαντικά.
- Με τη βοήθεια των cases ο reasoner προτρέπεται να μην υλοποιήσει ενέργειες οι οποίες έχουν αναληφθεί στο παρελθόν και απέφεραν αρνητικές επιπτώσεις στη λύση προβλημάτων.

2.5 Cases

2.5.1 Τι είναι τα cases.

Ένα case μπορεί να οριστεί ως ένα «κομμάτι γνώσης το οποίο αναπαριστά εμπειρία πάνω σε συγκεκριμένο γνωστικό τομέα, αποτελεί θεμελιώδες στοιχείο εκμάθησης από το reasoner για την υλοποίηση των στόχων του» (Kolodner 1993).

Τα cases αναπαριστούν εμπειρία. Με την εμφάνιση μιας νέας προβληματικής κατάστασης, αναζητούνται στη βάση γνώσης παλαιότερες προσπάθειες επίλυσης αντίστοιχων προβλημάτων. Αυτά αποτελούν καλό σημείο εκκίνησης, αρχικό σημείο για την έναρξη της διαδικασίας επίλυσης του νέου προβλήματος που εμφανίστηκε.

Τα cases περιέχουν:

- *Περιγραφή του προβλήματος.* Αποτελεί την περιγραφή του προβλήματος που επιδιώκουμε τη λύση του.
- *Λύση προβλήματος.* Αναφέρεται στη διαδικασία με την οποία ο reasoner αντιμετώπισε το πρόβλημα.
- *Anatropofodótηση.* Αξιολογείται η αποτελεσματικότητα της λύσης στην αντιμετώπιση του προβλήματος, εάν ήταν επιτυχής ή όχι, σε ποίες περιπτώσεις ήταν επιτυχής και γιατί. Σχετίζεται με το feedback του συστήματος από το χρήστη, προκειμένου ο reasoner να μπορέσει να προτείνει λύσεις μελλοντικά οι οποίες απέφεραν θετικά απότελέσματα σε παρελθοντικά προβλήματα και να απορρίψει άλλες.

2.5.2 Από τι αποτελούνται τα cases

Τα cases αποτελούν τα θεμελιώδη συστατικά στοιχεία του CBR. Από τη σκοπιά της γνωστικής επιστήμης, αποτελούν μια αφαιρετική περιγραφή μιας διαδικασίας λύσης ενός προβλήματος, Περιέχουν υπό αυτή την έννοια εμπειρία, γνώση πάνω σε συγκεκριμένους τρόπους επίλυσης προβλημάτων η οποία μπορεί να ανακτηθεί και χρησιμοποιηθεί σε μελλοντικές περιπτώσεις. Ενας τυπικός ορισμός του πεδίου του CBR και των cases που το απαρτίζουν, μπορεί να δοθεί, αφού πρώτα προσδιοριστούν έννοιες αναγκαίες για τη θεωρητική κατανόηση του πεδίου (Janesko 1995).

Αρχικά ορίζουμε μια γλώσσα με την οποία αναπαριστούμε την γνώση L . Η γλώσσα L αποτελείται από ένα πεπερασμένο σύνολο από σταθερές, κατηγορήματα και συναρτήσεις με τα οποία μπορούμε να περιγράψουμε το πεδίο των προβληματικών καταστάσεων και των λύσεων στις οποίες αυτά αντιστοιχούν. Με βάση αυτή τη γλώσσα μπορούμε να περιγράψουμε την εκάστοτε προβληματική κατάσταση. Η περιγραφή αυτή D ορίζεται ως ένα υποσύνολο της γλώσσας L .

Εάν υποθέσουμε την ύπαρξη των L_p και L_s ως γλώσσες με τις οποίες αναπαριστούμε την γνώση σε κάποιο συγκεκριμένο γνωστικό πεδίο, τέτοιες ώστε $L_p \subseteq L$ και $L_s \subseteq L$ με $L_p \cap L_s = \emptyset$, τότε το σύνολο $\Sigma = L_p \cup L_s$ αποτελεί το πεδίο γνώσης με το οποίο ασχολούμαστε. Μπορούμε να προχωρήσουμε στον ορισμό του case ως ένα διατεταγμένο ζεύγος $C = (P, S)$, στο οποίο $P \subseteq L_p$ και $S \subseteq L_s$ ενώ $\Sigma \cup P \cup S$ είναι αμετάβλητο σύνολο. Το P αποτελεί το σύνολο των προβληματικών καταστάσεων οι οποίες εμφανίζονται ενώ τις λύσεις αυτών τις αναζητούμε στο σύνολο S .

Δοθέντος των συνόλων Σ , L_p και L_s , ορίζουμε την Case Base CB ως το πεπερασμένο σύνολο $CB = \{C_1, C_2, \dots, C_n\}$. Τα στοιχεία C_i του συνόλου CB αποτελούν τα αρχικά (source) cases. Επιπλέον, ως target cases ορίζονται τα cases στα οποία δεν αντιστοιχεί λύση: $C_T = (P, \emptyset)$.

2.6 Case Library - Experience

Το ποιο σημαντικό τμήμα σε ένα σύστημα CBR αποτελεί η βιβλιοθήκη με τα cases. Αυτά αποτελούν και την συσσωρευμένη εμπειρία που έχει το σύστημα με την πάροδο του χρόνου. Η βιβλιοθήκη - συλλογή εμπειρίας μπορεί να συγκεντρώθει αρχικά από εμπειρογνώμονες. Τεχνικές όπως συνεντεύξεις με έμπειρα άτομα σε συγκεκριμένα γνωστικά αντικείμενα, παρακολούθηση της συμπεριφοράς τους προκειμένου να οδηγηθούμε σε συμπεράσματα για τον τρόπο που κατηγοριοποιούν τα προβλήματα, αναγάγουν τις προβληματικές καταστάσεις σε μικρότερης κλίμακας επιλύσιμα θέματα και επιλέγουν τις απαραίτητες λύσεις. Καθώς το σύστημα αναλίσκεται στην επίλυση προβλημάτων τόσο αυξάνεται η «εμπειρία» του για την αντιμετώπιση καταστάσεων, τόσο αυξάνεται και η βάση με τα cases που διατηρεί, αφού σε αυτά αποθηκεύεται η εμπειρία του.

Ο reasoner αρχικά ξεκινάει με ένα περιορισμένο σύνολο γνώσεων - εμπειρίας. Παρόλ' αυτά, Ένας «λιγότερο έμπειρος» reasoner έχει τη δυνατότητα να προτείνει λύσεις εξίσου αποτελεσματικές σε σχέση με έναν «έμπειρο» στην περίπτωση που

μπορεί να κατανοήσει την υπάρχουσα κατάσταση και δημιουργικά να νιοθετήσει λύσεις από εκείνες τις λίγες που έχει ήδη αποθηκευμένες. Αυτό μπορεί να γίνει εάν η λιγοστή εμπειρία του σχετίζεται άμεσα με το νεοεμφανισθέν πρόβλημα.

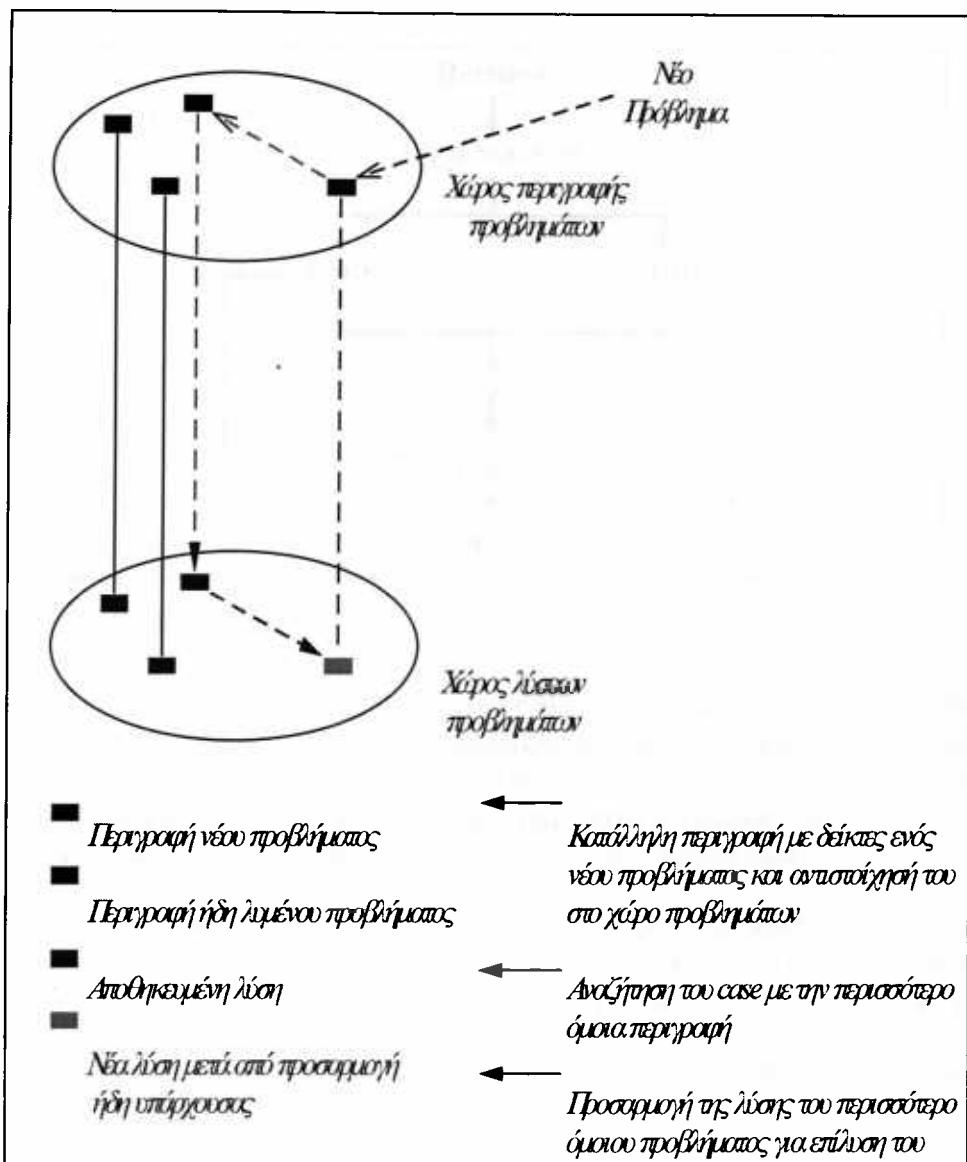
Γενικά, η αποτελεσματικότητα του reasoner και η ποιότητα των λύσεων που μπορεί να προτείνει σχετίζονται με την:

- Την εμπειρία που του έχει αρχικά δοθεί από τον χρήστη ή που έχει μόνος του δημιουργήσει μέσα από την τριβή με προβληματικές καταστάσεις.
- Την δυνατότητα να κατανοεί τις νέες καταστάσεις που εμφανίζονται και τις σχέσεις τους με παρελθόντες εμπειρίες.
- Την επιδεξιότητα στην υιοθέτηση παλιότερων λύσεων για αντιμετώπιση νεοεμφανιζόμενων προβλημάτων
- Την ικανότητα για αξιολόγηση της αποτελεσματικότητας των λύσεων που νιοθετεί και την αντίστοιχη επιδιόρθωση των παλαιοτέρων.
- Την επιδεξιότητα να ενοποιεί την νέα εμπειρία στην μνήμη για να την χρησιμοποιήσει μελλοντικά.

2.7 Βασικός τρόπος λειτουργίας του CBR

Το CBR μπορεί να ταξινομηθεί με βάση τις λειτουργίες του σε Problem Solving και Interpretative CBR (Janesko 1996). Το Problem solving ως στόχο έχει την υιοθέτηση παλαιότερων λύσεων για την επίλυση νέων προβλημάτων (*adaptation*). Το interpretative CBR σχετίζεται με την αξιολόγηση και αιτιολογία (*justification*) των cases.

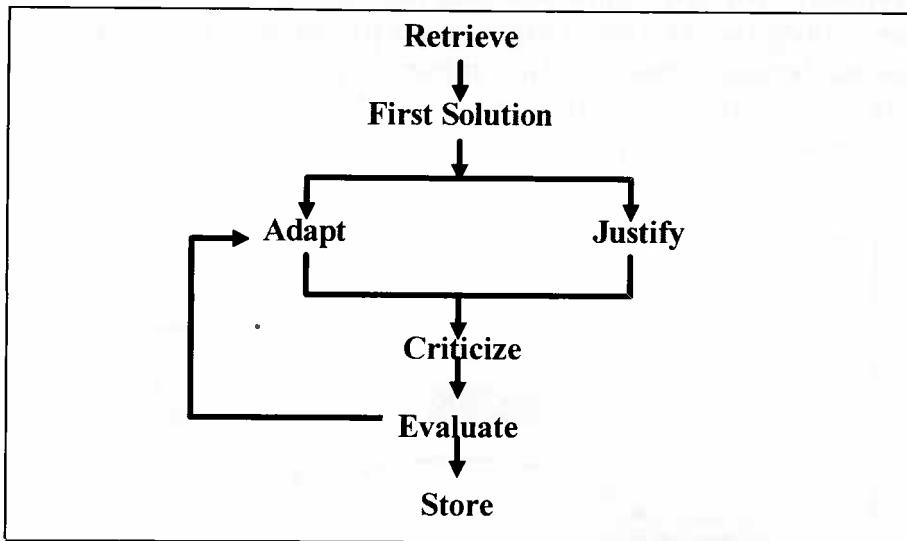
Στην πρώτη κατηγορία περιλαμβάνονται ενέργειες σχετικές με εκτίμηση καταστάσεων, ανάκτηση των cases, αξιολόγηση. Οι ομοιότητες και διαφορές μεταξύ παλαιότερων και νεότερων cases μπορούν να χρησιμοποιηθούν για τον καθορισμό του τρόπου με τον οποίο μπορούν λύσεις παλαιότερων περιπτώσεων να χρησιμοποιηθούν για την λύση νεότερων. Ο προσδιορισμός της ομοιότητας (*similarity*) παλαιότερων και νεότερων καταστάσεων αποτελεί το βασικό συστατικό της διαδικασίας επίλυσης προβλημάτων. Όπως παριστάνεται στο παρακάτω σχήμα, ο χώρος των προβληματικών καταστάσεων διαιρείται σε αυτόν με τις περιγραφές των προβλημάτων και σε αυτόν που περιλαμβάνει τις λύσεις αυτών. Με την εμφάνιση ενός νέου προβλήματος πραγματοποιείται προσπάθεια για κατηγοριοποίησή του και αντιστοιχίζεται με συγκεκριμένη περιγραφή. Έπειτα γίνεται προσπάθεια εύρεσης παρόμοιων περιγραφητών στη βάση γνώσης. Έχοντας εντοπίσει παρόμοια προβλήματα μπορούμε να αναζητήσουμε και τις λύσεις που έχουν ήδη υιοθετηθεί για αυτά. Η λύση του πιο συναφούς με το νέο πρόβλημα είναι εκείνη που τελικά θα επιλεγεί και από την οποία θα στηριχθεί και η λύση για το νέο πρόβλημα.



Εικόνα 15. Ο τρόπος οργάνωσης του χώρου προβλημάτων στο CBR

2.8 Ο κύκλος του CBR

Ο κύκλος του CBR παριστάνεται στο παρακάτω σχήμα (Kolodner 1996). Η αναζήτηση (*retrieve*) αποτελεί βασική λειτουργία στον κύκλο και σχετίζεται με την ανάκτηση συγγενών cases στη μνήμη. Η δεικτοδότηση των cases και η αναπαράσταση μέσω κατάλληλων δομών αποτελεί σημαντικό παράγοντα για την αποδοτική και γρήγορη ανάκτηση των cases. Η κριτική αξιολόγηση (*criticize*) των cases που εμφανίζονται ως πιθανές λύσεις αποσκοπεί στο φιλτράρισμα των cases, έτσι ώστε οι καλύτερες δυνατές λύσεις να προταθούν από τον reasoner ως λύση στο πρόβλημα. Η αξιολόγηση (*evaluation*) της αποτελεσματικότητας του reasoner πραγματοποιείται από τον χρήστη, με την βοήθεια του οποίου τα cases ενημερώνονται στην μνήμη, αναδιοργανώνονται, αξιολογείται η αποτελεσματικότητά τους, ξαναδεικτοδοτούνται και αποθηκεύονται (*Store*) για μελλοντική χρήση.



Εικόνα 16. Ο κύκλος του CBR

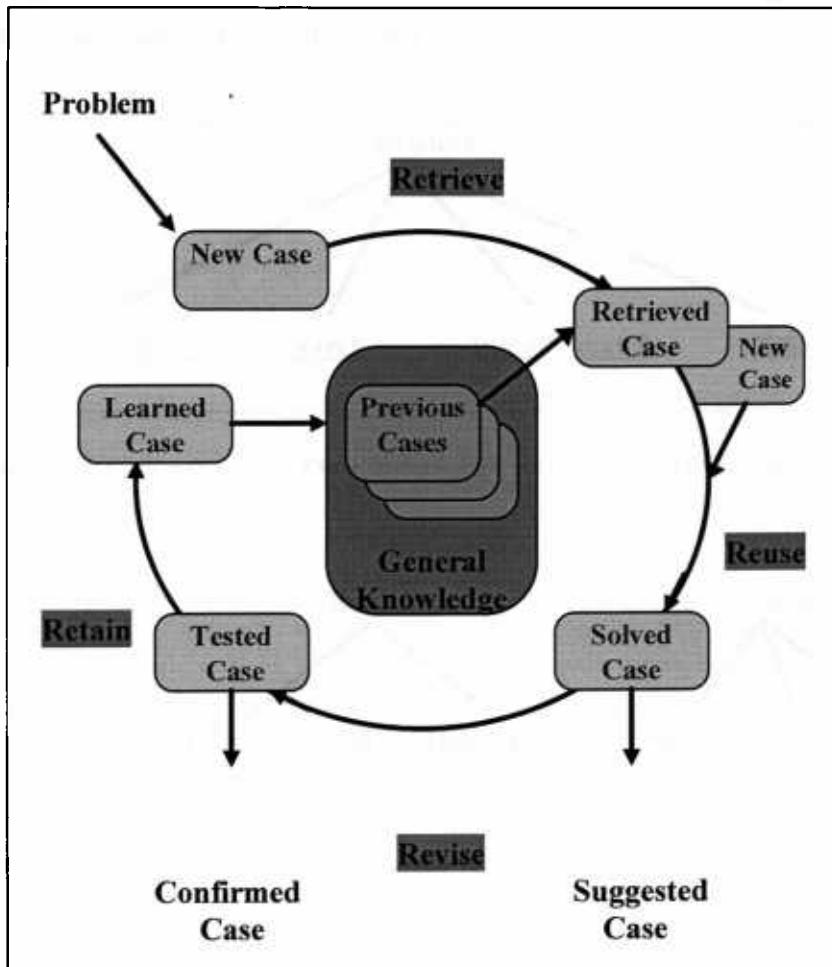
Στην περίπτωση του problem - solving CBR, αφού μια αρχική λύση προταθεί με βάση την προηγούμενη εμπειρία, η διαδικασία της προσαρμογής της (*adaptation*) στόχο έχει την αναθεώρηση και προσαρμογή της για να επιλύσει την νεοεμφανισθείσα κατάσταση. Η περαιτέρω επίκριση (*criticize*) της λύσης μπορεί να αποβεί αναγκαία μέχρι να προταθεί η τελική λύση στο πρόβλημα.

Στην περίπτωση του interpretive CBR στην διαδικασία της αιτιολόγησης (*justification*) της αρχικής προτεινόμενη λύσης συγκρίνονται η νέα με τις παλαιότερες λύσεις. Εξετάζονται οι ομοιότητες και διαφορές των νέων προβλημάτων με παλαιότερων, ενώ το βήμα της κρίσης (*criticize*) αποσκοπεί στον έλεγχο της αποτελεσματικότητας της λύσης, πριν προχωρήσει ο κύκλος στη διαδικασία της αποτίμησής της (*evaluate*).

Μια διαφορετική περιγραφή του κύκλου του CBR (Aadmont 1993) διακρίνει τις διαδικασίες του στις: αναζήτηση (*retrieve*) του περισσότερο συγγενούς case από τη βιβλιοθήκη των cases, επαναχρησιμοποίηση (*reuse*) της πληροφορίας και γνώσης που βρίσκεται αποθηκευμένη σε αυτό το case για την χρησιμοποίησή της στη λύση του προβλήματος, αναθεώρηση (*revise*) της προτεινόμενης λύσης και τέλος συγκράτηση (*retain*) της γνώσης και νεοαποκτηθείσας εμπειρίας για την χρήση της σε μελλοντικά προβλήματα.

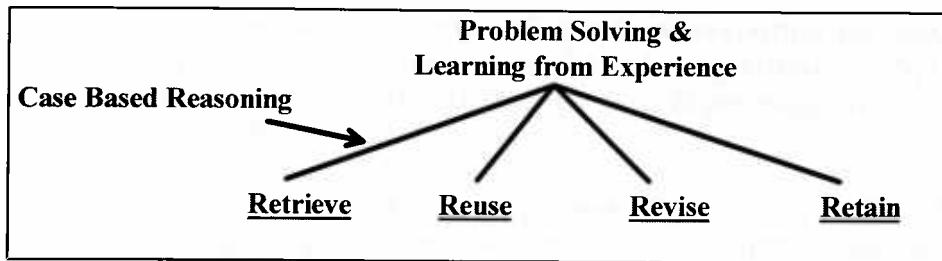
Η εμφάνιση ενός νέου προβλήματος αντιστοιχίζεται με μια περιγραφή η οποία αποτελεί ένα νέο case. Στηριζόμενοι σε αυτό το case αναζητείται ένα case από τα ήδη αποθηκευμένα στη βιβλιοθήκη (διαδικασία *retrieve*) που διατηρείται με τις προηγούμενες λύσεις. Αυτό συνενώνετε με το καινούργιο μέσα από τη διαδικασία της επαναχρησιμοποίησης (διαδικασίας *reuse*) και παράγεται μια πρώτη λύση (*solved case*). Η λύση αυτή αξιολογείται (μέσω της διαδικασίας *revise*). Η αξιολόγηση μπορεί να γίνει από εξωτερικούς παράγοντες, από κάποιον εμπειρογνώμονα, γνώστη παρόμοιων προβληματικών καταστάσεων και εάν κριθεί αναγκαίο επιδιορθώνεται και εφαρμόζεται ή εάν δεν είναι αυτό δυνατόν δεν χρησιμοποιείται ως λύση στο

πρόβλημα. Η νέα αυτή λύση - το νέο case που δημιουργείται, αποθηκεύεται στην βάση γνώσης για μελλοντική χρήση (διαδικασία retain). Παρατηρούμε πως κεντρικό σημείο στον κύκλο του CBR είναι η αποθηκευμένη γνώση (General Knowledge) με τα προηγούμενα αποκτηθέντα cases. Ο ρόλος της είναι καθοριστικός μιας και συνδέεται άμεσα με την ικανότητα του reasoner να προτείνει αποτελεσματικές λύσεις στα προβλήματα που εμφανίζονται.

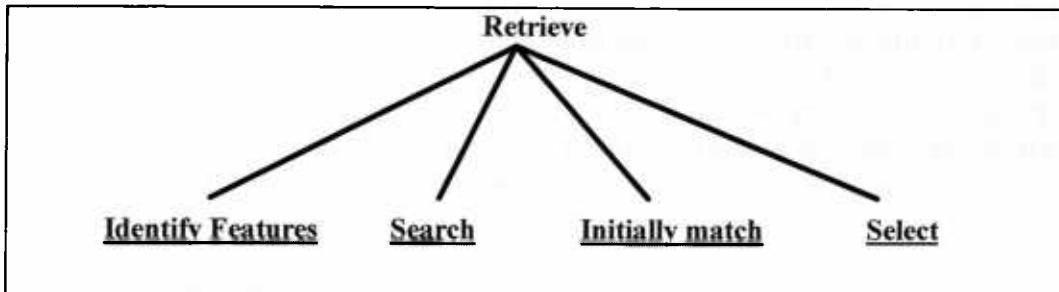


Εικόνα 17. Μια άλλη παράσταση του κύκλου του CBR

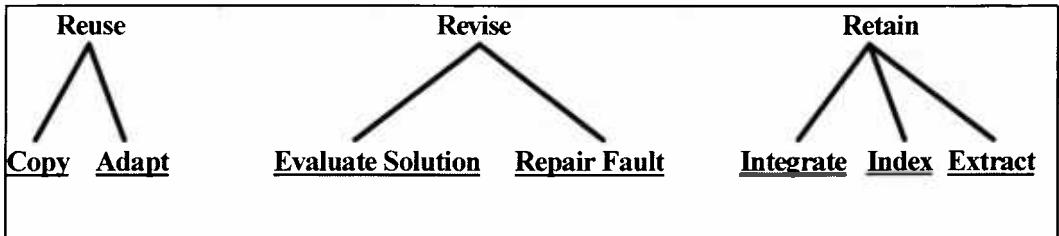
Κάθε μια από τις βασικές λειτουργίες του CBR υλοποιείται από μια σειρά επιμέρους ενεργειών. Στο παρακάτω σχήμα παριστάνονται οι βασικές από τις διαδικασίες που περιγράψαμε και οι περαιτέρω υπο-διαδικασίες οι οποίες τις συνιστούν.



Εικόνα 18. Μια task - oriented περιγραφή του CBR.



Εικόνα 19. Μια (sub)task - oriented περιγραφή της Retrieve λειτουργίας.



Εικόνα 20. Μια (sub)task - oriented περιγραφή των Reuse, Revise και Retain λειτουργιών

2.8.1 Retrieve

Η λειτουργία της ανάκτησης (retrieve) στοχεύει στην εύρεση του πλησιέστερου case που υπάρχει ήδη στη βάσης γνώσης με εκείνο που μόλις εμφανίστηκε και περιγράφει το νέο πρόβλημα. Οι υπολειτουργίες που απαρτίζεται είναι η αναγνώριση των χαρακτηριστικών δεικτοδότησης (identify features), το αρχικό ταίριασμα (initially match) με κάποια cases αναζήτηση (search) σε αυτά του καλύτερου για το ήδη υπάρχον πρόβλημα και η τελική επιλογή (select) του case (reference case) που θα μας οδηγήσει στη λύση του προβλήματός μας.

Η επιλογή των χαρακτηριστικών με τα οποία θα αρχίσει η διαδικασία της αναζήτησης είναι πρωταρχικής σημασίας. Αναφέρεται στην διαλογή από τα συμφραζόμενα του προβλήματος εκείνων των περιγραφητών τα οποία μπορούν να δώσουν μια καλή περιγραφή για τα πρόβλημα και την σύγκρισή του με τα υπάρχοντα cases. Η κατανόηση του προβλήματος περιλαμβάνει λειτουργίες όπως το φίλτραρισμα

των περιττών (noisy) περιγραφητών, την εξαγωγή συμπερασμάτων για άλλους χρήσιμους περιγραφητές που δεν είναι έκδηλοι αλλά είναι χρήσιμοι για τη διαδικασία της αναζήτησης, τον έλεγχο για την ορθότητα των περιγραφητών ως ικανοί να αντιπροσωπεύσουν το πρόβλημα, κτλ.

Αφού έχουν προσδιοριστεί οι περιγραφητές για το νέο πρόβλημα, χρησιμοποιούνται ως δείκτες, με τους οποίους γίνεται η αναζήτηση όμοιων στη βάση γνώσης. Αρχικά ανακτώνται πολλοί από τους οποίους απαιτείται επιλογή ενός. Αντιστοιχίζονται βάρη σε αυτούς ανάλογα με τη βαρύτητα που κάθε στοιχείο του έχει στην παράσταση του προβλήματος. Με αυτόν τον τρόπο είναι οργανωμένοι και οι περιγραφητές των ήδη αποθηκευμένων cases. Τα βάρη που προσδίδονται στα cases απορρέουν με κριτήρια όπως η δυνατότητα διαφοροποίησης (discrimination value) του case από τα άλλα, σημασιολογικής διαφοροποίησης. Cases που τα στοιχεία τους ταιριάζουν με όλα τα στοιχεία του διανύσματος των δεικτών του προβλήματος, αποτελούν σίγουρα αξιόπιστη πηγή από την οποία θα βρεθεί η τελική λύση. Επιλογή των cases μπορεί να πραγματοποιηθεί ακόμα και αν ταιριάζει ένα μόνο μέρος από το σύνολο των δεικτών τους με το αρχικό πρόβλημα.

Η αναζήτηση μπορεί να εξάγει πολλά cases με μεγάλο ομοιότητας με το νέο πρόβλημα. Στόχος είναι η επιλογή ενός, εκείνου που θα αποτελέσει το καλύτερο ξεκίνημα στη διαδικασίας μετατόπισης προς την βέλτιστη λύση. Αποτελεί περισσότερο πολύπλοκη διαδικασία από την αρχική της αναζήτησης, καθώς επανεξετάζεται η διαδικασία της αναζήτησης, τα χαρακτηριστικά των cases που αναζητήθηκαν (μήπως και απορριφθούν κάποια), η βάση γνώσης που υπάρχει και το εάν κάποια από τα εξαγόμενα cases αποτελούν χαρακτηριστικοί πρεσβευτές όσων αυτή περιγράφει, αλλά και η επιβεβαίωση με το χρήστη για περισσότερες πληροφορίες οι οποίες θα βοηθήσουν τη διαδικασία.

