Πανεπιστήμιο Πειραιώς

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ & ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

Κατεύθυνση Ψηφιακών Επικοινωνιών και Δικτύων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Εφαρμογές θεωρίας παιγνίων σε ασφάλεια δικτύων»

ΝΙΚΟΛΑΟΣ ΧΑΛΚΙΑΔΑΚΗΣ

ΑΜ: ΜΕ/07078

25/05/2009

Ευχαριστίες

Εκφράζω θερμές ευχαριστίες στον αδερφό μου Ευτύχιο Χαλκιαδάκη (ΕΜΠ, MSc, υπ. PHD) για την αμέριστη και αδιάκοπη βοήθεια και συνεργασία που μου παρείχε καθώς επίσης και τον Καθηγητή Σωκράτη Κάτσικα για την επίβλεψη και τις πολύτιμες συμβουλές του, που είχα σε όλη τη διάρκεια της προσπάθειας μου να εκπονήσω αυτήν την μεταπτυχιακή διπλωματική εργασία. Τέλος θέλω να ευχαριστήσω και να αφιερώσω αυτήν την εργασία στην οικογένεια μου, στον πατέρα μου Μανώλη, στην μητέρα μου Ελένη και στον αδερφό μου Ευτύχιο.

ΠΕΡΙΕΧΟΜΕΝΑ

1ο ΚΕΦΑΛΑΙΟ

ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ

1.1 ΕΙΣΑΓΩΓΗ

Η **θεωρία παιγνίων** (*game theory*) ξεκίνησε σαν κλάδος των οικονομικών με το σπουδαίο βιβλίο των Τζον φον Νόιμαν *(John von Neumann)* και Όσκαρ Μόργκενστερν *(Oskar Morgenstern)Theory of Games and Economic Behaviour* (Θεωρία Παιγνίων και Οικονομική Συμπεριφορά) πάνω σε παίγνια μηδενικού αθροίσματος (zero-sum games). Το κύριο αντικείμενό της είναι η ανάλυση των αποφάσεων σε καταστάσεις (παίγνια) στρατηγικής αλληλεπίδρασης (strategic interdependence).

Στους περαιτέρω θεμελιωτές ανήκουν:

- ο Τζων Φορμπς Νας *(John Forbes Nash)* (η ζωή του έγινε θέμα της ταινίας "ένας υπέροχος άνθρωπος"), ο οποίος γενίκευσε το πρόβλημα σε παίγνια μη μηδενικού αθροίσματος και πρόσφερε σαν λύση την ισορροπία Νας *(Nash Equilibrium)*
- ο Ράινχαρντ Ζέλτεν *(Reinhard Selten)* άνοιξε το δρόμο για ικανοποιητική λύση του προβλήματος σε δυναμικά παίγνια με την έννοια της ισορροπίας στα υποπαίγνια *(Subgame Perfect Nash Equilibrium)* και της ισορροπίας τρεμάμενου χεριού *(trembling hand perfect equilibrium)*
- ο Τζων Χαρσάνυι *(John Harsanyi)* ασχολήθηκε με παίγνια υπό μερική πληροφόρηση (Incomplete Information).

Για τις εργασίες τους τιμήθηκαν οι τρεις τελευταίοι το 1994 με το βραβείο της Σουηδικής Ακαδημίας Επιστημών στην μνήμη του Άλφρεντ Νομπέλ *(Alfred Bernhard Nobel)*. Είναι σίγουρο βέβαια ότι αν ο Τζον φον Νόιμαν ζούσε θα μοιραζόταν και αυτός το βραβείο.

Τα τελευταία 30 χρόνια, η θεωρία παιγνίων έχει βρει ευρύτατη εφαρμογή στα οικονομικά, όπου ολόκληροι κλάδοι στηρίζονται στις μεθόδους της, όπως π.χ. η βιομηχανική οργάνωση*(industrial organisation)*, ο σχεδιασμός μηχανισμών *(mechanism design)* με σπουδαιότερο υποκλάδο τον σχεδιασμό δημοπρασιών (auctions) κ.α.

Επίσης, η θεωρία παιγνίων χρησιμοποιείται και στην Πολιτική Οικονομία και ειδικά στη θεωρία της συλλογικής δράσης (Collective action), όπου εξηγεί ενδεχόμενα συνεργασίας μεταξύ των παικτών. Στη συγκεκριμένη εκδοχή, μιλάμε για παίγνια συνεργασίας (Cooperative Game Theory). Αυτό βρίσκεται σε άμεση συσχέτιση με τον ρόλο του κράτους και των θεσμών σε θέματα συνεργασίας. Χαρακτηριστικό παράδειγμα είναι η παροχή δημόσιων αγαθών και η φορολογία.

Επιπρόσθετα χρησιμοποιείται όμως ευρέως και σε άλλες επιστήμες, όπως εξελικτική βιολογία, ψυχολογία, κοινωνιολογία, πληροφορική, τηλεπικοινωνίες κλπ.

Το 2005 οι θεωρητικοί παιγνίων Τόμας Σέλλινγκ (*Thomas Schelling*) και Ρόμπερτ Άουμαν (Robert Aumann) κέρδισαν το Βραβείο Νομπέλ για τις Οικονομικές Επιστήμες.

Η Θεωρία Παιγνίων είναι η μελέτη του τρόπου με τον οποίο λαμβάνονται αποφάσεις από άτομα που αλληλεπιδρούν μεταξύ τους. Το «παίγνιο» είναι «μια ανταγωνιστική δραστηριότητα στην οποία οι παίκτες συναγωνίζονται σύμφωνα με ένα σύνολο κανόνων», όμως το εύρος της θεωρίας παιγνίων είναι πολύ μεγαλύτερο.
Η θεωρία παιγνίων έχει τις ρίζες της στους κλάδους των εφαρμοσμένων μαθηματικών. Μια άλλη ονομασία της θεωρίας παιγνίων είναι «επιστήμη της στρατηγικής», διότι αναλύει περιπτώσεις στις οποίες οι τύχες των ανθρώπων αλληλεξαρτώνται. Η θεωρία παιγνίων προσφέρει ένα συστηματικό τρόπο για το σχεδιασμό στρατηγικών σε περιπτώσεις όπου η τύχη του ενός εξαρτάται από τις πράξεις των άλλων.
Η θεωρία παιγνίων μπορεί να χρησιμοποιηθεί επομένως για να διαφωτίσει οικονομικά, πολιτικά βιολογικά και τεχνολογικά φαινόμενα. Αποτελεί ιδανικό εργαλείο για την ερμηνεία πολλών τύπων αποφάσεων, όπως επιχειρήσεις που ανταγωνίζονται με άλλες, πολιτικοί εκπρόσωποι που ανταγωνίζονται για ψήφους, ένορκοι που αποφασίζουν για μία καταδίκη, ζώα που παλεύουν για τη λεία τους, άτομα που συμμετέχουν σε μια δημοπρασία, αδέλφια που συμπεριφέρονται ανταγωνιστικά, ειδικοί που ανταγωνίζονται για τη διάγνωση ενός προβλήματος, νομοθέτες που ψηφίζουν υπό την πίεση των ενδιαφερόμενων ομάδων, καθώς και ο ρόλος της απειλής και τιμωρίας στις μακροχρόνιες σχέσεις.

1.2 ΣΤΡΑΤΗΓΙΚΗ ΦΟΡΜΑ ΠΑΙΓΝΙΩΝ

Τα μοντέλα παιγνίων βασίζονται στη θεωρία της ορθολογικής επιλογής (rational choice). Βάσει αυτής της θεωρίας αυτός που παίρνει την απόφαση επιλέγει τον βέλτιστο τρόπο δράσης ανάμεσα στις διάφορες εναλλακτικές λύσεις σύμφωνα με τις προτιμήσεις του. Δεν υπάρχει κανένας ποιοτικός περιορισμός στις προτιμήσεις του. Ο ορθολογισμός έγκειται στη συνέπεια των αποφάσεων του όταν έρχεται αντιμέτωπος με τις διάφορες διαθέσιμες επιλογές και όχι στη φύση των προτιμήσεών του.
Ένα παίγνιο περιλαμβάνει παίκτες, ενέργειες, πληροφορίες, στρατηγικές, οφέλη, αποτελέσματα και ισορροπίες. Οι παίκτες, οι ενέργειες και τα αποτελέσματα ορίζουν τους κανόνες του παιγνίου.

Παίκτες: αυτοί που λαμβάνουν τις αποφάσεις.
Ενέργειες: όλες οι πιθανές κινήσεις που μπορεί να κάνει ένας παίκτης.
Πληροφορία: αυτά που γνωρίζει ο κάθε παίκτης σε κάθε στάδιο του παιγνίου.
Στρατηγικές: οι κανόνες που υπαγορεύουν σε κάθε παίκτη ποια ενέργεια να επιλέξει σε κάθε στάδιο του παιγνίου.
Οφέλη: τα κέρδη ή τα αναμενόμενα κέρδη που θα λάβουν οι παίκτες, όταν όλοι επιλέξουν τις στρατηγικές τους και όταν έχει ολοκληρωθεί το παίγνιο και εκφράζονται από τη συνάρτηση αποδοχής u.
Αποτέλεσμα του παιγνίου: το σύνολο των εξαιρετικά ενδιαφερόντων αποτελεσμάτων που επιλέγει ο ερευνητής από τις αξίες των ενεργειών των ανταλλαγών και των άλλων μεταβλητών, μετά την ολοκλήρωση του παιγνίου.
Ισορροπία: ένας συνδυασμός στρατηγικών που αποτελείται από την καλύτερη στρατηγική για κάθε παίκτη στο παίγνιο.

1.3 ΚΥΡΙΑΡΧΗ ΣΤΡΑΤΗΓΙΚΗ – ΙΣΟΡΡΟΠΙΑ ΚΑΤΑ NASH

Στρατηγική είναι οι κανόνες που καθορίζουν τη συμπεριφορά των παικτών κατά τη διάρκεια ενός παιγνίου. Μια στρατηγική μπορεί να είναι πολύ απλή, όπως μια διαφημιστική καμπάνια, ή πολύ σύνθετη, όπως η απόφαση για τον καθορισμό της τιμής στην αρχή κάθε μήνα σε σχέση με τις πωλήσεις του προηγούμενου μήνα. Ιδιαίτερα χρήσιμη είναι η υπόθεση ότι οι παίκτες επιλέγουν τη στρατηγική τους ταυτόχρονα στην αρχή κάθε παιγνίου. Από τη στιγμή που επιλέγονται οι στρατηγικές, οι παίκτες δρουν σύμφωνα με αυτές. Υποθέτοντας ότι οι παίκτες ενεργούν βάσει της θεωρίας της ορθολογικής επιλογής, ο κάθε ένας επιλέγει τη στρατηγική με το μεγαλύτερο κέρδος. Συνοψίζοντας λοιπόν η κανονική ή στρατηγική μορφή ενός παιγνίου καθορίζει:

- Ένα πεπερασμένο σύνολο παικτών {1,2,…,*n*}
- Τις στρατηγικές των παικτών S_1 S_2 ... S_n
- Τις συναρτήσεις αποδοχών τους u_1 u_2 ... u_n, όπου $u_i : S_1 \times S_2 \times ... \times S_n \rightarrow R$

Για παράδειγμα μπορούμε να αναπαραστήσουμε στον πίνακα που δίνεται πιο κάτω ένα παίγνιο μεταξύ δύο παικτών (Παίκτης 1 και Παίκτης 2), όπου κάθε παίκτης έχει πεπερασμένο αριθμό στρατηγικών $S_1=\{s_{11}, s_{12}, s_{13}\}$ και $S_2=\{s_{21}, s_{22}\}$ αντίστοιχα.

		Player 2	
		s_{21}	s_{22}
Player 1	s_{11}	$u_1(s_{11},s_{21})$, $u_2(s_{11},s_{21})$	$u_1(s_{11},s_{22})$, $u_2(s_{11},s_{22})$
	s_{12}	$u_1(s_{12},s_{21})$, $u_2(s_{12},s_{21})$	$u_1(s_{12},s_{22})$, $u_2(s_{12},s_{22})$
	s_{13}	$u_1(s_{13},s_{21})$, $u_2(s_{13},s_{21})$	$u_1(s_{13},s_{22})$, $u_2(s_{13},s_{22})$

Πίνακας 1.1

Κυρίαρχη στρατηγική είναι η στρατηγική που υπερτερεί οποιασδήποτε άλλης, ανεξαρτήτως της στρατηγικής που θα επιλέξει ο αντίπαλος. Όμως τα κέρδη ενός παίκτη εξαρτώνται όχι μόνο από τη δική του στρατηγική, αλλά και από τη στρατηγική των άλλων παικτών, σχέση που αποτελεί το αναγκαίο συστατικό του παιγνίου.

Επομένως, όταν κάποιος παίκτης καλείται να διαλέξει στρατηγική πρέπει να λάβει υπόψη τις στρατηγικές που αναμένεται ότι θα ακολουθήσουν οι υπόλοιποι. Σε αυτή την αλληλεξάρτηση στηρίχθηκε η έννοια της **ισορροπίας κατά Nash**, από το όνομα του μαθηματικού John Nash, που ήταν ο πρώτος που διατύπωσε αυτή την ιδέα. Στην ισορροπία κατά Nash οι παίκτες επιλέγουν την καλύτερη στρατηγική, δεδομένου της απόφασης του αντιπάλου τους, με προϋπόθεση αυτό συμβαίνει ταυτόχρονα. Η έννοια της ισορροπίας κατά Nash είναι μια από τις σημαντικότερες για την εφαρμογή της θεωρίας των παιγνίων στην οικονομική συμπεριφορά. Αν και όλες οι κυρίαρχες λύσεις είναι ισορροπίες κατά Nash, ορισμένα παίγνια χωρίς μια κυρίαρχη λύση μπορεί να έχουν περισσότερες από μια ισορροπίες κατά Nash. Την ισορροπία κατά Nash μπορούμε να την εκφράσουμε με μαθηματική μορφή ως εξής: Στην κανονική μορφή του παιγνίου $\{S_1, S_2, ..., S_n, u_1, u_2, ..., u_n\}$, ένας συνδυασμός στρατηγικών είναι μία ισορροπία *Nash* αν, για κάθε παίκτη *i*, ισχύει ότι:

$$u_i(s_1^*,..., s_{i-1}^*, s_i^*, s_{i+1}^*,..., s_n^*) \geq u_i(s_1^*,..., s_{i-1}^*, s_i, s_{i+1}^*,..., s_n^*)$$

για όλα τα $s_i \in S_i$

Αυτό σημαίνει ότι το s_i^* ικανοποιεί τη μεγιστοποίηση της $u_i(s_1^*,...,s_{i-1}^*,s_i,s_{i+1}^*,...,s_n^*)$

Καταλαβαίνουμε λοιπόν ότι:

Στην κανονική μορφή του παιγνίου {S1 , S2 , ..., Sn , u1 , u2 , ..., un}, αν ο παίκτης 1, 2, ..., i-1, i+1, ..., n επιλέξει στρατηγικές $s_1,..., s_{i-1}, s_{i+1},..., s_n$, αντίστοιχα, τότε η συνάρτηση καλύτερης απάντησης του παίκτη i ορίζεται ως:

$$B_i(\ s_1,...,\ s_{i-1}, s_{i+1},...,\ s_n\ ) =$$
$$\{\ s_i \in\ S_i : u_i(\ s_1,...,\ s_{i-1}, s_i, s_{i+1},...,\ s_n\ )$$
$$\geq\ u_i(\ s_1,...,\ s_{i-1}, s_i', s_{i+1},...,\ s_n\ ),\quad s_i' \in\ S_i\ \}$$

Στην κανονική μορφή ενός παιγνίου {S1, ..., Sn , u1, ..., un},
ένας συνδυασμός στρατηγικών $(s_1^*,...,s_n^*)$ είναι ισορροπία Nash αν για κάθε παίκτη i ισχύει ότι:

$$s_i^* \in\ B_i(\ s_1^*,...,\ s_{i-1}^*,\ s_{i+1}^*, ...,\ s_n^*\ )$$

1.4 ΕΙΔΗ ΠΑΙΓΝΙΩΝ

Παίγνια μηδενικού αθροίσματος – παίγνια μη μηδενικού αθροίσματος

Στο παίγνιο μηδενικού αθροίσματος το κέρδος του ενός είναι η ζημιά του άλλου. Στο παίγνιο μη μηδενικού αθροίσματος όλοι οι παίκτες μπορεί να κερδίσουν ή να χάσουν, κάτι που εξαρτάται από τις ενέργειες του κάθε παίκτη. Σε όλα τα παίγνια μηδενικού αθροίσματος η κυρίαρχη λύση προκύπτει μέσα από τη χρήση της στρατηγικής ελαχίστου-μεγίστου. Σύμφωνα με αυτή, ο παίκτης προσπαθεί να ελαχιστοποιήσει το μέγιστο δυνατό αποτέλεσμα του αντιπάλου.

Παίγνια συνεργατικά – παίγνια μη συνεργατικά

Στο μη συνεργατικό παίγνιο, οι παίκτες δεν επιτρέπεται να ανταλλάσσουν πληροφορίες μεταξύ τους, ενώ στο συνεργατικό έχουν αυτή τη δυνατότητα.

Παίγνια δύο παικτών – παίγνια n παικτών

Ένα παίγνιο μπορεί να περιλαμβάνει δύο ή περισσότερους παίκτες.

Στατικά – δυναμικά παίγνια

Ένα παίγνιο είναι στατικό όταν όλοι οι παίκτες κινούνται ταυτόχρονα, ενώ είναι δυναμικό όταν οι παίκτες κινούνται κατά σειρά.

Παίγνια με τέλεια – ατελής, συμμετρική – ασύμμετρη, ολοκληρωμένη ή βέβαιη πληροφόρηση

Υπάρχουν τέσσερις χρήσιμοι τρόποι κατάταξης των πληροφοριών στα παίγνια:

Σε ένα παίγνιο με **τέλεια πληροφόρηση** κάθε παίκτης γνωρίζει την κάθε κίνηση που θα κάνει ο άλλος, πριν αυτός την κάνει.