2.8.2 Reuse

Δυο τρόποι υπάρχουν για την επαναχρησιμοποίηση των cases. Η διαδικασία της επαναχρησιμοποίησης παλαιότερης λύσης, μέσα από τον μετασχηματισμό αυτής (*transformational reuse*). Η παλαιότερη λύση δεν χρησιμοποιείται άμεσα στο νέο πρόβλημα αλλά μετασχηματίζεται (με τη βοήθεια υπάρχουσας γνώσης που σχετίζεται με διαδικασίας μετασχηματισμού), προκειμένου να αντιμετωπιστεί το νέο πρόβλημα. Στόχος δεν είναι η εξέταση των λύσεων του προβλήματος, όσο των διαφορών και ομοιοτήτων των λύσεων μεταξύ τους και του τρόπου μετασχηματισμών τους ώστε να ταιριάζουν στο νέο πρόβλημα.

Ο άλλος τρόπος είναι η επαναχρησιμοποίηση του τρόπου με τον οποίο δημιουργήθηκε η παλαιότερη λύση (*derivational reuse*). Εξετάζει τον τρόπο που επιλύθηκε το πρόβλημα που περιγράφεται στο ανακτημένο case. Το case αυτό κατακρατεί πληροφορία σχετικά με τον τρόπο που επίλυσε το πρόβλημα στο οποίο αναφέρεται, τα σημεία που επικεντρώθηκε η λύση, τους στόχους (goals), τις επιτυχίες και αποτυχίες της, το γενικό σχέδιο της (plan). Έπειτα εφαρμόζεται ξανά (replay) η διαδικασία ανάκτησης στο νέο πρόβλημα με στόχο την εύρεση νέων λύσεων, την αναζήτηση νέων στόχων στηριζόμενοι στους παλιούς ενώ νέα σχέδια μπορούν να υπάρξουν παρόμοια και πιο αποδοτικά από τα παλαιότερα.



2.8.3 Revise

Αφού έχει προταθεί μια λύση από την προηγούμενη διαδικασία, γεννιέται το πρόβλημα αναθεώρησής της, κυρίως όταν εμφανιστεί η περίπτωση αποτυχίας. Η φάση αποτελείται από την διαδικασία αποτίμησης (Evaluate Solution) η οποία αναλαμβάνει να νιοθετήσει τη λύση σε συνθήκες πραγματικού περιβάλλοντος, κυρίως με ερωτήσεις προς εμπειρογνόμονες. Στη διαδικασία της διόρθωσης (Repair Fault) ανιχνεύονται τα λάθη της συγκεκριμένης λύσης η οποία επιλέχθηκε και ανακτώνται εξηγήσεις για αυτά. Δημιουργούνται εξηγήσεις σχετικά με την αιτία που δεν υλοποιήθηκαν συγκεκριμένες λειτουργίες ή μέρη του σχεδίου όπως έπρεπε να γίνουν. Με βάση τα αποτελέσματα ανατροφοδοτείται το σύστημα με τις σχετικές πληροφορίες προκειμένου να τροποποιηθεί η λύση για την καλύτερη αυτή τη φορά λύση του προβλήματος.

2.8.4 Retain - Learning

Η αποτελεσματικότητα του reasoner στη διαδικασία λύσης προβλημάτων αυξάνεται με την πάροδο του χρόνου. Ο καλός τρόπος δεικτοδότησης αλλά και η κατακράτηση στοιχείων σχετικά με την αποδοτικότητα των λύσεων που κάθε φορά προτείνει, επιφέρει θετικά αποτελέσματα στον τρόπο που αντιδρά στο μέλλον. Η ενθύμηση παλαιότερων λύσεων και η προσαρμογή τους για να ταιριάζουν στο νέο πρόβλημα είναι αποτελεσματικότερη διαδικασία από εκείνη της εξ' αρχής εύρεσης της καλύτερης λύσης κάθε φορά.

Ένα από τα βασικά πλεονεκτήματα της μεθόδου είναι η δυνατότητα πρόβλεψης και αποφυγής λαθών που είχαν γίνει στο παρελθόν. Ο reasoner διατηρεί τα συστατικά στοιχεία κάθε προβλήματος, τα δεικτοδοτεί κατάλληλα με βάση τα σπουδαιότερα χαρακτηριστικά τους, μπορεί να προβλέψει λάθη που μπορούν να προκύψουν με την εφαρμογή τους και προσπαθεί να τα αποφύγει με την εφαρμογή κατάλληλων λύσεων.

Συγκεκριμένα η διαδικασία της εκμάθησης στοχεύει στην εύρεση και διατήρηση στη βάση γνώσης των χρήσιμων στοιχείων από την διαδικασία λύσης του νέου προβλήματος. Υπάρχουν τρόποι για την εκμάθηση τόσο των επιτυχιών όσο και αποτυχιών που η λύση έχει επιφέρει. Πολλές από τις πληροφορίες αυτής της φάσης προέρχονται από τη διαδικασία αποτίμησης της λύσης (evaluation solution) του προηγούμενου βήματος του κύκλου. Περιλαμβάνει διαδικασίες όπως η επιλογή των πληροφοριών από το case οι οποίες θα κατακρατηθούν, πως πρέπει να δεικτοδοτηθεί το case προκειμένου στην αποτελεσματική επαναχρησιμοποίησή του σε μελλοντικά παρόμοια προβλήματα, κτλ.

Μετά τη λύση του προβλήματος η βάση γνώσης του CBR πρέπει να αναθεωρηθεί. Εάν για τη λύση χρησιμοποιήθηκε ένα παλαιότερο case, πρέπει είτε να δημιουργηθεί ένα καινούργιο case είτε το παλιό να γενικευθεί έτσι ώστε να περιλαμβάνει και το νέο case. Εάν το πρόβλημα λύθηκε με τελείως διαφορετικό

τρόπο, όπως διεπαφή με το χρήστη, αλληλεπίδραση με δασκάλους, εμπειρογνώμονες, ένα εξολοκλήρου καινούργιο case δημιουργείται το οποίο περιλαμβάνει στοιχεία για τη νέα προβληματική κατάσταση. Σε όλες τις περιπτώσεις τα βασικά στοιχεία που χρησιμοποιούνται για την εκμάθηση είναι οι περιγραφητές των προβλημάτων, οι λύσεις στα προβλήματα αυτά καθώς και ένα είδος επεξήγησης ή αιτιολόγησης που δικαιολογεί γιατί η συγκεκριμένη λύση σχετίζεται με το συγκεκριμένο πρόβλημα.

Η δεικτοδότηση (indexing) των cases αποτελεί μια από τις σημαντικότερες λειτουργίες του CBR. Κύρια καθήκοντά του είναι ο προσδιορισμός των χαρακτηριστικών των cases με τα οποία θα πραγματοποιηθεί η δεικτοδότηση καθώς και η δομή που θα επιλεγεί για την αποθήκευση των cases. Μια πρώτη λύση μπορεί να είναι η χρησιμοποίηση όλων των χαρακτηριστικών των cases για τη δεικτοδότησή τους. Η αναζήτηση μπορεί να γίνει συγκρίνοντας ένα προς ένα τα διανύσματα δεικτών που αντιστοιχούν στα cases για εύρεση κοινών και μη στοιχείων.

Η ενοποίηση (integration) της ήδη υπάρχουσας βάσης γνώσης με την γνώση που βρίσκεται στα cases, αποτελεί το τελευταίο βήμα της διαδικασίας εκμάθησης. Αποτελεί ουσιαστικά τη συνέχεια της διαδικασίας δεικτοδότησης. Η ενοποίηση πραγματοποιείται με την αναδιάρθρωση της δομής των δεικτών. Τα βάρη τους αλλάζουν βασιζόμενοι στην επιτυχία ή αποτυχία χρήσης του αντίστοιχου case στην επίλυση προβλημάτων ή μέσα από την αλληλεπίδραση με το χρήστη.

Η κατάλληλες τροποποίησεις στη δομή των δεικτών και η ικανότητα του συστήματος στην αποτελεσματική εύρεση χαρακτηριστικών και σημείων δεικτοδότησης, αποτελεί βασική προϋπόθεση της αποδοτικής μάθησής του. Όσο αποδοτικότερη είναι η δεικτοδότηση τόσο αυξάνονται οι δείκτες απόδοσης σχετικά με χρόνους απόκρισης του συστήματος, και την ικανότητα να αντιμετωπίζει ουσιαστικά τα νέα εμφανιζόμενα προβλήματα.

2.9 Case Based Συστήματα

Μια κατηγοριοποίηση των CBR συστημάτων τα χωρίζει σε (Aadmont 1993):

- **Αυτόνομα Συστήματα.** Επιλύουν τα προβλήματα μόνα τους. Πραγματοποιούν τις λειτουργίες της ανάκτησης, προσαρμογής των υπαρχόντων λύσεων και αξιολόγησης των λύσεων, όπως πραγματοποιούνται από τα τυπικά έμπειρα συστήματα, αλλά με χρήση case based τεχνικών. Συστήματα τέτοιου είδους είναι τα CHEF, Julia, Casey, Protos, Hypo.
- Δεύτερη είναι η κατηγορία των συστημάτων στα οποία ο ανθρώπινος παράγοντας αποτελεί συστατικό στοιχείο στη λειτουργία του συστήματος (Συστήματα Ανθρώπου - Μηχανής). Το σύστημα αναλαμβάνει να πραγματοποιεί εκείνες τις λειτουργίες οι οποίες είναι δύσκολες για τους ανθρώπους (ανάκτηση και παρουσίαση των λύσεων), ενώ ο άνθρωπος αναλαμβάνει τις δύσκολες για το σύστημα λειτουργίες (προσαρμογή των ήδη γνωστών cases για εφαρμογή τους στο νέο πρόβλημα, αντιπαραβολή των παλαιότερων cases με τα νεοεμφανιζόμενα προβλήματα). Ένα απλό σύστημα τέτοιου είδους αποτελεί ένα σύστημα ανάκτησης μόνο. Παραδείγματα αποτελούν τα συστήματα Archie-2, Clavier, Scied.

- Τα *Ενσωματωμένα Συστήματα* αποτελούν μικρότερα τμήματα μεγαλύτερων εφαρμογών. Έχουν ως στόχο να υλοποιούν με έξυπνο τρόπο λειτουργίες ανάκτησης πληροφορίας χρήσιμης για την λειτουργία των άλλων υποσυστημάτων, εκμάθησης για νέους τύπους προβλημάτων.

2.9.1 Εφαρμογές που έχει χρησιμοποιηθεί το CBR

Το CBR, παρά την πρόσκαιρη θεμελίωσή του έχει εφαρμοστεί σε πολλές περιπτώσεις, ιδιαίτερα σε εκείνες όπου έχουν σχέση με πρόβλεψη καταστάσεων. Εφαρμογές σχετικές με εκτίμηση γεωλογικών αποθεμάτων, επιχειρησιακές στρατηγικές αποφάσεις, ανάλυση δανείων, πρόβλεψη χρεωκοπήσεων, έχουν υλοποιηθεί με CBR (Mott 1993). Ο τομέας ο οποίος «φαίνεται να ταιριάζει» περισσότερο (αναλογιζόμενοι τις εφαρμογές στις οποίες έχει ήδη χρησιμοποιηθεί), είναι τα αυτοματοποιημένα διαγνωστικά συστήματα (διάγνωση προβλημάτων σε σκληρούς δίσκους ηλεκτρονικών υπολογιστών, εργαλεία για επανόρθωση από προβληματικές καταστάσεις, διάγνωση προβλημάτων σε συστήματα συντήρησης αεροσκαφών).

Μέχρι σήμερα ένας αριθμός συστημάτων έχει κατασκευαστεί καλύπτοντας ποικίλους χώρους προβλημάτων, από εφαρμογές σε εμπορικά συστήματα, υπολογιστικά περιβάλλοντα και βιομηχανικές περιοχές. Η εταιρεία Lockheed (Mark 1996, Hennessy 1992,, Bradley 1994), έχει χρησιμοποιήσει ένα CBR σύστημα για να καθορίζει ποια αντικείμενα είναι καλύτερα να τοποθετούνται κάθε φορά στον κλίβανο για την επισκευή τους. Ο χειριστής περιγράφει στο σύστημα το σύνολο των αντικειμένων τα οποία πρέπει να επιδιορθωθούν, καθώς και την προτεραιότητα κάθε ενός. Αυτό με τη σειρά του δείχνει τρόπους με τον οποίο πρέπει να τοποθετηθούν τα αντικείμενα στον κλίβανο με τον καλύτερο και οικονομικότερο τρόπο, αναζητώντας παρόμοιες περιπτώσεις τοποθέτησης από την βιβλιοθήκη των cases.

Η εταιρεία NEC χρησιμοποιεί CBR ως μέρος ενός αρκετά πολύπλοκου συστήματος μέσω του οποίου πραγματοποιεί Business Process Reengineering (Kitano 1996). Αποτελεί αρκετά τολμηρή και φιλόδοξη προσπάθεια με την οποία δημιουργείται ένα καθολικό πλαίσιο στο οποίο καταγράφεται και διατηρείται η εμπειρία των εργαζομένων σχετικά με θέματα ποιότητας λογισμικού. Το έργο άρχισε το 1992 και κάθε χρόνο προστίθενται περίπου 3000 cases, προσφέροντας στους κατασκευαστές, 100 εκατ. δολάρια κέρδος στην εταιρεία το χρόνο.

Στην Compaq χρησιμοποιείται ένα CBR σύστημα στο τμήμα εξυπηρέτησης πελατών (Bradley 1994). Τα προβλήματα από τους πελάτες των συστημάτων της εταιρείας εισέρχονται ως input στο CBR σύστημα. Αυτό με τη σειρά του ανακαλεί τα πιο όμοια cases και τα παρουσιάζει στους χειριστές προκειμένου να επιλύσουν το πρόβλημα. Η εταιρεία έχει κάνει απόσβεση στο σύστημα μόλις στον πρώτο χρόνο λειτουργίας του. Επίσης εσωκλείνει ένα μικρό CBR σύστημα σε προγράμματα λογισμικού, τα οποία αναπτύσσει προκειμένου να ελέγχουν λειτουργία σε μια σειρά εκτυπωτές της.

Αυτά αποτελούν πολύ λίγα από τα παλαιότερα και πιο γνωστά συστήματα που έχουν αναπτυχθεί χρησιμοποιώντας συμπερασματολογία μέσω υποθέσεων,



Αποτελούν γλαφυρά παραδείγματα οτι μπορούν να διαδραματίσουν κύριο ρόλο στους μηχανισμούς λήψης αποφάσεων ενός οργανισμού και να ενοποιηθούν με τις υπάρχουσες μεθοδολογίες και τεχνικές. Παρόλ' αυτά ιδιαίτερη προσοχή αξίζει να προσδοθεί στο γεγονός οτι δεν παρέχουν όλα τα συστήματα τις ειδικές εκείνες λειτουργίες της προσαρμογής παλαιοτέρων λύσεων, βασικές για τη λειτουργία του CBR. Σε συγκεκριμένα γνωστικά πεδία είναι ευκολότερο βέβαια να χρησιμοποιηθούν τέτοιες τεχνικές, όπου τα πράγματα είναι περισσότερο ορισμένα, όπως στο χώρο της σχεδίασης (design) και κατασκευής (manufacturing).

2.9.2 Παρατηρήσεις κατά τη διαδικασία ανάπτυξης CBR συστημάτων

Μερικά στοιχεία αξίζουν ιδιαίτερη προσοχή κατά τη δημιουργία της βάσης γνώσης των cases, αλλά και την εν συνέχεια συντήρησή της. Η συνοχή της βάσης είναι σημαντικός τέτοιος παράγοντας, ο οποίος μπορεί να προέλθει από την απρόσεκτη, βιαστική εισαγωγή cases, χωρίς τον απαραίτητο προσεκτικό έλεγχο των όσων εισάγονται (O'Leary 1993). Ο πλεονασμός είναι από τα πλέον γνωστά προβλήματα που «ταλαιπωρούν» τους διαχειριστές βάσεων γνώσης. Έτσι και στο CBR δεν πρέπει να υπάρχει επανάληψη αποθηκευμένων cases. Κάθε case πρέπει εκφράζει κάτι το ξεχωριστό, ένα διαφορετικό στιγμότυπο. Η ύπαρξη πολλών ίδιων αποτελεί μεγάλο λάθος κατά τη σχεδιαστική διαδικασία, αλλά και τη διαδικασία εισαγωγής νέων cases και πρέπει να αποφεύγεται αυστηρά. Η πληρότητα της βάσης αποτελεί στοιχείο αναγκαίο προκειμένου το σύστημα να επιδεικνύει τις καταλληλότερες και σωστότερες κάθε φορά λύσεις, χωρίς περιθώρια σφαλμάτων. Τέλος η ορθότητα του τρόπου συμπερασματολογίας σχετίζεται με τον τρόπο με τον οποίο τα cases είναι οργανωμένα στη βάση γνώσης. Η δόμησή τους με διάταξη δενδρική, για παράδειγμα, μπορεί να οδηγήσει σε συμπεράσματα για το κατά πόσο το αποτέλεσμα που εκδόθηκε ήταν αυτό που έπρεπε να δοθεί (ακολουθήθηκε ο προκαθορισμένη τρόπος λήψης της απόφασης μέσα από τη διάσχιση του δένδρου, κτλ.).

Η επιτυχία ενός CBR συστήματος, όπως αναφέρθηκε ήδη σε προηγούμενη ενότητα, βασίζεται στην καλή δόμηση και δεικτοδότηση των cases. Όταν δεν έχει επιλεγεί καλός τρόπος δεικτοδότησης, όταν δεν υπάρχει οργάνωση και αποτελεσματική δόμηση των cases, παρουσιάζονται δυσλειτουργίες και δεν καθίσταται εφικτή η καλύτερη επιλογή λύσεων στα προβλήματα.

Πρέπει να επιλεγεί ένας καθολικός - αποδοτικός τρόπος για την δόμηση τον χωρισμό των cases σε clusters. Η επιλογή αντιπροσωπευτικών cases κρίνεται αναγκαία προκειμένου η διαδικασία συμπερασματολογίας να είναι γρήγορη, ευέλικτη, αλλά και το κόστος αποθήκευσης και τροποποίησης της βάσης των cases να είναι αποδεκτό.

Κατά τη διάρκεια της λειτουργίας των CBR συστημάτων μπορεί να δημιουργηθούν νέα cases, τα οποία να είναι ικανά για την επίλυση συγκεκριμένων προβλημάτων, μέσα από τις γνωστές διαδικασίες προσαρμογής των ήδη υπαρχόντων cases. Μερικά από τα cases αυτά (άλλα και μερικά από τα αρχικά της βάσης) μπορεί να οδηγούν σε λάθος συμπεράσματα, να εμπεριέχουν λανθασμένο τρόπο αντιμετώπισης των προβληματικών καταστάσεων. Η ύπαρξη τέτοιων cases σίγουρα δεν είναι

επιθυμητή και αναγκαία είναι η ύπαρξη μηχανισμών για την ανακάλυψη και απομάκρυνσή τους από τη βάση γνώσης.

Η ύπαρξη μιας φόρμουλας με την οποία θα είναι δυνατή η αξιολόγηση των cases είναι αναγκαία για την αποτελεσματική λειτουργία του CBR συστήματος.(Ketler 1993). Η αξιολόγηση των cases που έχουν ανακτηθεί, ως λύσεις σε κάποια προβληματική κατάσταση, πρέπει να γίνεται ώστε οι διαχειριστές της βάσης γνώσης να γνωρίζουν εάν το σύστημα όντως εκδίδει αποτελεσματικές λύσεις στα προβλήματα που παρουσιάζονται.

2.10 Case-Based Reasoning VS Analogical Reasoning

Είναι χρήσιμο να παραθέσουμε μερικές βασικές διαφορές μεταξύ CBR και συστημάτων που πραγματοποιούν Analogical Reasoning (AR). Το AR αναφέρεται σε τρόπο συμπερασματολογίας ο οποίος στηρίζεται στη σύγκριση των προβληματικών καταστάσεων με βάση την αναλογικότητα, ομοιότητα των επιμέρους χαρακτηριστικών τους, Κύριο χαρακτηριστικό του AR είναι οτι μπορεί να αναφέρεται σε λύσεις προβληματικών καταστάσεων διαφορετικών χώρων προβλημάτων. Μια πρωταρχική ειδοποιός διαφορά είναι οτι το CBR εφαρμόζεται σε ένα μόνο προβληματικό χώρο, ενώ το AR μπορεί να διασυνδεθεί με διαφορετικά περιβάλλοντα και χώρους προβλημάτων (Brown 1993). Αυτό καθιστά την εφαρμογή του AR δυσκολότερη διαδικασία, με πολύ υψηλό κόστος. Η συμπερασματολογία πραγματοποιείται συγκρίνοντας καταστάσεις αναλογικά, μια σύγκριση που πραγματοποιείται αρκετά δύσκολα μιας και πραγματοποιείται λαμβάνοντας στοιχεία από διαφορετικούς χώρους προβλημάτων.

Οι συγκρίσεις μεταξύ cases στο CBR πραγματοποιούνται μέσα από την εξέταση των χαρακτηριστικών (features) του νέου προβλήματος (target case) με τα αποθηκευμένα (source cases) - με τρόπους ανάκτησης από τους ήδη δημιουργημένους δείκτες (indexes). Αντίθετα στο AR λόγω του γενικού χαρακτήρα του, η σύγκριση των cases πραγματοποιείται μέσα από αρκετά αφαιρετικές δομές, με λιγότερο ακριβή τρόπο. Για να πραγματοποιηθεί με επιτυχία η ανάκτηση των cases απαιτείται η οργάνωση των cases σε ανώτερο ιεραρχικό επίπεδο, με λιγότερο οργανωμένο και τυπικά προσδιορισμένο τρόπο.

2.11 Διαφορές Case Based Reasoning με Expert Systems

Οι προσπάθειες οι οποίες έγιναν για να προσδώσουν «εξυπνάδα» σε προγράμματα λήψης αποφάσεων ήταν η ενσωμάτωση σε αυτά ενός μεγάλου αριθμού κανόνων οι οποίοι είναι ικανοί για τη λύση συγκεκριμένων προβλημάτων. Παρόλο που η κατηγορία αυτή των συστημάτων κερδίζει μεγάλη αποδοχή, δεν μπορεί σε καμία περίπτωση να χαρακτηριστούν από την ιδιότητα της «εξυπνάδας» μιας και δεν διακατέχονται από ένα πρωτογενές στοιχείο αυτής - τη δυνατότητα για μάθηση.

Δεν θα περιγράψουμε τα θετικά στοιχεία που τα παραδοσιακά έμπειρα συστήματα έχουν να προσφέρουν, μιας και λίγο ως πολύ είναι γνωστά (εύκολη

συμπερασματολογία και επεξήγηση, επαυξησιμότητα και κατανοησιμότητα των κανόνων, μπορούμε να προσθαφαιρέσουμε κανόνες χωρίς να επηρεάσουμε τη βάση γνώσης, κτλ) αλλά θα προσπαθήσουμε να παραθέσουμε με συνοπτικό τρόπο τις διαφορές που μπορούν να προσδιοριστούν στην σύγκριση μεταξύ του CBR και των Rule - based Expert Systems (Schank 1991):

Η λύση σε ένα έμπειρο σύστημα προκύπτει μέσα από την αλυσιδωτή εκτέλεση κανόνων - ο αριθμός των οποίων, ανάλογα με το πρόβλημα, μπορεί να αντιστοιχεί σε μερικές δεκάδες έως και εκατοντάδες και χιλιάδες. Στην περίπτωση που ξαναεμφανιστεί η ανάγκη για επίλυση του ίδιου ακριβώς προβλήματος, το έμπειρο σύστημα πρέπει να εκτελέσει όλους τους κανόνες με την ίδια σειρά, προκειμένου τελικά να παρουσιάσει την ίδια λύση με εκείνη που επέλεξε και προηγουμένως. Παίρνοντας ως παράδειγμα έναν άνθρωπο, το σίγουρο είναι ότι θα θυμόταν ότι είχε επιλύσει το πρόβλημα που του παρουσιάζεται και δεν θα προσπαθήσει να ξαναυπολογίσει την λύση από την αρχή. Αυτόν τον τρόπο προσπαθεί να πλησιάσει το CBR, με την συμπερασματολογία του να βασίζεται στην ήδη αποκτηθείσα εμπειρία και την κωδικοποίησή της στη βάση γνώσης που διατηρεί.

Αν στο έμπειρο σύστημα δοθεί ένα συγκεκριμένο πρόβλημα, στο οποίο όμως δεν αντιστοιχούν κάποιοι από τους κανόνες που περιέχει, δεν θα δώσει καμία απάντηση. Στην αντίστοιχη περίπτωση όμως, κάποιος έμπειρος θα προσπαθούσε να βρει κάποια απάντηση συνδυάζοντας λύσεις από προηγούμενα προβλήματα, συμπερασματολογώντας με βάση και την γνώση που έχει συλλέξει από το παρελθόν. Έτσι και τα CBR συστήματα προσπαθούν να μοιάσουν στην συμπερασματολογία που ακολουθεί ο άνθρωπος, παρουσιάζοντας καλύτερα αποτελέσματα σε σχέση με τα έμπειρα συστήματα κανόνων.

Η γνώση που τα έμπειρα συστήματα συγκεντρώνουν, την κωδικοποιούν σε ένα σύνολο κανόνων. Οι κανόνες αυτοί έχουν προέλθει από έμπειρους σε συγκεκριμένες γνωστικές περιοχές. Αυτοί προσπαθούν να κωδικοποιήσουν τον τρόπο που σκέπτονται όταν πρόκειται για τη λήψη μιας απόφασης με τη μορφή κανόνων. Η δυσκολία είναι μεγαλύτερη όταν και ο αριθμός των κανόνων είναι μεγάλος. Είναι προτιμότερο και εφικτότερο η γνώση που αποσπάται από τους έμπειρους να γίνεται με την χρήση υποθέσεων (cases) και όχι κανόνων (rules). Το τεράστιο πρόβλημα της απόκτησης γνώσης για τα συστήματα θα μειωνόταν εάν τα προγράμματα χρησιμοποιούσαν cases αντί κανόνες, μιας και αυτά προσεγγίζουν περισσότερο τον τρόπο που οι γνώση είναι οργανωμένη στη σκέψη των ανθρώπων.

Συνοψίζοντας με μερικά αρνητικά στοιχεία που αντιστοιχούν στα έμπειρα συστήματα, αναφέρουμε τη δυσκολία διαχείρισης της βάσης γνώσης - δομημένη σε κανόνες - ειδικά όταν ο αριθμός των κανόνων αυτών είναι αρκετά μεγάλος. Τα περισσότερα rule based συστήματα δεν διακρίνονται από ιδιαίτερες ικανότητες επεξήγησης - γιατί έλαβαν την συγκεκριμένη απόφαση - παρά με την παράθεση των κανόνων όπως αυτοί βρίσκονται καταγραμμένοι από τη διαδικασία του προγραμματισμού τους.

Υπάρχουν βέβαια και ορισμένα χαρακτηριστικά που σχετίζονται με τα CBR συστήματα, που τα κάνουν να διαφέρουν από άλλες τεχνικές, τρόπους και μηχανισμούς λήψης αποφάσεων (Kolodner 1993):

Η απόφαση για χρήση CBR τεχνικών είναι ευκολότερη στην περίπτωση που ο χώρος προβλημάτων στον οποίο αναφερόμαστε δεν είναι τυπικά ορισμένος, δεν μπορεί να γίνει πλήρως κατανοητός. Το CBR έχει δείξει ικανότητες για λύση προβλημάτων τα οποία είναι δύσκολο να μοντελοποιηθούν. Μπορεί να εκδίδει λύσεις κάνοντας υποθέσεις και παραδοχές με βάση τις προηγούμενες σχετικές περιπτώσεις, παρόλο που υπάρχει ελλιπής κατανόηση της γνωστικής περιοχής.

Τα CBR συστήματα χαρακτηρίζονται από ένα θεμελιώδες χαρακτηριστικό, την ικανότητα για μάθηση. Αυτή αφορά τόσο την μάθηση για το ποιοι τρόποι είναι οι περισσότερο αποτελεσματικοί για την επίλυση μιας κατηγορίας προβλημάτων, αλλά ταυτόχρονα και σημαδεύει τις λύσεις εκείνες οι οποίες δεν μπορούν να ανταποκριθούν αποτελεσματικά από τη διαδικασία επίλυσης. Αυτό πραγματοποιείται μέσα από τη διαδικασία της αξιολόγησης των λύσεων. Όταν το σύστημα οδηγείται προς έναν τρόπο λύσης, ο οποίος είχε χαρακτηριστεί ως ανίκανος να οδηγήσει σε θετικά αποτελέσματα, το σύστημα μέσα από την «ενθύμηση» αποτρέπει την παραπέρα εφαρμογή της.

Με την χρήση των cases, ο reasoner έχει τη δυνατότητα να επικεντρώσει την συμπερασματολογία του σε συγκεκριμένα μόνο, σημαντικά κομμάτια του προβλήματος, επιδεικνύοντας ποια από τα χαρακτηριστικά - στοιχεία του προβλήματος είναι αξιοσημείωτα. Η αρχή αυτή στηρίζεται στην υπόθεση πως τα στοιχεία που χρησιμοποιήθηκαν στο παρελθόν από παρόμοια cases, αυτά θα είναι εκείνα τα οποία θα λάβουμε υπόψιν στην τρέχουσα συμπερασματολογία.

Ως αρνητικά σημεία στο CBR μπορούμε να αναφέρουμε την πιθανότητα ένας reasoner να οδηγείται στην αποδοχή συγκεκριμένων cases και μόνον «τυφλά», χωρίς να προβαίνει σε ουσιαστική κρίση και επιλογή για αυτά που θα επιλέξει. Μπορεί να μην οδηγείται σε αμερόληπτες συγκρίσεις, αλλά να επηρεαστεί προς συγκεκριμένους τρόπους έκδοσης λύσεων - συγκεκριμένων cases τα οποία και εφαρμόζει.

Αντιστοιχίζοντας τα συστήματα λήψης αποφάσεων σχετικά με τον βαθμό της γνώσης και εμπειρίας που μπορεί να υπάρχει σε κάποιο χώρο προβλημάτων, προκειμένου να εφαρμοστούν, μπορούμε να χαρακτηρίσουμε τα CBR συστήματα ως καταλληλότερα όταν υπάρχει μεγάλη εμπειρία με λιγοστή γνώση. Αντίθετα τα Rule-based συστήματα εφαρμόζονται όταν η γνώση είναι αρκετά μεγάλη ενώ δεν υπάρχει εμπειρία συγκεντρωμένη στο συγκεκριμένο χώρο (Chi 1993). Χαρακτηριστικά αυτό φαίνεται και στον πίνακα που ακολουθεί.

Πίνακας 3. Αντιστοίχηση συστημάτων διαχείρισης γνώσης σε σχέση με την ποσότητα γνώσης και εμπειρίας του χώρου.

Experience		Knowledge	
	Rich	Poor	
Rich	None	Rule - based systems	
Poor	Case - based Systems	Integrated Systems	

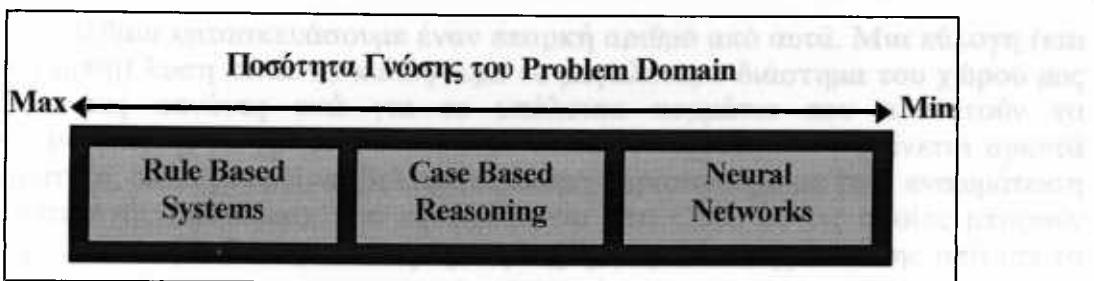
2.12 Δυνατότητες ενοποίησης στο CBR

Οι τεχνικές που στηρίζονται στο CBR αποτελούν ένα μόνο μέρος των πολιτικών - μεθοδολογιών που μπορεί να ακολουθούνται στα πλαίσια ενός οργανισμού. Η αρμονική συνύπαρξη του CBR με αυτές αποτελεί βασικό στοιχείο για την επικράτηση και την ευρεία διάδοσή του.

Η συνύπαρξη αυτή φαίνεται να είναι θεμιτή με τα υπόλοιπα στοιχεία που οργανώνουν ένα επιχειρησιακό περιβάλλον λήψης αποφάσεων, λογισμικό αλλά και ανθρώπινος παράγοντας (Mark 1996). Η αποδοχή και συνύπαρξη με τον ανθρώπινο παράγοντα, τον τρόπο που οι άνθρωποι σκέπτονται, λαμβάνουν αποφάσεις και ενεργούν είναι εξίσου σημαντικό στοιχείο. Πρέπει να υπάρχει κατανοητή και σαφής αντιστοίχηση στο πως ο χρήστης εκφράζει αντικείμενα και τις σχέσεις τους, τα οποία επιθυμεί να εισάγει στο CBR με το πως το CBR μεταφράζει τα αντικείμενα αυτά σε cases, τα δεικτοδοτεί, τα μετατρέπει και τα χρησιμοποιεί. Η παρουσίαση πληροφοριών στον χρήστη, μέσω γραφικών παραστάσεων, διαγραμμάτων, μπορούν να οδηγήσουν στην καλυτέρευση της διεπαφής μεταξύ συστήματος και ανθρώπινου παράγοντα.

Τα συνεχώς αναπτυσσόμενα πληροφοριακά συστήματα των οργανισμών, σε συνδυασμό με την ραγδαία ανάπτυξη των τεχνολογικών δυνατοτήτων αλλά και των πληροφοριών που πρέπει να τύχουν επεξεργασία από αυτά, αυξάνουν τις ανάγκες για αυτοματοποιημένα - έξυπνα - συστήματα, αλλά και τη συνύπαρξη αυτών με τις τεχνικές που ήδη εφαρμόζονται. Τα παραδοσιακά συστήματα βάσεων δεδομένων αντιστοιχούν στο μεγαλύτερο μερίδιο εγκατεστημένων συστημάτων για αποθήκευση και ανάκτηση πληροφοριών σήμερα. Τα συστήματα CBR που εμφανίζονται πρέπει να παρέχουν μια εύρωστη διεπαφή με τα παραδοσιακά, ήδη εγκατεστημένα συστήματα βάσεων δεδομένων που κυριαρχούν, προκειμένου στην ευρεία αποδοχή και εφαρμογή τους ως νέου τρόπου ανάκτησης και επεξεργασίας των πληροφοριών.

Ειδικότερα, το CBR μπορεί να θεωρηθεί οτι έρχεται να καλύψει την διαφορά ανάμεσα στα rule-based συστήματα (που έχουν ως προϋπόθεση την ύπαρξη μεγάλου όγκου δεδομένων για την συμπερασματολογία τους) και στα «knowledge-limited» συστήματα, όπου η ποσότητα της προϋπάρχουσας γνώσης δεν παίζει τόσο σημαντικό ρόλο) όπως τα νευρωνικά δίκτυα (neural networks), τα συστήματα αναγνώρισης υποδειγμάτων (pattern recognition), genetic algorithms, κτλ (Mott 1993).



Εικόνα 21. Ταξινόμηση των Συστημάτων σχετικά με την ποσότητα γνώσης του χώρου προβλημάτων που καλούνται να καλύψουν

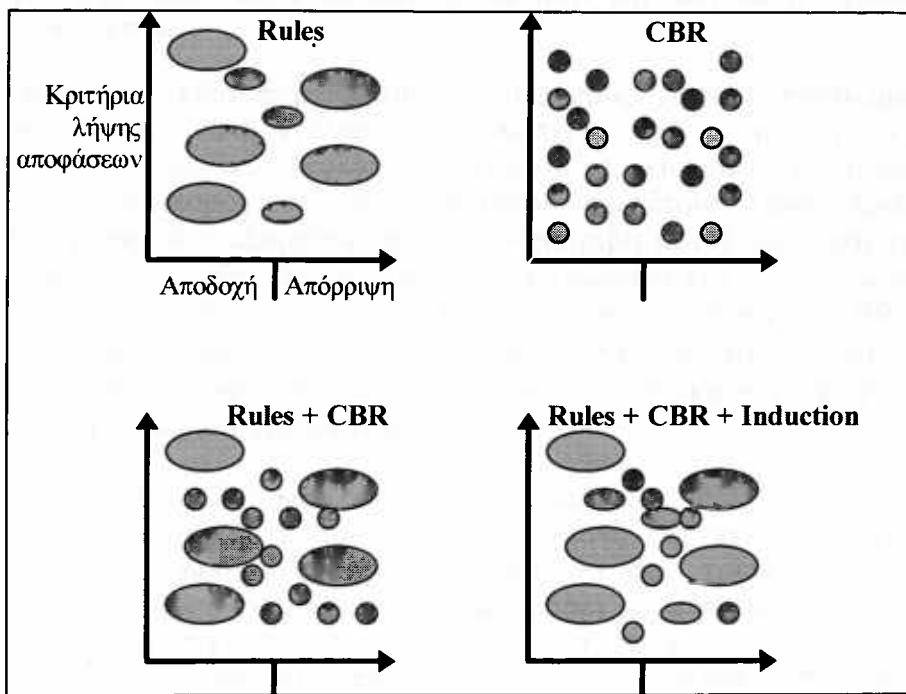
Τα rule-based Συστήματα είναι ικανά να επεξεργαστούν με πολύ αποτελεσματικό τρόπο μεγάλα ποσά γνώσης, σε περιοχές στατικές, όπου είναι πλήρως κατανοητές και μοντελοποιήσιμες. Οι λύσεις που μπορεί να προτείνουν, με αυτές τις προϋποθέσεις, είναι οι βέλτιστες, αλλά πολλές φορές τείνουν να είναι αρκετά στενές και απόλυτες. Η χρησιμοποίηση τεχνικών fuzzy λογικής (Munakata 1994) αποτελεί τη λύση στην οποία εμμένουν αρκετοί ερευνητές για να προσδώσουν περισσότερη ευελιξία στα συστήματα αυτά.

Οι «knowledge limited» τεχνικές, δεν στηρίζονται στην ύπαρξη μεγάλου όγκου μοντελοποιημένης γνώσης. Είναι ικανές να επεξεργάζονται μεγάλο αριθμό ακατέργαστων δεδομένων (raw data), χρησιμοποιώντας τεχνικές εκμάθησης και τρόπους εύρεσης σχέσεων μεταξύ των δεδομένων εισόδου και του ζητούμενου αποτελέσματος. Η δυνατότητα εκμάθησης τους δίνει συγκριτικό πλεονέκτημα σε σχέση με τα rule based συστήματα. Η ικανότητα να επεξεργάζονται ακατέργαστα δεδομένα μπορεί να βοηθήσει στο ξεδιάλεγμά τους και, σε συνδυασμό με ένα σύστημα CBR, με τους εν γένει μηχανισμούς προσδιορισμούς ομοιότητας (similarity assessment), που εφαρμόζει, την επαγωγή και τους μεθόδους δεικτοδότησης και εκμάθησης να αποτελέσουν ιδανική μέθοδο για εύρεση λύσεων σε χώρους προβλημάτων.

Αναφερόμενοι ξανά στα rule-based συστήματα, τα οποία και αποτελούν την πλειοψηφία από τα ήδη εγκατεστημένα knowledge-based συστήματα, οι δυνατότητες ενοποίησης με το CBR έχουν εξεταστεί και υλοποιηθεί σε μερικά συστήματα (Chi 1993, Prince 1994). Τα ενοποιημένα συστήματα μπορούν να καλύψουν ένα πιο ευρύ φάσμα προβλημάτων, εκφράζουν ένα ευρωστότερο τρόπο λήψης αποφάσεων και αιτιολόγησης των αποτελεσμάτων. Στα CBR συστήματα που έχουν χρησιμοποιηθεί κανόνες, αυτοί παίζουν τον ρόλο των πολιτικών, γενικών προδιαγραφών που πρέπει να ικανοποιούν οι λύσεις, ενώ μπορούν να σχετίζονται και με περισσότερο «τεχνικά» θέματα, όπως να λαμβάνουν τελικές αποφάσεις για την αποτελεσματικότητα της λύσης που εκδόθηκε από τον CB Reasoner, να λαμβάνουν υπόψιν επιπλέον πληροφορίες για την τελική προτεινόμενη λύση, κτλ.

Αντιμετωπίζοντας την έννοια της ενοποίησης αυτής γενικά, μπορούμε να πούμε ότι οι κανόνες μπορούν να καλύψουν μεγάλο όγκο, μεγάλα κομμάτια γνώσης, ενώ μπορούν να αντεπεξέλθουν λιγότερο αποδοτικά στις μικρότερες - στενότερες περιοχές του χώρου προβλημάτων, όπως φαίνεται στο παρακάτω σχήμα. Με τη χρήση cases από την άλλη πλευρά μπορούμε να καλύψουμε ολόκληρο των χώρο (problem

domain), εάν βέβαια κατασκευάσουμε έναν επαρκή αριθμό από αυτά. Μια εύλογη (και οικονομικά ορθή) λύση είναι να καλύψουμε το μεγαλύτερο διάστημα του χώρου μας χρησιμοποιώντας κανόνες ενώ για τα υπόλοιπα κομμάτια που αδυνατούν να καλυφθούν με αυτούς, να χρησιμοποιήσουμε cases. Η τεχνική αυτή φαίνεται αρκετά αποτελεσματική, αλλά μπορεί να βελτιωθεί ακόμα περισσότερο με την ενσωμάτωση μεθόδων επαγωγής (induction), που εφαρμόζονται στο CBR, με τις οποίες μπορούν επαγωγικά να καλυφθούν περισσότερες περιοχές, μεγαλύτερης έκτασης από ότι τα cases μόνα τους,



Εικόνα 22. Τρόποι κάλυψης του problem domain και η σχέση τους με τις Knowledge-based τεχνικές

2.13 Προσδοκίες από τον τομέα των CBR συστημάτων

Ο παραδοσιακός τρόπος συμπερασματολογίας της Τεχνητής Νοημοσύνης στηρίζεται στην ύπαρξη συγκεκριμένων τρόπων καθοδήγησης της συμπερασματολογίας, της διαδικασίας πρότασης μιας λύσης (Mark 1996). Αυτοί οι «τελεστέές», με σειρά ελέγχων και χειρισμών καθοδηγούν την διαδικασία λύσης (μέσα από μια σειρά κανόνων) ώσπου η καλύτερη δυνατή λύση να προταθεί. Στη συμπερασματολογία με βάση υποθέσεις (CBR), ανακαλείται από τις δομές μνήμης, τη βάση γνώσης, ένα συγκεκριμένο σύνολο από cases, τα οποία είναι ικανά να παρουσιάσουν κάποιο αποτέλεσμα σε συγκεκριμένα ερεθίσματα, input στο σύστημα. Η ανάγκη ύπαρξης τελεστών - τρόπων αυστηρής καθοδήγησης της συμπερασματολογίας δεν είναι μεγάλη. Έτσι, υπό αυτή την έννοια, το CBR δείχνει να αποτελεί την καλύτερη δύνατη λύση για την επίλυση (συγκεκριμένης, έστω) κατηγορίας προβλημάτων.

Τα συστήματα της TN προδίδουν την επιτυχία τους στην ύπαρξη συγκεκριμένων τρόπων σύνθεσης του αποτελέσματος (της λύσης) από τυποποιημένες διαδικασίες που τα καθιστούν ευέλικτα αλλά και ικανά να αντεπεξέλθουν σε πολλές κατηγορίες προβλημάτων. Το CBR καταφέρνει να είναι ευέλικτο και εύρωστο λόγω της δυνατότητας να αυξάνει αυτόμata τη βάση γνώσης του - τη βιβλιοθήκη με τα cases- αλλά και της ικανότητας να χαράσσει αυτόμata νέα μονοπάτια λύσεων μέσa από τους μεθόδους δεικτοδότησης που εφαρμόζει. Για αυτούς τους λόγους τα CBR συστήματα είναι και εκείνα τα οποία προβλέπονται να δώσουν νέους τρόπους για επίλυση προβληματικών καταστάσεων, μέσa από την αυτόματη προσαρμογή και εκμάθηση νέων λύσεων.

Η γνώση η οποία περιέχεται σε διάφορους χώρους προβλημάτων είναι δύσκολο έως αδύνατο να μοντελοποιηθεί, να περιγραφεί τυπικά, ή δεν μπορεί να παρασταθεί επαρκώς λόγω δυσκολίας κατανόησης και κατάλληλης οργάνωσής της. Τα CBR συστήματα μπορούν να χρησιμοποιηθούν σε τέτοιου είδους προβληματικές περιοχές. Ο reasoner δεν εξαρτάται από την επακριβή μοντελοποίηση της γνώσης, αλλά στη γνώση για το πότε θα πρέπει να ενεργοποιηθεί και να εφαρμόσει τα cases, στηριζόμενος σε παρελθούσα εμπειρία. Ο τρόπος με τον οποίο τα CBR συστήματα εξετάζουν την βάση γνώσης τους και ανακαλούν τα cases στηρίζεται σε εξέταση στοιχείων ομοιότητας (similarity) των cases, που τα κάνει ικανά να χρησιμοποιηθούν σε περιβάλλοντα με μεγάλη αβεβαιότητa.

Και με τα CBR συστήματα απαιτείται ένα αρχικό ξεδιάλεγμα της γνώσης που πρόκειται να χρησιμοποιηθεί για τους μηχανισμούς της συμπερασματολογίας. Η διαφορά με τις παραδοσιακές τεχνικές είναι ότι δεν χρειάζεται η γνώση να μεταφραστεί σε ακριβείς κανόνες, για να μπορέσει το σύστημα να είναι ικανό να προτείνει αποτελεσματικές λύσεις. Αντίθετα, τα cases αποτελούν πιο άμεσο - «φυσικό» - τρόπο παράστασης της γνώσης. Αυτά μπορούν στη συνέχεια να μεταφραστούν, με λιγότερο επώδυνο τρόπο, προκειμένου να γίνουν κατανοητά για επεξεργασία από τα υπολογιστικά συστήματα. Δεδομένου του μεγάλου κόστους δημιουργίας και συντήρησης της βάσης γνώσης μεγάλων συστημάτων, τα οποία στηρίζονται σε κλασσικές μεθόδους, και λόγω ραγδαίας αύξησης της γνώσης σε όλα σχεδόν τα πεδία προβλημάτων με το πέρασμα του χρόνου, τα CBR συστήματα είναι αυτά τα οποία αναμένεται να μειώσουν αισθητά το κόστος ανάπτυξης knowledge - based συστημάτων.

2.14 Συμπεράσματα

Το CBR φαίνεται να κερδίζει συνεχώς έδαφος και αποδοχή στον χώρο της Τεχνητής Νοημοσύνης. Η άποψη πως οι άνθρωποι περισσότερο θυμούνται παρά σκέπτονται, αποτελεί βασικό κορμό πάνω στον οποίο στηρίζει όλη τη φιλοσοφία του το CBR. Θυμόμαστε πράγματα που έχουμε ήδη πράξει, καθώς και τους συλλογισμούς που μας οδήγησαν στις συγκεκριμένες πράξεις, ενώ τις περισσότερες φορές δεν χρειάζεται να σκεφτούμε, απλά να θυμηθούμε τι σκεφτήκαμε παλαιότερα.

Αρκετή συζήτηση έχει γίνει στους κύκλους των μελετητών της Τεχνητής Νοημοσύνης (Riesbeck 1996) σχετικά με το πως πρέπει να οριστεί, ποιες οι θεμελιακές αρχές της και κατά πόσο «νοήμων» οντότητες αποσκοπεί να σχεδιάσσει.

καθώς και η ίδια η έννοια της νοημοσύνης και η συσχέτιση της με οντότητες λογισμικού, προγράμματα. Διαφαίνεται η σκέψη πως τα στόχος της TN και τα μελλοντικά συστήματα τα οποία θα κατασκευαστούν πρέπει να απαρτίζονται από μικρές «έξυπνες» οντότητες, παρά εξολοκλήρου μεγάλα «έξυπνα» προγράμματα. Στόχος δεν είναι η κατασκευή μεγάλων συστημάτων ικανά να πραγματοποιήσουν ότι και οι άνθρωποι μπορούν, αλλά μικρότερων προϊόντων, ευέλικτων, εύρωστων και ικανών να προσαρμόζονται εύκολα σε νέες απαιτήσεις και ανάγκες.

Αυτός είναι ένας λόγος που πολλοί μελετητές θεωρούν ότι η στροφή προς την κατασκευή έξυπνων αυτόνομων agents, ως το επόμενο βήμα της TN αποτελεί λανθασμένη επιλογή. Οι intelligent agents πρέπει να μετακινηθούν από την στρατηγική της δημιουργίας και ελέγχου (generate and test) προς εκείνη της επιλογής και προσαρμογής (select and adapt).

Προς αυτήν την στρατηγική κινούνται τα CBR συστήματα όπως έχουν θεμελιωθεί μέχρι σήμερα. Η προσαρμογή των παλαιότερα εφαρμόσιμων λύσεων και οι διαδικασίες εκμάθησης από την ήδη αποκτηθείσα εμπειρία αποτελεί τη δυσκολότερη λειτουργία των CBR συστημάτων. Τεχνικές οι οποίες έχουν εφαρμοστεί χαρακτηρίζονται από δυσκολία στην υλοποίησή τους. Για να μπορέσουν τα CBR συστήματα να διαδραματίσουν αποτελεσματικό ρόλο και να κερδίσουν ευρεία αποδοχή ως έξυπνες οντότητες σε μεγάλα συστήματα, ειδικό βάρος πρέπει να δοθεί στις τεχνικές προσαρμογής (adaptation) των παλαιότερων cases, στους τρόπους οργάνωσής τους στη μνήμη, καθώς και στους μηχανισμούς δεικτοδότησης και ανάκτησής τους. Αυτό αποτελεί άλλωστε και την κύρια ερευνητική περιοχή στο χώρο της ανάπτυξης αποδοτικών CBR συστημάτων.

3. ΕΝΟΠΟΙΗΣΗ CBR ΤΕΧΝΙΚΩΝ ΣΕ ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

3.1 Εισαγωγή

Σε αυτό το μέρος της εργασίας γίνεται μια προσπάθεια εφαρμογής των CBR τεχνικών στον τομέα των συστημάτων ανίχνευσης εισβολών. Προτείνουμε ένα γενικευμένο σύστημα, που με τη χρήση CBR τεχνικών επιλέγει το καλύτερο σύνολο αντιμέτρων που μπορούν να χρησιμοποιηθούν κάθε φορά, για την αντιμετώπισης της εμφανιζόμενης απειλής. Περιγράφουμε την αρχιτεκτονική του συστήματος, τις μονάδες και διαδικασίες που το συνθέτουν και τέλος γίνεται μια προσπάθεια χρησιμοποίησής του συστήματος σε ένα ήδη υπάρχον IDS.

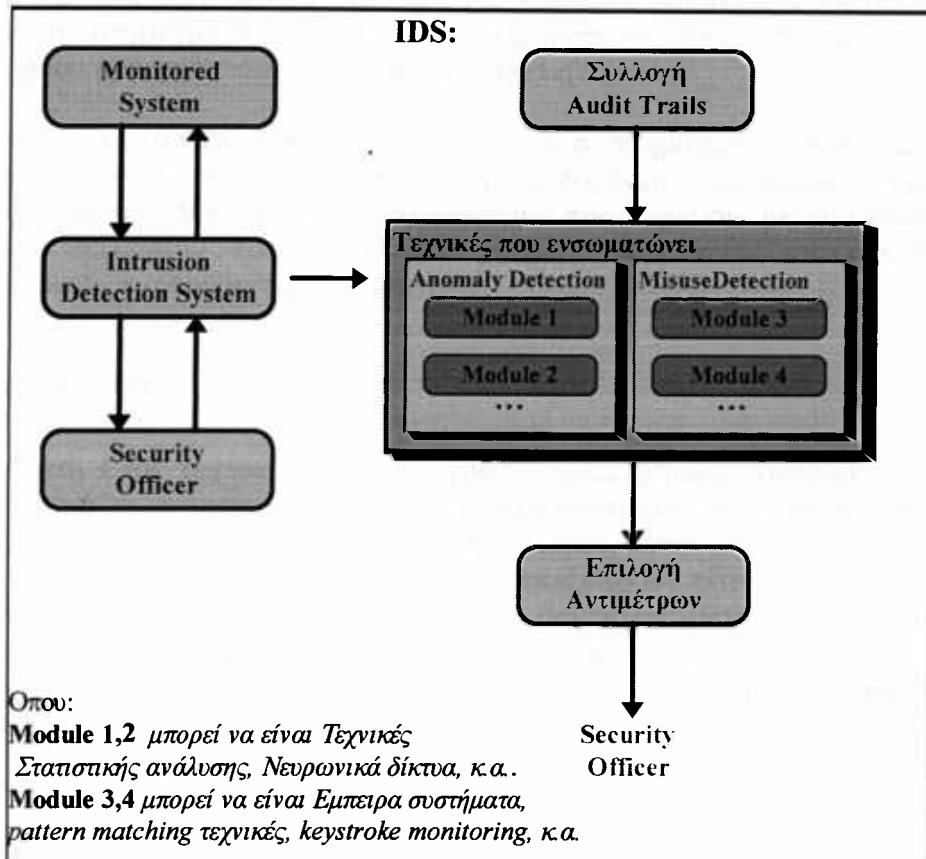
3.2 Περιγραφή του χώρου

Τα συστήματα ανίχνευσης εισβολών αποτελούν ένα μέρος από τις στρατηγικές ασφαλείας που μπορεί να εφαρμόσει ένας οργανισμός στα πλαίσια των πολιτικών ασφαλείας που θέτει. Η ανάγκη για χρησιμοποίηση IDS συστημάτων αυξάνει συνεχώς με την ολοένα αυξανόμενη ανάπτυξη αυτοματοποιημένων συστημάτων επεξεργασίας πληροφοριών από τους οργανισμούς. Η χρήση των δικτύων υπολογιστών αυξάνει συνεχώς. Ο αριθμός των διασυνδεδεμένων υπολογιστών μεγαλώνει όσο και τα άτομα που ασχολούνται με αυτούς. Αυτά καθιστούν την ανάγκη για αποδοτικά IDS ακόμα μεγαλύτερη, μέσα από τη βελτίωση των μηχανισμών τους σε όλες τις φάσεις λειτουργίας τους, από το αρχικό φιλτράρισμα των πληροφοριών έως την τελική απόφαση της επιλογής αντιμέτρων για την αντιμετώπιση της απειλής.

Τα IDS αποτελούν γενικά πολύπλοκα συστήματα τα οποία υλοποιούν λειτουργίες για anomaly detection (εύρεση μη φυσιολογικής, μη προβλέψιμης συμπεριφοράς των χρηστών) και misuse detection (εύρεση στοιχεία στην συμπεριφορά των χρηστών, τα οποία αντιστοιχούν σε ήδη γνωστά σενάρια παρελθουσών απειλών). Τα περισσότερα IDS αποσκοπούν στην εύρεση και των δυο κατηγοριών απειλών μέσα από την υλοποίηση τεχνικών που σχετίζονται με κάθε μια από τις δυο αυτές κατηγορίες. Για την ανακάλυψη anomaly detection, τεχνικές που έχουν χρησιμοποιηθεί είναι τα νευρωνικά δίκτυα, τεχνικές στατιστικής ανάλυσης, μέθοδοι ανακάλυψης των προδιαθέσεων των χρηστών, αυτόνομοι agents, χρήση γράφων, κ.α.. Για την Misuse detection έχουν χρησιμοποιηθεί έμπειρα συστήματα, τεχνικές βασισμένες σε υποδείγματα και μοντέλα παλαιότερων απειλών, κ.α. Εκτενέστερη περιγραφή των τεχνικών αυτών μπορεί να βρει ο αναγνώστης στο πρώτο κεφάλαιο της εργασίας.

Άλλες από τις τεχνικές είναι από παλιά θεμελιωμένες και καλά ορισμένες, ενώ άλλες βρίσκονται σε κάποιο ερευνητικό στάδιο. Όσες έχουν πάντως χρησιμοποιηθεί έχουν δείξει θετικά αποτελέσματα στον τομέα των IDS συστημάτων. Αυτό που πραγματοποιούν είναι το φιλτράρισμα των πληροφοριών, που το σύστημα διατηρεί για τις κινήσεις των χρηστών και εκδίδουν κάποια συμπεράσματα για την πιθανότητα εκδήλωσης απειλής. Δεν εκδίδουν την ύπαρξη της απειλής με βεβαιότητα, αλλά τα

συμπεράσματά τους για τις κινήσεις κάποιου χρήστη εισάγονται σε κάποιο μετέπειτα μέρος του IDS, το οποίο και αποφασίζει αν τελικά η παρατηρούμενη συμπεριφορά είναι απειλή ή όχι. Αυτό με τη σειρά του επιλέγει τα κατάλληλα αντίμετρα για την πάταξη της απειλής, με τη χρήση γνώσης που διατηρεί και με τη διεπαφή του με το διαχειριστή ασφαλείας του συστήματος.



Εικόνα 23. Παράσταση των σημαντικότερων μονάδων σε ένα σύστημα IDS

Το τμήμα λήψης αποφάσεων (ή Decision Module, DM) των συστημάτων αυτών αποτελεί μια από τις κρισιμότερες λειτουργίες των IDS. Πρέπει να είναι αρκετά ευέλικτο, ώστε να μπορεί να αναβαθμιστεί εύκολα με καινούργιες λύσεις σε νέες πιθανές απειλές, να είναι οικονομικό σπαταλώντας λίγους πόρους από το σύστημα και κυρίως να εκδίδει λύσεις οι οποίες θα ελαχιστοποιούν τις false negatives καταστάσεις. Αν κατηγοριοποιεί μια πράξη ως φυσιολογική ενώ αυτή δεν είναι, αποτελεί μεγάλο σφάλμα για την το IDS.