Δεδομένου αυτού του ορισμού, όλα τα παίγνια στα οποία οι παίκτες κινούνται ταυτοχρόνως είναι παίγνια **ατελούς πληροφόρησης**, καθώς οι παίκτες δε γνωρίζουν την ταυτόχρονη κίνηση του άλλου παίκτη. Εάν όλοι οι παίκτες έχουν τις ίδιες ακριβώς πληροφορίες όταν κινείται ο κάθε παίκτης, τότε το παίγνιο έχει **συμμετρική πληροφόρηση**. Εάν ορισμένοι παίκτες έχουν διαφορετικές πληροφορίες από τους άλλους, τότε το παίγνιο είναι **ασύμμετρης πληροφόρησης**.
Πολλά παίγνια απαιτούν από ένα μη παίκτη να κάνει κάποιες τυχαίες ενέργειες σε κάποιο σημείο του παιγνίου. Αυτός ο μη παίκτης ονομάζεται φύση. Αν ένα παίγνιο περιλαμβάνει φύση, αλλά αυτή δεν κινείται πρώτη ή αν η πρώτη κίνηση της φύσης παρατηρείται από όλους τους παίκτες, τότε το παίγνιο χαρακτηρίζεται από **ολοκληρωμένη πληροφόρηση**. Εάν η φύση δεν κινείται ποτέ μετά την κίνηση ενός από τους παίκτες, τότε το παίγνιο είναι **βέβαιης πληροφόρησης**.

Επαναλαμβανόμενα παίγνια

Ένα απλό παίγνιο ταυτόχρονης κίνησης που διαρκεί μια χρονική περίοδο επαναλαμβάνεται συνεχώς. Σε κάθε νέο γύρο οι παίκτες γνωρίζουν τις προηγούμενες κινήσεις των αντιπάλων τους. Τα επαναλαμβανόμενα παίγνια αυτής της μορφής ονομάζονται παίγνια σχεδόν τέλειας πληροφόρησης. Επειδή οι κινήσεις εκτελούνται ταυτοχρόνως, το παίγνιο πρέπει να είναι ατελούς πληροφόρησης.

Παίγνια μικτών στρατηγικών

Η θέση status quo είναι η **κυριαρχούμενη στρατηγική**. Η κυριαρχούμενη στρατηγική είναι η στρατηγική εκείνη που είναι πάντα χειρότερη από κάποια άλλη στρατηγική. Η **κυριαρχούμενη στρατηγική διακρίνεται σε** αυστηρώς κυριαρχούμενη και ασθενώς κυριαρχούμενη στρατηγική. Στην κανονική μορφή του παιγνίου $\{S_1 , S_2 , ..., S_n , u_1 , u_2 , ..., u_n\}$, όπου $s_i', s_i'' \in S_i$ στρατηγικές του παίκτη i. Η στρατηγική s_i' είναι ***αυστηρώς κυριαρχούμενη*** από την στρατηγική s_i'' αν $u_i(s_1, s_2, ... s_{i-1}, s_i', s_{i+1}, ..., s_n) < u_i(s_1, s_2, ... s_{i-1}, s_i'', s_{i+1}, ..., s_n)$ για όλα $s_1 \in S_1, s_2 \in S_2, ..., s_{i-1} \in S_{i-1}, s_{i+1} \in S_{i+1}, ..., s_n \in S_n$. Η στρατηγική s_i' είναι ***ασθενώς κυριαρχούμενη*** από την στρατηγική s_i'' αν $u_i(s_1, s_2, ... s_{i-1}, s_i', s_{i+1}, ..., s_n) \leq$ (αλλά όχι πάντα =) $u_i(s_1, s_2, ... s_{i-1}, s_i'', s_{i+1}, ..., s_n)$ για όλα $s_1 \in S_1, s_2 \in S_2, ..., s_{i-1} \in S_{i-1}, s_{i+1} \in S_{i+1}, ..., s_n \in S_n$. Είναι χρήσιμο να αναγνωριστούν οι κυριαρχούμενες στρατηγικές ως μη βιώσιμες επιλογές, ώστε να αποκλειστούν ως πιθανές λύσεις από κάθε παίγνιο. Σε κάποιες περιπτώσεις όμως, ακόμα και αν εξαλειφθούν οι κινήσεις status quo, δεν υπάρχει απλή λύση στο παίγνιο. Τότε, οι παίκτες πρέπει να παίξουν **μικτή στρατηγική**. Έστω G ένα παίγνιο n-παικτών με σετ στρατηγικών S1, S2 ,.., Sn.

Μία μεικτή στρατηγική S_i για τον παίκτη i είναι μία κατανομή πιθανοτήτων στα Si. Αν Si έχει έναν πεπερασμένο αριθμό καθαρών στρατηγικών π.χ. $S_i = \{s_{i1}, s_{i2}, ... s_{iK_i}\}$ τότε μία μεικτή στρατηγική είναι μία συνάρτηση $s_i : S_i \to \Re^+$ τέτοια ώστε $\sum_{j=1}^{K_i} s_i(s_{ij}) = 1$.

Γράφουμε την μεικτή αυτή στρατηγική $(s_i(s_{i1}), s_i(s_{i2}), ..., s_i(s_{iK_i}))$.

Στην καλύτερη μικτή στρατηγική, ο κάθε παίκτης επιλέγει τυχαία τις κινήσεις του, με βάση τις δεδομένες πιθανότητες που μεγιστοποιούν τα αναμενόμενα οφέλη του, δεδομένου ότι η τυχαία επιλεγμένη στρατηγική θα παιχτεί από τον αντίπαλο. Είναι δυνατόν να αποδειχθεί ότι υπάρχει πάντα ένα κατάλληλο σύνολο πιθανοτήτων για την επίλυση αυτών των προβλημάτων.

Πρέπει να σημειωθεί ότι Ισορροπία Μεικτών Στρατηγικών είναι:

- Μια κατανομή πιθανοτήτων για κάθε παίκτη.
- Οι κατανομές είναι αποτελούν την καλύτερη αντίδραση του κάθε παίκτη στον άλλο αναφορικά με τα αναμενόμενα κέρδη τους.

Παίγνια αλληλουχίας

Τα πιο συνήθεις παίγνια είναι στατικά παίγνια ατελούς πληροφόρησης και απεικονίζονται σε πίνακα. Υπάρχουν όμως πολλά παίγνια που παρουσιάζουν μια αλληλουχία, όπου ένας παίκτης κινείται πρώτος και ο κάθε παίκτης αντιδρά στην ενέργεια του προηγούμενου παίκτη. Όταν ένας παίκτης κινείται πρώτος είναι λάθος να απεικονίσουμε το παίγνιο με τη μορφή πίνακα, αφού οι παίκτες γνωρίζουν την κίνηση του αντιπάλου τους πριν αυτοί κάνουν τη δική τους κίνηση. Επομένως, τα παίγνια αυτού του τύπου είναι δυναμικά, τέλειας πληροφόρησης και απεικονίζονται με δένδρα παιγνίων. Η απεικόνιση με δένδρο παιγνίου ονομάζεται και εκτεταμένη μορφή ενός παιγνίου, ενώ η απεικόνιση με τον απλό πίνακα κερδών ονομάζεται στρατηγική μορφή ενός παιγνίου.

1.5 ΤΡΟΠΟΙ ΠΕΡΙΓΡΑΦΗΣ ΤΩΝ ΠΑΙΓΝΙΩΝ

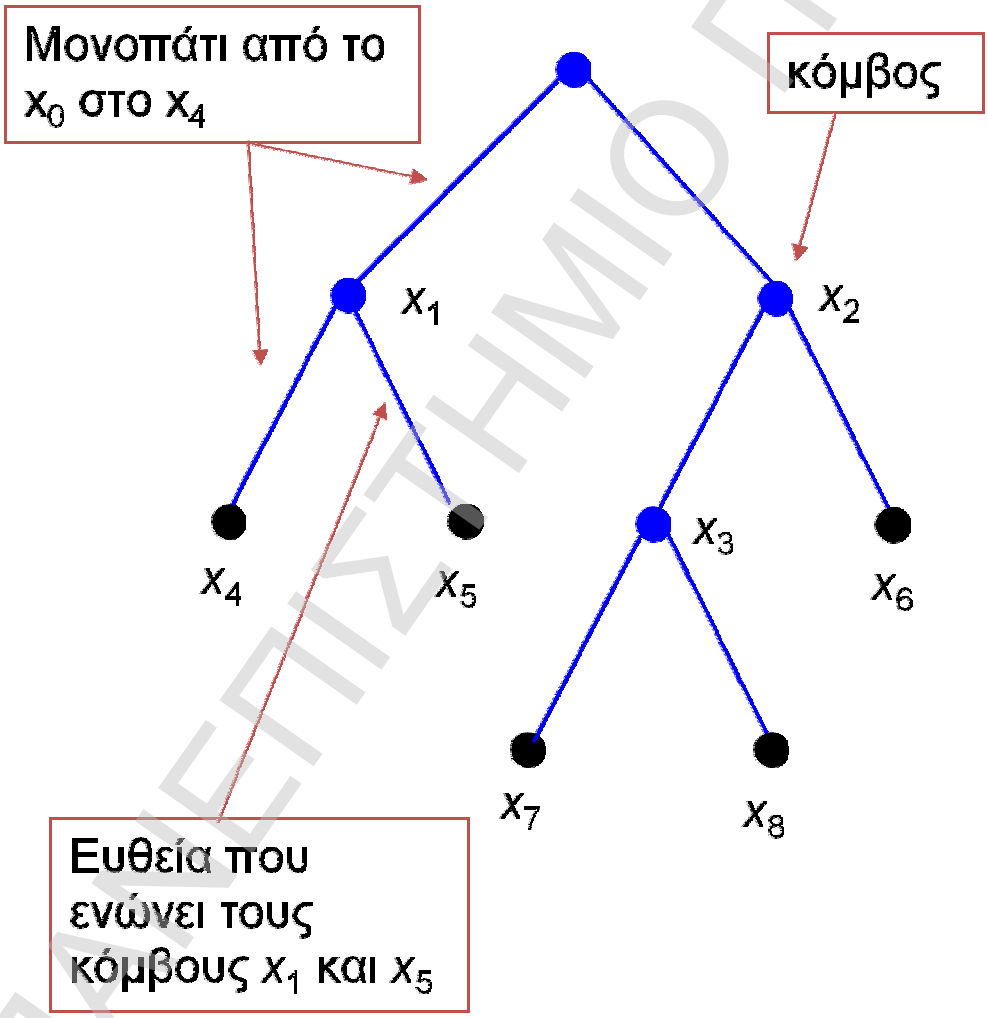
Ένα παίγνιο μπορεί να αναπαρασταθεί είτε με στρατηγική / κανονική μορφή ως πίνακας, είτε με εκτεταμένη μορφή ως δένδρο. Από μια εκτεταμένη μορφή ενός παιγνίου προκύπτει μόνο μια στρατηγική μορφή. Αντίθετα, σε μια στρατηγική μορφή ενός παιγνίου μπορεί να αντιστοιχούν περισσότερες από μια εκτεταμένες μορφές. Στη συνέχεια θα εξηγήσουμε αναλυτικά την εκτεταμένη και τη στρατηγική μορφή των παιγνίων.

Εκτεταμένη μορφή παιγνίου

Η εκτεταμένη (εκτατική) μορφή ενός παιγνίου καθορίζει:

- τους παίκτες
- πότε κάθε παίκτης κινείται
- ποιες είναι οι εναλλακτικές του παίκτη κάθε φορά που έχει την δυνατότητα να επιλέξει - κινηθεί
- τι γνωρίζει ο κάθε παίκτης κάθε φορά που έχει την δυνατότητα να επιλέξει - κινηθεί
- τις αποδόσεις κάθε παίκτη για κάθε συνδυασμό επιλογών - κινήσεων

Η εκτεταμένη μορφή μπορεί να παρασταθεί, όπως προαναφέρθηκε, με τη μορφή δένδρου όπως φαίνεται στο παρακάτω σχήμα.



Σχήμα 1.1

Όπως φαίνεται στο σχήμα 1.1 ένα δέντρο αποτελείται από κόμβους και ευθείες. Κάθε ευθεία ενώνει δύο κόμβους. Κάθε ζευγάρι κόμβων ενώνεται από ένα μοναδικό μονοπάτι.

Μονοπάτι είναι μία σειρά διακεκριμένων κόμβων x_1, x_2,..., x_n τέτοια ώστε x_i και x_{i+1} ενώνονται από μία μοναδική ευθεία, για i=1, 2, ..., n-1. Σε κάθε δέντρο ισχύουν οι εξής κανόνες:

- Σε κάθε δέντρο υπάρχει ένας αρχικός κόμβος από τον οποίο ξεκινάει το παίγνιο. Κάθε κόμβος εκτός του αρχικού έχει έναν μοναδικό κόμβο που προηγείται (predecessor). Κάθε κόμβος που δεν έχει επόμενο κόμβο (successor) ονομάζεται τελικός (terminal).
- Κάθε κόμβος εκτός του τελικού αντιπροσωπεύει έναν παίκτη.
- Για κάθε κόμβο εκτός του τελικού η ευθεία που τον ενώνει με τον επόμενο κόμβο αντιπροσωπεύει μία εναλλακτική που έχει στην διάθεση του ο παίκτης που αντιπροσωπεύεται από την συγκεκριμένο κόμβο.
- Ένα μονοπάτι από τον αρχικό κόμβο στον τελικό αντιπροσωπεύει μία πλήρη σειρά κινήσεων και καθορίζει την απόδοση του κάθε παίκτη.
- Η στρατηγική ενός παίκτη είναι ένα πλήρες σχέδιο δράσης και καθορίζει τι θα κάνει ο παίκτης σε κάθε περίπτωση.

Στρατηγική μορφή παιγνίου

Ένας δεύτερος τρόπος περιγραφής παιγνίου είναι η στρατηγική μορφή. Σε αυτή παρουσιάζονται όλες οι δυνατές στρατηγικές κάθε παίκτη και δηλώνονται οι αμοιβές ή απώλειες των παικτών, οι οποίες είναι αποτέλεσμα όλων των εναλλακτικών συνδυασμών των στρατηγικών που επιλέγουν. Στη στρατηγική μορφή δεν εμφανίζεται η χρονική στιγμή, δεν γνωρίζουμε δηλαδή ποιος παίκτης είναι πρώτος, ποιος είναι δεύτερος, αν παίζουν ταυτόχρονα ή διαδοχικά.
Η στρατηγική μορφή ενός παιγνίου αποτελείται από τα παρακάτω στοιχεία

- Ένα σύνολο παικτών (players).
- Τις στρατηγικές (strategies) των παικτών, οι οποίες αποτελούν ένα πλήρες σχέδιο κάθε παίκτη για το παίγνιο, δηλαδή, ένα σύνολο οδηγιών για το τι θα κάνει κάθε παίκτης κάθε φορά που καλείται να κινηθεί.
- Τα αποτελέσματα κάθε «παρτίδας» (payoffs). Κάτι που παίζεται και φτάνει σε ένα σημείο, τελειώνει και όταν τελειώνει παίρνει ο καθένας το μερίδιο του, δηλαδή, το τίμημα των επιλογών του στο παίγνιο.

Η στρατηγική μορφή μπορεί να απεικονιστεί με έναν πίνακα, στον οποίο οι σειρές αντιστοιχούν στις στρατηγικές του ενός παίκτη, ενώ οι στήλες αντιστοιχούν στις στρατηγικές του άλλου παίκτη. Σε κάθε κελί του πίνακα γράφονται οι αποδόσεις που σχετίζονται με το αντίστοιχο ζευγάρι στρατηγικών.

1.6 ΤΟ ΔΙΛΗΜΜΑ ΤΟΥ ΦΥΛΑΚΙΣΜΕΝΟΥ

Ένα από τα πιο γνωστά στρατηγικά παίγνια είναι το δίλημμα του φυλακισμένου. Το όνομά του προέρχεται από μια ιστορία που εμπλέκει δύο άτομα ύποπτα για έγκλημα. Αυτό το παίγνιο είναι ιδιαίτερα σημαντικό λόγω των ποικίλων περιπτώσεων, όπου στους συμμετέχοντες δίνονται παρόμοια κίνητρα με αυτά των υπόπτων του εγκλήματος.
Το παίγνιο έχει ως εξής. Δύο ύποπτοι για ένα μεγάλο έγκλημα κρατούνται σε ξεχωριστά κελιά. Υπάρχουν αρκετά αποδεικτικά στοιχεία για να καταδικαστούν και οι δύο για πλημμέλημα, αλλά όχι επαρκείς αποδείξεις ότι διέπραξαν το μεγάλο έγκλημα, εκτός εάν ένας από τους δύο «μαρτυρήσει» τον άλλο. Αν και οι δύο παραμείνουν σιωπηλοί, ο κάθε ένας θα καταδικαστεί για πλημμέλημα και θα εκτίσουν ένα χρόνο στη φυλακή. Εάν μόνο ο ένας παραδεχτεί την ενοχή του άλλου, θα ελευθερωθεί και θα παρουσιαστεί ως μάρτυρας στη δίκη του άλλου, ο οποίος θα εκτίσει τέσσερα χρόνια στη φυλακή. Εάν ομολογήσουν και οι δύο, ο καθένας θα καταδικαστεί σε τρία χρόνια φυλάκιση.

Το στρατηγικό παίγνιο μοντελοποιείται όπως φαίνεται παρακάτω:

- παίκτες: οι δύο ύποπτοι.
- ενέργειες: το σύνολο των τρόπων δράσης κάθε παίκτη, δηλαδή (δεν ομολογεί, ομολογεί).
- προτιμήσεις: έστω ότι η συνάρτηση πιθανών αποτελεσμάτων ορίζεται ως u(x,y).

Τότε τα αποτελέσματα για κάθε παίκτη θα είναι:

- Παίκτης 1: u1(δεν ομολογεί, δεν ομολογεί)=1, u1(δεν ομολογεί, ομολογεί)=4, u1(ομολογεί, ομολογεί)=3 και u1(ομολογεί, δεν ομολογεί)=0.
- Παίκτης 2: u2(δεν ομολογεί, δεν ομολογεί)=1, u2(δεν ομολογεί, ομολογεί)=0, u2(ομολογεί, ομολογεί)=3 και u2(ομολογεί, δεν ομολογεί)=4.