Τα έμπειρα συστήματα, οι στατιστικές τεχνικές και οι περισσότερες από τις τεχνικές που χρησιμοποιούνται για τον αρχικό προσδιορισμό της πιθανότητας ύπαρξης απειλής, έχουν ήδη εφαρμοστεί, ενώ αποτελούνται από προκαθορισμένες διαδικασίες και τρόπους ελέγχου των δεδομένων εισόδου τους, που καθιστούν τις λειτουργίες τους λίγο ως πολύ τυποποιημένες. Το έμπειρο σύστημα θα εκφράσει την πιθανότητα ένας χρήστης να ακολουθεί κάποια ήδη γνωστή συμπεριφορά, το νευρωνικό δίκτυο (πιο πολύπλοκα, αλλά και αυτό) θα μπορέσει να εκφράσει κάποιον βαθμό πιθανότητας σχετικά με τη «φυσιολογικότητα» των κινήσεων των χρηστών. Η

τελική επιλογή όμως έγκειται στο DM να αποφασίσει εάν όντως πραγματοποιείται μια απειλή και ποια είναι τα κατάλληλα αντίμετρα για την αντιμετώπισή της. Η διεπαφή με το διαχειριστή ασφαλείας (security officer, SO) είναι σίγουρα απαραίτητη για την λήψη της τελικής απόφασης, αλλά αυτή η επικοινωνία καλό θα ήταν να είναι η λιγότερη δυνατή μιας και εκ των προτέρων είναι δύσκολη σε ένα real time σύστημα. Η ολοένα και περισσότερη απεμπλοκή του SO από την διαδικασία λήψης απόφασης σχετικά με τα αντίμετρα που πρέπει να εφαρμοστούν, είναι επιθυμητή, λόγω του μεγάλου φόρτου εργασίας που γενικά αντιστοιχεί σε αυτόν.

Η ενσωμάτωση CBR τεχνικών στο DM των συστημάτων ανίχνευσης εισβολών φαίνεται να αποτελεί αποτελεσματική λύση, δεδομένων των πλεονεκτημάτων που αυτές ενσωματώνουν. Μπορούν να εφαρμοστούν προκειμένου, με την εμφάνιση της απειλής, να επιλέγουν το κατάλληλο σύνολο αντιμέτρων τα οποία και θα χρησιμοποιούνται για την αντιμετώπιση της.

3.3 Γιατί χρήση CBR?

Η χρήση CBR τεχνικών, από τα πρώτα μόλις βήματα εφαρμογής τους έχει φανεί να ταιριάζει περισσότερο στην αυτοματοποίηση συστημάτων πρόβλεψης συμπεριφοράς, ανακάλυψης και διόρθωσης λαθών, επανάκτησης (recovery) από προβληματικές καταστάσεις. Μπορούν να αντεπεξέλθουν ικανοποιητικά σε ασαφή, ανακριβή δεδομένα, σε πεδία γνώσης δύσκολα μοντελοποιήσιμα. Η χρήση της ήδη αποκτηθείσας γνώσης - εμπειρίας και η δυνατότητα εκμάθησης για νέους τρόπους λύσεων και χρησιμοποίησής του σε μελλοντικά προβλήματα, βοηθάει τους διαχειριστές γνώσης στην μείωση της αλληλεπίδρασης τους με το σύστημα.

Τα DM των συστημάτων ανίχνευσης εισβολών έχουν να αντιμετωπίσουν συνθήκες οι οποίες τείνουν να επαναλαμβάνονται. Οι λύσεις σε εισβολές μπορούν να επαναχρησιμοποιηθούν μιας και οι ίδιες οι εισβολές μπορεί να ξαναεμφανιστούν. Αυτό που θα συνέβαινε σε μια rule-based προσέγγιση είναι να διασχιζόταν, κάθε φορά που εμφανιζόταν μια παρόμοια συνθήκη, όλο το δένδρο των κανόνων, προκαλώντας άσκοπη κατανάλωση πόρων αλλά και χρονικό κόστος. Με την επαναχρησιμοποίηση των προηγούμενων λύσεων και τη δυνατότητα εκμάθησης νέων, το CBR θα μπορούσε να παίξει ουσιαστικό ρόλο στην μείωση των χρόνων απόκρισης σπαταλώντας λιγότερους πόρους του συστήματος.

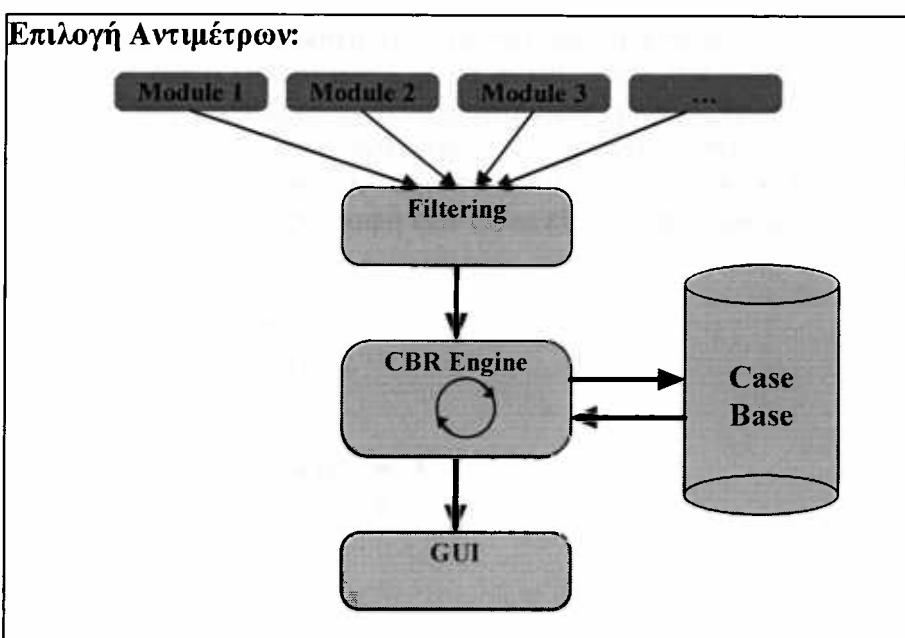
Το CBR μπορεί να μάθει. Αυτό έχει ως συνέπεια με την εμφάνιση μιας καινούργιας συνθήκης, όπου υπάρχει δυσκολία απόφασης στην ύπαρξη η όχι απειλής, με την αλληλεπίδραση με τον SO, το σύστημα να δημιουργήσει νέα cases, τα οποία να ενσωματώσει στη βάση γνώσης του και να τα χρησιμοποιήσει σε μελλοντικές εμφανίσεις παρόμοιων απειλών.

Το CBR έχει τη δυνατότητα να εκδίδει πάντα μια λύση, ακόμα και αν αυτή δεν φαίνεται να είναι η βέλτιστη. Με την προσαρμογή των ήδη γνωστών cases, μπορεί να αποφασίσει σχετικά αμερόληπτα για τις λύσεις που θα προτείνει για την αντιμετώπιση της απειλής. Αντίθετα, με τη χρήση μιας rule-based μεθοδολογίας, μπορεί να μην προτεινόταν ποτέ σύνολο αντιμέτρων, αν τύγχανε να μην ικανοποιούνταν συγκεκριμένες υποθέσεις για την εκτέλεση μιας σειράς κανόνων.

Η γνώση που ήδη διαχειρίζεται το DM για την λήψη των αποφάσεων, μπορεί να δομηθεί με cases πιο εύκολα και αποτελεσματικά. Αλλά και ο τρόπος που συμπερασματολογεί, προσεγγίζει περισσότερο την φιλοσοφία των cases, τα οποία κωδικοποιούν στιγμιότυπα γνώσης συνοπτικά και οργανωμένα.

3.4 Αρχιτεκτονική του Συστήματος

Το σύστημα δέχεται ως είσοδο τα αποτελέσματα που εκδίδονται από τα modules του IDS που πραγματοποιούν το anomaly και misuse Detection. Τα αποτελέσματα αυτά περνούν από μια διαδικασία φιλτραρίσματος. Μετατρέπονται σε μορφή κατανοητή από το επόμενο τμήμα, το CBR engine, όπως φαίνεται από το σχήμα που ακολουθεί.



Εικόνα 24. Αρχιτεκτονική του νέου συστήματος

Το CBR Engine είναι υπεύθυνο για τη συμπερασματολογία σχετικά με το ποια από τα αντίμετρα θα εφαρμοστούν, συγκρίνοντας τα νέα cases, όπως αυτά εισέρχονται από τη διαδικασία φιλτραρίσματος, με εκείνα που βρίσκονται αποθηκευμένα στην Case Base.

Αναλαμβάνει τις διαδικασίες αναγνώρισης των σημαντικών χαρακτηριστικών (features) των cases που εισέρχονται για την δεικτοδότησή τους, με βάση κάποιο λεξικό όρων, χρήσιμο για τον προσδιορισμό των πιο σημαντικών χαρακτηριστικών. Μετά τον χαρακτηρισμό του νέου case, αναζητεί από την Case Base, με βάση τεχνικές μέτρησης της ομοιότητας των χαρακτηριστικών των cases, τα πλησιέστερα, τα οποία και θα χρησιμοποιήσει ως λύση για την αντιμετώπιση της απειλής. Τα cases που προκύπτουν από την αναζήτηση αυτή συγκρίνονται με το αρχικό, προκειμένου να προσδιοριστούν ομοιότητες και το περισσότερο όμοιο case κρατείται για

χρησιμοποίησή του ως λύση. Όσως είναι αναγκαία η τροποποίηση του επιλεγμένου case για να ταιριάζει ακριβώς στο νέο. Το ανακτημένο case αλλάζει προκειμένου να ταιριάζει στην νέα απειλή και είναι αυτό που τελικά θα επιλεγεί ως λύση. Προηγείται μια διαδικασία ελέγχου της νέας αυτής λύσης προκειμένου να διαπιστωθεί η αποτελεσματικότητά της στην αντιμετώπιση της απειλής. Ο έλεγχος αυτός μπορεί να αναφέρεται σε προσομοίωση του συστήματος με τη νέα λύση, από την οποία αντλούμε συμπεράσματα για την ορθότητά της, όταν αυτή θα εφαρμοστεί, σε επιθεώρηση από τον διαχειριστή ασφαλείας σχετικά την πιθανότητα επιτυχίας της.

Αν το νέο case εγκριθεί για την εφαρμογή του, μπορεί να δεικτοδοτηθεί και να αποθηκευθεί στην Case Base. Στην περίπτωση που αποτύχει να εφαρμοστεί, αποθηκεύονται στην Case Base οι λόγοι για την αποτυχία της λύσης, προκειμένου να ληφθούν υπόψιν σε μελλοντικές προσπάθειες επίλυσης, για να μην υποπέσει στα ίδια λάθη το σύστημα (learning from failures (Schank 1991)).

Η Case Base αποτελεί τη βάση γνώσης την οποία χρησιμοποιεί το CBR Engine για την επίλογή των κατάλληλων κάθε φορά αντιμέτρων. Τα cases - αντίμετρα είναι δεικτοδοτημένα έτσι ώστε να επιτυγχάνεται γρήγορη εύρεση, τροποποίηση αλλά και τοποθέτηση νέων όταν κρίνεται αναγκαίο. Καλή σχεδιαστική επίλογή είναι η οργάνωσή της με δενδρική δομή, αξιοποιώντας τα πλεονεκτήματα που αυτή προσφέρει. Μια γενικευμένη περιγραφή των cases είναι η παρακάτω:

```

Case name_1 is
    variable_1 = content_1
    variable_2 = content_2
    ...
    ...
solution is
    variable_s_1 = content_s_1
    variable_s_2 = content_s_2
    ...
    ...
end;

Case name_2 is
    variable_1 = content_1
    variable_2 = content_2
    ...
    ...
solution is
    variable_s_1 = content_s_1
    variable_s_2 = content_s_2
    ...
    ...
end;

```

Σε κάθε ένα από τα πεδία - μεταβλητές του case, αντιστοιχεί ένα βάρος (weight). Με τα βάρη υπολογίζεται η ομοιότητα των cases με το νεοεμφανιζόμενο και επιλέγονται εκείνα που η συνολικός βαθμός ομοιότητας είναι μεγαλύτερος.

Τέλος ο διαχειριστής ασφαλείας πρέπει να έχει τη δυνατότητα, μέσω μιας εύχρηστης γραφικής διεπαφής (GUI - Graphical User Interface) να παρακολουθεί την λειτουργία του συστήματος. Με αυτήν θα μπορεί να ελέγχει το περιεχόμενο των

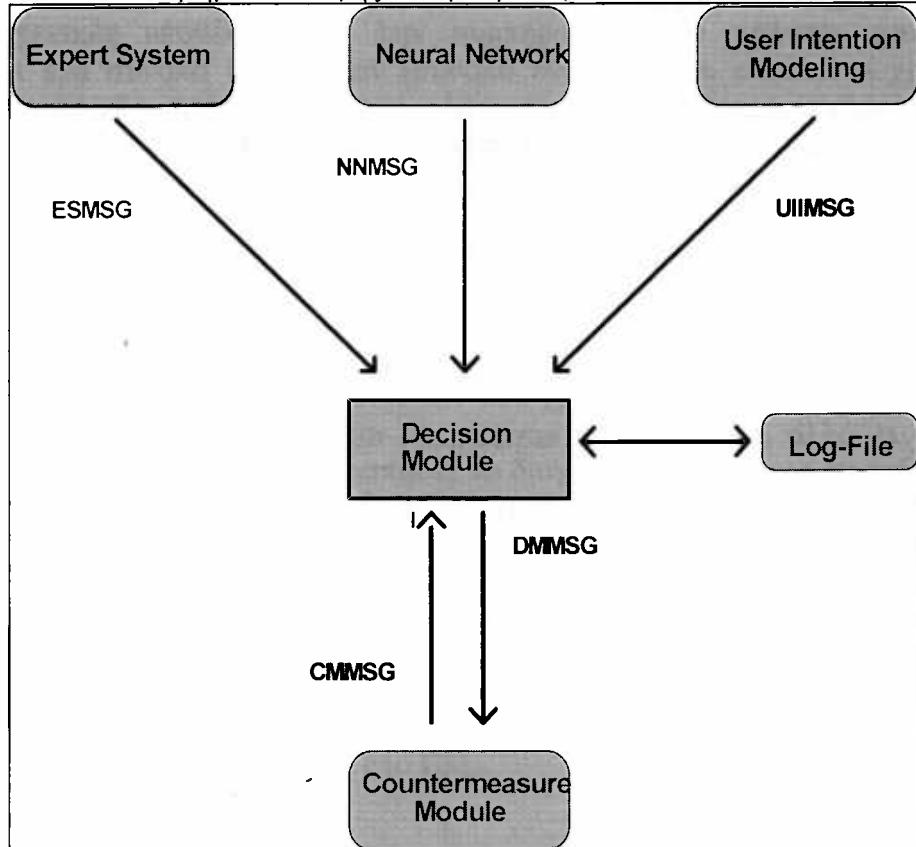
αντιμέτρων που εκδίδονται, να ελέγχει τις λύσεις πριν αυτές υλοποιηθούν, να δημιουργεί νέα cases, να τροποποιεί γενικά την Case Base, καθώς και να αντλεί στατιστικές πληροφορίες για την λειτουργία του συστήματος.

3.5 Περιγραφή υπάρχοντος IDS

Θα γίνει μια προσπάθεια ενσωμάτωσης του συστήματος που προτείνουμε σε ένα ήδη υπάρχον σύστημα ανίχνευσης εισβολών. Θα επιλέξουμε το SECURENET, το οποίο κάνει την διάκριση στο Decision Module μέρος και εκείνου της επιλογής των αντιμέτρων, αποτελεί καινούριο σύστημα, ενσωματώνοντας πολλές νεότερες τεχνικές (πχ. νευρωνικά δίκτυα, τεχνικές προσδιορισμού προδιαθέσεων των χρηστών, κ.α.). Θα περιγράψουμε τις διαδικασίες του SECURENET τις οποίες θα διατηρήσουμε και στο νέο μέρος με την χρήση CBR, εκείνες που θα παραλείψουμε καθώς και μια γενική περιγραφή του συστήματος με έμφαση τα τμήματα των Decision Module και Countermeasures Module.

3.5.1 Περιγραφή Decision Module στο Securennet

Ο κύριος ρόλος του DM στο SECURENET είναι η λήψη της τελικής απόφασης σχετικά με το αν πραγματοποιείται απειλή. Επικοινωνεί με τέσσερα μέρη, το Έμπειρο σύστημα, το Νευρωνικό δίκτυο, το τμήμα με τις τεχνικές προσδιορισμού προδιαθέσεων και το τμήμα επιλογής αντιμέτρων (countermeasure Module, CM).



Εικόνα 25. Η επικοινωνία των οντοτήτων του SECURENET με το σύστημα λήψης αποφάσεων

Το DM αρχίζει να λειτουργεί όταν τουλάχιστον κάποια από τα προηγούμενα τμήματα εκδώσει μήνυμα. Τα μηνύματα αυτά έχουν την ίδια μορφή και για τις τρεις μονάδες.

Πίνακας 4. Μήνυμα από ES, NN, UII προς το DM.

Πεδίο	Περιγραφή
System_id	Το σύστημα που εκδίδει το μήνυμα: ES ή NN ή UII
Node_id	Ο κόμβος στον οποίο πραγματοποιείται πιθανή εισβολή
Time	Ο χρόνος στον οποίο εμφανίζεται η απειλή
Record_id	Αριθμός σειράς που προσδιορίζει το μήνυμα
User_id	Προσδιοριστής του χρήστη
Hypothesis_type	Τύπος υπόθεσης
Level_of_conf	Επίπεδο εμπιστοσύνης
Level_penet	Βαθμός επικινδυνότητας της επίθεσης από τον εισβολέα
Param_number	Αριθμός επιπλέον παραμέτρων
Params	Παράμετροι

Τα σπουδαιότερα από τα πεδία αυτά είναι το **hypothesis_type**, το οποίο περιέχει γενικές υποθέσεις για την συμπεριφορά του χρήστη, **params**, που περιγράφει ένα σύνολο εκφράσεων (σύνολο εντολών που εκτελεί ο χρήστης και «περίεργων» συνδυασμών τους) που οδήγησαν το αντίστοιχο module να εκδώσει alarm και **level_of_confidence**, που αντιστοιχεί ένα βαθμό εμπιστοσύνης από 0 έως 9 στην παραπάνω υπόθεση. Η βαθμολόγηση με 0 σημαίνει ότι δεν υπάρχει εμπιστοσύνη, ενώ το 9 υποδηλώνει ότι υπάρχει εμπιστοσύνη στην παραπάνω υπόθεση. Ο ρόλος του DM είναι ουσιαστικά να επιβεβαιώσει (αύξηση του πεδίου εμπιστοσύνης) ή να απορρίψει (μείωση του πεδίου εμπιστοσύνης) της υπόθεσης, όπως αυτή έχει παρουσιαστεί.

Εάν από την εξέταση των εντολών του χρήστη, μέσα από το πεδίο **params**, διαπιστωθεί ότι ο χρήστης κινείται «περίεργα» στο σύστημα, αλλάζει δικαιώματα αρχείων που δεν του ανήκουν, προσπαθεί να διαγράψει αρχεία του συστήματος, κτλ, το DM διατηρεί το επίπεδο εμπιστοσύνης για την υπόθεση στο ίδιο επίπεδο ή το ανεβάζει. Εάν εκδοθούν δυο ή περισσότερα alarms στην ίδια χρονική στιγμή, τότε το μεγαλύτερο επίπεδο εμπιστοσύνης είναι εκείνο το οποίο θα χρησιμοποιηθεί και θα σταλεί στον διαχειριστή ασφαλείας και στο CM.

Το output που εκδίδει το DM είναι επίσης τυποποιημένο. Παρακάτω διακρίνονται μερικά από τα σπουδαιότερα πεδία του. Το αποτέλεσμα αυτό εκδίδεται και στο διαχειριστή ασφαλείας και στο CM.

Πίνακας 5. Μήνυμα από το DM στο CM

Πεδίο	Περιγραφή
System_id	Το σύστημα που εκδίδει το μήνυμα
Node_id	Ο κόμβος στον οποίο πραγματοποιείται πιθανή εισβολή
Time	Ο χρόνος στον οποίο εμφανίζεται η απειλή
Record_id	Αριθμός σειράς που προσδιορίζει το μήνυμα
User_id	Προσδιοριστής του χρήστη
Level_of_conf	Επίπεδο εμπιστοσύνης
Level_penet	Βαθμός επικινδυνότητας της επίθεσης από τον εισβολέα
Attack_classes	Κατηγοριοποίηση της απειλής

Τα σημαντικότερα πεδία είναι το **level_of_confidence** και το **attack_classes**, το οποίο δίνει πληροφορία στον SO και στο CM σχετικά με το τι είδος απειλής είναι αυτή που εκδηλώνεται.

Το πεδίο **attack_classes** αντιστοιχίζεται με τιμές όπως φαίνεται στον παρακάτω πίνακα:

Πίνακας 6. Attack Classes.

Attack_class	Συμπτώματα
No attack	Used only by the DM for the report and a log file
Trojan Horse	Unexpected file operations, inappropriate source code, unexpected communications
Logic Bomb	Inappropriate source code, operations on sensitive resources
Insider Attack	User operates outside user model threshold, operations on sensitive resources, inappropriate creation and manipulation of data instances
Password Cracking	Repeated failed attempts to establish another identity, operations on passwd file
System Programming Attacks	Attempt to exploit known weaknesses in a system routine
Outsider Access Violation	Repeated failed access to establish ana identity; attempts to use default system passwords
Denial of Service	Unexpected loss of contact with victim system, large amounts of meaningless traffic jamming available bandwidth
Trapdoor Attack	Inappropriate source code, operations on sensitive resources

3.5.2 Παράδειγμα σεναρίου εισβολής

Υποθέτουμε ότι ένας χρήστης αντιγράφει το αρχείο **/bin/sh** στην δική του περιοχή και στη συνέχεια αλλάζει τα δικαιώματα του αρχείου έτσι ώστε να έχει *sgid* και *suid 0*. Οι εντολές που ο χρήστης εκτελεί είναι:

```
system% cp /bin/sh <file_name>
system% chmod ug+xs <file_name>
```

Οι κινήσεις του χρήστη καταγράφονται στα audit trails που διατηρεί το σύστημα. Με την εξέτασή τους από το émpeiro σύστημα (για παράδειγμα), ενεργοποιούνται ορισμένοι κανόνες με τους οποίους συμπεραίνεται ότι μάλλον πρόκειται για εκδήλωση εισβολής και συγκεκριμένα για πιθανό δούρειο íππο. Ένας κανόνας αντιλαμβάνεται την κλήση «**open**» με παράμετρο το αρχείο «**/bin/sh**», ένας άλλος διαπιστώνει την κλήση «**create**» για το αρχείο **<file_name>** με το ίδιο pid με την «**open**» (μιας και πρόκειται για εκτέλεση της εντολής «**cp /bin/sh <file_name>**»), ενώ ένας τρίτος κανόνας διαπιστώνει την εκτέλεση της εντολής «**chmod**» με παράμετρο το αρχείο **<file_name>**.

Το émpeiro σύστημα δημιουργεί ένα alert το οποίο στέλνει στο DM προκείμενου να λάβει την τελική απόφαση για την πραγματοποίηση ή όχι απειλής. Το μήνυμα προς το DM είναι το παρακάτω, με συμπληρωμένα τα σπουδαιότερα από τα πεδία του.

Πίνακας 7. Μήνυμα από το ES στο DM.

Πεδίο	Περιγραφή
System_id	ES
Node_id	
Time	
Record_id	
User_id	202
Hypothesis_type	610010
Level_of_conf	9
level_penet	9
param_number	5
params	R10010c:Trojan_horse_has_been_prepared User=202 File=/users/evil/mybinsh/ Owner=evil Group=other

Το DM λαμβάνοντας υπόψιν την υπόθεση με αριθμό 610010 την οποία έχει προσδώσει το ES, αντιστοιχεί στην παράμετρο **attack_classes** την τμή: «Insider Attack, System Programming Attach, Trojan Horse». Δεδομένης της μεγάλης εμπιστοσύνης που δείχνει το ES για πιθανή εισβολή, το DM στέλνει μήνυμα και στο

CM και στον διαχειριστή του συστήματος, για την εκδήλωση πιθανής εισβολής, παραθέτοντας πληροφορίες για το χρήστη και τις κινήσεις του στο σύστημα (**params**). Η απόφαση στην οποία καταλήγει το DM είναι οτι πραγματοποιείτε εισβολή με μεγάλο επίπεδο εμπιστοσύνης - βεβαιώτητας της μορφής «Insider Attack, System Programming Attach, Trojan Horse», με μεγάλο βαθμό επικινδυνότητας και η οποία καταγράφεται σε ένα log-file για μελλοντική αναφορά. Εαν το DM διακρίνει οτι δεν υπάρχει εκδήλωση απειλής, τότε δεν προχωράει στην αποστολή μηνύματος στο CM, αλλά σταματάει τη διαδικασία. Το μήνυμα προς το CM έχει την παρακάτω μορφή (τα σημαντικότερα από τα πεδία του):

Πίνακας 8. Μήνυμα από το DM στο CM.

Πεδίο	Περιγραφή
System_id	Solaris2.5.1
Node_id	193.92.123.18
Time	080995132500
Record_id	12345
User_id	202
Level_of_conf	9
Level_penet	6
Attack_class	64

Στόχος του CM είναι να παράγει μια λίστα από προτεινόμενα αντίμετρα και μια μικρή περιγραφή τους σχετικά με το κάθε αντίμετρο, βασισμένο στις πληροφορίες που αναγράφονται στο μήνυμα που έλαβε από το DM, και κυρίως από την κατηγοριοποίηση της απειλής, την επικινδυνότητα της εισβολής και το παρελθόν του χρήστη.

Το μήνυμα το οποίο στέλνεται από το CM στον SO είναι της παρακάτω μορφής:

Πίνακας 9. Μήνυμα από το CM προς τον SO

Πεδίο	Περιγραφή
System_id	Solaris2.5.1
Node_id	193.92.123.18
Time	080995132500
Record_id	12345
User_id	202
Countermeasure_no	5
cm_description	Με αυτό το αντίμετρο ο χρήστης θα ερωτηθεί για το συνθηματικό του. Αν δεν δοθεί σωστή απάντηση έως και την Τρίτη φορά, ο χρήστης φεύγει αναγκαστικά (log out) από το σύστημα «Ρώτα το χρήστη για το Password που έχει»
cm_subject	

Μετά την αναφορά στον SO των αντιμέτρων αυτός μπορεί να επιλέξει κάποια για την καταστολή της, να αγνοήσει την απειλή ή και να αναζητήσει διαφορετικό σύνολο αντιμέτρων. Στην περίπτωση επιλογής κάποιου αντιμέτρου από τον SO, αυτό

στέλνεται στο CM, το οποίο με τη σειρά του δίνει οδηγίες στους agents οι οποίοι αναλαμβάνουν να υλοποιήσουν τις τελικές ενέργειες για την καταστολή της απειλής.

Το CM αντλεί στοιχεία από δύο πίνακες. Ο πρώτος αντιστοιχεί τις απειλές σχετικά με την επικινδυνότητά τους και τις κινήσεις που πρέπει να κάνει ο διαχειριστής ασφαλείας. Κάθε αντίμετρο αναλογεί σε αντίστοιχης επικινδυνότητας απειλή και πάίρνει τιμή από 0 - 10. Μια τιμή από 1 - 4 σημαίνει ότι ένας χρήστης έχει διαπιστώσει παρεμβάσεις, ενοχλήσεις και διαφοροποιήσεις στη συνήθη καθημερινή εργασία του. Από 5 - 9 σημαίνει ότι οι παρεμβάσεις αυτές γίνονται αντιληπτές από μια ομάδα χρηστών, ενώ η τιμή 10 αντιστοιχεί στον μεγαλύτερο βαθμό στον οποίο το σύστημα πρέπει να κλείσει

Ενας δεύτερος πίνακας αντιστοιχεί σε υποδείξεις που κάνει το CM προς τον SO για ανάληψη συγκεκριμένων αντιμέτρων:

Πίνακας 10. Κατάλογος αντιμέτρων

Αριθμός	Αντίμετρο
1	Alert the System manager
2	Grab a snapshot of the process table
3	Tune the level of auditing security
4	Ask the user for their password (X Window Version)
5	Ask the user for their password (TTY Version)
6	Kill a process or a parent of a process
7	Log out a user
8	Suspend a user's login account
9	Restrict access to a service NIS
10	Restrict access to a service cron
11	Restrict access to a service mail
12	Restrict access to a service route
13	Restrict access to a node
14	Shutdown service NIS
15	Shutdown service cron
16	Shutdown service mail
17	Shutdown service route
18	Put a node into emergency mode
19	Shutdown a node

3.5.3 Δυνατότητες βελτίωσης

Το μέρος του SECURENET το οποίο αποφασίζει για τη λήψη η όχι αντιμέτρων και ποιών για την καταστολή πιθανής απειλής χαρακτηρίζεται από στατικότητα σε πολλά σημεία της λειτουργίας του. Αρχικά η βάση γνώσης (περιεχόμενα των αντιμέτρων, κατηγοριοποίηση των απειλών, κτλ), δεν έχει την δυνατότητα αλλαγής. Η διαχειριστής ασφαλείας έχει τη δυνατότητα είτε να απορρίψει τα προτεινόμενα αντίμετρα, υιοθετώντας κάποιο δικό του, το οποίο δεν αναφέρεται στη βάση, είτε να

επιλέξει κάποιο από αυτά που το CM του προτείνει. Ήταν χρήσιμο, προτείνοντας κάποιο νέο αντίμετρο ο διαχειριστής ασφαλείας, το σύστημα να μπορεί να διατηρήσει τη λύση, να την αποθηκεύσει στην βάση γνώσης και να την εφαρμόσει αργότερα στην περίπτωση εμφάνισης της ίδιας ή παρόμοιας απειλής.

Με τι υπάρχουντες τεχνικές, ο διαχειριστής ασφαλείας ενημερώνεται και ερωτάται πάντα για την εμφάνιση απειλής από την πιο καταστροφική έως και την πιο μικρή. Είναι άσκοπο να ενοχλείται συνεχώς ο διαχειριστής ασφαλείας για την έγκριση ή και επιλογή των αντιμέτρων που μπορούν να εφαρμοστούν, ειδικά όταν πρόκειται για μια απειλή η οποία έχει εμφανιστεί πολλές φορές στο παρελθόν, και οι τρόποι αντιμετώπισης της έχουν γίνει λίγο ως πολύ τυποποιημένοι. Επιπλέον είναι αδύνατο να βρίσκεται ο διαχειριστής πάντα διαθέσιμος για να παρακολουθεί την πορεία του συστήματος, μιας και οι εισβολείς μπορούν να επέμβουν στο σύστημα διάφορες ώρες της ημέρας (και τη νύχτα).

Το DM σε ένα σύστημα αντιμετώπισης εισβολών μπορεί να παίξει αποτελεσματικό ρόλο στην μείωση των false negatives λαθών, που αποτελεί και τον κριτιμότερο ίσως παράγοντα επιτυχίας των IDS συστημάτων. Παρόλο που τα προηγούμενα τμήματα εκδίδουν, μέσω των αρκετά επιτυχημένων μηχανισμών που ενσωματώνουν την πιθανότητα έκδοσης απειλής, εκφράζοντας κάποια υπόθεση για τη διενέργεια της και αντιστοιχίζοντας την με συγκεκριμένο επίπεδο εμπιστοσύνης, το DM δεν συμπερασματολογεί ουσιαστικά, για την απόφαση αν όντως πρόκειται ή όχι για απειλή. Ενημερώνεται από τη βάση σχετικά με το περιεχόμενο της υπόθεσης, που έχουν εκφράσει τα προηγούμενα επίπεδα, ελέγχει κρίσιμες παραμέτρους και απλά αντιστοιχεί στην απειλή έναν τίτλο (αν πρόκειται για insider attack, password cracking, Trojan horse, κτλ.). Αυτό που πρέπει να υλοποιεί είναι επιπλέον λειτουργίες, να ελέγχει περισσότερες παραμέτρους σχετιζόμενες με ιστορικά στοιχεία ή και να επικοινωνεί άμεσα με τον διαχειριστή ασφαλείας ζητώντας να εκφράσει την άποψή του για την πιθανότητα διενέργειας απειλής. Η κρίσιμη επεξεργασία πραγματοποιείται από άλλο τμήμα, το CM, το οποίο ούτε αυτό έχει τη δυνατότητα να αφομοιώνει νέες λύσεις και πρακτικές κατά την αντιμετώπιση απειλών.

Είναι χρήσιμη η ενσωμάτωση τεχνικών με τις οποίες, το υποσύστημα επιλογής της τελικής απόφασης για την πραγματοποίηση ή όχι απειλής και των αντιμέτρων προς αυτήν, να μπορεί να είναι περισσότερο ευέλικτο και αποτελεσματικό. Αυτό μπορεί να επιτευχθεί με ενοποίηση μηχανισμών εκμάθησης, με τη διεπαφή με τον διαχειριστή για νέους τρόπους λύσεων σε νέες απειλές, με περισσότερη αυτονομία και ανεξαρτησία από τον διαχειριστή, εκτός και αν αυτό κρίνεται αναγκαίο. Αναγκαίες είναι δυνατότητες συμπερασματολογίας με βάση την ήδη αποκτηθείσα γνώση για επίλυση παλαιότερων απειλών, τροποποίησης των υπαρχόντων αντιμέτρων για να ταιριάζουν στις νέες ανάγκες και προκλήσεις.

Με τις παραπάνω ιδιότητες, το σύστημα θα έχει την ικανότητα να ελαχιστοποιεί τα false negative λάθη. Ήταν μπορεί εκδίδει σήματα κινδύνου όταν πρέπει και θα υλοποιεί αντίμετρα μόνο όταν πραγματοποιείται απειλή. Επίσης καθίσταται ικανή η μεταφορά του για λειτουργία και σε άλλα συστήματα, αφού διατηρεί ευελιξία και αυτονομία.

3.6 Εφαρμογή του προτεινόμενου συστήματος στο SECURENET

Γίνεται προσπάθεια ενοποίησης των CBR τεχνικών στο SECURENET. Θα διατηρηθεί η υπάρχουσα δομή του, έως και το σημείο όπου εκδίδονται τα μηνύματα από τα ES, NN, και UII στο DM. Το DM θα ενοποιηθεί με το υπάρχον CM, αποτελώντας ένα νέο module το οποίο θα συμπερασματολογεί με χρήση cases. Τα cases θα περιέχουν τα αντίμετρα τα οποία θα εφαρμόζονται για την αντιμετώπιση των πιθανών απειλών, όπως αυτές περιγράφονται από τις προηγούμενες ενότητες (ES, NN, UII). Η δομή της βάσης γνώσης του SECURENET θα διατηρηθεί στο μέγιστο δυνατό βαθμό. Επιπλέον θα έχει τη δυνατότητα να αυξάνεται δυναμικά, καταργώντας τη στατικότητα της υπάρχουσας βάσης γνώσης του συστήματος, να ενημερώνεται για νέους τρόπους αντιμετώπισης απειλών, καθιστώντας το περισσότερο ευέλικτο και αποδοτικό.

3.6.1 Οργάνωση της βάσης γνώσης

Τα μηνύματα που προέρχονται από τα ES, NN, και UII, θα εισέρχονται στην οντότητα Filtering στην οποία θα υφίστανται κάποιου είδους «ξεδιάλεγμα». Η οντότητα αυτή κρίθηκε αναγκαία, για την διατήρηση της συμβατότητας με τις διαδικασίες του SECURENET. Το υποσύστημα αυτό θα μετατρέπει τα μηνύματα σε source cases, τα οποία θα τροφοδοτούν τους μηχανισμούς CBR για την αναζήτηση παρόμοιων στη βάση γνώσης. Από το φιλτράρισμα αυτό το case που προκύπτει είναι το ακόλουθο.

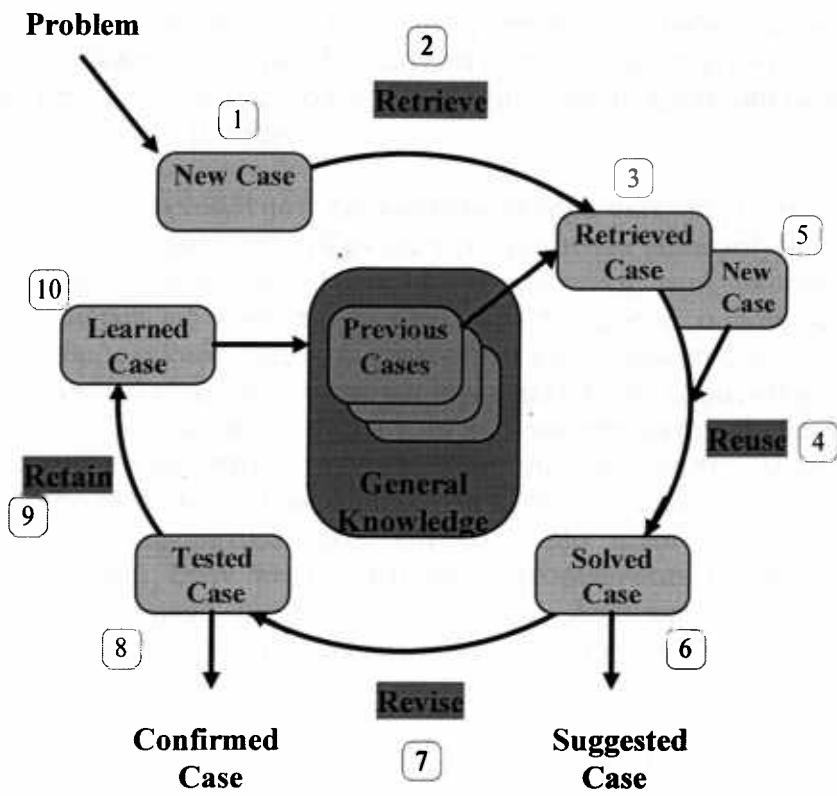
```
Case case_name is
    System_Id
    User_Id
    Node_Id
    Time
    Hypothesis_Type
    level_of_Confidence
    Level_of_Penet
    params
    Num_Params
```

```
Solution is
    User_Id
    Node_Id
    Time
    Attack_Class
    Level_of_Confidence
    Level_of_Penet
    Cm_Description
    Cm_Subject
```

End

Η επεξήγηση των πεδίων είναι αντίστοιχη με τις περιγραφές που έχουν αναφερθεί στους παραπάνω πίνακες. Μερικά πεδία δεν περιέχονται στο case όπως **Record_Id**, ο οποίος δεν έχει νόημα ύπαρξης μιας και το σύστημα διαχείρισης της βάσης γνώσης αλλάζει, δεν περιέχει εγγραφές αλλά cases. Το πρώτο μέρος του case περιγράφει την πιθανή απειλή, όπως αυτή καταγράφηκε από το σύστημα (**System_Id**), η οποία προκλήθηκε την χρονική στυγμή **Time** από τον χρήστη **User_Id**, ο οποίος επενεργούσε στον κόμβο **Node_Id** του δικτύου. Στις κινήσεις (**params**) του (**num_params** σε αριθμό) το σύστημα **System_Id** αντιστοιχεί επίπεδο εμπιστοσύνης **Level_of_Confidence** στην υπόθεση **Hypothesis_Type** που θεώρησε σχετικά με τις διαθέσεις του χρήστη, οι οποίες έχουν οδηγήσει σε βαθμό επικινδυνότητας **Level_of_Penet**.

Οι τιμές στις παραπάνω μεταβλητές είναι αρκετές για να περιγράψει κανείς την πιθανότητα εκδήλωσης εισβολής και την σημαντικότητά της, με την αντιστοίχηση αυτής ενός βαθμού επικινδυνότητας. Το δεύτερο μέρος του case αποτελεί την αντίδραση του IDS στην πιθανή αυτή απειλή. Με την εμφάνιση του νέου case (1), το CBR υποσύστημα «ξεδιαλέγει» τα σημαντικότερα από τα χαρακτηριστικά του (indexing features - keywords), μετατρέποντάς το σε συγκρίσιμη μορφή με τα ήδη υπάρχοντα (2). Το αποτέλεσμα της αναζήτησης, (3) θα αποτελέσει μια πρώτη λύση στην διαδικασία εύρεσης του αντιμέτρου. Αν περισσότερα από ένα βρεθούν να ταιριάζουν με την περιγραφή του αρχικού case, επιλέγεται αυτό με την μεγαλύτερη ομοιότητα. Στη συνέχεια, το επιλεγμένο case θα υποστεί μια διαδικασία μετασχηματισμού (4), προκειμένου να αντιμετωπίζει περισσότερο αποτελεσματικά, με καλύτερο σύνολο αντιμέτρων, την εισβολή. Αν δεν ταιριάζει κανένα από τα ήδη αποθηκευμένα, ζητείται από τον διαχειριστή ασφαλείας να δημιουργήσει ένα καινούργιο case (5) το οποίο και θα αντιστοιχεί στην λύση της άγνωστης ως τώρα απειλής.



Εικόνα 26. Βήματα εκτέλεσης του CBR κύκλου.

Τα αντίμετρα που φαίνεται οτι μπορούν να καταστείλουν την απειλή προτείνονται στον διαχειριστή ασφαλείας (6). Μέσα από την αναθεώρηση της λύσης (7), εάν αυτή αποδειχθεί αποτελεσματική (8), το σύστημα προχωρεί σε διαδικασία εκμάθησης (9) του νέου αυτού τρόπου αντιμετώπισης της απειλής, και το καινούργιο case (10) αποθηκεύεται στη βάση των cases, μέσα από μηχανισμούς δεικτοδότησης, και αναδιοργάνωσης της δομής των δεικτών.

Η βάση γνώσης αρχικά μπορεί να περιέχει λίγα cases, όσα είναι εκείνα που θα τοποθετήσει ο διαχειριστής ασφαλείας. Με την πάροδο του χρόνου όμως τα cases θα αυξάνονται. Η αύξηση των cases θα προκύψει με την εμφάνιση νέων, διαφορετικών απειλών, οι οποίες απαιτούν διαφορετικά αντίμετρα για την αντιμετώπισή τους.

3.6.2 Απόδοση βαρών

Για να μπορέσει το CBR Engine να επιλέξει το case που μοιάζει περισσότερο με το νέο, χρειάζονται ευέλικτες και γρήγορες τεχνικές, προσδιορισμού της ομοιότητας, μιας και το σύστημα λειτουργεί σε real time βάση. Τεχνικές που μπορούν να εφαρμοστούν είναι πολλές (O'Leary 1993), κάθε μια με τα θετικά και αρνητικά της

στοιχεία, άρρηκτα δεμένες με τον τρόπο που η CBR οντότητα οργανώνει τα cases (δένδρα, δίκτυα, frames, κτλ) (Chi 1993, Prince 1994, Muniz-Avila 1995). Μια τεχνική που εφαρμόζεται σχεδόν πάντα είναι η απόδοση βαρών στα χαρακτηριστικά των cases. Από τα βάρη αυτά προσδιορίζονται οι πιο «σημαντικοί» όροι για την διαδικασία δεικτοδότησης, και στους οποίους στηρίζεται η προσπάθεια προσδιορισμού της ομοιότητα των cases μεταξύ τους.

Από την δεικτοδότηση προκύπτουν δένδρα δεικτών, τα οποία σαρώνονται (όχι ολόκληρα κάθε φορά) υπολογίζοντας την ομοιότητα (similarity) ανάμεσα στα cases. Η similarity παίρνει τιμή από 0 έως 1. Η μηδενική τιμή υποδηλώνει ότι τα cases διαφέρουν ριζικά ως προς το περιεχόμενό τους, ενώ ο βαθμός 1 σημαίνει ότι ο μέγιστος βαθμός ομοιότητας έχει εμφανιστεί και το case που βρίσκεται αποθηκευμένο στη βάση, αποτελεί ακριβή λύση για την απειλή που εμφανίσθηκε. Στην περίπτωση που η μεγαλύτερη ομοιότητα πάρει τιμή περίπου στη μέση του διαστήματος [0,1], τότε χρειάζεται να εφαρμοστούν τεχνικές προσαρμογής για την λύση του προβλήματος. Συνήθως αυτό πετυχαίνεται με δημιουργία ενός νέου case στη βάση, το οποίο περιέχει στοιχεία από διαφορετικά cases και το οποίο είναι σε θέση να εκφράζει μια καινούργια λύση. Στην περίπτωση που κατορθώνεται η επίτευξη πολύ χαμηλού ποσοστού ομοιότητας μεταξύ των cases, η δημιουργία του case είναι μάλλον αναγκαστική και μάλιστα η απαρχής δημιουργία ενός καινούργιου με παρέμβαση του διαχειριστή.

Στην δική μας περίπτωση, τα βάρη που αντιστοιχούν στα πεδία φαίνονται παρακάτω:

Πίνακας 11. Αντιστοίχηση βαρών στα χαρακτηριστικά του case

Χαρακτηριστικό	Βάρος
System_Id	0
User_Id	5
Node_Id	10
Time	5
Hypothesis_type	25
Level_of_confidence	25
Level_of_penet	15
Params	15

Τα πεδία **Hypothesis_type** και **Level_of_confidence** αποτελούν τα σημαντικότερα πεδία. Ανάλογα με το είδος της υπόθεσης, στην οποία αντιστοιχεί η πιθανή εισβολή, (όπως περιγράφεται από το ES, NN, και το UII), σε συνδυασμό και με το βαθμό εμπιστοσύνης που δίδεται στην υπόθεση από τις οντότητες αυτές, τόσο αυξάνει η σιγουριά και «καχυποψία» του DM ότι η απειλή μάλλον είναι πραγματική. Ο βαθμός που δίδεται στο πεδίο **Level_of_penet** αντιστοιχεί σε αμέσως μικρότερο βαθμό βάρους ίσο με του **params**. Ο βαθμός στον οποίο έχει προχωρήσει η εκδήλωση της απειλής, η επικινδυνότητά της για το σύστημα, καθώς και χρήσιμες

πληροφορίες για τις κινήσεις του χρήστη, αποτελούν πολύ κρίσιμους παράγοντες για την λήψη μέτρων για την καταστολή της. Στη συνέχεια ακολουθούν, με μικρότερα βάρη συγκριτικά με τις πρώτες μεταβλητές, τα υπόλοιπα πεδία. Από αυτές το σημαντικότερο είναι ο κόμβος (**Node_Id**) στον οποίο πραγματοποιείται η πιθανή εισβολή. Αν ένας κόμβος περιέχει περισσότερο «ευαίσθητες» πληροφορίες σε σχέση με τους άλλους και ένας χρήστης εμφανιστεί να κινείται «παράξενα» σε αυτόν (ενώ δεν έχει δικαιώματα πρόσβασης στα αρχεία του συγκεκριμένου κόμβου), τότε πρόκειται για πιθανή εισβολή.

3.7 Υλοποίηση του Συστήματος

Θα υποθέσουμε ότι το υποσύστημα Filtering έχει προσαρμοστεί για τις ανάγκες του περιβάλλοντος που μας ενδιαφέρει (SECURENET). Στη συνέχεια τα εξαγόμενα από αυτό cases θα εισαχθούν σε ένα CBR εργαλείο προκειμένου να εξεταστεί η αποδοτικότητα συστήματος. Η υλοποίηση έχει περισσότερο την έννοια της προσομοίωσης του συστήματος σε συνθήκες εμφάνισης απειλών, ικανές όμως για να μας φανερώσουν ενδείξεις απόδοσης και ευρωστίας για το σύστημα που παρουσιάζεται.

3.7.1 Προσδιορισμός των cases που θα αποτελέσουν τη βάση γνώσης

Αρχικά προσδιορίζονται μερικά αντιπροσωπευτικά cases τα οποία θα εισαχθούν στο CBR εργαλείο για επεξεργασία.

Το πρώτο αναφέρεται στην απειλή που περιγράφηκε σε προηγούμενη παράγραφο και αντιστοιχεί στο:

Case case name is

System Id	<i>Expert System</i>
User Id	<i>mgk</i>
Node Id	<i>dias.aueb.gr</i>
Time	<i>809350118</i>
Hypothesis Type	<i>610010</i>
level of Confidence	<i>9</i>
Level of Penet	<i>9</i>
Num params	<i>5</i>
params	<i>R10010c:Trojan_horse_has_been_prepared User=mgk File=/users/evil/mybinsh/ Owner=evil Group=other</i>

Solution is

User Id	<i>mgk</i>
Node Id	<i>dias.aueb.gr</i>
Time	<i>809350118</i>
Attack Class	<i>Insider attack, System Programming Attack, Trojan Horse</i>
Level of Confidence	<i>9</i>
Level of Penet	<i>9</i>
Cm Description	<i>Με αυτό το αντίμετρο ο χρήστης θα ερωτηθεί για το συνθηματικό του. Αν Δεν δοθεί σωστή απάντηση έως και την Τρίτη φορά, ο χρήστης φεύγει αναγκαστικά (log out) από το σύστημα</i>
Cm Subject	<i>«Ρώτα το χρήστη για το Password που έχει»</i>

End

Το επόμενο case αντιστοιχεί σε ένα χρήστη (evil) ο οποίος δημιούργησε ένα sgid αρχείο (sgid_file) στο ευρετήριο /users/evil/files/. Παρόλο που είναι γνωστό ότι ο χρήστης αυτός μπορεί να δημιουργεί τέτοιουν είδους αρχεία, ωστόσο το αρχείο αυτό τοποθετήθηκε και εκτελέστηκε από ένα ευρετήριο χρήστη. Το case που αντιστοιχεί στην αντιμετώπιση της πιθανής αυτής απειλής είναι:

Case case name is

<u>System_Id</u>	<i>Expert System</i>
<u>User_Id</u>	<i>evil</i>
<u>Node_Id</u>	<i>knossos.aueb.gr</i>
<u>Time</u>	<i>809188835</i>
<u>Hypothesis_Type</u>	<i>610005</i>
<u>level_of_Confidence</u>	<i>1</i>
<u>Level_of_Penet</u>	<i>9</i>
<u>Num_params</u>	<i>6</i>
<u>params</u>	<i>R10005c:Probable_Trojan_horse.A_sgid_file_belonging_to_a_sensitive_group_but_localized_in_a_home_directory_was_executed. User=evil File=/users/evil/files/sgid_file Owner=evil Group=other Path=/users/hacker Home_Path=/users/hacker</i>

Solution is

<u>User_Id</u>	<i>evil</i>
<u>Node_Id</u>	<i>knossos.aueb.gr</i>
<u>Time</u>	<i>809188835</i>
<u>Attack_Class</u>	<i>Insider attack</i>
<u>Level_of_Confidence</u>	<i>1</i>
<u>Level_of_Penet</u>	<i>9</i>
<u>Cm_Description</u>	<i>Ειδοποίησε τον system manager για τις «Παράξενες» δραστηριότητες του συγκεκριμένου χρήστη</i>
<u>Cm_Subject</u>	<i>«Alert the system manager»</i>

End

Τα προηγούμενα cases (μαζί και με άλλα τα οποία προσδιορίζονται από την προσπάθεια αντιμετώπισης υποθετικών απειλών) εισάγονται στο CBR εργαλείο για να προσδιοριστεί και τεχνικά η αξιοπιστία του συστήματος.

3.7.2 Επιλογή CBR Shell

Χρησιμοποιήθηκε η δεύτερη έκδοση του CBRWorks (Richter 1996). Αποτελεί προϊόν λογισμικού που αναπτύχθηκε στα πλαίσια του INRECA project (Traphoener 1995). Αποτελεί εργαλείο το οποίο ενσωματώνει τεχνικές case-based reasoning και induction, παρέχοντας ένα εύρωστο περιβάλλον για την περιγραφή του γενικού πλαισίου (context) του problem domain που μας ενδιαφέρει. Περιγράφει τον χώρο προβλημάτων με χρήση ειδικής γλώσσας (CASUEL). Παρέχει γραφικό περιβάλλον σε διάφορα συστήματα (X-Windows, Microsoft Windows, Apple Macintosh, OS/2).

Αρχικά προσδιορίζεται ο χώρος προβλημάτων στον οποίο αναφερόμαστε. Δημιουργούμε το αρχικό *concept*, το οποίο αποτελεί (κατά μια αφηρημένη έννοια) τον υψηλότερο κόμβο στην ιεραρχία της διάρθρωσης των cases, τον οποίο ακολουθούν και «κληρονομούν» όλες οι έννοιες οι οποίες δημιουργούμε για τις ανάγκες της κάλυψης του χώρου προβλημάτων. Η παράσταση των cases ακολουθεί την αντικειμενοστραφή προσέγγιση. Οι classes αναφέρονται ως concepts και τα slots ως attributes. Στη συνέχεια προσδιορίζονται οι σχέσεις μεταξύ τους, οργανώνονται οι έννοιες (concepts) σε μια δενδρική δομή. Οι κόμβοι του δένδρου περιγράφουν τις έννοιες που έχουν οριστεί ενώ οι σχέσεις μεταξύ τους περιγράφουν τις σχέσεις «*is sub-concept of*», όπου κάθε έννοια χαμηλότερου επιπέδου κληρονομεί τα χαρακτηριστικά αυτής που βρίσκεται σε ανώτερο ιεραρχικό επίπεδο.

Παρέχονται τρόποι για τον προσδιορισμό των attributes που θα περιέχει κάθε Case. Καθορίζονται οι τύποι τους (integer, string, text, κ.α.), ενώ δίνεται η δυνατότητα δημιουργίας καινούργιων τύπων για τις ανάγκες του χώρου προβλημάτων, στους οποίους αντιστοιχίζονται βαθμοί ομοιότητας (similarities) μεταξύ τους. Δίνεται η δυνατότητα αντιστοίχησης βαρών στα attributes των cases,

Αφού έχει οριστεί η βάση γνώσης, μέσω ειδικής διεπαφής εισάγονται στοιχεία σε αυτήν, σε κάθε case, ενώ παρέχονται τρόποι για δημιουργία επερωτήσεων case-queries στη βάση, παρουσιάζονται τα cases, οι ομοιότητες που έχουν με το αρχικό case, αναπαριστάνεται γραφικά ομοιότητά τους, κτλ.

Η γλώσσα που χρησιμοποιείται για την περιγραφή των εννοιών, των cases και των σχέσεων μεταξύ τους είναι η CASUEL (Bergmann 1994). Χρησιμοποιείται για την αναπαράσταση της γνώσης που αντιστοιχεί σε ένα χώρο προβλημάτων. Ακολουθεί αντικειμενοστραφή φιλοσοφία στην αναπαράσταση της γνώσης, σε ASCII αρχεία. Εχει τη δυνατότητα να περιγράψει επαρκώς την ιεραρχία των εννοιών, τις σχέσεις κληρονομικότητας που τις διακρίνουν, τα attributes των cases και τα περιεχόμενά τους

3.7.3 Στοιχεία απόδοσης του συστήματος

Δημιουργήθηκε μια μικρή βάση από cases, τα οποία εισήχθηκαν στο CBRWorks προκειμένου να παρουσιαστούν στοιχεία λειτουργίας του συστήματος, όταν αυτό τεθεί σε πραγματική λειτουργία. Η δημιουργία των cases και η τοποθέτησή τους στο CBR Shell έχει την έννοια της προσομοίωσης. Δυστυχώς τα IDS τα οποία έχουν κατά καιρούς αναπτυχθεί είτε έχουν ερευνητικό χαρακτήρα και στοχεύουν στην ανάδειξη νέων τρόπων για ανίχνευση παρεισφρητικής συμπεριφοράς, χωρίς, πολλές φορές να έχουν μπει ποτέ σε λειτουργία (!), είτε έχουν κατασκευαστεί από ιδρύματα με στόχο την ανίχνευση εισβολών στα συγκεκριμένα περιβάλλοντα τα οποία έχουν αναπτυχθεί. Αυτό καθιστά την εύρεση συστημάτων IDS για μελέτη δύσκολη διαδικασία, ακόμα δε δυσκολότερη την μελέτη τους σε πραγματικό περιβάλλον.

Επίσης δεν υπάρχουν τρόποι - μετρικές για την αξιολόγηση των ήδη υπαρχόντων IDS. Αποτελεί ίσως πολιτική των οργανισμών που τα χρησιμοποιούν να μην εκδίδουν πληροφορίες για τη δομή και λειτουργία τους. Ο ολοένα αυξανόμενος

ρυθμός των διασυνδεδεμένων υπολογιστικών συστημάτων και οι διαφορετικές τεχνολογίες που αυτά ενσωματώνουν, δημιουργεί νέους τρόπους εισβολών και τρόπων παραβίασης της ασφάλειάς τους, με αποτέλεσμα την αδυναμία ύπαρξης φόρμουλας προσδιορισμού της απόδοσης των IDS.

Αυτά καθιστούν (προς το παρόν) την αξιολόγηση του συστήματος που παρουσιάστηκε σε πραγματικές συνθήκες λειτουργίας ανέφικτη μιας και υπάρχει δυσκολία εύρεσης πραγματικών δεδομένων, τα οποία και θα χρησιμοποιηθούν για την προσπάθεια αξιολόγησης.

Μπορούμε να αναφέρουμε οτι αυξάνοντας το μέγεθος της βάσης γνώσης, δεν σημαίνει οτι αυξάνει και ο χρόνος απόκρισης του συστήματος. Το κόστος δημιουργίας μιας βάσης γνώσης με cases, (στην περίπτωση χρήσης k-d δένδρων (multidimensional binary search tree) (Wess 1995)) υπολογίζεται σε $O[k^*n^*log n]$. Στην χειρότερη περίπτωση αυτό μετατρέπεται σε $O[k^*n^2]$. Το μέσο κόστος αναζήτησης ενός case από τη δενδρική αυτή δομή, ανέρχεται σε $O[log n]$ (Στη χειρότερη περίπτωση $O[n]$).

Υποθέτουμε ένα IDS που ενσωματώνει τεχνικές εμπείρων συστημάτων, νευρωνικών δικτύων και CBR. Τα υποσυστήματα αυτά δέχονται ως είσοδο τα audit trails που περιγράφουν τις κινήσεις των χρηστών, ενώ τα αποτελέσματά τους δίδονται στο υποσύστημα λήψης αποφάσεων για την τελική επιλογή των αντιμέτρων που μπορούν να χρησιμοποιηθούν (αν τελικά υπάρχει εισβολή). Θεωρούμε οτι ο χρόνος απόκρισης του συστήματος (Denault 1992) είναι ο ελάχιστος από τους χρόνους που χρειάζεται για να αποκριθεί το έμπειρο σύστημα, το νευρωνικό δίκτυο και το υποσύστημα CBR.

$$T_{reaction} = \min(T_{NN}, T_{ES}, T_{CBR})$$

Συγκεκριμένα, $T_{reaction}$ είναι ο χρόνος αντίδρασης του IDS. Υπολογίζεται από την πρώτη δράση της εισβολής και τελειώνει τη στιγμή που έχει ανιχνευθεί. Ο T_{NN} αντιστοιχεί στον χρόνο απόκρισης του νευρωνικού δικτύου, και οι T_{ES}, T_{CBR} είναι οι χρόνοι για το έμπειρο σύστημα και το CBR αντίστοιχα.

Ο χρόνος T_{NN} είναι δύσκολο να υπολογιστεί δεδομένης της ιδιαιτερότητας του νευρωνικού δικτύου. Πρέπει να συνυπολογιστούν στοιχεία για τον χρόνο εκμάθησής του, τον αριθμό των επιπέδων που περιέχει, τον τύπο του (single pass ή back propagation scheme) καθώς και τον τρόπο υλοποίησής του (hardware, software ή hybrid).