Τα παραπάνω αποτελέσματα παρουσιάζονται σε πίνακα ως εξής:

		Παίκτης 2	
		Δεν ομολογεί	*Ομολογεί*
Παίκτης 1	*Δεν ομολογεί*	1,1	4,0
	Ομολογεί	0,4	3,3

Εξετάζοντας τα τέσσερα δυνατά ζεύγη ενεργειών, είναι εμφανές ότι η μοναδική ισορροπία κατά Nash είναι (ομολογεί, ομολογεί). Δεδομένου ότι ο παίκτης 2 επιλέξει να ομολογήσει, ο παίκτης 1 προτιμά να ομολογήσει παρά να σιωπήσει.
Επιπλέον, δεδομένου ότι ο παίκτης 1 επιλέξει να ομολογήσει, ο παίκτης 2 προτιμά επίσης να ομολογήσει. Καμία άλλη ενέργεια δεν αποτελεί ισορροπία κατά Nash, διότι: (δεν ομολογεί, δεν ομολογεί) δεν ικανοποιεί, διότι όταν ο παίκτης 2 επιλέξει να σιωπήσει, το αποτέλεσμα του παίκτη 1 είναι καλύτερο εάν αυτός ομολογήσει, παρά εάν δεν ομολογήσει. (ομολογεί, δεν ομολογεί) επίσης δεν ικανοποιεί, επειδή όταν ο παίκτης 1 επιλέξει να ομολογήσει, ο παίκτης 2 έχει καλύτερο αποτέλεσμα εάν αυτός ομολογήσει, παρά εάν δεν ομολογήσει. (δεν ομολογεί, ομολογεί) δεν ικανοποιεί, διότι όταν ο παίκτης 2 επιλέξει να ομολογήσει, ο παίκτης 1 προτιμά να ομολογήσει παρά να μην ομολογήσει, αφού έχει καλύτερο αποτέλεσμα.

Συνοψίζοντας, στη μοναδική ισορροπία κατά Nash στο δίλημμα του φυλακισμένου και οι δύο παίκτες επιλέγουν να ομολογήσουν. Συγκεκριμένα, το κίνητρο της ελεύθερης επιλογής εξαλείφει την πιθανότητα να συμβεί το κοινά επιθυμητό ζεύγος (δεν ομολογεί, δεν ομολογεί). Η ισορροπία κατά Nash εδώ προσφέρει σε κάθε παίκτη την καλύτερη δυνατή ενέργεια, όχι μόνο εάν ο άλλος επιλέξει την ενέργεια της ισορροπίας (δηλαδή να ομολογήσει), αλλά και εάν αποφασίσει να ενεργήσει αντίθετα (δηλαδή να μην ομολογήσει). Η λύση της ομολογίας είναι ευνοϊκή για κάθε παίκτη, όταν αυτός αναμένει ότι και ο άλλος θα επιλέξει να ομολογήσει. Όμως ακόμα και αν δεν υπήρχε αυτή η προσδοκία, πάλι θα συνέφερε τον παίκτη να επιλέξει την ομολογία, κάτι που δεν συμβαίνει σε όλα τα παίγνια.

Το δίλημμα του φυλακισμένου μοντελοποιεί μια κατάσταση, στην οποία υπάρχουν κέρδη από τη συνεργασία (ο κάθε παίκτης προτιμά και οι δύο να επιλέξουν να μην ομολογήσουν, παρά και οι δύο να ομολογήσουν), αλλά ο καθένας έχει ένα κίνητρο στην «ελεύθερη επιλογή» (δηλαδή να ομολογήσει) σύμφωνα με ό,τι κάνει ο άλλος. Το παίγνιο είναι σημαντικό όχι επειδή είναι ενδιαφέρον να κατανοηθούν τα κίνητρα των φυλακισμένων να ομολογήσουν, αλλά επειδή πολλές άλλες περιπτώσεις έχουν παρόμοιες δομές.

1.6.1 ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΔΙΛΗΜΜΑΤΟΣ ΤΟΥ ΦΥΛΑΚΙΣΜΕΝΟΥ

Ο ΠΟΛΕΜΟΣ ΤΩΝ ΟΠΛΩΝ

Υπό ορισμένες υποθέσεις όσον αφορά στις προτιμήσεις των διαφόρων χωρών, ο πόλεμος των όπλων μπορεί να μοντελοποιηθεί ως το δίλημμα του φυλακισμένου. Η υπόθεση είναι ότι κάθε χώρα μπορεί να κατασκευάσει ένα οπλοστάσιο με πυρηνικές βόμβες ή να απέχει από την κατασκευή. Επιπλέον, κάθε χώρα θα έχει το δυνατό βέλτιστο αποτέλεσμα εάν αυτή κατασκευάσει βόμβες, ενώ άλλη χώρα όχι. Το επόμενα λιγότερα καλύτερα αποτελέσματα έχουν ως εξής: καμία χώρα δεν έχει βόμβες, και οι δύο χώρες έχουν βόμβες, και το χειρότερο όταν μόνο η άλλη χώρα κατασκευάσει βόμβες.

Ο παραλληλισμός με το δίλημμα του φυλακισμένου γίνεται εάν το «σιωπεί» αντικατασταθεί με «δεν κατασκευάζει βόμβες» και το «ομολογεί» με το «κατασκευάζει βόμβες».

BACH Ή STRAVINSKY

Στο δίλημμα του φυλακισμένου το κυρίαρχο ερώτημα είναι εάν οι παίκτες θα επιλέξουν να συνεργαστούν και να σιωπήσουν. Στο παρακάτω παίγνιο οι παίκτες συμφωνούν ότι είναι καλύτερο να συνεργαστούν από το να μη συνεργαστούν, αλλά διαφωνούν για το ποιο θα είναι το καλύτερο αποτέλεσμα. Το παίγνιο παρουσιάζεται παρακάτω. Δύο άτομα επιθυμούν να βγουν έξω μαζί. Υπάρχουν δύο συναυλίες, μια με μουσική του Bach και μια με μουσική του Stravinsky. Το ένα άτομο προτιμά το Bach και το άλλο το Stravinsky. Εάν πάνε σε άλλη συναυλία από αυτή που επιθυμούν, ο καθένας θα είναι το ίδιο δυσαρεστημένος ακούγοντας τη μουσική του άλλου συνθέτη.
Όταν είναι μόνοι, ο καθένας είναι αδιάφορος μεταξύ της μουσικής του Bach και του Stravinsky. Αυτό το παίγνιο είναι επίσης γνωστό ως «η μάχη των φύλων», παρόλο που η διαμάχη αυτή δε συμβαίνει πιο συχνά σε άτομα διαφορετικών φύλων.

Ο πίνακας του παιγνίου έχει ως εξής:

		Παίκτης 2	
		Bach	Stravinsky
Παίκτης 1	*Bach*	2,1	0,0
	Stravinsky	0,0	1,2

Προκειμένου να ευρεθεί η ισορροπία κατά Nash, πρέπει να εξεταστούν τα παρακάτω ζεύγη ενεργειών:

- (Bach, Bach): εάν ο παίκτης 1 επιλέξει Stravinsky, τότε το αποτέλεσμα μειώνεται από 2 σε 0 και εάν ο παίκτης 2 επιλέξει Stravinsky τότε το αποτέλεσμα μειώνεται από 1 σε 0. Επομένως, η απόκλιση από το ζεύγος αυτό προκαλεί μείωση στο κέρδος για κάθε παίκτη, έτσι το ζεύγος αποτελεί ισορροπία κατά Nash.
- (Bach, Stravinsky): εάν ο παίκτης 1 επιλέξει Stravinsky, τότε το αποτέλεσμα αυξάνεται από 0 σε 1. Έτσι το ζεύγος αυτό δεν αποτελεί ισορροπία κατά Nash. (Stravinsky, Bach): εάν ο παίκτης 1 επιλέξει Bach, τότε το αποτέλεσμα αυξάνεται από 0 σε 2. Έτσι το ζεύγος αυτό δεν αποτελεί ισορροπία κατά Nash.
- (Stravinsky, Stravinsky): εάν ο παίκτης 1 επιλέξει Bach τότε το αποτέλεσμά του μειώνεται από 1 σε 0 και εάν ο παίκτης 2 επιλέξει Bach τότε το αποτέλεσμα μειώνεται από 2 σε 0. Επομένως, η απόκλιση από το ζεύγος αυτό προκαλεί μείωση στο κέρδος για κάθε παίκτη, έτσι το ζεύγος αποτελεί ισορροπία κατά Nash.

Συνεπώς, το παίγνιο αυτό έχει δύο ισορροπίες κατά Nash: (Bach, Bach) και (Stravinsky, Stravinsky). Αυτό σημαίνει ότι και τα δύο αυτά ζεύγη ενεργειών αποτελούν σταθερά κοινωνικά στερεότυπα. Εφόσον και οι δύο παίκτες επιλέξουν τον Bach, κανένας από τους δύο δεν έχει κίνητρο να αποκλίνει από την απόφαση αυτή, το ίδιο και εάν επιλέξουν Stravinsky. Μοντελοποιώντας για παράδειγμα τις επιλογές των ανδρών σε σχέση με των γυναικών, η ισορροπία κατά Nash δείχνει ότι δύο κοινωνικά στερεότυπα είναι σταθερά: και οι δύο παίκτες επιλέγουν είτε την επιθυμητή από τις γυναίκες ενέργεια είτε την επιθυμητή από τους άντρες ενέργεια.
Όπως και το δίλημμα του φυλακισμένου, το παραπάνω παίγνιο μοντελοποιεί μια πληθώρα καταστάσεων. Για παράδειγμα, δύο εκπρόσωποι του ίδιου πολιτικού κόμματος που θέλουν να πάρουν θέση πάνω σε ένα θέμα. Υποθέτοντας ότι διαφωνούν για την τέλεια λύση, προτιμούν να λάβουν την ίδια θέση παρά διαφορετικές, διότι το δεύτερο θα οδηγήσει σε σύγχυση τους ψηφοφόρους.
Ένα άλλο παράδειγμα είναι η συγχώνευση δύο εταιριών που χρησιμοποιούν διαφορετική μηχανογραφική υποστήριξη. Δυο τμήματα της ίδιας επιχείρησης θα είναι καλύτερο να χρησιμοποιούν την ίδια τεχνολογία υπολογιστών και κάθε εταιρία προτιμά η κοινή τεχνολογία να είναι αυτή που χρησιμοποιήθηκε στο παρελθόν. Στα δύο αυτά παραδείγματα έχει εφαρμογή το παραπάνω παίγνιο.

ΚΟΡΩΝΑ Ή ΓΡΑΜΜΑΤΑ

Το παρακάτω παίγνιο έχει ως βασικό στοιχείο του τη διαμάχη και όχι τα συνεργασία. Δύο άτομα επιλέγουν ταυτόχρονα εάν επιθυμούν να δείξουν κορώνα ή γράμματα. Εάν δείξουν την ίδια πλευρά, ο παίκτης 2 πληρώνει στον παίκτη 1 ένα δολάριο, ενώ εάν δείξουν διαφορετικές πλευρές, ο παίκτης 1 πληρώνει στον παίκτη 2 ένα δολάριο. Ο κάθε παίκτης ενδιαφέρεται για το ποσό των δολαρίων που θα εισπράξει και φυσικά επιθυμεί να εισπράξει περισσότερα από ότι λιγότερα.

Ο πίνακας του παιγνίου φαίνεται παρακάτω:

		Παίκτης 2	
		Κορώνα	*Γράμματα*
Παίκτης 1	*Κορώνα*	1,-1	-1,1
	Γράμματα	-1,1	1,-1

Το παίγνιο αυτό ονομάζεται «πλήρως ανταγωνιστικό», διότι τα ενδιαφέροντα των παικτών είναι διαμετρικά αντίθετα: ο παίκτης 1 επιθυμεί να έχει την ίδια αντίδραση με τον άλλο παίκτη, ενώ ο παίκτης 2 θέλει να έχει την αντίθετη. Εξετάζοντας κάθε ένα από τα τέσσερα ζεύγη ενεργειών, φαίνεται ότι δεν υπάρχει ισορροπία κατά Nash.

Για τα ζεύγη ενεργειών (κορώνα, κορώνα) και (γράμματα, γράμματα) ο παίκτης 2 προτιμά να αλλάξει την επιλογή του, ενώ για ζεύγη ενεργειών (κορώνα, γράμματα) και (γράμματα, κορώνα) ο παίκτης 1 προτιμά να αλλάξει την επιλογή του. Επομένως, το παίγνιο έχει ένα στοχαστικό σταθερό ρυθμό, με βάση τον οποίο κάθε παίκτης επιλέγει τις ενέργειές του με πιθανότητα ½. Εάν ο παίκτης 2 επιλέξει κάποια ενέργεια με πιθανότητα ½, τότε και ο παίκτης 1 επιλέγει μια ενέργεια με την ίδια πιθανότητα.

Αυτό το παίγνιο μπορεί να μοντελοποιήσει τις επιλογές εμφάνισης νέων προϊόντων από μια εδραιωμένη επιχείρηση και μια νεοεισερχόμενη σε μια αγορά καθορισμένου μεγέθους. Κάθε επιχείρηση μπορεί να επιλέξει έναν από δύο διαφορετικούς τρόπους εμφάνισης για το προϊόν. Η εδραιωμένη επιχείρηση προτιμά το νέο προϊόν να διαφέρει από το δικό της, έτσι ώστε οι πελάτες της να μην μπουν στον πειρασμό να αγοράσουν το προϊόν της νέας εταιρίας, ενώ η νεοεισερχόμενη επιχείρηση προτιμά τα προϊόντα να μοιάζουν. Ένα δεύτερο παράδειγμα είναι η σχέση μεταξύ δύο ανθρώπων, από τους οποίους ο ένας θέλει να μοιάζει στον άλλο, ενώ ο δεύτερος όχι.

2ο ΚΕΦΑΛΑΙΟ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

2.1 ΕΙΣΑΓΩΓΗ

Όπως ακριβώς χρησιμοποιούμε τις κλειδαριές για να προστατεύσουμε την περιουσία μας, έτσι και οι υπολογιστές και τα δίκτυα δεδομένων χρειάζονται προϋποθέσεις που θα εξασφαλίζουν την προστασία των πληροφοριών. Η ασφάλεια στο περιβάλλον του Internet είναι και σημαντική αλλά και δύσκολη. Είναι σημαντική επειδή η αξία των πληροφοριών είναι μεγάλη – οι πληροφορίες μπορούν να αγοραστούν και να πωληθούν απευθείας, ή μπορεί να χρησιμοποιηθούν έμμεσα για τη δημιουργία νέων προϊόντων και υπηρεσιών που αποφέρουν μεγάλα κέρδη. Η ασφάλεια σε ένα διαδίκτυο είναι δύσκολη επειδή συνεπάγεται την κατανόηση του χρόνου και του τρόπου με τους οποίους οι συμμετέχοντες χρήστες, υπολογιστές, υπηρεσίες και δίκτυα θα μπορούν να εμπιστευτούν το ένα το άλλο, καθώς και την κατανόηση των τεχνικών λεπτομερειών του υλικού δικτύων και των πρωτοκόλλων. Η ασφάλεια είναι απαραίτητη σε κάθε υπολογιστή και σε κάθε πρωτόκολλο, ένα αδύνατο σημείο αρκεί για να διακυβεύσει την ασφάλεια ολόκληρου του δικτύου. Ακόμα πιο σημαντικό είναι το ότι, επειδή το πρωτόκολλο TCP/IP υποστηρίζει μεγάλη ποικιλία χρηστών, υπηρεσιών και δικτύων και επίσης το διαδίκτυο μπορεί να εκτείνεται σε πολλές περιοχές πολιτικής και οργανισμών, οι συμμετέχοντες ιδιώτες και οργανισμοί πιθανώς να μην συμφωνούν όλοι σε ένα συγκεκριμένο επίπεδο εμπιστοσύνης ή πολιτικών για το χειρισμό των δεδομένων.

2.2 ΠΡΟΣΤΑΣΙΑ ΠΟΡΩΝ

Υπό την ευρεία έννοια, οι όροι *ασφάλεια δικτύου* και *ασφάλεια πληροφοριών* αφορούν την πεποίθηση ότι οι πληροφορίες και οι υπηρεσίες που είναι διαθέσιμες σε ένα δίκτυο δεν θα μπορούν να προσπελαστούν από μη εξουσιοδοτημένους χρήστες. Ασφάλεια σημαίνει προστασία, εξασφάλιση της ακεραιότητας των δεδομένων, αποτροπή της μη εξουσιοδοτημένης πρόσβασης στους πόρους των υπολογιστών, αποτροπή της κατασκοπίας ή της υποκλοπής και αποφυγή του ενδεχόμενου διακοπής των υπηρεσιών. Φυσικά, όπως ακριβώς και η φυσική περιουσία δεν είναι απολύτως ασφαλής απέναντι στο έγκλημα, έτσι και κανένα δίκτυο δεν είναι απολύτως ασφαλές. Οι οργανισμοί καταβάλλουν προσπάθειες για να προστατεύσουν τα δίκτυα για τον ίδιο λόγο που προσπαθούν να προστατεύσουν τα κτίρια και τα γραφεία τους: τα στοιχειώδη μέτρα ασφαλείας μπορούν να αποθαρρύνουν τις εγκληματικές ενέργειες, δυσκολεύοντας κατά πολύ την πραγματοποίηση τους.

Η παροχή ασφάλειας για τις πληροφορίες απαιτεί την προστασία τόσο των φυσικών όσο και των αφηρημένων πόρων. Στους φυσικούς πόρους περιλαμβάνονται οι παθητικές συσκευές αποθήκευσης, όπως οι δίσκοι και τα CD-ROM, καθώς και οι ενεργητικές συσκευές, όπως οι υπολογιστές των χρηστών. Σε ένα περιβάλλον δικτύου, η φυσική ασφάλεια εκτείνεται στα καλώδια, τις γέφυρες και τους δρομολογητές που αποτελούν την υποδομή του δικτύου. Στην πραγματικότητα, αν και σπάνια γίνεται αναφορά στη φυσική ασφάλεια, αυτή παίζει συχνά σημαντικό ρόλο στο συνολικό σχεδιασμό ασφάλειας. Είναι προφανές ότι η φυσική ασφάλεια μπορεί να αποτρέψει τα φαινόμενα δολιοφθοράς (π.χ. την απενεργοποίηση ενός δρομολογητή με σκοπό να δρομολογηθούν τα πακέτα μέσω μιας εναλλακτικής, λιγότερο ασφαλούς διαδρομής).