Ο χρόνος T_{ES} αντιστοιχεί στον μέσο χρόνο αναζήτησης μιας εγγραφής στη βάση του έμπειρου συστήματος. Σε όρους πολυπλοκότητας μεταφράζεται σε $O[log n]$ (στην χειρότερη περίπτωση $O[n]$). Οι αντίστοιχες τιμές στην περίπτωση του CBR (για ανάκτηση cases) είναι $O[log n]$ και $O[n]$ αντίστοιχα.

Η ανάλυσης της απόδοσης των συστημάτων ανίχνευσης εισβολών είναι δύσκολη διαδικασία (όπως αναφέραμε και προηγούμενα). Αυτό που μπορεί να εξαχθεί ως τελικό συμπέρασμα είναι οτι η ενσωμάτωση CBR τεχνικών μπορεί να αυξήσει την απόδοση, ευελιξία και εν γένη αποδοτικότητα των IDS, με τα ιδιαίτερα

χαρακτηριστικά της μάθησης, ευκολίας παράστασης και αναθεώρησης της γνώσης, δυνατότητα εφαρμογής του σε δύσκολα μοντελοποιήσιμα πεδία που το διακρίνουν. Αν υποθέσουμε ότι στο σύστημα IDES, το έμπειρο σύστημα που χρησιμοποιήθηκε είχε πολυπλοκότητα της τάξεως που αναφέραμε και ο χρόνος απόκρισής του ήταν λιγότερος από λεπτό, συμπεραίνουμε ότι με τη χρήση νέων τεχνικών και με την αναμενόμενη έρευνα που υπάρχει σε αυτές, η δυνατότητα επίτευξης επιπέδου λειτουργίας τάξεως real time ή real time, μπορεί να επιτευχθεί.

Στο Παράρτημα που^{*} ακολουθεί παρουσιάζονται μερικές από τις αντιπροσωπευτικές οθόνες του προγράμματος κατά τη λειτουργία του. Εισάγαμε ορισμένα cases που αναπαριστούν εισβολές, και παρατηρούμε την αντίδραση του συστήματος μέσω του CBR Shell.

4. ΕΡΕΥΝΗΤΙΚΕΣ ΠΡΟΤΑΣΕΙΣ

Ενδιαφέρον παρουσιάζει η εφαρμογή του συστήματος σε ένα πραγματικό περιβάλλον (δεδομένου ότι θα ξεπεραστούν οι εν γένει δυσκολίες που ήδη περιγράψαμε). Ήταν χρήσιμη η τροποποίηση του CBR Shell ή ακόμα και η κατασκευή ενός ξεχωριστού, το οποίο θα υλοποιεί τις αναγκαίες μόνον λειτουργίες ενός CBR συστήματος, προκειμένου να είναι ταχύτερο και αποδοτικότερο (τα περισσότερα CBR Shells που έχουν εμφανιστεί αποτελούν εργαλεία γενικής χρήσης). Το υποσύστημα Filtering μπορεί να τροποποιηθεί έτσι ώστε να μετατρέπει τα μηνύματα από τα υπόλοιπα modules του IDS σε κατανοητά cases. Με αυτόν τον τρόπο, το σύστημα θα μπορέσει να λειτουργήσει σε real-time πλατφόρμα και θα μπορέσουν στη συνέχεια να εξαχθούν χρήσιμα στοιχεία για την αποτελεσματικότητά του.

Ερευνητές της Τεχνητής Νοημοσύνης θεωρούν τις τεχνικές CBR ως κατάλληλες για την κατασκευή συστημάτων τα οποία θα ενσωματώνουν «ευφύή» λειτουργίες. Στόχος δεν είναι η κατασκευή μεγάλων σε κλίμακα συστημάτων τα οποία θα περιέχουν νοημοσύνη με την οποία θα πραγματοποιούν οτι και οι άνθρωποι μπορούν. Εκείνο που κρίνεται αναγκαιότερο είναι η κατασκευαστή συστημάτων τα οποία θα εμπεριέχουν έξυπνες λειτουργίες. Οι λειτουργίες αυτές δείχνουν ότι μπορούν να υλοποιηθούν αποδοτικά με χρήση τεχνικών CBR, λόγω των πλεονεκτημάτων που κατέχουν, συγκριτικά με άλλες παρεμφερείς τεχνικές του ίδιου χώρου (έμπειρα συστήματα, παραδοσιακές rule based μεθοδολογίες).

Για να μπορέσει όμως να ενισχύσει την επιρροή του, πρέπει να αντεπεξέλθει σε ορισμένα από τα μειονεκτήματα που το χαρακτηρίζουν. Τα σημαντικότερα προβλήματα που πρέπει να αντιμετωπιστούν έχουν σχέση με τον τρόπο οργάνωσης της βάσης γνώσης, δεικτοδότησης των cases και προσαρμογής των παλαιότερων λύσεων. Ο τρόπος δεικτοδότησης της βάσης αποτελεί το σημαντικότερο παράγοντα επιτυχίας για το CBR. Από αυτόν εξαρτώνται η ταχύτητα εύρεσης των cases, η απόδοση στην εκμάθησή του. Γενικά οι τρόποι δεικτοδότησης στηρίζονται σε πολύπλοκες και ακριβείς τεχνικές. Οι τεχνικές προσαρμογής που χρησιμοποιούνται επίσης, από τη μια είναι δύσκολο να γενικευτούν ακόμα δε δυσκολότερο να υλοποιηθούν. Από αυτές εξαρτάται η ευελιξία που χαρακτηρίζει τα συστήματα CBR,

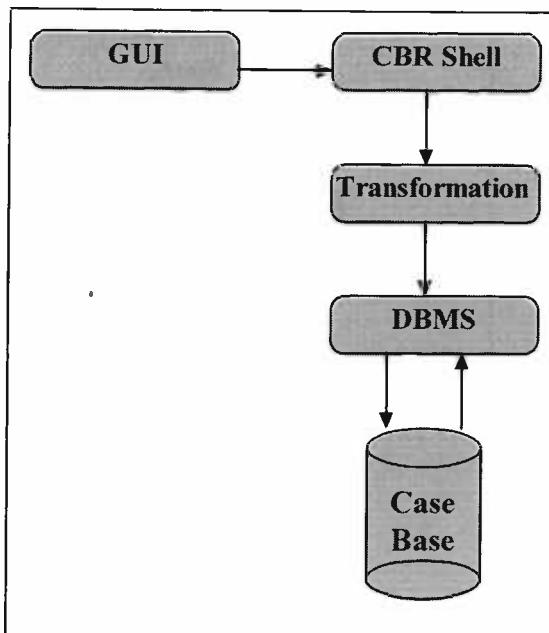
η δυνατότητα επίλυσης νέων προβλημάτων και η δυνατότητα επιδιόρθωσης παλιότερων λύσεων που είχε αποτύχει η εφαρμογή τους.

Αυτή είναι και η πορεία της έρευνας που πραγματοποιείται σήμερα στον χώρο ανάπτυξης συστημάτων CBR. Η ανακάλυψη πιο αποτελεσματικών τρόπων δεικτοδότησης, καλύτερα ορισμένων και αποδοτικών τρόπων οργάνωσης της γνώσης, πιο εύρωστων τρόπων προσαρμογής των λύσεων, ώστε να είναι πάντα ικανές να εκδίδουν λύση. Με αυτόν τον τρόπο θα επέλθει μείωση του κόστους ανάπτυξης CBR συστημάτων, καθώς και δυνατότητα επεξεργασίας μεγάλης κλίμακας βάσεων γνώσης.

Η ενοποίηση των τεχνικών CBR με υπάρχουσες μεθοδολογίες και τεχνικές, όπως οι παραδοσιακές των εμπείρων συστημάτων και γενικά των rule based μεθοδολογιών, αλλά και νεότερων όπως νευρωνικά δίκτυα, genetic algorithms κρίνεται αναγκαία για την ευρεία αποδοχή και χρήση του. Η ενοποίηση με τα rule based συστήματα είναι εφικτή με τρεις τρόπους.

Μπορούν να χρησιμοποιηθούν για την υποστήριξη του CBR στις κύριες λειτουργίες που αυτό εκτελεί. Το CBR εκδίδει μέσω μηχανισμών που ενσωματώνει γρήγορα λύσεις στα προβλήματα. Οι λύσεις αυτές μπορούν να φιλτραριστούν από κάποιο έμπειρο σύστημα, που οργανώνει σε μορφή κανόνων γενικές πολιτικές για την εφαρμογή των λύσεων που εκδίδει το CBR. Μπορεί να υπάρξει και ο αντίστροφος ρόλος, όπου το CBR καθοδηγεί την συμπερασματολογία Rule based συστημάτων. Μια τρίτη μορφή που μπορεί να πάρει η ενοποίηση αυτή είναι η χρήση του CBR ως μια ισόβαθμη οντότητα με τις άλλες, κυρίως στα πλαίσια μεγάλων στην κλίμακα συστημάτων (multistrategy reasoning systems).

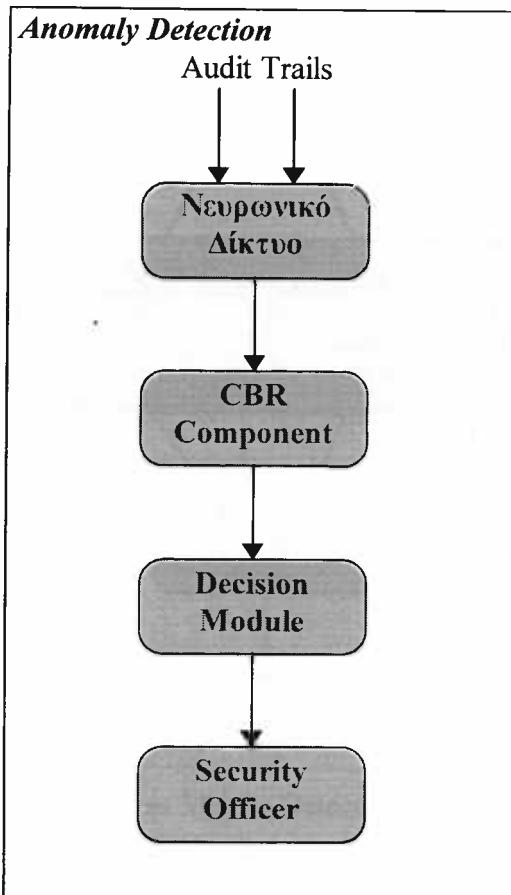
Η τεχνικές που χρησιμοποιούνται για ανάκτηση πληροφοριών σήμερα στηρίζονται στην πλειοψηφία τους στα παραδοσιακά συστήματα βάσεων δεδομένων (DBMS). Η συνύπαρξη των CBR συστημάτων με τα DBMS μπορεί να οδηγήσει σε καλύτερα αποτελέσματα, συνδυάζοντας την ακριβή επιλογή και σταθερότητα των DBMS με την ευελιξία στην πρόταση λύσεων από το CBR. Τα DBMS ανακτούν στοιχεία από τη βάση γνώσης στηριζόμενα στην υλοποίηση τελεστών ομοιότητας μεταξύ της ερώτησης (query) και των στοιχείων της βάσης. Αντίθετα το CBR ανακτά στοιχεία από τη βάση γνώσης στηριζόμενο στην ομοιότητα (similarity assessment) των χαρακτηριστικών του target και source case. Η ενοποίηση των δυο συστημάτων προμηνύει αποδοτικά αποτελέσματα τόσο στην ακρίβεια των λύσεων όσο και στον πλουραλισμό τους.



Εικόνα 27. Ενοποίηση τεχνικών CBR με συστήματα DBMS

Ο χρήστης μέσω διεπαφής (GUI) αλληλεπιδρά με το CBR Shell. Η βάση γνώσης είναι αποθηκευμένη σε μορφή πινάκων σε παραδοσιακό DBMS. Το CBR Shell δεν μπορεί να επικοινωνήσει άμεσα με τη βάση γνώσης. Χρειάζεται μια διαδικασία μετασχηματισμού του query που εκδίδει το CBR σε κατανοητή μορφή για το DBMS. Το DBMS δεν μπορεί να εκτελέσει queries που σχετίζεται με προσδιορισμό ομοιότητας χαρακτηριστικών, παρά με ακριβή έλεγχο με βάση παραμέτρους - κριτήρια. Προσπάθειες για ενοποίηση CBR με DBMS συστήματα έχουν γίνει στο παρελθόν. Αποτελεί όμως ενδιαφέρουσα πρόταση για ανάκτηση πληροφοριών, συνδυάζοντας την σταθερότητα του DBMS με την ευελιξία του CBR.

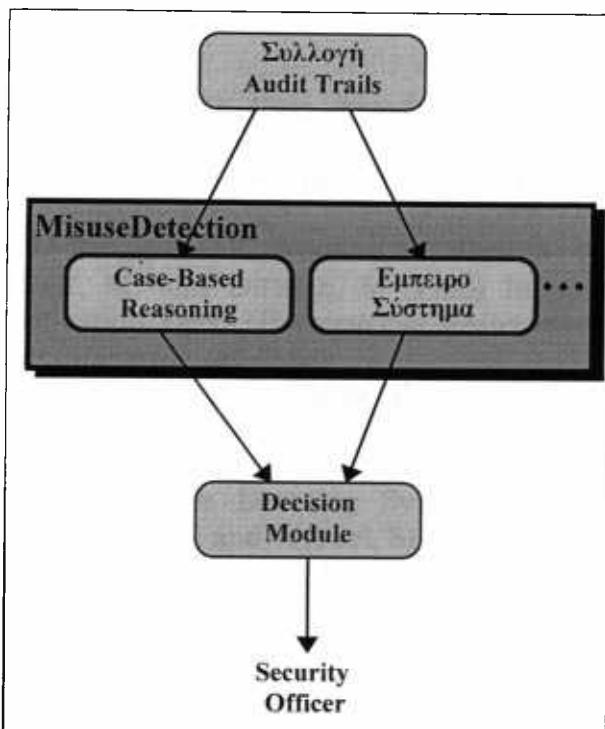
Ενδιαφέρον αποκτά η ενοποίηση τεχνικών CBR με «Knowledge Limited» συστήματα όπως τα Νευρωνικά Δίκτυα. Αυτά έχουν δείξει ότι αποτελούν άριστα φίλτρα πληροφοριών. Η χρήση τους σε συστήματα ανίχνευσης εισβολών έχει δείξει ότι απορρίπτουν τις περιττές πληροφορίες από τα audit trails κατά 80%. Η εφαρμογή ενός υποσυστήματος που θα δέχεται τις πληροφορίες αυτές στην έξοδο του Νευρωνικού Δικτύου, το οποίο θα φιλτράρει και θα αναζητεί και αυτό στοιχεία παρεισφρήσεων στις κινήσεις του χρήστη φαίνεται να αποτελεί καλή σχεδιαστική επιλογή. Ένα τέτοιο σύστημα φαίνεται παρακάτω:



Εικόνα 28. Χρήση τεχνικών CBR για Anomaly Detection

Το Νευρωνικό Δίκτυο φιλτράρει τις πληροφορίες και διοχετεύει μόνο τις απαραίτητες για την συμπερασματολογία στο υποσύστημα CBR. Αυτό με τη σειρά του, λαμβάνοντας τις πληροφορίες σχετικά με τις πιθανές «περιεργες» κινήσεις εφαρμόζει τους δικούς του μηχανισμούς συμπερασματολογίας, προκειμένου να ενισχύσει ή να απορρίψει την συγκεκριμένη πρόταση. Το τελικό μήνυμα στέλνεται στο υποσύστημα λήψης αποφάσεων (DM).

Οι τεχνικές CBR μπορούν να χρησιμοποιηθούν και σε άλλα τμήματα των συστημάτων ανίχνευσης εισβολών. Λόγω της ευέλικτης συμπερασματολογίας που ενσωματώνουν μπορούν να χρησιμοποιηθούν αποτελεσματικά για misuse detection. Οι CBR τεχνικές υπερτερούν σε πολλά σημεία σε σχέση με τα έμπειρα συστήματα και γενικά με την rule-based συμπερασματολογία (Schank 1991). Η βάση γνώσης, με χρήση CBR τεχνικών θα οργανώνεται με cases (τα οποία αποτελούν σχεδόν πάντα καλύτερη παράσταση της γνώσης στους χώρους προβλημάτων). Οι πληροφορίες που λαμβάνοντα από τα audit trails μετατρέπονται σε cases, και ζητείται η εύρεση παρόμοιων στη βάση γνώσης. Αν το case που ταιριάζει περισσότερο με το source case (όπως αυτό προέκυψε από τα audit trails), προσδώσει στοιχεία παρεισφροητικής συμπεριφοράς για τη συμπεριφορά του χρήστη, τότε αυτό μεταβιβάζεται στο υποσύστημα λήψης αποφάσεων για την τελική επιλογή του αντίμετρου.



Εικόνα 29. Χρήση τεχνικών CBR για Misuse Detection

Απαιτείται, βέβαια, προσπάθεια από το διαχειριστή στην εισαγωγή νέων σεναρίων - νέων cases με απειλές - αλλά αποτελεί άλλωστε και το βασικό πρόβλημα σε όλες τις τεχνικές misuse detection που υπάρχουν. Με τις τεχνικές εκμάθησης όμως που ενσωματώνουν, η διεπαφή με τον διαχειριστή θα είναι η λιγότερη δυνατή, μιας και το σύστημα μπορεί να μάθει για νέες υπογραφές εισβολών. Η ταχύτητα στην έκδοση συναγερμού για πιθανή απειλή είναι σίγουρα μεγάλη, μιας και δεν χρειάζεται να διασχίζεται κάθε φορά όλο το δένδρο των κανόνων της βάσης γνώσης. Με τις ολοένα και αποδοτικότερες νεοεμφανιζόμενες τεχνικές οργάνωσης δεικτοδότησης των cases (μιας και το CBR αποτελεί ενεργή ερευνητική περιοχή), οι συναγερμοί που θα εκδίδονται προβλέπεται να είναι αποτελεσματικότεροι και ταχύτεροι.

5. ΕΠΙΣΚΟΠΗΣΗ

Δείξαμε οτι τα συστήματα ανίχνευσης εισβολών διακρίνονται από μειονεκτήματα, τα οποία μπορούν να ξεπεραστούν με την ενσωμάτωση νέων τεχνικών από τον χώρο της Τεχνητής Νοημοσύνης. Με τις τεχνικές αυτές θα μπορέσουν να γίνουν πιο ευέλικτα και αποτελεσματικά ενώ θα μπορέσει να επιτευχθεί πραγματική real time απόκριση στις εισβολές που παρουσιάζονται.

Εκφράζουμε την πεποίθηση πως οι τεχνικές CBR, εκτός των ιδιαίτερων στοιχείων που τις χαρακτηρίζουν, αλλά και σε όρους πολυπλοκότητας, μπορούν να διαδραματίσουν ιδιαίτερο ρόλο στην επίτευξη του σκοπού αυτού.

6. ВІБЛІОГРАФІА

- Aamodt, A. and Plaza, E. (1993) Case based Reasoning: Foundational Issues, Methodological Variations and System Approaches. *AICom - Artificial Intelligence Communications*, 7, 1. Available online at URL: «<http://www.iiia.csic.es/People/enric/AICom.html>»
- Althoff, K., Manago, M., Bergmann, R., Maurer, F., Wess, S., Auriol, E., Conruyt, N., Traphoner, R., Brauer, M. and Dittrich, S. (1995) Induction and Case - Based Reasoning for Classification Tasks, *University of Kaiserlautern*. Available online at URL: «<http://wwwagr.informatik.uni-kl.de>»
- Anderson, J. P. (1980) Computer Security Threat Monitoring and Surveillance, *James P. Anderson Co.*
- Anthony, F. and Ashwin, R. (1995) A Comparative Utility Analysis of Case - Based Reasoning and Control - Rule Learning Systems. *Lecture Notes in Artificial Intelligence*, 912, (eds. Lavrac, N. and Wrobel, S), Springer Verlag.
- Auriol, A., Wess, S., Manago, M., Althoff, K. and Traphoner, R. (1995) INRECA: a seamlessly Integrated System Based on Inductive Inference and Case Based Reasoning, *Lecture Notes in Artificial Intelligence*, 1010, (eds. Veloso, M. and Aadmont, A.), Springer Verlag, pp. 371-380.
- Bellovin, S. M, (1990) There be Dragons, *AT&T Bell Laboratories*. Available online at URL: «ftp://ftp.research.att.com/dist/internet_security/dragons.ps»
- Bergmann, R. (1994) CASUEL: A Common Case Representation Language, *Esprit Project 6322, University of Kaiserlautern*. Available online at URL: «<http://ftpagr.informatik.uni-kl.de>»
- Bradley, A. P. (1994) Case-based Reasoning: Business Applications, *IEEE Expert*, 7, 3, pp. 40-42.
- Brown, M. (1993) A Memory Model for Case Retrieval by Activation Passing, University, PhD Thesis, University of Manchester. Available online at URL: «<ftp://ftp.cs.man.ac.uk/pub/TR/>»
- Cheswick, B. (1990) The Design of a Secure Internet Gateway, *USENIX Summer Conference Proceedings*. Available online at URL: «ftp://ftp.research.att.com/dist/internet_security/gateway.ps»
- Cheswick, B. (1992) An Evening with Berferd in Which a Cracker is Lured, Endured and Studied, *AT&T Bell Laboratories*. Available online at URL: «ftp://ftp.research.att.com/dist/internet_security/berferd.ps»
- Chi, R., Chen, M. and Kiang M. (1993) Generalized Case - Based Reasoning System for Portfolio Management, *Expert Systems With Applications*, 6, pp. 67-76.
- Chung, M., Puketza, N., Olsson, R.A. and Mukherjee, B. (1994) Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing Intrusions, *University of California*. Available online at URL: «<http://www.cs.ucdavis.edu>»
- Crosbie, M. and Spafford G. (1995b) Active Defence of a Computer System using Autonomous Agents, *Purdue University*. Available online at URL: «<http://www.cs.purdue.edu>»
- Darzentas, J. and Spyrou, T. (1994) SECURENET: An intelligent System for Detecting and Preventing Attacks in Open Networks, User Intention Modelling. Deliverable 4, *European RACE Programme (SECURENET (R2113) Project)*.
- Debar, H. and Dorizzi, B. (1992b) An Application of a Recurrent Network to an Intrusion Detection System, *IEEE*. pp 478 - 483.

- Debar, H., Becker, M. and Siboni, D. (1992a) A neural Network component for Intrusion Detection System, *IEEE*, pp. 240 - 250.
- Denault, M., Gritzalis, D., Karagiannis, D. and Spirakis, P. (1992) Intrusion Detection approach and performance issues of the SECURENET system, *European RACE Programme (SECURENET (R2057) Project)*.
- Denning, D.E (1987) An Intrusion - Detection Model, *IEEE transactions on Software Engineering, SE-13*, 2, pp. 222-232.
- Doumas, A., Mavroudakis, K., Katsikas, S. and Gritzalis, D. (1992) Design of a neural netework for virus recognition / classification, *Research Laboratory of Samos, Department of Mathematics, University of the Aegean*.
- Frank, J. (1994) Artificial Intelligence and Intrusion Detection: Current and Future Directions, *University of California*, Available online at URL: «<http://www.cs.ucdavis.eu>»
- Garfinkel, S. and Spafford, G. (1996) *Practical Unix and Internet Security*, O'reilly & Associates, Inc. 2nd Edition.
- Garvey, D.T and Lunt, F.T. (1991) Model - Based Intrusion Detection, in *Proceedings of the 15th National Computer Security Conference*.
- Globig, C. and Wess, S. (1995) Learning in Case Based Classification Algorithms, *University of Kaiserlautern*. Available online at URL: «<http://wwwagr.informatik.uni-kl.de>»
- Grosbie, M. and Spafford, G. (1995a) Applying Genetic Programming to Intrusion Detection, *Purdue University*. Available online at URL: «<http://www.cs.purdue.edu>»
- Guiner, B. (1991) Computer «virus» identification by neural networks, *ACM SIGSAC*, 9,4, pp. 49 - 59.
- Hennessy, D. and Hinkle, D. (1992) Applying Case-Based Reasoning in Autoclave Loading, *IEEE Expert*.
- Holder D. (1992) A Rule-Based Intrusion Detection System, *Proceedings of the IFIP on IT Security: the Need for International Cooperatikon*, (eds. G. G. Gable and W.J. Caclli), Elsevier Science Publishers B.V. (North-Holland)
- Huang, Y. and Miles, R. (1996) Using Case-based techniques to enhance constraint satisfaction problem solving, *Applied Artificial Intelligence*, 10, pp. 307-328.
- Janetsko, D., Wess, S. and Melis, E. (1995) Goal Driven Similarity Assessment, *University of Kaiserlautern*. Available online at URL: «<http://wwwagr.informatik.uni-kl.de>»
- Kantzavelou, I. and Patel, A. (1995) Issues of Attack in Distributes Systems - A generic Attack Model, *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, (ed. P. Horser), Chapman & Hall.
- Katsikas, S. and Theodoropoulos, N. (1996) Defending Networks: the expert system component of SECURENET, *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, (ed. P. Horser), Chapman & Hall.
- Katsikas, S.(1997) SECURENET: An intelligent System for Detecting and Preventing Attacks in Open Networks, Overview of Specifications for Neural Network, Simulators, ESDM, *Deliverable 5, European RACE Programme (SECURENET (R2113) Project)*.
- Ketler, K. (1993) Case - Based Reasoning: An Introduction, *Expert Systems With Applications*, 6, pp. 3-8.

- Kioundouzis, E. A. and Kokolakis. S. A. (1996), An analyst's view of IS security, in *proceedings of 12th International Conference on Information Security*, IFIP '96, Samos, Greece.
- Kitano, H. and Shimazu, H. (1996) The Experience Sharing Architecture: A Case Study in Corporate-Wide Case-Based Software Quality Control, in *Case-Based Reasoning, Experiences, Lessons and Future Directions*, (ed. D. Leake), The AAAI press, The MIT press, pp. 31 - 65.
- Kokolakis, S.A. (1995) Is there a need for new Information Security Models, *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, (ed. P. Horser), Chapman & Hall.
- Kolodner, J. (1993) *Case-based Reasoning*, Morgan Kaufman Publishers.
- Kolodner, J. and Leake, D. (1996) A tutorial Introduction to Case - Based Reasoning, in *Case-Based Reasoning, Experiences, Lessons and Future Directions* (ed. D. Leake), The AAAI press, The MIT press, pp. 31 - 65.
- Kuhn, T. (1970) *The Structure of Scientific Revolutions*, Chicago-University of Chicago, 2nd edition.
- Kumar, S. (1995) A Classification and Detection of Computer Intrusions, PhD Thesis, *Purdue University*. Available online at URL: «<http://www.cs.purdue.edu>»
- Leake, D. (1996) CBR in Context: the Present and future, in *Case-Based Reasoning, Experiences, Lessons and Future Directions*, (ed. D. Leake), The AAAI press, The MIT press. pp. 3-30.
- Lunt, F.T (1993) A survey of intrusion detection techniques. *Computers & Security*, 12, pp. 405-418.
- Lunt, F.T and Jagannathan, R.(1988) A Prototype Real - Time intrusion-Detection Expert System, in *Proceedings of the 1988 IEEE Symposium on Security and Privacy*.
- Lunt, F.T., Jagannathan, R. and Whitehurst, (1989) A. Knowledge - Based Intrusion Detection, in *Proceedings of the 1989 AI Systems in Government Conference*. Washington, DC.
- Lunt, F.T., Tamaru, A., Gilham, F., Jagannathan, R., Jalali, G. and Neumann, P.G. (1992) A Real-Time Intrusion - Detection Expert System (IDES), *Technical report*, Computer Science Laboratory, SRI International, California.
- Mark, W., Simoudis, E. and Hinkle, D. (1996) Case-Based Reasoning: Expectations and Results, in *Case-Based Reasoning, Experiences, Lessons and Future Directions*, (ed. D. Leake), The AAAI press, The MIT press, pp. 269 - 294.
- Mott, S. (1993) Case-Based Reasoning: Market, Applications, and fit with other technologies, *Expert Systems With Applications*, 6, pp 97-104.
- Mukherjee, B., Heberlein, L.T. and Levitt, K.N. (1994) Network Intrusion Detection, *IEEE Network May/June*, pp. 26-41.
- Munakata, T.and Jani, Y. (1994) Fuzzy systems: An Overview, *Communications of the ACM*, 37,3, pp. 69-76.
- Muniz-Avila, H. and Huellen, J. (1995) Retrieving cases in Structured Domains by Using Goal Dependencies, *Lecture Notes in Artificial Intelligence*, 1010, (eds. Veloso, M. and Aadmont, A.), Springer Verlag, pp. 241-252.
- O'Leary, D. E. (1993) Verification and Validation of Case-Based Systems, *Expert Systems With Applications*, 6, pp. 57-66.
- Prince, C.J. and Pegler, I.S. (1994) Deciding Parameter Values With Case-Based Reasoning, University of Wales. Available online at URL: «<http://www.aber.ac.uk>».