Η προστασία ενός αφηρημένου πόρου, όπως είναι οι πληροφορίες, είναι συνήθως πιο δύσκολη από την παροχή φυσικής προστασίας, επειδή οι πληροφορίες είναι κάτι το αόριστο. Η ασφάλεια των πληροφοριών συμπεριλαμβάνει πολλές πτυχές προστασίας:

- *Ακεραιότητα δεδομένων.* Ένα ασφαλές σύστημα πρέπει να προστατεύει τις πληροφορίες από τη μη εξουσιοδοτημένη τροποποίηση.
- *Διαθεσιμότητα δεδομένων.* Το σύστημα πρέπει να εγγυάται ότι οι εξωτερικοί χρήστες δεν θα είναι σε θέση να αποτρέψουν τη νόμιμη πρόσβαση στα δεδομένα (π.χ. κανένας εξωτερικός χρήστης δεν θα πρέπει να είναι σε θέση να αποκλείσει πελάτες από το να προσπελάσουν μια τοποθεσία του Ιστού).

- *Εξασφάλιση απορρήτου ή εμπιστευτικότητας.* Το σύστημα δεν πρέπει να επιτρέπει σε εξωτερικούς χρήστες να δημιουργούν αντίγραφα των δεδομένων καθώς αυτά μεταφέρονται μέσω ενός δικτύου, ή να κατανοούν τα περιεχόμενα τους στην περίπτωση που δημιουργούνται αντίγραφα.
- *Εξουσιοδότηση*. Παρόλο που η φυσική ασφάλεια ταξινομεί συχνά τους ανθρώπους και τους πόρους σε ευρείες κατηγορίες (π.χ. τα άτομα που δεν ανήκουν στο προσωπικό δεν επιτρέπεται να χρησιμοποιήσουν ένα συγκεκριμένο χώρο), η ασφάλεια των πληροφοριών πρέπει να είναι πιο περιοριστική (π.χ. ορισμένα τμήματα του αρχείου ενός υπαλλήλου είναι διαθέσιμα μόνο στο τμήμα προσωπικού, άλλα είναι διαθέσιμα μόνο στον εργοδότη του υπαλλήλου και άλλα είναι διαθέσιμα μόνο στο τμήμα μισθοδοσίας).
- *Πιστοποίηση ταυτότητας.* Το σύστημα θα πρέπει να επιτρέπει σε δύο οντότητες που επικοινωνούν μεταξύ τους να επαληθεύουν τις ταυτότητές τους.
- *Αποφυγή επανάληψης.* Για να μην είναι δυνατή η αποτύπωση αντιγράφων πακέτων και η μετέπειτα χρήση τους από εξωτερικούς χρήστες, το σύστημα πρέπει να εμποδίζει την αποδοχή ενός αναμεταδιδόμενου αντίγραφου πακέτου.

2.3 ΠΟΛΙΤΙΚΗ ΠΛΗΡΟΦΟΡΙΩΝ

Για να μπορέσει ένας οργανισμός να επιβάλει μια στρατηγική ασφάλειας δικτύου, θα πρέπει πρώτα να εκτιμήσει τους κινδύνους και να αναπτύξει μια σαφή πολιτική όσον αφορά την πρόσβαση στις πληροφορίες και την προστασία τους. Η πολιτική καθορίζει τα άτομα στα οποία θα παραχωρηθεί πρόσβαση σε κάθε είδος πληροφοριών, τους κανόνες που πρέπει να ακολουθεί κάθε άτομο κατά τη διάδοση των πληροφοριών σε άλλους, και μια δήλωση για το πώς θα αντιδράσει η εταιρεία στις παραβάσεις.

Η πολιτική των πληροφοριών ξεκινά από τους ανθρώπους, επειδή:

Συνήθως ο άνθρωπος είναι το πιο ευάλωτο σημείο οποιουδήποτε σχεδιασμού ασφαλείας. Ένας εργαζόμενος που είναι κακοπροαίρετος, απρόσεκτος, ή όχι καλά ενημερωμένος σχετικά με την πολιτική πληροφοριών μιας εταιρείας, μπορεί να θέσει σε κίνδυνο ακόμα και την καλύτερη ασφάλεια.

2.4 ΑΣΦΑΛΕΙΑ INTERNET

Η ασφάλεια στο Internet είναι δύσκολη, επειδή τα αυτοδύναμα πακέτα που ταξιδεύουν από μία προέλευση προς έναν προορισμό συχνά περνούν μέσα από πολλά ενδιάμεσα δίκτυα και δρομολογητές, που δεν ανήκουν ή δεν ελέγχονται ούτε από τον αποστολέα ούτε από τον παραλήπτη. Επομένως, δεν είναι δυνατό να θεωρείται το περιεχόμενο των αυτοδύναμων πακέτων αξιόπιστο, επειδή μπορεί να υποκλαπούν ή να τροποποιηθούν. Για να δώσουμε ένα παράδειγμα, ας φανταστούμε ένα διακομιστή που επιχειρεί να χρησιμοποιήσει την *πιστοποίηση ταυτότητας προέλευσης* για να επαληθεύσει ότι οι αιτήσεις προέρχονται από έγκυρους πελάτες. Η πιστοποίηση ταυτότητας προέλευσης απαιτεί από το διακομιστή να εξετάσει τη διεύθυνση IP προέλευσης κάθε εισερχόμενου αυτοδύναμου πακέτου και να δεχτεί μόνο τις αιτήσεις που προέρχονται από υπολογιστές οι οποίοι υπάρχουν σε μια εξουσιοδοτημένη λίστα. Η πιστοποίηση ταυτότητας προέλευσης είναι *αδύναμο μέτρο,* επειδή είναι εύκολο να διασπαστεί. Πιο συγκεκριμένα, ένας ενδιάμεσος δρομολογητής μπορεί να παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση ενός διακομιστή και να καταγράψει τη διεύθυνση IP ενός έγκυρου πελάτη. Στη συνέχεια ο ενδιάμεσος δρομολογητής μπορεί να κατασκευάσει μια αίτηση με την ίδια διεύθυνση προέλευσης (και να υποκλέψει την απάντηση). Το σημαντικό σημείο είναι ότι:

Μια μέθοδος εξουσιοδότησης που χρησιμοποιεί τη διεύθυνση IP ενός απομακρυσμένου υπολογιστή για να πιστοποιήσει την ταυτότητά του δεν είναι επαρκής σε ένα μη ασφαλές διαδίκτυο. Ένας απατεώνας που αποκτά έλεγχο σε κάποιον ενδιάμεσο δρομολογητή μπορεί να αποκτήσει πρόσβαση υποδυόμενος έναν εξουσιοδοτημένο χρήστη.

Οι πιο ισχυρές μέθοδοι πιστοποίησης ταυτότητας απαιτούν κρυπτογράφηση. Για να κρυπτογραφήσει ο αποστολέας ένα μήνυμα, εφαρμόζει μια μαθηματική συνάρτηση που αναδιατάσσει τα ψηφία σύμφωνα με ένα κλειδί το οποίο είναι γνωστό μόνο στον αποστολέα. Ο παραλήπτης χρησιμοποιεί μια άλλη μαθηματική συνάρτηση, για να αποκρυπτογραφήσει το μήνυμα. Με την προσεκτική επιλογή του αλγορίθμου κρυπτογράφησης, του κλειδιού, και των περιεχομένων των μηνυμάτων, τα ενδιάμεσα μηχανήματα θα είναι σχεδόν αδύνατο να αποκωδικοποιήσουν τα μηνύματα ή να κατασκευάσουν έγκυρα μηνύματα.

2.5 ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ

Οι πλέον τυπικές απειλές και επιθέσεις για την ασφάλεια των δεδομένων κατά την διακίνηση τους μέσα από δίκτυα και κυρίως από το Internet είναι οι παρακάτω:

- Υποκλοπή (Sniffing) ή απλή παρακολούθηση της κυκλοφορίας των μηνυμάτων .
- Προσποίηση (Spoofing) υποκειμένου επικοινωνίας.
- Πειρατεία σύνδεσης (Session hijacking).
- Αλλοίωση ή αφαίρεση δεδομένων με αποτέλεσμα την τροποποίηση μηνυμάτων.
- Εισαγωγή νόθων μηνυμάτων.
- Παρεμπόδιση παροχής υπηρεσιών (Denial of service).
- Αποστολή ιών.

Υποκλοπή (Sniffing). Η υποκλοπή δεδομένων είναι ιδιαίτερα απλή σε κοινόχρηστα μέσα όπως για παράδειγμα σε τοπικά δίκτυα Ethernet. Με χρήση π.χ. μιας Network Interface Card – (NIC) που έχει προγραμματιστεί να διαβάζει όλα τα πακέτα στο Ethernet ανεξαρτήτως διευθύνσεως, μπορεί κάποιος να καταγράφει όλα τα πακέτα του δικτύου συμπεριλαμβανομένων και των login συνομιλιών, που περιέχουν passwords και στη συνέχεια να αποκτήσει δυνατότητα σύνδεσης σε υπολογιστές που δεν είχε δικαίωμα πρόσβασης. Μπορεί επίσης να διαβάσει εμπιστευτικά δεδομένα που διακινούνται στο δίκτυο. Επειδή η υποκλοπή διευκολύνεται όταν ο εισβολέας είναι φυσικά συνδεδεμένος στο δίκτυο, απαιτείται προσεχτικός έλεγχος των φυσικών συνδέσεων από τον διαχειριστή του δικτύου.

Προσποίηση (Spoofing). Στα IP δίκτυα και το Internet η μετάδοση των δεδομένων γίνεται πάντα μέσα από πακέτα στην προμετωπίδα των οποίων υπάρχει η IP διεύθυνση του αποστολέα καθώς και αυτή του παραλήπτη. Με την τεχνική του spoofing ο επιτιθέμενος τοποθετεί στην προμετωπίδα του IP πακέτου μια διαφορετική διεύθυνση αποστολέα προσποιούμενος με αυτόν τον τρόπο ότι είναι κάποιος άλλος ώστε να ξεγελάσει τον απέναντι συνομιλητή να αρχίσει επικοινωνία μαζί του.

Πειρατεία στην σύνδεση. (Session Hijacking). Παρόμοια αλλά περισσότερο εξελιγμένη απειλή από το spoofing, όπου ο επιτιθέμενος προσπαθεί να αποκτήσει τον έλεγχο σε μια ήδη ανοικτή επικοινωνία μεταξύ δύο υπολογιστών και να υποκαταστήσει έτσι τον ένα από τους συνομιλητές.

Η επίθεση αυτή καθιστά την αρχική αναγνώριση ταυτότητας του συνομιλητή ανεπαρκή, καθώς ο επιτιθέμενος μπορεί με τον τρόπο αυτό να υποκαταστήσει έναν συνομιλητή του οποίου η ταυτότητα ελέγχθηκε και επιβεβαιώθηκε με αυστηρότητα κατά την έναρξη της συνομιλίας. Η ταυτότητα του συνομιλητή είναι πλέον ανάγκη να ελέγχεται σε τακτά χρονικά διαστήματα καθ' όλη την διάρκεια της συνομιλίας για να εξασφαλίζεται ο κίνδυνος από τέτοιες επιθέσεις.

Αλλοίωση ή αφαίρεση δεδομένων. Ο επιτιθέμενος στην περίπτωση αυτή όχι μόνο διαβάζει υποκλέπτοντας τα δεδομένα αλλά τα τροποποιεί ή τα καταστρέφει ή ακόμα και τα εξαφανίζει ώστε να μην ληφθούν ποτέ από τον παραλήπτη.

Εισαγωγή νόθων μηνυμάτων όπου στην συνομιλία δυο μερών παρεισφρύουν μηνύματα που δεν ανήκουν σε αυτούς.

Παρεμπόδιση λειτουργίας. (Denial of service). Ο επιτιθέμενος στην περίπτωση αυτή προσπαθεί να παρεμποδίσει την αποστολή και λήψη δεδομένων υπερφορτώνοντας π.χ. το κανάλι επικοινωνίας.

Αποστολή ιών. Είναι μια από τις συχνότερες απειλές ιδιαίτερα στο διαδίκτυο όπου ο επιτιθέμενος αποστέλλει προγράμματα που μπορούν να έχουν ποικίλες επιπτώσεις από πλήρη καταστροφή αρχείων και δεδομένων μέχρι την απλή παρενόχληση του παραλήπτη. Συχνά οι ιοί μεταφέρονται μέσω του ηλεκτρονικού ταχυδρομείου ή άλλων μέσων και αναπαράγονται αυτόματα ώστε να διαδίδονται ταχύτατα σε πολλούς ανυποψίαστους χρήστες.

2.6 ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Μερικά από τα βασικά θέματα ασφάλειας στα δίκτυα είναι τα παρακάτω:

- Επιβεβαίωση ταυτότητας (Authentication)
- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα δεδομένων (Data Integrity)
- Δικαιοδοσία πρόσβασης (Authorization)
- Απάρνηση ενέργειας ή πράξης (Non repudiation)

Επιβεβαίωση ταυτότητας (Authentication). Αφορά την επιβεβαίωση της ταυτότητας του συνομιλητή, καθώς στις επικοινωνίες μέσω δικτύων έχει σημασία το πρόσωπο ή ο Η/Υ με τον οποίο είμαστε σε επικοινωνία, να είναι όντως αυτός που νομίζουμε.

Εμπιστευτικότητα (Confidentiality). Εμπιστευτικότητα στην επικοινωνία σημαίνει ότι κανείς μη εξουσιοδοτημένος δεν μπορεί να έχει πρόσβαση και να διαβάσει τα δεδομένα που μεταφέρονται μέσω του δικτύου. Η κρυπτογράφηση είναι ένας αποτελεσματικός τρόπος αντιμετώπισης του κινδύνου αυτού.

Ακεραιότητα δεδομένων (Data Integrity). Ακεραιότητα των δεδομένων σημαίνει ότι τα δεδομένα με κανένα τρόπο δεν έχουν τροποποιηθεί ή καταστραφεί κατά την μεταφορά τους μέσω του δικτύου.

Δικαιοδοσία πρόσβασης (Authorization). Τα συστήματα δικαιοδοσίας πρόσβασης επιτρέπουν την πρόσβαση μόνον σε εξουσιοδοτημένους χρήστες. Σε μεγάλα υπολογιστικά συστήματα που εξυπηρετούν πολυάριθμους χρήστες η μη αυστηρή τήρηση του Authorization ή οι αδυναμίες των λειτουργικών συστημάτων μπορεί να επιτρέψουν σε εισβολείς την πρόσβαση σε μη επιτρεπτούς πόρους.

Απάρνηση ενέργειας ή πράξης (Non repudiation). Στην περίπτωση αυτή το ένα από το δύο συμβαλλόμενα μέρη στην επικοινωνία απαρνείται την συναλλαγή (π.χ. αποστολή ή λήψη μηνύματος) που έκανε. Ένας ιστορικά γνωστός τρόπος αντιμετώπισης είναι η επιβεβαίωση της συναλλαγής από ένα τρίτο κοινά αποδεκτό φορέα (trusted party) όπως για παράδειγμα του τηλεπικοινωνιακού οργανισμού στην περίπτωση του TELEX.

2.7 ΑΝΤΙΜΕΤΩΠΙΣΗ ΘΕΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ

Για την αντιμετώπιση των απειλών και γενικότερα των θεμάτων ασφαλείας υπάρχει πληθώρα τεχνικών για την κάθε περίπτωση όπως τεχνικές που σχετίζονται με την αναγνώριση, με την διόρθωση , ή με την παρεμπόδιση επίθεσης. Η κρυπτογράφηση, οι ψηφιακές υπογραφές, το γέμισμα των κυκλοφοριακών κενών, τα firewalls, η αλυσιδωτή των μηνυμάτων, η χρονοσφραγίδα, το intrusion detection, ειδικά πρωτόκολλα όπως π.χ. IPSec, L2TP, L2F, PAP, CHAP, TACACS αποτελούν ειδικά παραδείγματα τέτοιων τεχνικών. Στη συνέχεια θα αναφερθούμε σε τεχνικές Authentication, σε τεχνικές κρυπτογράφησης στις ψηφιακές υπογραφές, στα VPN, καθώς και σε ορισμένα πρωτόκολλα όπως το IPSec που χρησιμοποιούνται ευρέως στα VPN.

2.7.1 AUTHENTICATION (Επιβεβαίωση ταυτότητας)

Ο έλεγχος της πρόσβασης των χρηστών στους κοινόχρηστους πόρους και τους υπολογιστές του δικτύου είναι ζωτικής σημασίας για την ασφάλεια. Είναι ευνόητο ότι σε κάθε δίκτυο και κάθε σύστημα μηχανογράφησης πρέπει να διασφαλίζεται ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στους υπολογιστές, στις βάσεις δεδομένων και γενικότερα στα σημεία του δικτύου που φυλάσσονται κρίσιμα ή ευαίσθητα στοιχεία ή γίνονται συναλλαγές.

Η επιβεβαίωση ταυτότητας γενικότερα βασίζεται σε τρία διαφορετικά στοιχεία:

- Κάτι που γνωρίζουμε π.χ. ένας κωδικός πρόσβασης, συνθηματικό ή password. Αδύνατο σημείο είναι ότι συχνά τέτοιοι κωδικοί είναι δυνατόν να υποκλαπούν ή να προβλεφθούν. Δυνατό σημείο η ευκολία χρήσης μέσα από δίκτυα.
- Κάτι που έχουμε π.χ. κλειδί, κάρτα. Επίσης μπορεί να χαθεί ή να κλαπεί. Η χρήση έξυπνων καρτών μπορεί εύκολα να υλοποιηθεί και μέσω δικτύων εφόσον υπάρξει ευρέως αποδεκτή διεθνής τυποποίηση.
- Βιομετρικά στοιχεία π.χ. δακτυλικά αποτυπώματα, αναγνώριση φωνής, ίριδας ή κόρης οφθαλμού, αναγνώριση προσώπου κ.λ.π. Είναι ισχυρό στοιχείο ταυτοπροσωπίας αλλά έχει υψηλό κόστος υλοποίησης λόγω των απαιτούμενων συσκευών, για να χρησιμοποιηθεί μέσω δικτύου δεδομένων.

Όταν υπάρχει ανάγκη για αυστηρή επιβεβαίωση ταυτότητας τότε χρησιμοποιούνται ταυτόχρονα περισσότερα από ένα στοιχεία, όπως για παράδειγμα στην ανάληψη χρημάτων από την αυτόματη ταμειολογιστική μηχανή (ATM) μιας τράπεζας όπου απαιτείται πέρα από την ειδική κάρτα που διαθέτει ο χρήστης να πληκτρολογήσει και ένα προσωπικό κωδικό πρόσβασης που πρέπει να απομνημονεύει.

Μια ιδιαίτερη μορφή κωδικού πρόσβασης είναι το One Time Password (OTP) που έχει την ιδιομορφία να διαφοροποιείται κάθε φορά που αποστέλλεται ώστε να μην είναι δυνατή η επαναχρησιμοποίηση του και κατά συνέπεια η υποκλοπή του. Μειονέκτημα της μεθόδου αυτής που περιγράφεται στο RFC 2289 είναι η δυσκολία χρήσης του όταν το πλήθος των χρηστών είναι μεγάλο. Στη συνέχεια θα αναφερθούμε στις αρχές λειτουργίας των πρωτοκόλλων PAP και CHAP, που έχουν χρήση στην επιβεβαίωση ταυτότητας.

Password Authentication Protocol (PAP)

Το πρωτόκολλο αυτό είναι σχετικά απλό και σχεδιάστηκε για την επιβεβαίωση ταυτότητας ενός υπολογιστή Α που επικοινωνεί με κάποιον άλλο Β μέσου του PPP πρωτοκόλλου επικοινωνίας.

Η αναγνώριση του Α γίνεται στην αρχική φάση αποκατάστασης μιας PPP σύνδεσης, με αποστολή από τον Α δύο στοιχείων, ενός κωδικού χρήστη και ενός password. Ο υπολογιστής Β στην άλλη πλευρά αποστέλλει πίσω στον Α την επιβεβαίωση της αναγνώρισης εφόσον ο συνδυασμός των δύο στοιχείων ταιριάζει.

Το PAP πολύ απλό και καθόλου ασφαλές επειδή η αποστολή του κωδικού χρήστη και του password δεν είναι κρυπτογραφημένη. Επίσης παρέχεται η ευχέρεια σε ένα επιτιθέμενο να κάνει πολλές προσπάθειες έως ότου μαντέψει ένα σωστό συνδυασμό.

Challenge Handshake Authentication Protocol (CHAP)

Το CHAP έχει την ίδια χρήση με το PAP σε ζεύξεις PPP αλλά είναι περισσότερο ασφαλές. Χρησιμοποιείται για την επιβεβαίωση ταυτότητας τόσο στην αρχή της σύνδεσης όσο και στο ενδιάμεσο. Η διαδικασία είναι τριών διαδρόμων δηλαδή:

- Ο υπολογιστής Α ζητάει καταρχήν την ταυτότητα του συνδεόμενου Β αποστέλλοντας σε αυτόν ένα μήνυμα πρόσκλησης (Challenge message).
- Ο συνδεόμενος Β λαμβάνει το μήνυμα πρόσκλησης και εφαρμόζοντας σε αυτό ένα προσυμφωνημένο αλγόριθμο hash, υπολογίζει ένα μικρού μεγέθους digest, το οποίο στέλνει πίσω στον αποστολέα Α.
- Ο αποστολέας Α που είναι και παράλληλα ο ελεγκτής της ταυτότητας του Β, επιβεβαιώνει την αυθεντικότητα του Β εφόσον το ληφθέν digest είναι ίδιο με το υπολογιζόμενο, δηλαδή εφόσον η απάντηση είναι η αναμενόμενη.

Η αναμενόμενη αυτή μπορεί να επαναληφθεί οποτεδήποτε κατά την διάρκεια της επικοινωνίας ώστε να επιβεβαιώνεται συχνά ότι η άλλη πλευρά εξακολουθεί να είναι η πραγματική και δεν έχει υποκατασταθεί από κάποιον ανεπιθύμητο ενδιάμεσο.

Με το CHAP σε περίπτωση αποτυχίας της αρχικής επιβεβαίωσης η σύνδεση διακόπτεται και ο απέναντι υπολογιστής πρέπει να ξεκινήσει αποκατάσταση νέας σύνδεσης εξαρχής πράγμα που δυσκολεύει τις πολλαπλές προσπάθειες διείσδυσης.

Τα μειονεκτήματα των πρωτοκόλλων PAP και CHAP είναι ότι δεν διαφοροποιούν την πρόσβαση σε διαφορετικούς χρήστες και δεν μπορούν να δώσουν διαφορετικά προνόμια σε αυτούς. Επίσης λόγω του γεγονότος ότι βασίζονται σε passwords που πρέπει να μοιράζονται σε κάθε διαφορετικό χρήστη, η διαχείριση σε περιβάλλον με πολυάριθμους χρήστες γίνεται δυσχερής.

2.7.2 ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Κρυπτογράφηση είναι η διαδικασία εκείνη που επιτυγχάνει την αλλοίωση της όψης ενός μηνύματος, με τέτοιο τρόπο ώστε να μην γίνεται κατανοητό από μη εξουσιοδοτημένα πρόσωπα, χωρίς την αλλοίωση αυτού καθεαυτού του μηνύματος.

Με τον όρο **κρυπτογραφία** (cryptography) αναφερόμαστε στην επιστήμη που ασχολείται με τα θέματα αυτά, ενώ με τους όρους **κρυπτογράφηση** (encryption) και **αποκρυπτογράφηση** (decryption) στις διαδικασίες και τεχνικές που χρησιμοποιούνται, ενώ τέλος η μεθοδολογία σπασίματος της κρυπτογράφησης ονομάζεται **κρυπτανάλυση.**

Η σύγχρονη κρυπτογράφηση βασίζεται σε δύο στοιχεία:

- Τον *Αλγόριθμο* και
- Το *Κλειδί*

Ο **Αλγόριθμος** είναι μια μαθηματική ή λογική συνάρτηση που μετατρέπει το αρχικό μήνυμα (plaintext), με τη βοήθεια μιας σειράς ψηφίων (bit) που καλούνται **κλειδί**, σε κρυπτογραφημένο μήνυμα (cipher text) που δεν είναι αναγνώσιμο από μη εξουσιοδοτημένο πρόσωπο. Ο Αλγόριθμος συνήθως είναι δημοσιοποιημένος, ενώ το κλειδί είναι το μυστικό μέρος, η παράμετρος που επηρεάζει τον αλγόριθμο κρυπτογράφησης. Στο σχήμα 2.1 φαίνεται η σχέση όλων αυτών.

Το προς κρυπτογράφηση ονομάζεται “plaintext” ενώ το κρυπτογραφημένο “cipher text” και “cryptogram”. Το σύνολο των μηχανισμών που χρησιμοποιούμε για την τροποποίηση μηνύματος ονομάζεται cipher. Στην ουσία η κρυπτογράφηση μετατρέπει το προς αποστολή κείμενο σε κρυπτογράφημα προκειμένου να το περάσει μέσα από το δίκτυο προς τον δέκτη όπου θα γίνει η αποκρυπτογράφηση.

Το πλήθος των κλειδιών που μπορεί να χρησιμοποιήσει ένας αλγόριθμος εξαρτάται από τον αριθμό των bit στο κλειδί. Για παράδειγμα ένα κλειδί των 8 bit υποστηρίζει 2^8=256 διαφορετικούς συνδυασμούς, άρα κλειδιά.

Ο βαθμός δυσκολίας για την διάσπαση του κώδικα εξαρτάται από το μήκος του κλειδιού, ενώ για το κλειδί των 8-bit απαιτούνται κλάσματα του δευτερολέπτου, για ένα κλειδί των 100 bit για να ψάξει ένας υπολογιστής 2^100 συνδυασμούς θέλει μερικούς αιώνες.

Σχήμα 2.1 Τεχνική Ιούλιου Καίσαρα

Οι βασικές μέθοδοι που ακολουθούνται στην κρυπτογράφηση είναι οι της αντικατάστασης και της αντιμετάθεσης.

Με την **αντικατάσταση** κάθε σύμβολο αντιστοιχείται σε κάποιο άλλο σαφώς καθορισμένο. Για παράδειγμα η μέθοδος που αποδίδεται στον Ιούλιο Καίσαρα αντιστοιχεί στο κάθε γράμμα ένα άλλο γράμμα όπως φαίνεται στο σχήμα 2.1. Η λέξη open θα αντικατασταθεί με τη λέξη zapy. Η μέθοδος φαίνεται ασφαλής καθώς για να αποκρυπτογραφηθεί ένα μήνυμα μπορεί να γίνουν όλοι οι συνδυασμοί των 26 γραμμάτων, δηλαδή 26!=4*10^26 και χρειάζεται αρκετός χρόνος.

Με την **αντιμετάθεση** τροποποιείται η θέση του κάθε συμβόλου μέσα στο μήνυμα, έτσι που στο προηγούμενο παράδειγμα η λέξη open γίνεται eonp.

Η μοντέρνα κρυπτογράφηση χρησιμοποιεί συνδυασμό αντιμετάθεσης και αντικατάστασης, με τη διαφορά του ότι η αντικατάσταση γίνεται με τη βοήθεια συναρτήσεων και πολύπλοκων μαθηματικών υπολογισμών.

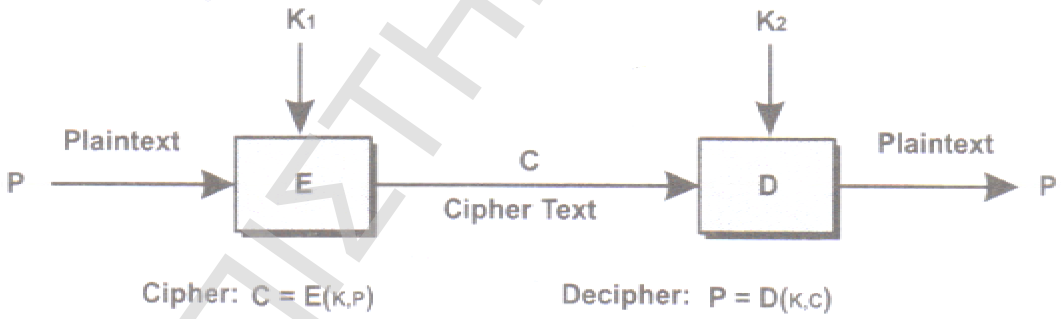
Στην κρυπτογράφηση που βασίζεται σε κλειδιά, διακρίνουμε δύο κατηγορίες, την συμμετρική και την ασύμμετρη.

Η παλαιότερη μέθοδος της κρυπτογράφησης είναι η συμμετρική που καλείται και μυστικού κλειδιού, καθώς και τα δύο μέρη της επικοινωνίας χρησιμοποιούν το ίδιο μυστικό κλειδί. Βασικό μειονέκτημα της συμμετρικής κρυπτογράφησης αναφέρεται το ότι τα συμβαλλόμενα μέρη πρέπει να συμφωνούν κάθε φορά το κλειδί, ενώ αν μιλάς με πολλούς με πολλούς πρέπει κάθε φορά να θυμάσαι το σωστό κλειδί. Επίσης επειδή μπορεί να χρησιμοποιείται το ίδιο κλειδί από περισσότερους χρήστες, δεν γίνεται σαφές το ποιος έστειλε το μήνυμα, αφού ο ένας μπορεί να ισχυρίζεται ότι το έστειλε ο άλλος.

Για να λυθεί αυτό το πρόβλημα χρησιμοποιείται η **ασύμμετρη** κρυπτογράφηση και η τεχνική του δημόσιου κλειδιού. Η κρυπτογράφηση αυτή βασίζεται στη λογική του **ζεύγους κλειδιών** (ιδιωτικό - δημόσιο), όπου μηνύματα που κρυπτογραφούνται με το ένα κλειδί αποκρυπτογραφούνται με το άλλο και αντίστροφα.

Ένας χρήστης διατηρεί αυστηρά μυστικό το ιδιωτικό του κλειδί, ενώ μπορεί να δώσει το δημόσιο κλειδί, σε όσους επιθυμούν να του στέλνουν κρυπτογραφημένα μηνύματα. Στο σχήμα φαίνεται ότι ο παραλήπτης Β έχει δώσει στον αποστολέα Α το δημόσιο κλειδί για να του στείλει μηνύματα, ενώ φαίνεται ότι ο μόνος που μπορεί να διαβάσει αυτά τα μηνύματα είναι ο κάτοχος του ιδιωτικού κλειδιού, δηλαδή ο Β.

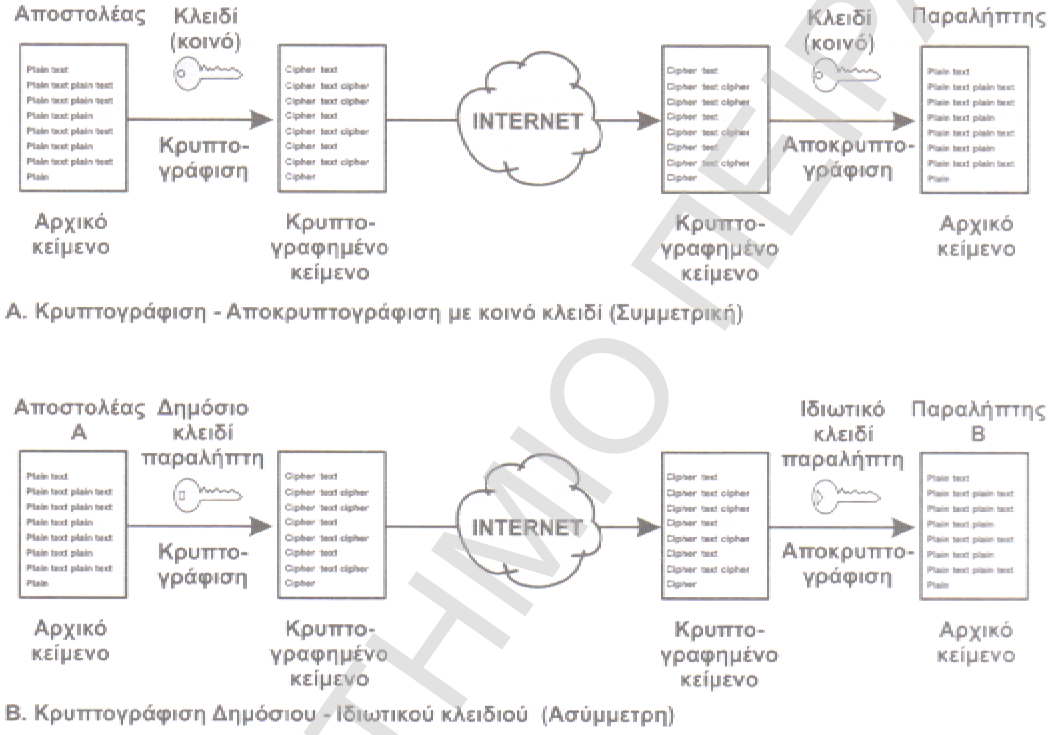
Στην αντίστροφη περίπτωση αποστολής μηνύματος από τον Β στον Α, ο Β έχει δύο δυνατότητες. Με την πρώτη χρησιμοποιεί το δημόσιο κλειδί του Α και ο Α αποκρυπτογραφεί το μήνυμα με το δικό του ιδιωτικό κλειδί. Η χρήση του μοναδικού ιδιωτικού κλειδιού στην κωδικοποίηση ενός μηνύματος αντιστοιχεί στην υπογραφή του μηνύματος από τον αποστολέα. Στην περίπτωση αυτή ο παραλήπτης είναι βέβαιος για την ταυτότητα του αποστολέα, αλλά δεν είναι βέβαιος ότι κανείς άλλος που κατέχει το δημόσιο κλειδί του αποστολέα, δεν έχει διαβάσει το ίδιο μήνυμα.



ΣΧΗΜΑ 2.2 Κρυπτογράφηση

Εναλλακτικά ο Β αποστέλλει το μήνυμα κωδικοποιώντας το με το δικό του ιδιωτικό κλειδί, ενώ ο Α το αποκρυπτογραφεί με το δημόσιο κλειδί του Β που έχει στην κατοχή του. Στην αυτή περίπτωση, ο Α είναι απόλυτα βέβαιος για την ταυτότητα του αποστολέα καθώς το ιδιωτικό κλειδί του Β είναι μοναδικό.

Έτσι τα κλειδιά αυτά χρησιμοποιούνται για δυο διαφορετικούς σκοπούς, ο ένας για να προσφέρει εμπιστευτικότητα μηνύματος και ο άλλος για να αποδεικνύει την αυθεντικότητα του αποστολέα. Μια πολύ γνωστή τεχνική για την κρυπτογράφηση δημόσιου και ιδιωτικού κλειδιού είναι η RSA που αναπτύχθηκε από τους καθηγητές του MIT Ronald Rivest, Adir Samir, Leonard Adelman.



ΣΧΗΜΑ 2.3 Συμμετρική και ασύμμετρη κρυπτογράφηση

2.7.3 ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ

Μια παράπλευρη επέκταση της χρήσης της κρυπτογράφησης με την τεχνική του δημόσιου και του ιδιωτικού κλειδιού, είναι η ψηφιακή υπογραφή. Η χρήση του ιδιωτικού κλειδιού, το οποίο είναι μοναδικό και καλά φυλασσόμενο από τον ιδιοκτήτη του για την κρυπτογράφηση ενός κειμένου, μπορεί να θεωρηθεί ως η προσωπική ψηφιακή υπογραφή του.

Πρέπει να σημειωθεί εδώ ότι ένα μεγάλο σε μεγάλο μήκος κείμενο θέλει πολύ χρόνο επεξεργασίας για να κρυπτογραφηθεί και να αποκρυπτογραφηθεί με την τεχνική του δημόσιου και ιδιωτικού κλειδιού. Προς τούτο δημιουργείται με κάποιο τρόπο μία μικρού μήκους ακολουθία bit η οποία ονομάζεται digest. Η κρυπτογράφηση αυτού του digest με το ιδιωτικό κλειδί χρησιμοποιείται ως ψηφιακή υπογραφή.

Επί πλέον η τεχνική του digest επιβεβαιώνει το κατά πόσον το κείμενο δεν έχει τροποποιηθεί, καθώς η παραμικρή αλλαγή στο κείμενο θα έχει ως αποτέλεσμα διαφορετικό digest.

Ο πιο γνωστός τρόπος δημιουργίας του digest ενός κειμένου είναι η χρήση ειδικών αλγορίθμων που ονομάζονται μονοσήμαντες συναρτήσεις hash (one-way hash functions). Οι συναρτήσεις αυτές δεν χρησιμοποιούν κλειδιά, απλώς είναι ένας τρόπος μονοσήμαντης δημιουργίας από ένα μήνυμα, μιας ακολουθίας χαρακτήρων συγκεκριμένου μήκους (π.χ. 16 byte).