- Puketza, J.N., Zhang, K., Chung, M., Mukherjee, B. and Olsson, R.A. (1996) A Methodology for Testing Intrusion Detection Systems, *University of California*. Available online at URL: «<http://www.cs.ucdavis.edu>»
- Richter, M. and Traphoener, R. (1996) CBRworks evaluation prototype, University of Kaiserlautern. *University of Kaiserlautern*. Available online at URL: «<ftp://ftpagr.informatik.uni-kl.de>».
- Riesbeck, C. (1996) What Next? The Future of Case-Based Reasoning in Post-Modern AI, in *Case-Based Reasoning, Experiences, Lessons and Future Directions*, (ed. D. Leake), The AAAI press, The MIT press, pp. 371-388.
- Rumelhart, D., Widrow, B. and Lehr, M. (1994) The Basic Ideas in Neural Networks, *Communications of the ACM*, 37,3, pp. 87-92.
- Salton, G. (1989) *Automatic Text Processing*, Addison - Wesley.
- Schank, R. (1996) Goal - Based Scenarios: Case Based Reasoning Meets Learning by Doing, in *Case-Based Reasoning, Experiences, Lessons and Future Directions*, (ed. D. Leake), The AAAI press, The MIT press, pp. 295 - 347.
- Schank, R. and Slade, S. (1991) The Future of Artificial Intelligence: Learning From Experience, *Applied Artificial Intelligence*, 5, pp. 97-107.
- Spafford, E.H. and Kumar, S. (1995) Pattern Matching Model for Misuse Intrusion Detection, *Purdue University*. Available online at URL: «<http://www.cs.purdue.edu>»
- Spirakis, P., Katsikas, S., Gritzalis, D., Allegre, F., Androultsopoulos, D., Darzentas, J., Gigante, C., Karagiannis, D. and Spyrou, T. (1995) SECURENET: A network-oriented intelligent intrusion prevention and detection system, *European RACE Programme (SECURENET (R2057) Project)*.
- Spyrou, T. and Darzentas, J. (1995b) Intention Modelling: Approximating Computer User Intentions for Detection and Prediction of Intrusions, *Research Laboratory of Samos, Department of Mathematics, University of the Aegean*.
- Spyrou, T. and Telesco, R. (1995a) Combining Techniques from Intelligent Decision Support Systems: An Application in Network Security, *6th meeting of EURO Working group on DSS, Samos, Greece*. (eds. Darzentas, J. Darzentas. Jenny. S. and Spyrou T.), University of the Aegean.
- Stallings, W. and Hall, P. (1995) *Network and Internetwork Security Principles and Practice*, IEEE Press.
- Staniford-Chen, S., Cheung, S., Crawford, R., Dilger, M., Frank, J., Hoagland, J., Levitt, K., Wee, C., Yip, R. and Zerkle, D. (1996) GrIDS: A Graph Based Intrudion Detection Systems for Large Networks, *University of California*. Available online at URL: «<http://www.cs.ucdavis.edu>»
- Theodoropoulos, N. and Tzamos, T. (1996) SECURENET: An intelligent System for Detecting and Preventing Attacks in Open Networks, Final Project Report *European RACE Programme (SECURENET II (R2113) Project)*.
- Traphoener, R. (1995) INRECA Documentation, *Esprit Project 6322, University of Kaiserlautern*. Available online at URL: «<ftp://ftpagr.informatik.uni-kl.de>»
- Wess, S., Althoff, K. and Derwand, G. (1995) Using k-d Trees to Improve the retrieval Step on Case - Based Reasoning, *University of Kaiserlautern* Available on online at URL: «<http://wwwagr.informatik.uni-kl.de>»
- Wooldridge, M. and Nicholas R.J. (1994) Intelligent Agents: Theory and Practice, *Knowledge Engineering Review*, 115-152.
- Zerkle, D. and Levitt, K. (1995) NetKuang - A Multi-host Configuration Vulnerability Checker, *University of California*. Available online at URL: «<http://www.cs.ucdavis.edu>»



- Κιουντούζης, Ε. (1994) *Ασφάλεια Πληροφοριακών Συστημάτων*. Εκδόσεις Ευγ.
Μπένου, Αθήνα.
- Κοκολάκης, Σ. (1994) Χρήση Τεχνικών Τεχνητής Νοημοσύνης στην Ασφάλεια
Πληροφοριακλων, *Οικονομικό Πανεπιστήμιο Αθηνών*.
- Σπύρου, Θ., Δαρζέντας, Ι. (1992) Τεχνητή Νοημοσύνη και Ασφάλεια Συστημάτων
Πληροφορικής, *Πανεπιστήμιο Αιγαίου*

7. ΠΑΡΑΡΤΗΜΑ

Στο πρώτο μέρος του παραρτήματος περιγράφονται συνοπτικά μερικά συστήματα ανίχνευσης εισβολών. Αποτελούν συστήματα όχι τόσο μεγάλης κλίμακας όπως αυτά που έχουν ήδη περιγραφεί στο πρώτο μέρος της εργασίας, αλλά ενδιαφέροντα συστήματα ως προς τις μεθοδολογίες και τεχνικές που ενσωματώνουν, παρέχοντας ενδείξεις για την κατάσταση που επικρατεί στον χώρο της ανίχνευσης εισβολών.

Στο δεύτερο μέρος γίνεται αναφορά σε δυνατότητες ενοποίηση CBR με τεχνικές induction (οι τεχνικές αυτές έχουν ήδη χρησιμοποιηθεί σε συστήματα CBR, με πολύ καλά αποτελέσματα απόδοσης(Althoff 1995)). Δίδεται επίσης έμφαση στη διαδικασία εκμάθησης και παρατίθενται χρήσιμες παρατηρήσεις.

Στο τρίτο και τελευταίο μέρος του Παραρτήματος περιγράφεται ένα στιγμιότυπο του χώρου προβλημάτων με την γλώσσα αναπαράστασης CASUEL (Bergmann 1994). Στη συνέχεια εισήχθηκε η βάση γνώσης στο εργαλείο CBR Works (Richter 1996) και παρατίθενται χαρακτηριστικές οθόνες κατά τη λειτουργία του.

Παρουσίαση γνωστών Συστημάτων Ανίχνευσης Εισβολών

HAYSTACK (Anomaly and misuse detection, non Real Time, Host Based)

Αποτελεί IDS (Mukherjee 1994) που αποσκοπεί στην ανακάλυψη παρεισφρήσεων σε συστήματα mainframe (Unisys 1100 / 2200), για την προστασία των ευαίσθητων πληροφοριών που αυτά περιέχουν. Αποτελείται από δύο ενότητες προγραμμάτων. Η πρώτη, εγκατεστημένη στο mainframe, συλλέγει τις αναγκαίες πληροφορίες για την κίνηση των χρηστών (log files, audit data) και αφού τις μετατρέψει σε κατάλληλη μορφή, μεταφέρονται μέσω μαγνητικής ταινίας ή ειδικής γραμμής επικοινωνίας στην άλλη ενότητα, για επεξεργασία. Αυτή έχει εγκατασταθεί σε ένα κοινό PC, όπου επεξεργάζεται τα δεδομένα προσπαθώντας να ανακαλύψει σκόπιμες παραβιάσεις από εισβολείς, masquerade attacks, πληροφορίες που έχουν διαρρεύσει, μοχθηρή (malicious) χρήστη του συστήματος. Εάν ανακαλύψει ανώμαλη συμπεριφορά, μεταφέρει στον υπεύθυνο ασφαλείας την αντίστοιχη πληροφόρηση, ενώ του παρέχει δυνατότητες διαχείρισης της βάσης δεδομένων που διατηρεί. Στοιχεία απόδοσης έχουν δείξει πως μιας μέρας audit πληροφορία, χρειάζονται επεξεργασία λίγων ωρών για ανακάλυψη εισβολής (δεν μπορεί να χρησιμοποιηθεί σε real time βάση).

MIDAS (Anomaly and misuse detection, Real Time, Host Based)

Αποτελεί έμπειρο σύστημα (Mukherjee 1994), το οποίο μπορεί να παρακολουθεί ένα υπολογιστικό σύστημα (mainframe της NCSC) για αναγνώριση εισβολών σε συνθήκες πραγματικού χρόνου. Στηρίζεται στην στατιστική ανάλυση της δραστηριότητας των χρηστών, την δημιουργία προφίλ δράσης για κάθε χρήστη, όπου θα καταγράφεται η φυσιολογική του συμπεριφορά, οι νόρμες και συνήθειές του. Εάν ένας χρήστη δείξει συμπεριφορά που διαφέρει στατιστικά από την καθιερωμένη, αυξάνεται η υποψία του συστήματος, για πιθανό εισβολέα.

Υπάρχουν ειδικοί κανόνες, που εάν συμβούν οι προϋποθέσεις και ενεργοποιηθούν, είναι αρκετοί για να σταλθεί ένα επείγον σήμα στον διαχειριστή ασφαλείας. Μια άλλη κατηγορία κανόνων σχετίζεται με την εν γένει συμπεριφορά του όλου συστήματος. Είναι αντίστοιχοι με τους κανόνες για την συμπεριφορά των χρηστών, μόνο που ενεργοποιούνται εάν προκύψουν “παράξενες” συνθήκες σε ολόκληρο το σύστημα.

Wisdom and Sense (Anomaly detection, Real Time, Host Based)

Αποτελεί έμπειρο σύστημα (Mukherjee 1994) βασισμένο στην στατιστική ανάλυση της δράσης των χρηστών και παρακολουθεί, σε συνθήκες πραγματικού χρόνου, τη δραστηριότητα VAX/VMS υπολογιστών. Στόχος του W&S αποτελεί η ανακάλυψη εισβολών, ανώμαλης συμπεριφοράς και ιών. Από τα audit trails, δημιουργούνται κανόνες, σύμφωνα με κάθε εγγραφή των πληροφοριών αυτών (audit records), και κατακρατούνται στοιχεία όπως το όνομα του χρήστη, τις διεργασίες που



εκτελούνται στο λογαριασμό του, τα δικαιώματά του στο σύστημα, το ποσοστό των πόρων που χρησιμοποιεί.

Οι κανόνες που δημιουργούνται, οργανώνονται σε δένδρα και σύνολα δένδρων (δάση). Είναι αναγνώσιμοι και μπορούν να αλλαχθούν από το διαχειριστή ασφαλείας, εάν θέλει κάτι να προσθέσει ή εάν ανακαλύψει ασυνέπειες, ασάφειες. Δημιουργούνται στατιστικά προφίλ για κάθε χρήστη, έτσι ώστε το σύστημα να μπορεί συγκρίνει την τρέχουσα από την εν γένη συμπεριφορά του και να διαπιστώνει εάν παρεκκλίνει από τις νόρμες και διαθέσεις του.

NADIR (Network Anomaly Detection and Intrusion Reporter)

(*Anomaly and misuse detection, non Real Time, Network Based*)

Αποτελεί έμπειρο σύστημα (Mukherjee 1994), που παρακολουθεί την δραστηριότητα δικτύου (Los Alamos National Laboratory). Έχει τη δυνατότητα να παρακολουθεί τη δράση 9.000 χρηστών, οι οποίοι συνδέονται μέσω mainframes έως και απλών τερματικών. Λαμβάνει από το δίκτυο audit trails με τη δράση των χρηστών. Επεξεργάζοντάς τα δίνεται σημασία στην ταυτότητα του χρήστη ο οποίος επιθυμεί κάποια ενέργεια, τη μηχανή μέσω της οποίας ενεργεί, ποια μηχανή του δικτύου προσπαθεί να προσπελάσει, κτλ. Κάθε εβδομάδα τα δεδομένα αυτά τυγχάνουν επεξεργασίας κεντρικά και με τη βοήθεια έμπειρου συστήματος, αποφασίζεται εάν παρατηρείται ανώμαλη συμπεριφορά και πιθανή εισβολή.

Παγίδες προς τους εισβολείς

Έχουν εμφανιστεί τρόποι για την πρόληψη εισβολών, την καταγραφή τους και ανάληψη μέτρων για την αντιμετώπισή τους, οι οποίες βασίζονται στην εξαπάτηση (Cheswick 1992, Cheswick 1990, Bellovin 1990) των εισβολέων. Με τη χρήση κατάλληλων εργαλείων και τεχνικών, γίνεται προσπάθεια μελέτης της δράσης των εισβολέων, των μεθόδων, τρόπων που χρησιμοποιούν για να προσβάλουν το σύστημα. Έπειτα από την μελέτη της συμπεριφοράς τους, γίνεται η καταγραφή της σε log αρχεία. Στόχος είναι η ενημέρωση άλλων διαχειριστών συστημάτων, πιθανών μελλοντικών θυμάτων του ίδιων εισβολέων.

Οι τεχνικές σχετίζονται στη δημιουργία ψεύτικων υπηρεσιών, αλλαγή των υπαρχόντων (ftp, telnet, κτλ), με νέες που έχουν υψηλότερο βαθμό ασφάλειας, αυστηρότερες δικλείδες ασφαλείας και ελέγχονται συνεχώς για την καταγραφή παράτυπης δράσης. Υπάρχουν ψεύτικες μηχανές (dummy servers) οι οποίες προσομοιώνουν τις λειτουργίες UNIX συστημάτων. Μια εντολή της μορφής *rm -rf* (διαγραφή όλων των αρχείων του συστήματος), σε μια τέτοια μηχανή, από κάποιον εισβολέας που έχει καταφέρει να αποκτήσει δικαιώματα υπερχρήστη (root), δεν έχει καμία αρνητική επίπτωση στο σύστημα. Με αυτόν τον τρόπο παραπλανάτε ο (κακόβουλος) εισβολέας, πως δήθεν έχει αποκτήσει δικαιώματα υπερχρήστη και μπορεί ακόμα και να διαγράψει τα πάντα στο σύστημα. Αυτό που πετυχαίνει είναι να δίνει στους διαχειριστές ασφαλείας στίγματα για την συμπεριφορά του στο target system και πληροφορίες για να ανακαλυφθεί η ταυτότητά του.



Άλλες τεχνικές αναφέρονται στην εξαπάτηση πακέτων (packet suckers). Αποτελούν προγράμματα που παρακολουθούν και καταγράφουν τις πληροφορίες που μεταδίδονται και λαμβάνονται από μια υποδοχή (socket), Πολλές απειλητικές προσπάθειες καταγράφονται με αυτόν τον τρόπο από επίδοξους εισβολείς (προσπάθειες για κλοπή του αρχείου των συνθηματικών, παρακολούθησης της δραστηριότητας του δικτύου (network sniffers), κτλ).

Χρήσιμοι είναι οι μηχανισμοί reverse finger. Όταν ένας χρήστης κάνει login στο σύστημα, μπορεί να εντοπιστεί από που συνδέεται με αντίστροφο finger. Μπορούμε να δούμε κάθε στιγμή ποιοι και από που έχουν συνδεθεί και να οδηγηθούμε σε συμπεράσματα για πιθανή εισβολή. Εάν για παράδειγμα αντιληφτούμε τον ίδιο χρήστη να συνδέεται από διαφορετικές γεωγραφικά περιοχές, τότε ίσως πρόκειται για πιθανή εισβολή.

Sukuang, Netkuang

Πολλές από τις περιπτώσεις παραβίασης σε UNIX περιβάλλοντα, προέρχονται από την κακή διάρθρωση, ρύθμιση (misconfiguration) των στοιχείων του συστήματος. Παρόλο που μπορεί να υπάρχουν τεχνικές ασφαλείας, η κακή διάρθρωση των οντοτήτων λογισμικού, μπορεί να κάνει το σύστημα ευπαθές σε εισβολές. Τέτοια συστήματα, που εξετάζουν ένα αυτόνομο κόμβο (παράδειγμα αποτελεί το COPS (Computer Oracle Password and security System)), χρησιμοποιούν ένα σύνολο προγραμμάτων φλοιού (shell scripts), με τα οποία εξετάζουν κακές διαρθρώσεις, ασυνέπειες, γνωστά bugs στο λογισμικό των συστημάτων.

Το Sukuang αποτελεί παρόμοιο σύστημα (Zerkle 1995). Στηριζόμενο σε κανόνες, ελέγχει παραλείψεις στα δικαιώματα προσπέλασης αρχείων, ασυνέπειες στη δομή των ευρετηρίων, κτλ. Οι κανόνες προσπαθούν να εντοπίσουν τον τρόπο με τον οποίο κινείται ο επίδοξος εισβολέας στην προσπάθειά του να επεκτείνει τα δικαιώματά του, να γίνει υπερχρήστης και τελικά να εξαπολύσει την απειλή του στο σύστημα. Παραδείγματα κανόνων που περιέχουν είναι: “ένας χρήστης μπορεί να γράψει σε ένα ευρετήριο, τότε μπορεί να τροποποιήσει όλα τα αρχεία του ευρετηρίου” και “ένας χρήστης που μπορεί να αντικαταστήσει το αρχείο συνθηματικών, μπορεί να αποκτήσει δικαιώματα υπερχρήστη”. Το Sukuang δεν μπορεί να χρησιμοποιηθεί σε δικτυακά περιβάλλοντα.

Αντίθετα, τέτοια συστήματα είναι το SATAN (Security Administration’s Tool for Analyzing Networks), το Internet scanner, τα οποία εξετάζουν ένα δίκτυο για εντοπισμό σημείων τρωτότητας (vulnerabilities). Ελέγχουν για ύποπτες καταστάσεις του δικτύου, κακορυθμισμένο λογισμικό, παλιές εκδόσεις λογισμικού με γνωστά bugs, κτλ. Ένα παρόμοιο σύστημα είναι και το Netkuang.

Στηρίζει την λειτουργία του στο οτι ο χρήστης - εισβολέας προσπαθεί να υλοποιήσει στόχους (goals) και έπειτα από μια σειρά επιτυχημένων προσπαθειών να είναι σε θέση να προσβάλει το δίκτυο. Οι στόχοι του εισβολέα κατηγοριοποιούνται στους εξής: να γίνει χρήστης του συστήματος (να αποκτήσει login και password), να γίνει μέλος μιας ομάδας (group), να αποκτήσει δικαιώματα σε ένα αρχείο (να γράψει, τροποποιήσει, αντικαταστήσει τα περιεχόμενά του). Εάν κάποιος χρήστης, για



παράδειγμα, αποκτήσει δικαιώματα τροποποίησης στο ευρετήριο */etc*, έχει τη δυνατότητα να γίνει υπερχρήστης του συστήματος. Ένα παράδειγμα στόχου μπορεί να είναι: "αντικατέστησε το αρχείο */etc/passwd* στον host *knossos.aueb.gr*)

Άλλα Συστήματα

Κατά καιρούς έχουν αναπτυχθεί και άλλα συστήματα ανίχνευσης εισβολών (Mukherjee 1994), είτε σε επίπεδο παρακολούθησης της λειτουργίας μεμονωμένων υπολογιστών είτε δικτύων, έπεκτείνοντας τις δυνατότητες υπαρχόντων IDS ή στηριζόμενα σε νέες ιδέες και τεχνικές.

To DIDS (Distributed Intrusion Detection System) (*Anomaly and misuse detection, Real Time, Network Based*), για παράδειγμα, επεκτείνει τις δυνατότητες του NSM, προσφέροντας παρακολούθηση του δικτύου από χρήστες που συνδέονται μέσω dial up γραμμών. Καλύπτει την αδυναμία του NSM να οδηγείται σε alert, εάν η πληροφορία που μεταφέρεται είναι κρυπτογραφημένη και αποτελεί επέκτασή του για παρακολούθηση δικτύων ευρείας ζώνης (WAN). Στηρίζεται στην κατανεμημένη παρακολούθηση των δικτυακών λειτουργιών και στο κεντρικό φίλτραρισμα και επεξεργασία τους.

To ISOA (Information Security Officer's Assistant) (*Anomaly and misuse detection, Real Time, Network Based*), αποτελεί εργαλείο για την παρακολούθηση UNIX συστημάτων σε συνθήκες πραγματικού χρόνου. Βασίζεται στην ανάλυση των audit πληροφοριών και στη χρήση έμπειρου συστήματος και στατιστικών μεθόδων για την καταγραφή των προφίλ των χρηστών. Μήνυμα παραβίασης προς τον υπεύθυνο ασφαλείας στέλνεται εάν ξεπεραστούν προκαθορισμένα όρια (thresholds), τα οποία αναλογούν στη διαφορά της τρέχουσας συμπεριφοράς του χρήστη από την προβλεπόμενη.

Παρόμοια είναι η φιλοσοφία του ComputerWatch (*Limited misuse detection, Non Real Time, Host Based*). Διατηρεί στατιστικά στοιχεία για τη συμπεριφορά των χρηστών, για ομάδες χρηστών και για το σύστημα γενικά. Δεν χρησιμοποιείται για real time ανάλυση, ενώ ο διαχειριστής ασφαλείας μπορεί μέσω επερωτήσεων (queries) να αντλήσει πληροφορία για την ύπαρξη απλών παραβιάσεων (security breaches).

To Discovery (*Anomaly detection, Non Real Time, Network Based*) κινείται και αυτό στη διατήρηση στατιστικών προφίλ και ανώτατων ορίων ευαισθησίας, με τη διαφορά πως αναφέρεται στην παρακολούθηση συναλλαγών βάσεων δεδομένων. Έχει δείξει αποτελεσματική λειτουργία σε DBMS με εκατομμύρια εγγραφές, αποκαλύπτοντας προσπάθειες πρόσβασης από μη εξουσιοδοτημένους χρήστες, μη επιτρεπτές συναλλαγές από εξουσιοδοτημένα λογικά υποκείμενα και άκυρες (invalid) συναλλαγές.

Χρήσιμες πληροφορίες για συστήματα ανίχνευσης εισβολών μπορεί να βρει ο αναγνώστης στο (Mukherjee 1994) καθώς και στο URL: <http://www.sri.org>

Ενοποίηση CBR με άλλες τεχνικές

Induction και CBR

Οι έννοιες και τεχνικές που το CBR ενσωματώνει έχουν χρησιμοποιηθεί αποτελεσματικά σε υπο-συστήματα, ενσωματωμένα σε μεγαλύτερα συστήματα, στα οποία βασικό χαρακτηριστικό είναι η «έξυπνη» επεξεργασία των πληροφοριών (έμπειρα συστήματα, συστήματα στήριξης αποφάσεων, κτλ. Η χρήση του CBR με άλλες τεχνικές όπως η επαγωγή (*induction*), μπορεί να αποβεί αποτελεσματική, βελτιώνοντας τις δυνατότητες του CBR. Με το CBR μπορούμε να ανακαλύψουμε ομοιότητες ενός καινούργιου case με κάποιου παλαιότερου. (case αναφοράς). Η χρήση παλαιότερης εμπειρίας αποτελεί θεμελιώδες στοιχείο στη διαδικασία εύρεσης των όμοιων παλαιότερων cases και του τρόπου με τον οποίο θα προσαρμοστούν οι λύσεις τους σε νέα προβλήματα.

Με την επαγωγή (Althoff 1995), μπορούμε αυτόμata να εξάγουμε γνώση από τα cases που έχουμε ήδη στη βάση γνώσης (cases αναφοράς). Οι έννοιες οι οποίες εξάγονται οργανώνονται σε δενδρική μορφή (decision trees). Έπειτα με χρήση κατάλληλων αλγορίθμων μπορεί να ανακτηθεί και να χρησιμοποιηθεί στη διαδικασία επίλυσης προβλημάτων.

Στην περίπτωση των επαγωγικών συστημάτων που χρησιμοποιούν cases, όταν προκύψει η ανάγκη για δημιουργία ενός νέου case, πρέπει να ενημερωθούν οι περιγραφητές που αναφέρονται στις συγκεκριμένες γνωστικές περιοχές της βάσης γνώσης. Αυτό σημαίνει ότι οι περιγραφητές πρέπει να ξαναοριστούν από την αρχή. Αντίθετα με ότι συμβαίνει στα CBR συστήματα, όπου απλά αυτό που αρκεί είναι η τοποθέτηση ενός νέου case στη βάση και η πρόσδωση σε αυτό ενός βαθμού ομοιότητας (similarity measure) για την διακριτοποίησή του με τα υπόλοιπα.

Οι δυο τεχνικές δεν είναι ξένες μεταξύ τους. Μπορούν να συνεργαστούν και να προσδώσουν ικανοποιητικά αποτελέσματα. Οι μηχανισμοί του CBR μπορούν να βοηθήσουν στη διερμηνεία, αναζήτηση και εκμάθηση των cases, ενώ η χρήση των τεχνικών επαγωγής μπορεί να διαδραματίσει συμβουλευτικό ρόλο, ειδικά όταν ο αριθμός των cases έχει αυξηθεί σημαντικά. Με αυτόν τον τρόπο θα υπάρχει δυνατότητα φιλτραρίσματος των πληροφοριών, αιτιολόγησης κάποιας απόφασης, μέσω των αφαιρετικών δομών που χρησιμοποιούν (δένδρα, κτλ.).

Χρήση δένδρων στη δόμηση των cases

Η χρήση δένδρων έχει χρησιμοποιηθεί ως μέρος CBR συστημάτων για καλυτέρευση των δεικτών δεικτοδότησης και αναζήτησης των cases. Η χρήση κ-*d* trees (Wess 1995), έχει δείξει θετικά αποτελέσματα στην οργάνωση των cases σε μια βάση γνώσης.

Μια από τις γνωστότερες τεχνικές αναζήτησης cases στη βάση είναι αυτή της nearest neighbor search. Τα cases μπορούν να παρασταθούν ως σημεία σε

πολυδιάστατο χώρο αναζήτησης όπου τα χαρακτηριστικά των cases αντιστοιχούν σε ξεχωριστές διαστάσεις. Με τη χρήση ενός δυαδικού δένδρου αναζήτησης πολλών διαστάσεων (k-d Tree) μπορούμε να αναζητήσουμε τα περισσότερο όμοια cases (nearest neighbors) με κάποιο δοσμένο case, σε ένα σύνολο n cases που το καθένα περιγράφεται με k διαστάσεις.

Το δένδρο που δημιουργείται μπορεί να παρασταθεί ως ένα πολυδιάστατο οργανωμένο δίκτυο, οι κόμβοι του οποίου έχουν οργανωθεί με τέτοιο τρόπο ώστε να πετυχαίνεται αποτελεσματικότερη αναζήτηση των cases που κάθε φορά ζητούνται. Με βάση των ομοιότητα των cases αυτά αναλογούν στο δένδρο σε αντιστοιχα φύλλα του. Κάθε κόμβος του δένδρου απαρτίζεται - οδηγεί σε ένα σύνολο από cases ενώ ο κόμβος - ρίζα αναπαριστά το σύνολο της βάσης γνώσης. Κάθε φύλλο του δένδρου αντιστοιχεί σε ένα σύνολο από cases, τα οποία έχουν συγκεκριμένα όμοια χαρακτηριστικά μεταξύ τους. Η δημιουργία της καλύτερης δυνατής οργάνωσης του δένδρου είναι κρίσιμο σημείο, ώστε αυτό να παραμένει ισορροπημένο (και αναδρομικά για κάθε ένα από τους εσωτερικούς κλάδους του).

Μια μέθοδος για τον υπολογισμό των βαρών (Auriol 1995) σε ένα σύστημα που υλοποιεί CBR με χρήση k-d trees είναι:

$$\text{SIM}(\alpha, \beta) = \sum w_{ij} \times \text{sim}_i(A_i(\beta), A_i(\beta))$$

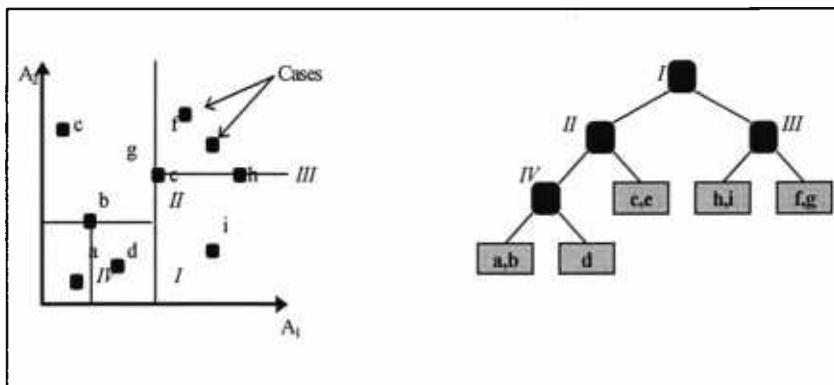
Στόχος είναι η αποφυγή αναζήτησης όλων των cases της βάσης γνώσης με την κάθε εμφάνιση ενός καινούργιου. Για το σκοπό αυτό καθορίζεται μια τιμή καθολικής ομοιότητας (similarity) SIM η οποία υπολογίζεται και αποθηκεύεται στο δένδρο περιέχοντας την ομοιότητα των cases α και β ($\text{SIM}(\alpha, \beta)$). Ταυτόχρονα διατηρούνται μικρότερης κλίμακας ομοιότητες («τοπικές») sim , μεταξύ των p χαρακτηριστικών A_i από τα οποία αποτελούνται τα cases. (η τιμή $A_i(\alpha)$ αντιστοιχεί στην τιμή του A_i χαρακτηριστικού του case α).

Οι αρχικές τιμές των δεικτών τίθενται χειρωνακτικά, ενώ αλλάζουν σταδιακά με την πάροδο του χρόνου. Η συμμετοχή του χρήστη στη διαδικασία υλοποίησης του συστήματος είναι αρκετά σημαντική, δεδομένου ότι χρειάζεται γνώση για τον κατάλληλο χαρακτηρισμό των cases με συγκεκριμένο βάρος - αξία, μια αρκετά επιρρεπής σε σφάλματα διαδικασία, γι' αυτό και στόχος των συστημάτων είναι να την περιορίσουν στον μικρότερο δυνατό βαθμό.

Για τον υπολογισμό της ομοιότητας (similarity) μεταξύ των cases μπορούν να χρησιμοποιηθούν πολλοί αλγόριθμοι. Η μέθοδος η οποία είναι κοινά αποδεκτή για την αποτελεσματικότητά της και έχει εφαρμοστεί σε πολλά συστήματα ανάκτησης πληροφοριών είναι αυτή που βασίζεται στην εντροπία (Salton 1989). Αποτελεί μέθοδο προσδιορισμού του περιεχομένου της πληροφορίας (information content) ενός όρου - χαρακτηριστικού μιας συλλογής - βάση γνώσης. Όσο μεγαλύτερο το information content ενός χαρακτηριστικού, τόσο καλύτερα μπορεί να χρησιμοποιηθεί για indexing (περιέχει καλύτερη πληροφορία για τον διαχωρισμό του (discrimination value) σε σχέση με τα άλλα στοιχεία της συλλογής).