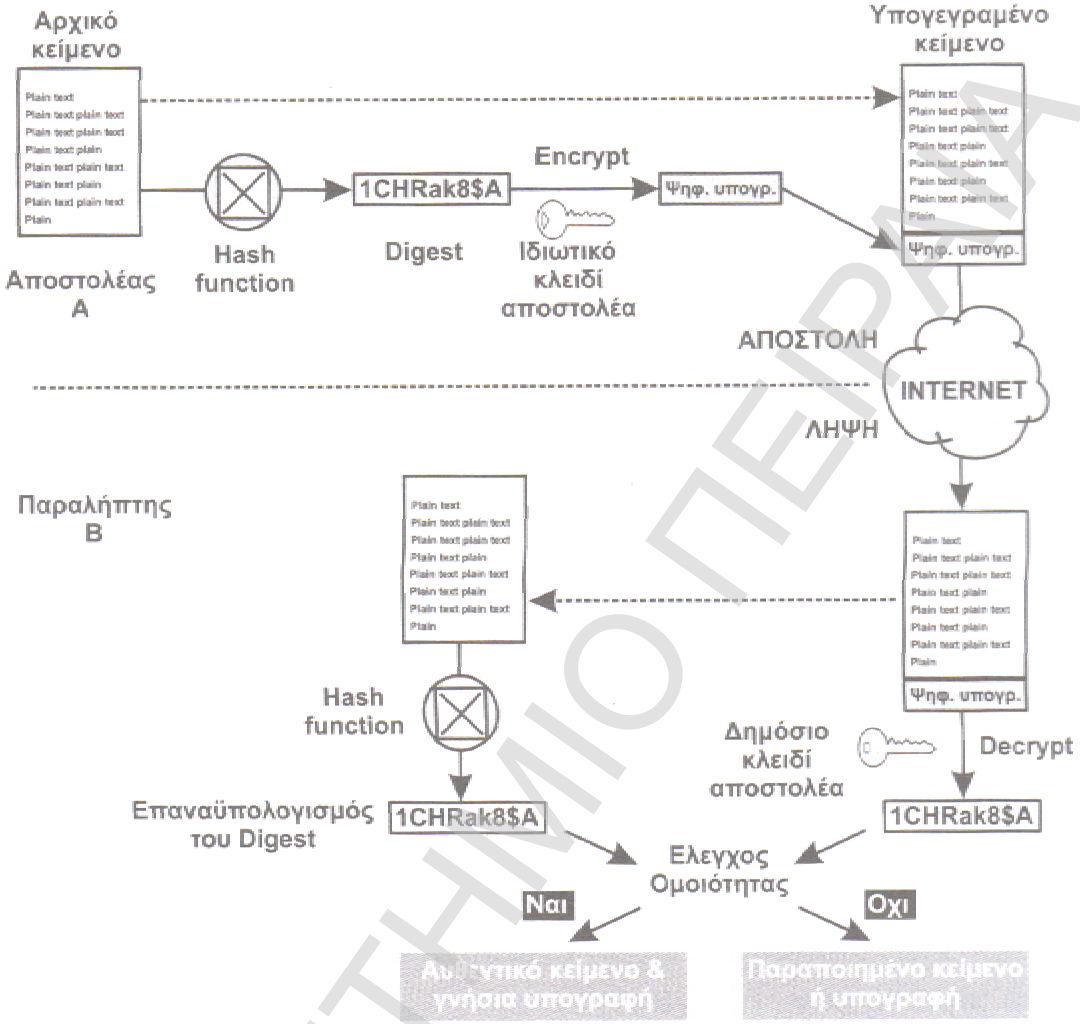
Στο σχήμα 2.4 περιγράφεται η διαδικασία αυτή της ψηφιακής υπογραφής, η οποία επιβεβαιώνει αφενός την ταυτότητα του αποστολέα και αφετέρου την ακεραιότητα των δεδομένων που παραλήφθηκαν.

Ας υποθέσουμε ότι ο αποστολέας Α επιθυμεί να στείλει ένα κείμενο στον Πριν την αποστολή κατασκευάζει το digest του κειμένου εφαρμόζοντας μια συνάρτηση hash σε αυτό. Στη συνέχεια κρυπτογραφεί το digest με το ιδιωτικό του κλειδί κατασκευάζοντας έτσι την ψηφιακή υπογραφή. Αφού επισυναφθεί η ψηφιακή υπογραφή στο τέλος του κειμένου, τούτο αποστέλλεται στον αποδέκτη Β.

Ο Β διαχωρίζει το κείμενο από την ψηφιακή υπογραφή. Στη συνέχεια αποκρυπτογραφεί την ψηφιακή υπογραφή, χρησιμοποιώντας το δημόσιο κλειδί του Α, αποκαλύπτοντας το digest που ήρθε από τον Α. Παράλληλα εφαρμόζει την ίδια συνάρτηση hash επί του κειμένου δημιουργώντας ένα νέο digest, το οποίο πρέπει να ταιριάζει με αυτό που αποκαλύφθηκε από την ψηφιακή υπογραφή. Εάν τα δύο αυτά digest είναι διαφορετικά, τούτο σημαίνει ότι το κείμενο αλλοιώθηκε κατά τη μετάδοση, ή ότι η υπογραφή δεν είναι γνήσια.

PKI

Όπως φαίνεται παραπάνω για να υλοποιείται με αξιόπιστο τρόπο η τεχνική των δημόσιων και ιδιωτικών κλειδιών, πρέπει να υπάρχει μια οργανωμένη υποδομή που να ασχολείται με τα θέματα έκδοσης, διανομής, διαχείρησης, πιστοποίησης, ακύρωσης κλπ κλειδιών. Η υποδομή αυτή είναι ως Υποδομή Δημοσίου Κλειδιού ή Public Key Infrastructure (PKI).



ΣΧΗΜΑ 2.4 Ψηφιακή υπογραφή

Certification Authority (CA)

Η ομορφιά του μηχανισμού της ασύμμετρης κρυπτογραφίας με ένα ζευγάρι κρυπτογραφικά κλειδιά (ιδιωτικό – δημόσιο) όπου το ένα κάνει κρυπτογράφηση και το άλλο αποκρυπτογράφηση, γρήγορα σκόνταψε σε ένα πρακτικό πρόβλημα που έπρεπε πρώτα να επιλυθεί. Αν και ο ιδιοκτήτης των δύο αυτών κλειδιών μπορεί να φυλάξει και να κρύψει σε ασφαλές σημείο το ιδιωτικό του κλειδί, ενώ μπορεί ελεύθερα να μοιράσει το δημόσιο κλειδί, δεν είναι δυνατόν να αποδείξει σε κάθε συναλλασσόμενο ότι το δημοσιευμένο αυτό κλειδί πράγματι ανήκει στο πρόσωπο που ισχυρίζεται ότι του ανήκει.

Αυτό που πραγματικά χρειάζεται είναι ένας αξιόπιστος μηχανισμός που μόνιμα να επιβεβαιώνει ότι το δημόσιο κλειδί ανήκει σε συγκεκριμένο ιδιοκτήτη.

Το ρόλο αυτό της τρίτης έμπιστης οντότητας (Third Trusted Party – TTP) παίζει η αρχή της πιστοποίησης CA. Η αρχή πιστοποίησης (Certification Authority – CA) είναι δηλαδή ένας οργανισμός που συνδέει διάφορες οντότητες, όπως χρήστες, με το δημόσιο κλειδί τους πιστοποιώντας ότι το συγκεκριμένο δημόσιο κλειδί ανήκει στον συγκεκριμένο ιδιοκτήτη.

Ψηφιακά πιστοποιητικά

Η πιστοποίηση της ιδιοκτησίας του δημοσίου κλειδιού από τον συγκεκριμένο ιδιοκτήτη γίνεται με το ψηφιακό πιστοποιητικό που εκδίδει η αρχή πιστοποίησης. Τα ψηφιακά πιστοποιητικά είναι μια ακολουθία χαρακτήρων στην οποία δηλώνονται το ένα μετά το άλλο τα παρακάτω:

- Το όνομα του ιδιοκτήτη.
- Το δημόσιο κλειδί του.
- Άλλα πιθανόν στοιχεία για τον ιδιοκτήτη π.χ. διεύθυνση, εταιρεία. κ.λ.π.
- Τα στοιχεία της αρχής πιστοποίησης που εξέδωσε το πιστοποιητικό.
- Τον αύξοντα αριθμό και το τύπο του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού.
- Την ψηφιακή υπογραφή της αρχής πιστοποίησης που το εξέδωσε.

Η προδιαγραφή X.509 περιγράφει αναλυτικά την δομή και το περιεχόμενο των πιστοποιητικών καθώς και τις διαδικασίες έκδοσή τους.

Με την βοήθεια του δημόσιου κλειδιού της αρχής που εξέδωσε το πιστοποιητικό, είναι εφικτός ο έλεγχος της γνησιότητας του πιστοποιητικού. Ο έλεγχος αυτός γίνεται ακολουθώντας την ίδια ακριβώς διαδικασία της ψηφιακής υπογραφής που περιγράφηκε παραπάνω.

Το ψηφιακό πιστοποιητικό χρησιμοποιείται για να επιβεβαιώνεται από τους τρίτους τόσο η ταυτότητα της πιστοποιούσας αρχής, καθώς είναι υπογεγραμμένο από αυτή, όσο και η ορθότητα του συνδυασμού δημόσιου κλειδιού και του ιδιοκτήτη του.

Στο σημείο αυτό πρέπει να σημειώσουμε ότι υπάρχουν δύο τρόποι δημιουργίας ζευγών δημόσιων – ιδιωτικών κλειδιών για την κρυπτογράφηση και τις ψηφιακές υπογραφές.

Ο πρώτος τρόπος είναι η έκδοση τους από την πιστοποιούσα αρχή (CA) η οποία παραδίδει στον ιδιοκτήτη τόσο το ζεύγος των κλειδιών όσο και το πιστοποιητικό του δημόσιου κλειδιού.

Ο δεύτερος τρόπος είναι να εκδίδεται το ζεύγος των κλειδιών από εξοπλισμό (Η/Υ) του ίδιου του χρήστη. Ο χρήστης στέλνει το δημόσιο κλειδί του στην αρχή πιστοποίησης για να του χορηγηθεί το ψηφιακό πιστοποιητικό. Η μέθοδος αυτή πλεονεκτεί στο ότι το ιδιωτικό κλειδί υπάρχει και παραμένει σε ένα και μοναδικό μέρος (ιδιοκτήτης) αλλά μειονεκτεί στο ότι ο χρήστης υποχρεούται να διατηρεί ο ίδιος μηχανισμό έκδοσης και διαχείρισης των κλειδιών.

Για την διανομή των δημόσιων κλειδιών υπάρχουν πρωτόκολλα που βασίζονται στην προδιαγραφή X.500, στην πράξη όμως χρησιμοποιούνται απλούστερες μορφές τους όπως το LDAP (Lightweight Directory Access Protocol) που έχει αναπτυχθεί ειδικά για περιβάλλον TCP/IP.

2.8 VPN

Ένα νοητό ιδιωτικό δίκτυο ή Virtual Private Network (VPN) είναι ένα ιδιωτικό δίκτυο που βασίζεται σε κοινόχρηστη δικτυακή υποδομή όπως το Internet, διατηρώντας όμως τα χαρακτηριστικά ασφάλειας και διαχείρισης του καθαρού ιδιωτικού δικτύου. Η υλοποίηση ενός VPN επιτυγχάνεται κατά βάση με ειδικές συσκευές ή και λειτουργίες που εγκαθίστανται στα άκρα του κοινόχρηστου δικτύου και οι οποίες δημιουργούν ασφαλείς διόδους για τη μεταφορά των δεδομένων μέσω του κοινόχρηστου δικτύου.

Τα VPN διακρίνονται σε τρεις κατηγορίες:

- Απομακρυσμένης πρόσβασης (Remote access) VPN
- Ενδοδίκτυα (Intranet) VPN
- Extranet VPN

Το **απομακρυσμένης πρόσβασης** (remote access) VPN επιτρέπει σε κινητούς χρήστες με φορητούς Η/Υ ή σε μικρούς απομακρυσμένους χρήστες, την πρόσβαση στο εταιρικό δίκτυο με ασφαλή τρόπο, μέσω του Διαδικτύου.

Τα **Ενδοδίκτυα** (Intranet) είναι ως γνωστόν ιδιωτικά δίκτυα που βασίζονται στην τεχνολογία του Internet (IP, router κ.λ.π.).

Το **Extranet** επεκτείνει την έννοια του Intranet πέρα από τα όρια του εταιρικού δικτύου, διασυνδέοντας σε αυτό μέσω του Internet εξωτερικούς συνεργάτες, οι οποίοι διαθέτουν ή ανήκουν σε ξεχωριστά εταιρικά δίκτυα.

Πλεονέκτημα των VPN δικτύων είναι ότι γίνεται οικονομικότερη χρήση των δικτύων, διευκολύνεται η ασφαλής σύνδεση κινητών και απομακρυσμένων χρηστών καθώς επίσης διευκολύνεται η διασύνδεση μεταξύ εταιρειών.

Ως μειονέκτημα αναφέρονται ο πρόσθετος εξοπλισμός, η αυξημένη απαιτούμενη χωρητικότητα που δημιουργεί η διαδικασία της ενθυλάκωσης καθώς και η πολυπλοκότητα που δημιουργείται σε σύνθετα δίκτυα.

Ένα δίκτυο VPN πρέπει να καλύπτει τουλάχιστον τις παρακάτω απαιτήσεις:

Επιβεβαίωση ταυτότητας χρηστών (Authentication). Λόγω του γεγονότος ότι ένα VPN χρησιμοποιεί δημόσια δίκτυα πρέπει να εξασφαλίζει την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες και να πιστοποιεί την ταυτότητα ενός εκάστου χρήστη.

Κρυπτογράφηση. Για τον ίδιο λόγο είναι απαραίτητη η κρυπτογράφηση ώστε να μην είναι δυνατή η υποκλοπή αλλά ούτε και η τροποποίηση των μηνυμάτων.

Διαχείριση Διευθύνσεων. Λόγω του ότι ένα πακέτο διέρχεται μέσω του δημόσιου δικτύου χρησιμοποιώντας τεχνικές tunnel, ενθυλακώνεται σε νέο πακέτο με διαφορετικό IP Header και συνεπώς νέες IP διευθύνσεις από αυτές που έχει το αρχικό πακέτο. Αυτό οδηγεί στην ανάγκη διαχείρισης των διευθύνσεων και της αντιστοίχησή τους.

Για τα θέματα του authentication και της κρυπτογράφησης αναφερθήκαμε προηγουμένως, ενώ η διαχείριση διευθύνσεων αναπτύσσεται στη συνέχεια.

Διαχείριση διευθύνσεων

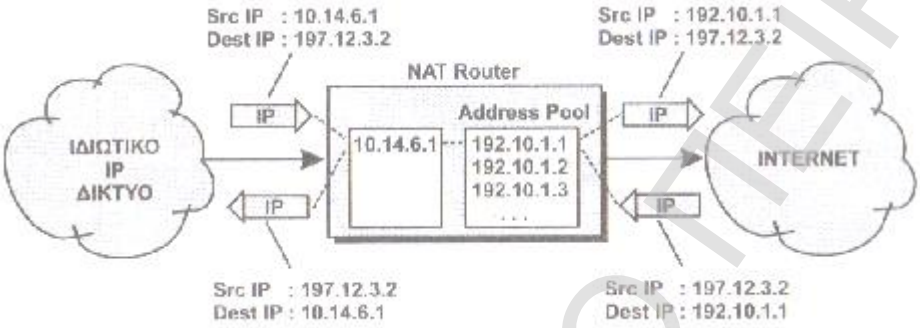
Για την μετατροπή των διευθύνσεων ενός εσωτερικού ιδιωτικού δικτύου σε διευθύνσεις του δημοσίου ανοικτού δικτύου Internet, χρησιμοποιείται η τεχνική **NAT** (Network Address Translation). Με την τεχνική αυτή μπορούμε στατικά ή δυναμικά να αντιστοιχούμε εσωτερικές προς εξωτερικές διευθύνσεις.

Με τη στατική προσέγγιση του NAT υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των εξωτερικών διευθύνσεων με ισάριθμες εσωτερικές. Πιο χρήσιμη όμως είναι η δυναμική αντιστοιχία όπου κάθε φορά που ένας εσωτερικός χρήστης πρόκειται να περάσει στο εξωτερικό δίκτυο του αποδίδεται μια ελεύθερη διεύθυνση από μια δεξαμενή διαθέσιμων διευθύνσεων, η οποία δεσμεύεται κατά τη διάρκεια της επικοινωνίας και απελευθερώνεται με το πέρας της.

Με τον τρόπο αυτό μπορούμε να χρησιμοποιούμε λίγες διευθύνσεις του Internet για πολυάριθμους εσωτερικούς χρήστες αρκεί το πλήθος των ταυτόχρονων συνδέσεων να μην υπερβαίνει το πλήθος των διευθύνσεων της δεξαμενής.

Έτσι με την αποσύνδεση εσωτερικών και εξωτερικών IP διευθύνσεων, διευκολύνεται η χρήση για ιδιωτικά δίκτυα, εσωτερικής IP διευθυνσιοδότησης κατηγορίας Α που επιτρέπει μεγαλύτερη ευελιξία και πρακτικά απεριόριστο πλήθος χρηστών.

Στο σχήμα φαίνεται ο μηχανισμός τροποποίησης διευθύνσεων όπου η διεύθυνση 10.14.6.1 αντιστοιχείται στην διεύθυνση Internet 192.10.1.1, με σκοπό την επικοινωνία με την εξωτερική διεύθυνση 197.12.3.2.