Για την εύρεση του περισσότερου όμοιου case στο k-d tree, οδηγούμαστε βάση του βαθμού ομοιότητας που θέλουμε να πετύχουμε από τα κλαδιά του δένδρου σε κάποιο φύλο το οποίο περιέχει εκείνα τα cases που μπορεί να χρησιμοποιηθούν. Από αυτά, εκείνο με τον μεγαλύτερο βαθμό ομοιότητας θα χρησιμοποιηθεί ως πηγή για την εύρεση λύσης στο νέο μας πρόβλημα. Εάν αναζητούμε ένα σύνολο από n cases, μπορούμε, με την χρήση μιας ουράς να διατηρούμε τα cases με την καλύτερη τιμή ομοιότητας με το αρχικό. Στο τέλος της διάσχισης του δένδρου θα έχουμε αποθηκεύσει στην ουρά τα n cases τα οποία αποτελούν αντιπροσωπευτικότερα δείγματα για τη λύση του προβλήματος.

Στο παρακάτω σχήμα περιγράφεται ένας διδιάστατος χώρος σε αντίστοιχο 2-d δένδρο. Το βασικότερο μέρος στην διαδικασία κατασκευής του δένδρου είναι η παράμετρος τεμαχισμού (*partitioning attribute*). Αυτή καθορίζει σε πόσα τμήματα θα χωριστεί αρχικά ο χώρος στον οποίο αναφερόμαστε και στον οποίο περιγράφονται τα cases με βάση τα βάρη τους. Αρχικά επιλέγεται το αρχικό case το οποίο μπορεί να θεωρηθεί οτι «βρίσκεται στο κέντρο» του χώρου που βρίσκονται τα cases (με βάση τα βάρη που του αντιστοιχούν στις δύο διαστάσεις). Αφού η παράμετρος τεμαχισμού είναι δύο, ο χώρος τεμαχίζεται σε δύο μέρη. Αυτά αντιστοιχούν στα δύο πρώτα κλαδιά από τη ρίζα του δένδρου που δημιουργείται. Η διαδικασία επαναλαμβάνεται αναδρομικά σε κάθε ένα από τα μέρη που έχουν δημιουργηθεί. Το σύνολο των εναπομεινάντων τα οποία δεν χωρίζονται περαιτέρω (σταματάει η αναδρομή), αποτελεί έναν αριθμό που έχει οριστεί ως bucket size. Αποτελεί τον μέγιστο αριθμό των cases, (ο οποίος έχει καθοριστεί εξ' αρχής) που μπορεί να περιλαμβάνει κάθε φύλλο του δένδρου.



Εικόνα 1. Ένας χώρος αναζήτησης δύο διαστάσεων και το αντίστοιχο k-d δένδρο

Μια πιο λεπτομερή ματιά στη διαδικασία εκμάθησης

Στην προσπάθειά μας να επιλύσουμε κάποιο καινούργιο πρόβλημα, συχνά θυμόμαστε παρελθούσες καταστάσεις, οι λύσεις των οποίων αν προσαρμοστούν, μπορούν να ταιριάζουν με το νέο πρόβλημα. Οι προβληματικές καταστάσεις με τις λύσεις και τις επεξηγήσεις βρίσκονται οργανωμένες σε δομές μνήμης. Η διαδικασία εκμάθησης πραγματοποιείται όταν αυτές οι δομές πρέπει να αλλαχθούν. Αρχίζουμε να μαθαίνουμε όταν κατά τη διαδικασία επεξεργασίας των δομών αυτών παρουσιάστηκαν ανωμαλίες, δεν ακολουθήθηκε η προβλεπόμενη σειρά στην εκτέλεση γεγονότων, δεν

υλοποιήθηκε από κάποιον αυτό που είχε αναλάβει να πραγματοποιήσει, ή μια πράξη που πραγματοποιήσαμε είχε ένα αναπάντεχο διαφορετικό αποτέλεσμα.

Όταν ανακαλύπτουμε τον εαυτό μας σε μια ασυνήθιστη κατάσταση, την χαρακτηρίζουμε ως τέτοια γιατί δεν έχουμε βρεθεί σε αντίστοιχες καταστάσεις στο παρελθόν. Αυτή η κατάσταση αποτελεί και την κινητήρια δύναμη για την διαδικασία εκμάθησης. Θέλουμε να θυμόμαστε την καινούργια αυτή κατάσταση, έτσι ώστε να την ανακτήσουμε από την μνήμη όταν παρουσιαστεί κάποια αντίστοιχη στο μέλλον. Αυτή η αποτυχία είναι ουσιαστικά και η διαδικασία που ωθεί στην δημιουργία μιας καινούργιας κατάστασης, ενός καινούργιου case, οδηγώντας μας στον χαρακτηρισμό *case-based learning* ή *learning from experience* (Schank 1991).

Όσο περισσότερο παραστατική και έντονη είναι η εμπειρία μας, τόσο διευκολύνεται και η διαδικασία εκμάθησής μας. Η εμπειρία για να χρησιμοποιείται σωστά και άμεσα όταν αυτή χρειάζεται, πρέπει να είναι οργανωμένη με τον καλύτερο δυνατό τρόπο. Δεν είμαστε σε θέση να μάθουμε εάν δεν έχουμε οργανωμένη ην εμπειρία σε κατάλληλες δομές μνήμης και δεν είμαστε σε θέση να τροποποιούμε τις δομές αυτές εύκολα. Μεταφέροντας το πρόβλημα στον τομέα των CBR συστημάτων, προκειμένου να «μάθουν» για ένα καινούργιο case, πρέπει αρχικά να υπάρχει κάποιο παρόμοιο στη μνήμη - βάση των cases. Όταν το ήδη υπάρχον case μας οδηγήσει σε κατάσταση που δεν είναι προβλεπόμενη (προτείνει λύση για κάποιο πρόβλημα η οποία δεν είναι αποδεκτή, παρουσιαστούν κενά - ασυνέπειες στη διαδικασία επίλυσης, κτλ) τότε ένα νέο δημιουργείται. Απαιτείται η σύγκριση με το ήδη υπάρχον προκειμένου να ανεβρεθούν κάποια κοινά στοιχεία που μπορούν να υιοθετηθούν και αναπαριστά με τη σειρά του μια καινούργια κατάσταση στην οργανωμένη διάταξη των cases στη μνήμη.

Η αποτυχία κάποιου παλαιότερου case να παρουσιάσει ικανοποιητική λύση, παρακινεί το σύστημα σε μια ώθηση για εκμάθηση (Schank 1996). Από τη στιγμή που θα παρουσιαστεί η ανάγκη για δημιουργία του καινούργιου case, πρέπει να αποθηκευτεί με τέτοιο τρόπο στις δομές μνήμης, έτσι ώστε να είναι ικανή η μελλοντική ανάκτησή του για την εφαρμογή του. Το καινούργιο case περιέχει πολλά κοινά στοιχεία με το ήδη υπάρχον - από το οποίο και προήλθε- και επιπλέον χαρακτηριστικά τα οποία σχετίζονται με συγκεκριμένες προσδοκίες που διατηρούμε οτι θα μπορέσει να αντιμετωπίσει το νέο case.

Η διαδικασία εκμάθησης από τον reasoner μπορεί ειδωθεί και σαν ένας έξυπνος τρόπος κατηγοριοποίησης των αντικειμένων (cases), στο χώρο των k- διαστάσεων που αναφέρονται (Globig 1995). Στο πεδίο του CBR χρησιμοποιούνται τεχνικές nearest neighbor για την κατηγοριοποίηση των cases στο συγκεκριμένο πεδίο γνώσης που κάθε φορά αναφέρεται. Η βασική ιδέα είναι η χρησιμοποίηση γνώσης ήδη γνωστών cases στην επίλυση νέων προβλημάτων. Αυτό πραγματοποιείται σε όλη τη διάρκεια του κύκλου του CBR, από την αρχική αναζήτηση παρόμοιων περιγραφητών έως την εκμάθηση νέων τρόπων λύσης και ενσωμάτωσή τους σε παλαιότερα cases με τη διεύρυνση αυτών ή τη δημιουργία νέων cases, όπως έχει ήδη περιγραφεί σε παραπάνω σημείο.

Μπορούμε να θεωρήσουμε τα cases ως δυάδες $(x, \text{class}(x))$, όπου x είναι η περιγραφή του case και $\text{class}(x)$ η κατηγοριοποίησή του σε συγκεκριμένο χώρο. Δοθέντος ενός νέου case με άγνωστη κατηγοριοποίηση $(y,?)$, στόχος του συστήματος είναι η εύρεση στην βάση γνώση που διατηρεί (Case Base, CB), του πλησιέστερου γείτονα (nearest neighbor) $(x, \text{class}(x))$, δοθέντος ενός μέτρου απόστασης (distance measure) d . Έπειτα θεωρεί οτι η κατηγοριοποίηση $\text{class}(x)$ του πλησιέστερου γείτονα είναι και η κατηγοριοποίηση του μη κατηγοριοποιημένου case $(y,?)$. $(y, \text{class}(x))$.

Σε αντίθεση με άλλες μεθόδους οι οποίες χρησιμοποιούν την έννοια της έννοιας - γνώσης σχετικά με κάποιο χώρο (problem domain) ρητά (συστήματα κανόνων, δένδρων), στα case based συστήματα η γνώση περιγράφεται υποκειμενικά από το ζεύγος (CB, d).

Ενας απλός αλγόριθμος ο οποίος χρησιμοποιείται για εκμάθηση σε CBR συστήματα μπορεί να περιγραφεί ως εξής:

1. Ορίζουμε τη βάση γνώσης $CB = \{\}$ και αρχικοποιούμε το distance measure d
2. Με την εμφάνιση ενός νέου case: $(y, \text{class}(y))$
3. Αναζήτησε στη βάση γνώσης CB για κάποιο case: $(x, \text{class}(x)) \in CB$ τέτοιο ώστε η απόσταση d μεταξύ τους να είναι η ελάχιστη $d_{\min}(y, x)$
4. Εάν η $\text{class}(y)$ δεν υπάρχει $((y, ?))$ τότε:
 - (a) Όρισε την $\text{class}(x)$ ως την κατηγορία στην οποία θα ανήκει και το $(y, ?)$ $(y, \text{class}(x))$
 - (β) Ζήτησε την γνώμη του χρήστη για την εύρεση $\text{class}(y)$ του $(y, ?)$
5. Εάν $\text{class}(y) = \text{class}(x)$ τότε η κατηγοριοποίηση είναι σωστή αλλιώς η κατηγοριοποίηση είναι λάθος.
6. Τροποποίησε το d ή και την βάση γνώσης CB σε σχέση με την κατηγοριοποίηση που έχει ήδη γίνει
7. Ξεκίνα τον αλγόριθμο ξανά από το βήμα 2

Το σύστημα τελικά μπορεί να εκπαιδευτεί είτε αλλάζοντας τη βάση γνώσης CB , είτε και από την αλλαγή του d . Κατά τη διάρκεια της εκμάθησης το σύστημα δέχεται μια ακολουθία από cases X_1, X_2, \dots, X_k με $X_i = (x_i, \text{class}(x_i))$ και εκδίδει μια σειρά από ζεύγη $(CB_1, d_1), (CB_2, d_2), \dots, (CB_k, d_k)$ τέτοια ώστε $CB_i \in \{X_1, X_2, \dots, X_k\}$. Στόχος είναι να βρεθεί ένα ζευγάρι (CB_n, d_n) τέτοιο ώστε να μην χρειάζεται περαιτέρω αλλαγή (Έπειτα $\forall m \geq n$ $(CB_n, d_n) = (CB_m, d_m)$), δεδομένου οτι αποτελούν καλό κατηγοριοποιητή για την γνώση που περιέχεται C .

Η διαδικασία της εκμάθησης δεν είναι μόνο χαρακτηριστικό των CBR συστημάτων. Και άλλα συστήματα χρησιμοποιούν μεθόδους εκμάθησης, δεδομένων των θετικών αποτελεσμάτων που αυτή μπορεί να επιφέρει σε ένα σύστημα λήψης αποφάσεων. Παρόλ' αυτά όμως το CBR πλεονεκτεί σε πολλά σημεία σε σχέση με άλλα συστήματα. Για περισσότερες πληροφορίες ο αναγνώστης μπορεί να απευθυνθεί στο (Anthony 1995) όπου παρουσιάζονται ενδιαφέροντα θέματα αξιολόγησης των CBR με Control Rule Learning (CRL) συστήματα. (Τα CRL συστήματα στηρίζονται σε μια βιβλιοθήκη κανόνων ελέγχου (*control rule library*), τους οποίους εφαρμόζει δίνοντας τη δυνατότητα στο σύστημα να αποδέχεται ή να απορρίπτει διάφορες καταστάσεις -



συνθήκες από τις οποίες περνάει. Με αυτόν τον τρόπο δημιουργείται ένα μονοπάτι - στο δένδρο των κανόνων - που εμπεριέχει τις λύσεις, για κάποιο πρόβλημα, και το οποίο αποθηκεύεται για μελλοντική χρήση.)

Περιγραφή της γνώσης με τη γλώσσα CASUEL και οθόνες από το CBRWorks

Παρουσιάζεται η βάση γνώσης του χώρου με τη γλώσσα CASUEL. Δημιουργούνται πέντε αρχεία καθένα από τα οποία περιγράφει συγκεκριμένες ιδιότητες της βάσης γνώσης.

Το «**security_domain.domain**» αποτελεί το βασικό αρχείο στην αναπαράσταση της γνώσης. Περιγράφει τα βασικά στοιχεία της βάσης. Το όνομα της δομής της γνώσης (context), το ζητούμενο πεδίο από κάθε case (το οποίο και προτείνεται ως λύση για την αντιμετώπιση της απειλής), το στοιχείο (attribute) αναφοράς του case

```
defdomain security_domain
  declaration_file "security_domain.types"
  "security_domain.values" "security_domain.slots"
  "security_domain.objects" ;
  case_file "security_domain.cases" ;
  case_structure Context;
  target Context Cm_Subject;
  case_reference Context Hypothesis_type;
  languages greek french english japaneesee english.
```

Στο «**security_domain, objects**» αναφέρονται τα ονόματα των attributes από τα οποία αποτελείται η βάση των cases.

```
defclass Context
  a_kind_of class;
  slots Node_id User_id Level_of_Penetration
  Hypothesis_type Level_of_Confidence System_id
  Time Params Cm_Description Cm_Subject
  Num_Params Attack_Class.
```

Στο «**security_domain.types**» ορίζονται οι καινούργιοι τύποι δεδομένων οι οποίοι δημιουργούνται για τις ανάγκες του συγκεκριμένου χώρου προβλημάτων καθώς και οι τιμές που αυτοί μπορούν να πάρουν.

```
deftype System_Id_Type_Definition
    a_kind_of taxonomy;
    range [Expert_SystemNeural_NetworkUser_Intention_Identification].

deftype Attack_class_Type_Definition
    a_kind_of taxonomy;
    range
[No_AttackTrojan_HorseLogic_BombInsider_AttackPassword_CrackingSystem_Progr
amming_AttacksOutsider_Access_ViolationDenial_of_ServiceTrapdoor_AttackKnow
n_Attack].

deftype Level_of_Penetration_Type_Definition
    a_kind_of integer;
    range [1..10].

deftype Node_id_Type_Definition
    a_kind_of taxonomy;
    range
[dias_aueb_grknossos_aueb_grfaestos_aueb_grposeidon_aueb_grminoas_aueb_gr].

deftype Cm_Subject_Type_Description
    a_kind_of taxonomy;
    range
[Alert_the_system_managerGrab_a_snapshot_of_the_process_tableTune_the_level
_if_auditing_securityAsk_the_user_for_their_password_X_Window_Version_Ask_
the_user_for_their_password_TTY_Version_Kill_a_process_or_a_parent_of_a_pr
ocessLog_out_a_userSuspend_a_user_s_login_accountRestrict_access_to_a_servi
ce_NISRestrict_access_to_a_service_CRONRestrict_access_to_a_service_MAILRes
trict_access_to_a_service_ROUTERestrice_access_to_a_nodeShutdown_service_NI
SShutdown_service_CRONShutdown_service_MAILShutdown_service_ROUTEPut_a_node
_onto_emergency_modeShutdown_a_node].

deftype Level_of_Confidence_Type_Definition
    a_kind_of integer;
    range [1..10].
```

Στο «**security_domain.slots**» προσδιορίζονται σε ποιους τύπους δεδομένων αντιστοιχούν τα attributes.

```
defslot Num_Params of Context
    type integer.

defslot User_id of Context
    type string.

defslot Level_of_Penetration of Context
    type Level_of_Penetration_Type_Definition;
    question english "The Level of Penetration value...".

defslot Level_of_Confidence of Context
    type Level_of_Confidence_Type_Definition;
    question english "The Level of Confidence value...".

defslot Node_id of Context
    type Node_id_Type_Definition;
    question english "Which is the node proposing the alert ?".

defslot System_id of Context
    type System_Id_Type_Definition;
    question english "The system Id value ...".

defslot Params of Context
    type string;
    question english "Which are the Params ?".

defslot Cm_Description of Context
    type string;
    question english "This is the Countermeasure Description ...".

defslot Cm_Subject of Context
    type Cm_Subject_Type_Description.

defslot Time of Context
    type integer.

defslot Hypothesis_type of Context
    type integer;
    question english "What is the Hypothesis_Type value ?".

defslot Attack_Class of Context
    type Attack_class_Type_Definition.
```

Τέλος το «**security_domain.cases**» περιλαμβάνει τα cases αποτελούν τη βάση γνώσης. Ενδεικτικά παρουσιάζονται μερικά από αυτά:

```
defcase 1
objects
    case Case1
        Attack_Class: System Programming Attack,
        Cm_Description: «This countmeasure will
        ask the user for his password again. They
        will be logged out if an incorrect answer is given three
        times»,
        Cm_Subject: Ask the user for their
        password,
        Hypothesis_Type: 610010,
        Level_of_Confidence: 9,
        Level_of_Penetration: 9,
        Node_id: dias.aueb.gr,
        Num_Params: 5,
        Params: «R10010: A Trojan Horse has been
        prepared|User=mgk |file=/users/evil/mybinsh/
        |Owner=evil|Group=other»,
        System_id: Expert System,
        Time: 809350118,
        User: mgk.

defcase 2
objects
    case Case2
        Attack_Class: Trojan Horse,
        Cm_Description: «Alert the system manager for the acts of
        the user ...»,
        Cm_Subject: Alert the system manager,
        Hypothesis_Type: 610005,
        Level_of_Confidence: 1,
        Level_of_Penetration: 9,
        Node_id: knossos.aueb.gr,
        Num_Params: 6,
        Params: «R10005: Probable Trojan Horse has
        been prepared|User=evil|file=/users/evil/
        files/sgid_file/|Owner=evil|Group=other|Path\users/hacke
        r|Home_path=/users/hacker»,
        System_id: Expert System,
        Time: 8091888358,
        User: evil.

defcase 3
objects
    case Case3
        Attack_Class: Insider Attack,
        Cm_Description: «Suspend users account for
        2 weeks. This will help the user to think
        about his evil behavior...»,
        Cm_Subject: Suspend the users login account,
        Hypothesis_Type: 610110,
        Level_of_Confidence: 9,
        Level_of_Penetration: 6,
        Node_id: faestos.aueb.gr,
        Num_Params: 3,
        Params: «R610110: Probable Insider Attack
        has been prepared|User=mike|Owner=mike|
        Group=other| Path=/users/hacker»,
```

```

System_id: User Intention Identification,
Time: 809453423,
User: mike.

defcase 4
objects
case Case4
Attack_Class: Password Cracking,
Cm_Description: «The user must logout immediately because
this will cause unpredictable results to the system...»,
Cm_Subject: Log out a user,
Hypothesis_Type: 620002,
Level_of_Confidence: 4,
Level_of_Penetration: 6,
Node_id: minoas.aueb.gr,
Num_Params: 4,
Params: «R610110: Probable Insider Attack
has been prepared|User=john...»,
System_id: Neural Network,
Time: 809362342,
User: john.

defcase 5
objects
case Case5
Attack_Class: Denial of Service,
Cm_Description: «The table of processes must be examined
in order to find out if the services are closed
intentionally...»,
Cm_Subject: Grab a snapshot of the process table,
Hypothesis_Type: 610115,
Level_of_Confidence: 8,
Level_of_Penetration: 4,
Node_id: poseidon.aueb.gr,
Num_Params: 4,
Params: «R610115: Probable Denial of
service has been prepared|User=webmaster|
file=/usr/local/etc/ httpd/...»,
System_id: Neural Network,
Time: 809123234,
User: webmaster.

```

Η βάση γνώσης αφού περιγράφηκε με την γλώσσα αναπαράστασης CASUEL, εισήχθηκε στο CBRWorks προκειμένου να επεξεργαστεί. Στις παρακάτω οθόνες παρουσιάζονται αντιπροσωπευτικά δείγματα από τη λειτουργία του συστήματος.

The screenshot shows the CBR-Works Case Base application window. On the left, there is a 'Case-List' pane containing entries for Case1, Case2, Case3, Case4, and Case5. To the right, there are two main sections: 'Attributes' and 'Case1' and 'Case2'. The 'Attributes' section lists various parameters like attackClass, cmDescription, cmSubject, etc., with their corresponding values. Below these are two rows for 'Case1' and 'Case2', each showing the same set of attributes with slightly different values. At the bottom of the window, there are status indicators: 'Mod: CBa', '#C: 5', and '#Att: 12'.

	Attributes	Case1	Case2
attackClass	System Programming AI Trojan Horse		
cmDescription	This Countermeasure w Alert the system, manag		
cmSubject	Ask the user for their p Alert the system manag		
hypothesisType	610010	610005	
levelOfConfidence	9	1	
levelOfPenetration	9	9	
nodeId	dias.aueb.gr	knossos.aueb.gr	
numParams	5	6	
params	R10010:Trojan Horse h R10005c:Probable Troj		
systemId	Expert System	Expert System	
time	809350118	809188835	
userId	mgk	evil	

Στην οθόνη δείχνεται ο τρόπος παράστασης των cases, με το CBRWorks.

The screenshot shows the CBR Works Query Editor window. It displays a table with columns for 'Attributes', 'Case3', 'Filter', and 'Weights'. The 'Attributes' column lists various parameters. The 'Case3' column shows specific values for each parameter. The 'Filter' column contains filter operators like '=', '~=' or 'noFilter'. The 'Weights' column lists numerical values ranging from 50 to 700. The table is as follows:

Attributes	Case3	Filter	Weights
attackClass		noFilter	1
cmDescription		noFilter	1
cmSubject		noFilter	1
hypothesisType	610110	=	700
levelOfConfidence	9	=	600
levelOfPenetration	6	noFilter	700
nodeId	faestos.aueb.gr	noFilter	50
numParams	3	noFilter	50
params	R610110:Probable Insic	noFilter	50
systemId	User Intention Identifica	noFilter	50
time	809453423	~ =	100
userId	mike	noFilter	50

Με τον Query Editor μπορούμε να εισάγουμε τιμές για τα attributes που επιθυμούμε. Υπάρχει η δυνατότητα εισαγωγής φίλτρου για τον περιορισμό των αποτελεσμάτων της αναζήτησης. Μπορούμε να αντιστοιχίσουμε με βάρη τα attributes των cases, επηρεάζοντας με αυτόν τον τρόπο τη διαδικασία τις αναζήτησης, δίνοντας έμφαση σε συγκεκριμένες υποθέσεις που θέτουμε.

CBR-Works Consultation

File Edit Design Tools Retrieval Navigation Help

Attributes Query Case1

attackClass	?	System Programming At	
cmDescription	?	This Countermeasure w	
cmSubject	?	Ask the user for their pa	
hypothesisType	610010	610010	
levelOfConfidence	9	9	
levelOfPenetration	6	9	
nodeId	poseidon.aueb.gr	dias aueb.gr	
numParams	?	5	
params	?	R10010 Trojan Horse h	
systemId	Expert System	Expert System	
time	?	809350118	
userId	mgk	mgk	

Com: User Filter: Weight: Case: 1 of 1 Sim1: 0.593

Στην οθόνη παρουσιάζεται το αποτέλεσμα της αναζήτησης του query case που αναφέραμε προηγούμενα.

CBR-Works Query Editor

File Edit Design Tools Query Help

Attributes Query Filter Weights

attackClass	?	noFilter	1
cmDescription	?	noFilter	1
cmSubject	?	noFilter	1
hypothesisType	610010	noFilter	200
levelOfConfidence	9	noFilter	150
levelOfPenetration	6	noFilter	200
nodeId	poseidon.aueb.gr	noFilter	100
numParams	?	noFilter	1
params	?	noFilter	1
systemId	Expert System	noFilter	1
time	?	noFilter	1
userId	mgk	=	200

Θέτοντας ένα περισσότερο «χαλαρό» query (παραπάνω οθόνη), παίρνουμε ως αποτέλεσμα περισσότερα από ένα cases (όπως φαίνεται στην οθόνη που ακολουθεί).

CBR-Works Consultation

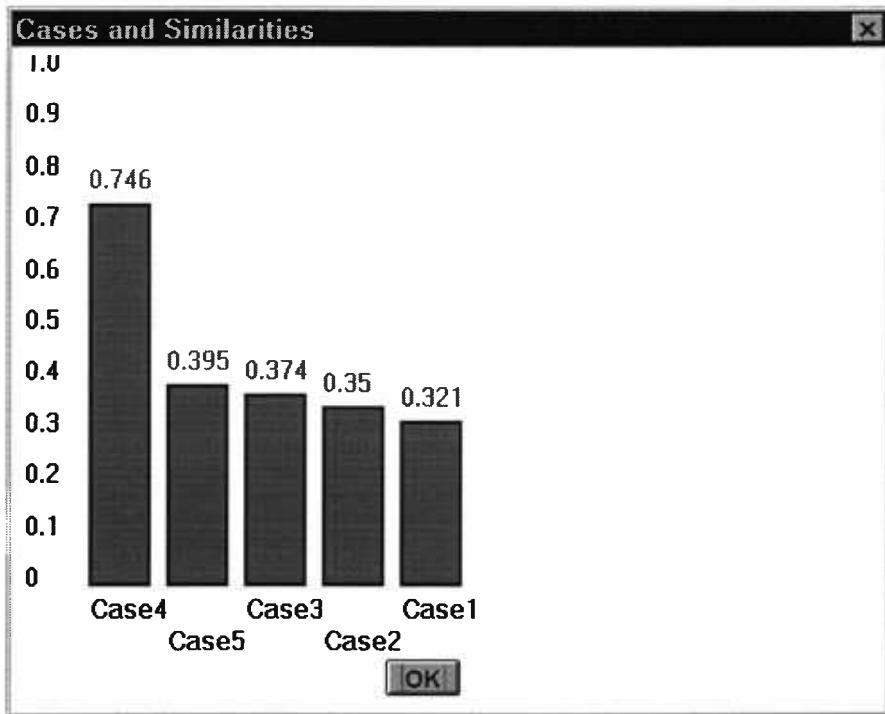
File Edit Design Tools Retrieval Navigation Help

Attributes Query Case Case4 Case5

attackClass		Password Cracking	Denial of Service
cmDescription		The user must logout if the process	
cmSubject		Log out a user	Grab a snapshot of the
hypothesisType	620002	620002	610115
levelOfConfidence	4	4	8
levelOfPenetration	6	6	4
nodeId	minoas.aueb.gr	minoas.aueb.gr	poseidon.aueb.gr
numParams		4	4
params		R620002:Probable Pas:	R10115:Probable Denia
systemId	Neural Network	Neural Network	Neural Network
time		809362342	809123234
userId	john	john	webmaster

Con: user Filter: Weight: Case: 1 of 5 Sim1: 0.746 Sim2: 0.395

Υπάρχουν τρόποι με τους οποίους μπορούμε να διαπιστώσουμε το βαθμό ομοιότητας που το αρχικό case έχει με τα case τα οποία ανακτήθηκαν. Ενας τρόπος γραφικής αναπαράστασης είναι ο παρακάτω.



Με την μελέτη του συστήματος μπορούν να διατυπωθούν χρήσιμα συμπεράσματα για τον τρόπο που αυτό θα συμπεριφερθεί σε πραγματικές συνθήκες λειτουργίας.

- Εκδίδει πάντα λύση. Ακόμα και αν δεν υπάρχει ακριβώς το ίδιο case στη βάση, το πλησιέστερο σε αυτό θα επιλεγεί και θα προταθεί στον διαχειριστή ασφαλείας ως λύση.

- Ο διαχειριστής μπορεί να επηρεάσει άμεσα την διαδικασία της συμπερασματολογίας. Η αλλαγή των βαρών αλλά και η εισαγωγή φίλτρων κατά την κατασκευή του query, δίνει τη δυνατότητα να περιορίσει ή και να διευρύνει το query και το πλάτος της γνώσης που θα εξεταστεί. Ο διαχειριστής έχει την ευχέρεια με αυτόν τον τρόπο να ορίσει ανώτατα όρια ευαισθησίας (thresholds), ανάλογα με τις εκάστοτε ανάγκες ή και ώρες λειτουργίας του συστήματος - σημαντικό στοιχείο για κάθε IDS.