Σχήμα 2.5 NAT

Tunneling

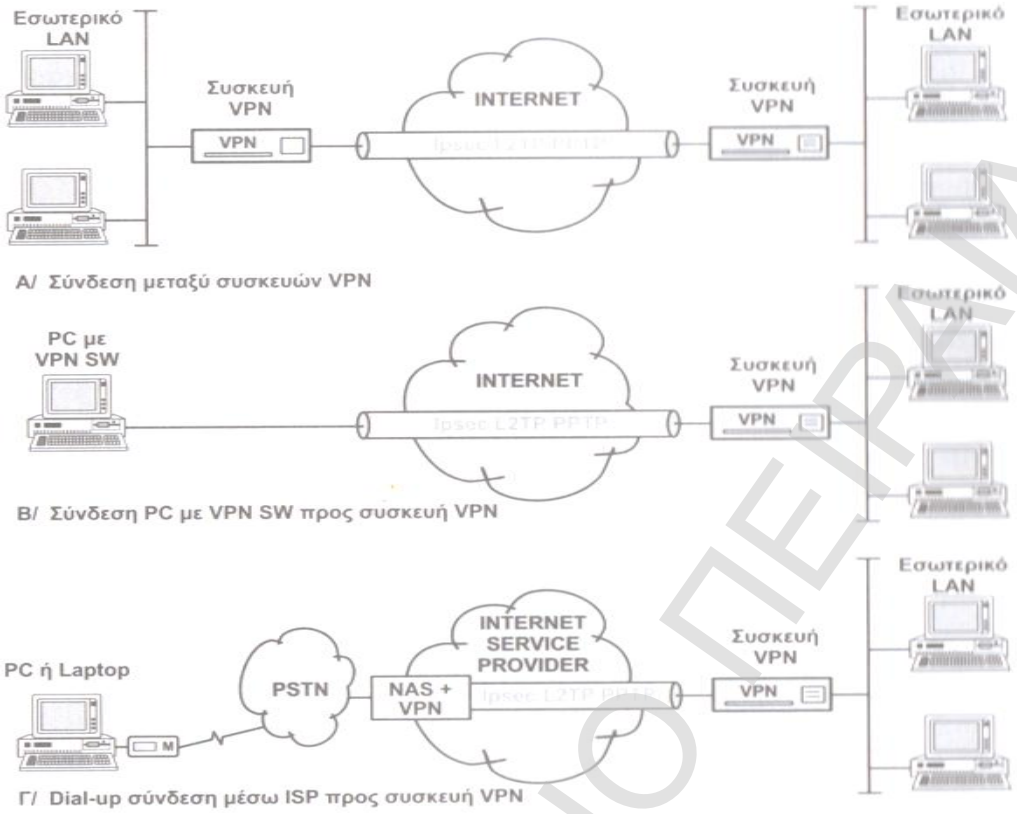
Το tunneling είναι η τεχνική εκείνη που ενθυλακώνει ένα αρχικό πακέτο σε ένα νέο διαφορετικό συνήθως πρωτοκόλλου και πρωτοεμφανίστηκε για να επιτρέψει τη μεταφορά δεδομένων μέσω δικτύων που χρησιμοποιούν διαφορετικά πρωτόκολλα.

Στην περίπτωση του VPN επειδή απαιτείται η μετάδοση δεδομένων ενός ασφαλούς εσωτερικού δικτύου μέσω του ανοικτού εξωτερικού δικτύου Internet, χρησιμοποιείται ενθυλάκωση για λόγους ασφαλείας, ακόμη και στην περίπτωση που τα δύο δίκτυα χρησιμοποιούν το ίδιο πρωτόκολλο IP.

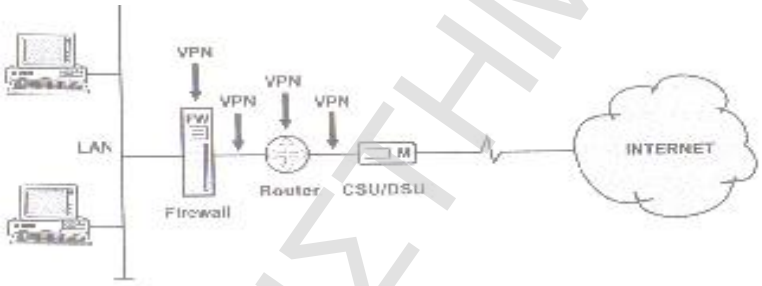
Υπάρχουν δύο κατηγορίες tunneling, το Επιπέδου 2 και το Επιπέδου 3. Αντιπροσωπευτικά πρωτόκολλα για ενθυλάκωση β' επιπέδου είναι το **PPTP** και **L2TP** ενώ για το επίπεδο 3 το **IPSec**.

Ως προς τον τρόπο υλοποίησης διακρίνουμε τις εξής περιπτώσεις:

α. Δύο τμήματα ενός εταιρικού δικτύου διασυνδέονται μέσω του Internet χρησιμοποιώντας συσκευές VPN στα δύο άκρα (σχήμα 2.6). Αυτό χρησιμοποιείται για δημιουργία εκτεταμένων Intranet ή για διασύνδεση διαφορετικών εταιρικών δικτύων.



Σχήμα 2.6 Υλοποίηση VPN



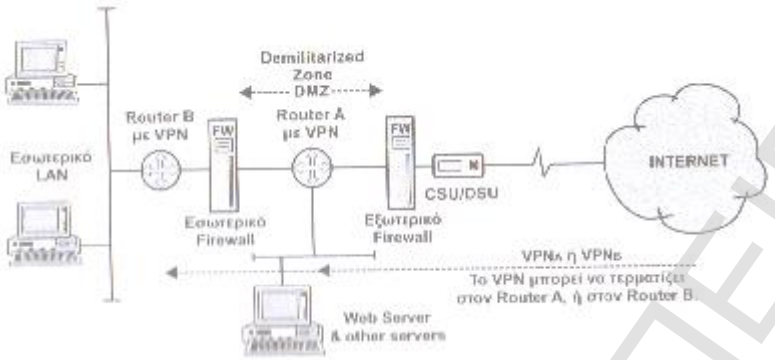
Σχήμα 2.7 Πιθανές θέσεις συσκευής ή λειτουργίας VPN

β. Σύνδεση ενός απομονωμένου PC ή φορητού με το εταιρικό δίκτυο μέσω του Internet. Στην περίπτωση αυτή το VPN υλοποιείται στην μεν πλευρά του εταιρικού δικτύου με κατάλληλη συσκευή (π.χ. router, firewall) στην δε πλευρά του PC με κατάλληλο λογισμικό που ονομάζεται VPN client.

γ. Σύνδεση ενός απομονωμένου PC ή φορητού με το εταιρικό δίκτυο μέσω μεικτής σύνδεσης (σχήμα) όπου το PC συνδέεται μέσω dialup σύνδεσης με συσκευή Network Access Server η οποία διαθέτει VPN για τη σύνδεση μέσω Internet με το εταιρικό δίκτυο. Η περίπτωση αυτή συνήθως υλοποιείται από ISP έτσι ώστε να μην είναι αναγκαία η ύπαρξη κατάλληλου λογισμικού στο απομονωμένο PC.

VPN και Firewall

Όπως φαίνεται και στο σχήμα 2.7, μια συσκευή VPN ή οι λειτουργίες VPN μπορεί να βρίσκεται σε εναλλακτικές θέσεις.



Σχήμα 2.8 Θέση VPN και Firewall

Στις περισσότερες περιπτώσεις αυτό υλοποιείται στον router ή στο Firewall. Ως γνωστόν το VPN παρέχει δυνατότητες επιβεβαίωσης ταυτότητας (authentication) και κρυπτογράφησης. Το **Firewall** από την πλευρά του καλύπτει τα θέματα εξουσιοδότησης πρόσβασης, έτσι που ο συνδυασμός των δύο λειτουργιών να είναι απαραίτητος για ένα ασφαλές δίκτυο.

Στην πράξη μια δημοφιλής προσέγγιση είναι η του σχήματος 2.8, όπου υπάρχουν δυο Firewall, ένα προς το Διαδίκτυο και ένα προς το εσωτερικό δίκτυο και όπου η μεταξύ τους περιοχή ονομάζεται αποστρατικοποιημένη περιοχή ή Demilitarized Zone (DMZ). Στην περιοχή **DMZ** συνήθως τοποθετούνται διάφοροι server όπως mail servers, FTP server, Web server, ενώ αυτή χαρακτηρίζεται ως ευάλωτη σε αντίθεση με το εσωτερικό δίκτυο γιατί οι server αυτοί στην πράξη έχουν αντίγραφα των πραγματικών server που βρίσκονται ασφαλείς στο εσωτερικό του δικτύου.

Το VPN μπορεί να βρίσκεται στο εσωτερικό δίκτυο, τερματίζοντας έτσι το tunneling μιας εξωτερικής VPN σύνδεσης σε ένα πολύ ασφαλές σημείο, αλλά με το μειονέκτημα της δημιουργίας διαδρομών μέσα στο firewall για το πέρασμα της κυκλοφορίας VPN, που καθιστούν το σύστημα πλέον ευάλωτο.

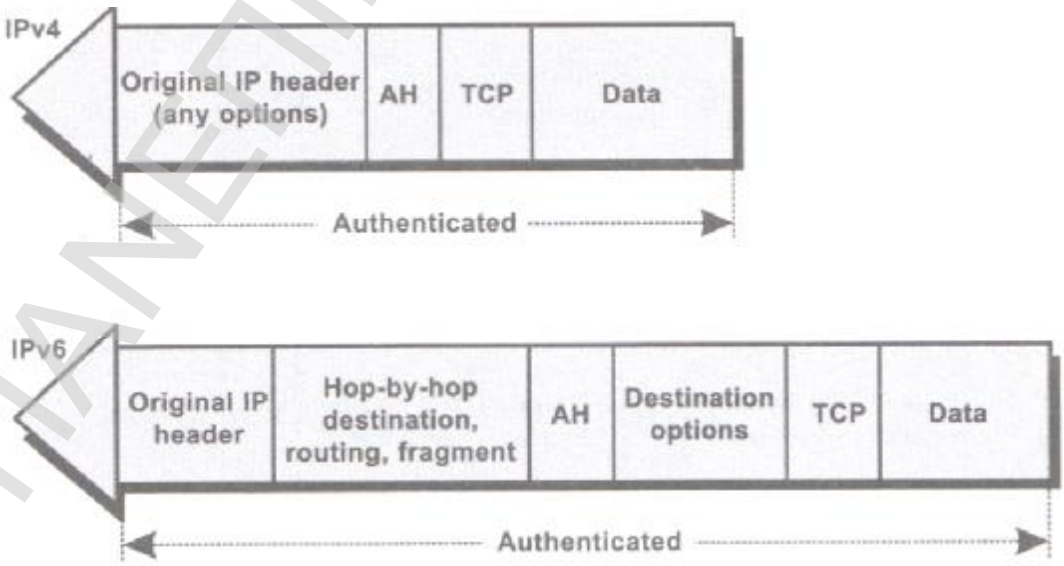
Εναλλακτικά το VPN μπορεί να τερματίζει στην DMZ, οπότε δεν δημιουργεί οδεύσεις μέσω του εσωτερικού firewall, αλλά από την άλλη πλευρά το VPN τερματίζει σε μια όχι και τόσο ασφαλή περιοχή. Για τα VPN τα πιο χρήσιμα σύνολα πρωτοκόλλων είναι το PPTP, το L2TP και το IPSec που παρουσιάζεται παρακάτω ως το πιο αντιπροσωπευτικό και το πλέον χρησιμοποιούμενο.

2.9 IPSec

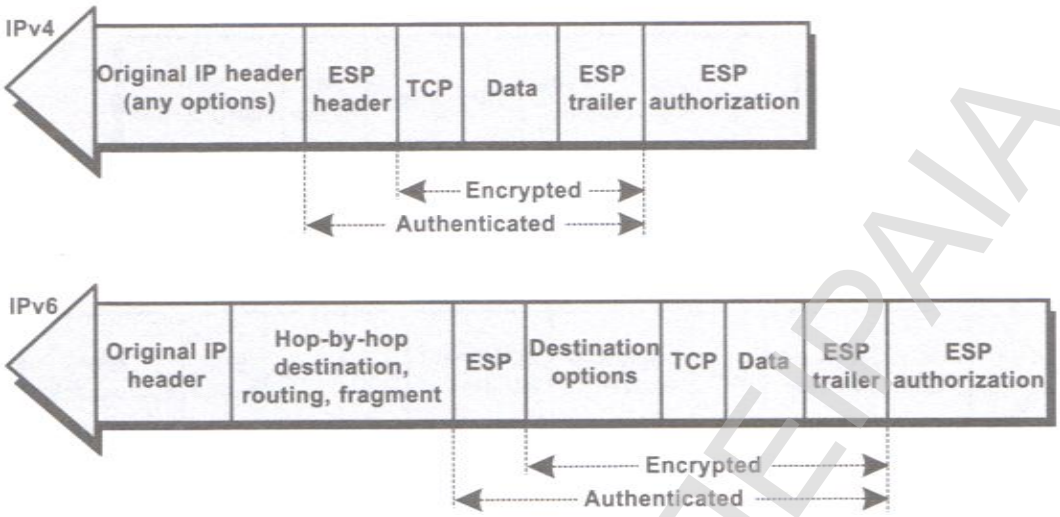
Το IPSec είναι ένα σύνολο από πρωτόκολλα τρίτου επιπέδου που σχεδιάστηκαν από το 1995 για να καλύψουν καταρχάς τα θέματα ασφαλείας του IPv6 και της αυξημένης ανάγκης για ασφάλεια στο κλασσικό IPv4, το IPSec προσαρμόστηκε ώστε να είναι συμβατό και με το IPv4. Στην πράξη χρησιμοποιεί διάφορες τυποποιημένες τεχνικές κρυπτογραφίας προκειμένου να παρέχει εμπιστευτικότητα, ακεραιότητα δεδομένων και authentication. Το IPSec προσδιορίζει δυο headers στα πακέτα IP για να διαχειρισθούν authentication και κρυπτογράφηση, τον AH (Authentication Header) και τον ESP (Encapsulating Security Payload).

Προκειμένου να υπάρχει ασφαλής ανταλλαγή δεδομένων, στην περίπτωση μας αυθεντικά ή και κρυπτογραφημένα, αμφότερα τα μέρη της επικοινωνίας πρέπει να συμφωνήσουν για τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιήσουν, για τον μηχανισμό ανταλλαγής κλειδιών αλλά και για την συχνότητα αλλαγής των κλειδιών. Αυτή η συμφωνία ενσωματώνεται στο SA (Security Association), που είναι στην ουσία ένα ασφαλές «κανάλι» επικοινωνίας μεταξύ αποστολέα και παραλήπτη. Επειδή το SA είναι μονής κατεύθυνσης (Simplex), σε μια επικοινωνία απαιτούνται δύο SA, ένα για κάθε κατεύθυνση.

Ο authentication header AH καλύπτει τα περισσότερα θέματα authentication του IP. Το βασικό στοιχείο του AH είναι το checksum της κρυπτογράφησης που συνοδεύει το περιεχόμενο του πακέτου, ενώ ο AH εισάγεται στο πακέτο αμέσως μετά τον IP header. Σημειωτέον ότι με τον AH δεν μπορούμε να κρατήσουμε εμπιστευτικά τα δεδομένα, παρά μόνο να μην επιστρέψουμε την τροποποίηση τους.

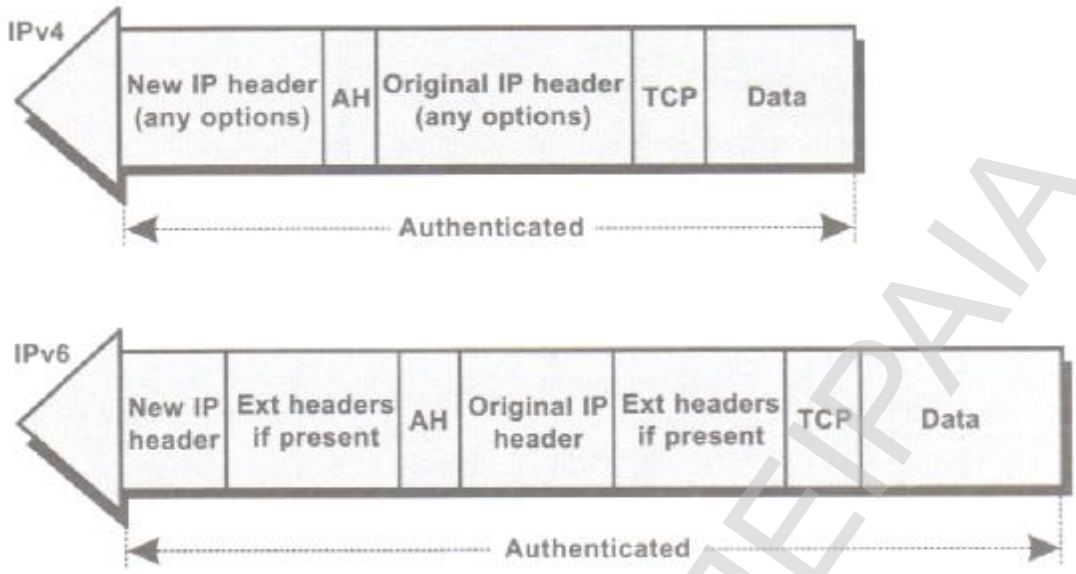


Σχήμα 2.9 Transport mode AH

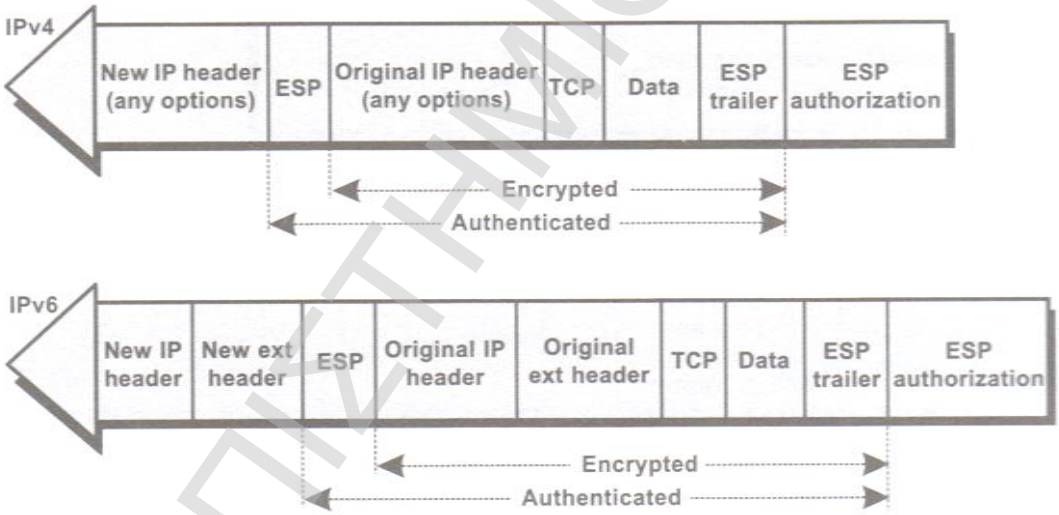


Σχήμα 2.10 Transport mode ESP

Το ESP (Encapsulating Security Payload) είναι αρμόδιο τόσο για το authentication όσο και για την κρυπτογράφηση του πακέτου, ενώ μπορεί να χρησιμοποιηθεί και αποκλειστικά για κρυπτογράφηση. Το AH και το ESP χρησιμοποιούνται με διαφορετικούς τρόπους ανάλογα με την μορφή το IPSec, την transport και την tunnel. Στην πράξη αν χρειαζόμαστε μόνο authentication χωρίς κρυπτογράφηση, χρησιμοποιούμε το AH, δηλαδή στις περιπτώσεις εκείνες που η βασική απαίτηση είναι ο αποκλεισμός των μη εξουσιοδοτημένων. Στις περιπτώσεις που απαιτείται επιπλέον του authentication και κρυπτογράφηση ή μόνο κρυπτογράφηση, τότε χρησιμοποιείται το ESP.



Σχήμα 2.11 Tunnel mode AH



Σχήμα 2.12 Tunnel mode ESP

Το IPSec λειτουργεί σε δυο μορφές, transport και tunnel, όπου στην πρώτη το πακέτο μεταφέρεται αυτοτελώς ενώ στη δεύτερη ενθυλακώνεται σε νέο IP πακέτο.

Στην περίπτωση της **transport** μορφής αυτό που προστατεύεται είναι το τμήμα του πακέτου πέραν του IP header. Όταν εφαρμόζεται ο AH σε ένα transport πακέτο, όλο το πακέτο καλύπτεται από authentication.

Όταν τώρα ένα ESP εφαρμόζεται σε transport πακέτο επιπλέον του προηγούμενου τα δεδομένα ανωτέρων επιπέδων που μεταφέρονται, κρυπτογραφούνται. Συνήθως ο τρόπος χρησιμοποιείται σε μικρά δίκτυα.

Με την tunnel το αρχικό πακέτο ενθυλακώνεται σε ένα νέο πακέτο IP. Με τον τρόπο αυτό έχουμε μεγαλύτερη ασφάλεια από την transport μετάδοση, καθώς σε ενέργειες επιβεβαίωσης ταυτότητας και κρυπτογράφησης καλύπτουν όλο το αρχικό πακέτο. Όταν εφαρμόζεται AH σε tunnel όλο το πακέτο γίνεται authenticate, ενώ όταν εφαρμόζεται ESP, ο νέος IP header είναι το μόνο που δεν κρυπτογραφείται. Στα σχήματα 2.9 έως και 2.12 βλέπουμε τις διαφορές αυτές.

3ο ΚΕΦΑΛΑΙΟ

ΕΦΑΡΜΟΓΕΣ ΜΕ ΤΗ ΜΕΘΟΔΟ ΤΟΥ INTRUSION DETECTION SYSTEM

3.1 ΕΙΣΑΓΩΓΗ

Ο Peter Denning υποστηρίζει, ότι η Επιστήμη των Υπολογιστών πάντα επεκτείνεται, κάθε φορά που σχετίζεται ένας τομέας μαζί της δημιουργώντας έτσι ένα νέο πεδίο έρευνας. Ως παράδειγμα, έχει αναπτυχθεί μια μεγάλη ποικιλία από διαφορετικά εργαλεία, μεθόδους και τεχνικές μέχρι και σήμερα για το Intrusion Detection. Ωστόσο, τα ίδια προβλήματα βασανίζουν αυτόν τον τομέα χωρίς να διαφαίνεται ιδιαίτερη πρόοδος. Ως εκ τούτου, είναι αναγκαίο να γίνει μια στροφή σε έρευνα νέων πεδίων της επιστήμης έτσι ώστε να δοθούν λύσεις.

Ο τομέας του Intrusion Detection περιλαμβάνει τις έννοιες της παρακολούθησης και της απόφασης. Το ID είναι η παρακολούθηση των γεγονότων που συμβαίνουν σε ένα σύστημα και η απόφαση για το αν ένα γεγονός είναι φυσικό ή αφύσικο. Η λέξη «φυσικό» ορίζει κάθε γεγονός που είναι συνεπές με την πολιτική ασφαλείας που υπάρχει για το σύστημα, και η λέξη «αφύσικο» ορίζει κάθε γεγονός που απειλεί αυτήν την πολιτική της ασφάλειας του συστήματος. Εξάλλου, όπως το IT είναι μια αλληλεπίδραση ανθρώπου-υπολογιστή έτσι και το ID στην ασφάλεια δικτύων είναι μια αλληλεπίδραση.

3.2 ΤΙ ΕΙΝΑΙ ΤΟ ID ΚΑΙ ΤΟ IDS;

Τα τελευταία χρόνια με την εκθετική αύξηση του Internet, όσο αναφορά τα συστήματα που συνδέονται σε αυτό και τις συνεχώς αναπτυσσόμενες εφαρμογές και δικτυακές υπηρεσίες, έχει αυξηθεί και το πλήθος των κακόβουλων χρηστών, οι οποίοι υλοποιούν ολοένα και πιο έξυπνες, πολύπλοκες και επιζήμιες δικτυακές επιθέσεις.
Με δεδομένη την εξέλιξη αυτή, τα κλασσικά μέτρα ασφάλειας δεν φαίνεται να επαρκούν για την προστασία των συστημάτων και των πληροφοριών που περιέχουν αυτά και συνεχώς γίνεται προσπάθεια για ανάπτυξη νέων μηχανισμών ασφάλειας, που θα παρέχουν την επιθυμητή προστασία από δικτυακές επιθέσεις.
Μία σχετικά νέα και συνεχώς αναπτυσσόμενη μέθοδος προστασίας, είναι η αυτοματοποιημένη Ανίχνευση Επιθέσεων (Intrusion Detection).
Ο όρος ***Intrusion Detection*** σημαίνει ***Ανίχνευση Επιθέσεων*** και έχει να κάνει με την παρακολούθηση των γεγονότων που συμβαίνουν σε ένα σύστημα ή ένα δίκτυο και την ανάλυσή τους για σημάδια επιθέσεων.

Επίθεση χαρακτηρίζεται ως οποιαδήποτε προσπάθεια για παραβίαση της *εμπιστευτικότητας*, *ακεραιότητας*, *διαθεσιμότητας* ή *των μηχανισμών ασφάλειας* ενός συστήματος ή ενός δικτύου.
Οι επιθέσεις πραγματοποιούνται από άτομα που έχουν πρόσβαση στους στόχους τους μέσω του Internet, από εξουσιοδοτημένους χρήστες που προσπαθούν να αποκτήσουν περισσότερα δικαιώματα από αυτά που τους έχουν δοθεί και από εξουσιοδοτημένους χρήστες οι οποίοι εκμεταλλεύονται τα δικαιώματα που τους έχουν δοθεί με κακό σκοπό.
Ο όρος **I*ntrusion* Detection *Systems* (IDSs)** σημαίνει ***Συστήματα Ανίχνευσης Επιθέσεων*** και έχει να κάνει με software ή hardware προϊόντα, που αυτοματοποιούν την παραπάνω διαδικασία παρακολούθησης και ανάλυσης. Η εξέλιξη των IDSs, είναι ραγδαία τα τελευταία χρόνια και συνεχώς γίνονται προσπάθειες για βελτίωσή τους, κυρίως στον τομέα των συμπτωμάτων από *False Positives* και *False Negatives* που παρουσιάζουν.

False Positives
Είναι οι λανθασμένες επισημάνσεις που παράγει ένα IDS, όταν ανιχνεύσει κάποιο γεγονός σαν περίπτωση πιθανής επίθεσης ενώ δεν είναι. Τα False Positives είναι δυνατόν να προκύψουν από κακή ρύθμιση του IDS ή από περιπτώσεις γεγονότων που δεν μπορούν να διαχωριστούν σαφώς από μία επίθεση.

False Negatives
Είναι οι περιπτώσεις επιθέσεων τις οποίες το IDS δεν κατάφερε μετά από την εξέτασή τους να τις επισημάνει. Τα False Negatives συνήθως προκύπτουν από κακή ρύθμιση του IDS ή από την εμφάνιση μίας νέας επίθεσης για την οποία δεν υπάρχει προηγούμενη γνώση. Με την τρέχουσα μορφή τους τα IDSs παρέχουν σημαντική υποστήριξη στα ήδη υπάρχοντα μέτρα προστασίας ενός δικτύου και σε συνδυασμό με άλλους μηχανισμούς ασφάλειας, αποτελούν ένα σημαντικό εργαλείο για την παρακολούθηση και την αποτροπή δικτυακών επιθέσεων.

Το Intrusion Detection βοηθά τα συστήματα των υπολογιστών να προετοιμάζονται κατάλληλα για να μπορούν να χειρίζονται κατάλληλα τις επιθέσεις. Αυτός ο στόχος ολοκληρώνεται συλλέγοντας πληροφορίες από διάφορες πηγές συστημάτων και δικτύων, και έπειτα αναλύονται αυτές οι πληροφορίες για τυχόν προβλήματα ασφαλείας. Σε μερικές περιπτώσεις, το intrusion Detection επιτρέπει στο χρήστη να προσδιορίζει απαντήσεις σε πραγματικό χρόνο για τις παραβιάσεις του συστήματος.

Τα συστήματα του Intrusion Detection εκτελούν διάφορες λειτουργίες όπως:

• Έλεγχος και ανάλυση της δραστηριότητας χρηστών και συστημάτων

• Έλεγχος των διαμορφώσεων και αδυναμιών των συστημάτων

• Αξιολόγηση των κρίσιμων αρχείων των συστημάτων

• Αναγνώριση της δραστηριότητας διάφορων μοντέλων επίθεσης σε σχέση με γνωστές επιθέσεις

• Στατιστική ανάλυση για τα ασυνήθιστα σχέδια δραστηριότητας

• Έλεγχος της διαχείρισης των λειτουργικών συστημάτων, με την αναγνώριση της δραστηριότητας των χρηστών επισημαίνοντας παραβιάσεις της πολιτικής του συστήματος

Μερικά συστήματα παρέχουν πρόσθετα χαρακτηριστικά γνωρίσματα, περιλαμβάνοντας:

• Αυτόματη εγκατάσταση λογισμικού από τους vendors λογισμικού παρέχοντας patches

• Εγκατάσταση και λειτουργία των decoy servers για την καταγραφή πληροφοριών σε σχέση με τους εισβολείς.

Ο συνδυασμός αυτών των χαρακτηριστικών γνωρισμάτων επιτρέπει στους διαχειριστές των συστημάτων να χειριστούν ευκολότερα την παρακολούθηση του λογιστικού ελέγχου, και την αξιολόγηση των συστημάτων και των δικτύων τους. Αυτή η τρέχουσα δραστηριότητα αξιολόγησης και λογιστικού ελέγχου είναι ένα απαραίτητο μέρος της υγιούς διοικητικής πρακτικής ασφάλειας.

Η «Θεωρία Παιγνίων» είναι ένας κλάδος της θεωρίας αποφάσεων , η οποία ασχολείται με το ποιες αποφάσεις πρέπει να παρθούν με βάση τα εκάστοτε προβλήματα που εμφανίζονται. Πολλοί κλάδοι έχουν σχετικές θεωρητικές τεχνικές όπως των Οικονομικών Επιστημών, της Νομικής, Βιολογίας, Ψυχολογίας και Πολιτικής Φιλοσοφίας. Οι ομοιότητες μεταξύ του Intrusion Detection και του Game Theory, χρήζουν περαιτέρω μελέτης και έρευνας. Ως εκ τούτου, η εφαρμογή της Θεωρίας Παιγνίων στο Intrusion Detection θα δείξει πόσο αυτή η νέα προσέγγιση θα βελτιώσει το ID δίνοντας θετικά αποτελέσματα.

3.3 ΧΡΗΣΙΜΟΤΗΤΑ ΤΩΝ IDSs

Καθώς οι δικτυακές επιθέσεις έχουν αυξηθεί κατά πολύ τα τελευταία χρόνια τόσο σε πλήθος όσο και σε βαθμό επικινδυνότητας, τα IDSs αποτελούν μία απαραίτητη προσθήκη στην πολιτική ασφάλειας κάθε οργανισμού.
Η *Ανίχνευση Επιθέσεων* επιτρέπει στους οργανισμούς να προστατέψουν τα συστήματά τους και τις πληροφορίες που βρίσκονται σε αυτά, από κινδύνους που προκύπτουν από την αυξημένη δικτυακή διασύνδεση μεταξύ των συστημάτων τους.
Υπάρχουν διάφοροι λόγοι για τους οποίους είναι απαραίτητη η χρήση των IDSs:
1. Για ανίχνευση επιθέσεων και άλλων παραβιάσεων ασφάλειας που δε ανιχνεύονται από άλλα μέτρα προστασίας. Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ένα ή περισσότερα συστήματα, όταν διάφορες, δημόσια γνωστές αδυναμίες ασφάλειας των συστημάτων αυτών δεν έχουν διορθωθεί.

Παρόλο που κάθε διαχειριστής πρέπει και μπορεί σχετικά εύκολα να διορθώνει τις αδυναμίες αυτές, υπάρχουν διάφοροι λόγοι για τους οποίους αυτό δεν συμβαίνει.

- Σε περιβάλλοντα με πολλά συστήματα, ο διαχειριστής τους συνήθως δεν έχει την δυνατότητα αλλά ούτε και τον χρόνο να ενημερώσει τα συστήματα που πρέπει, με νέες διορθώσεις των αδυναμιών ασφάλειάς τους.
- Οι χρήστες των συστημάτων κάνουν χρήση διάφορων λογισμικών που θεωρούνται επικίνδυνα, με την έννοια ότι μπορούν να προκαλέσουν τρύπες ασφάλειας σε ένα σύστημα.
- Τόσο οι διαχειριστές όσο και οι χρήστες κάνουν λάθη στην ρύθμιση και την χρήση των συστημάτων και των υπηρεσιών που προσφέρουν.
- Οι χρήστες χρησιμοποιούν μειωμένης ασφάλειας μηχανισμούς πρόσβασης στα συστήματα, όπως ατυχώς επιλεγμένα passwords.

Σε έναν ιδανικό κόσμο οι δημιουργοί λογισμικού θα μείωναν στο ελάχιστο τις αδυναμίες ασφάλειάς στα προϊόντα που διανέμουν και οι διαχειριστές θα ενημέρωναν και θα διόρθωναν τα συστήματά τους γρήγορα και αξιόπιστα. Στον πραγματικό όμως κόσμο αυτό σπάνια συμβαίνει, ενώ νέες αδυναμίες και ελαττώματα στην ασφάλεια συστημάτων, εμφανίζονται σε καθημερινή βάση. Με την χρήση ενός IDS η προσπάθεια ή και η επιτυχία ενός επιτιθέμενου να παραβιάσει κάποιο σύστημα μέσω της εκμετάλλευσης μιας γνωστής αδυναμίας σε αυτό, θα γινόταν αντιληπτή. Επίσης με την βοήθεια του IDS, γνωστοποιείται η αδυναμία που οδήγησε στην παραβίαση του συστήματος και παράγονται χρήσιμα συμπεράσματα που βοηθούν στην αποκατάσταση του συστήματος και την διόρθωση της αδυναμίας, που οδήγησε στην παραβίασή του.

2. Για την ανίχνευση αναγνωριστικών ενεργειών που προηγούνται μίας επίθεσης. Για την πραγματοποίηση μίας επίθεσης συνήθως υπάρχουν κάποια στάδια που προηγούνται αυτής. Ο επιτιθέμενος πρώτα εξετάζει τον υποψήφιο στόχο του, ώστε να συγκεντρώσει πληροφορίες για αυτόν και να εντοπίσει ένα σημείο εσόδου, το οποίο θα του επιτρέψει να πραγματοποιήσει την επίθεση με επιτυχία. Αυτό επιτυγχάνεται μέσω του *Scanning*.
Δίχως την ύπαρξη ενός IDS, ο επιτιθέμενος είναι πολύ πιθανό να πραγματοποιήσει τις αναγνωριστικές του κινήσεις ανενόχλητος και χωρίς να γίνει αντιληπτός. Ένα IDS θα είχε την δυνατότητα να εντοπίσει τις κινήσεις αυτές του επιτιθέμενου και να πάρει κάποια μέτρα, όπως να καταγράψει το γεγονός, να ειδοποιήσει τους υπεύθυνους ασφάλειας για αυτό ή και να εμποδίσει τον επιτιθέμενο να τις ολοκληρώσει.

3. Για την συγκέντρωση πληροφοριών που αφορούν επιθέσεις που πραγματοποιήθηκαν, οι οποίες θα βοηθήσουν στην αποκατάσταση των συστημάτων που παραβιάστηκαν και στην διόρθωση αδυναμιών και παραλήψεων στα ήδη υπάρχοντα μέτρα ασφάλειας. Ακόμα και στην περίπτωση που ένα IDS δεν μπορεί να εμποδίσει μία επίθεση, μπορεί να συλλέξει διάφορες πληροφορίες και στοιχεία για αυτήν που θα χρησιμοποιηθούν τόσο για την αποκατάσταση του συστήματος και την διόρθωση των αδυναμιών ασφάλειάς του, όσο και για τον εντοπισμό του επιτιθέμενου και την ποινική δίωξή του.

4. Για να αποτραπούν επίδοξοι επιτιθέμενοι, καθώς υπάρχει μεγαλύτερο ρίσκο να εντοπιστούν και να τιμωρηθούν. Όταν ο υποψήφιος επιτιθέμενος συνειδητοποιήσει ότι ένα δίκτυο ή ένα σύστημα προστατεύεται από ένα IDS, διστάζει να συνεχίσει την προσπάθειά του καθώς υπάρχουν περισσότερες πιθανότητες να γίνει αντιληπτός και να συλληφθεί.
5. Για αποτελεσματικότερη σχεδίαση και εφαρμογή πολιτικής ασφάλειας. Με την χρήση των IDSs συλλέγονται πληροφορίες και παρατηρούνται *patterns* από ενέργειες που πραγματοποιούνται καθημερινά εναντίον ενός δικτύου και των συστημάτων του, τα οποία μπορούν να βοηθήσουν στη σχεδίαση πιο αξιόπιστων μέτρων ασφάλειας, προσαρμοσμένων ώστε να αντιμετωπίζουν τα γεγονότα και τους κινδύνους που απειλούν το συγκεκριμένο δίκτυο, και να οδηγήσουν στην αποτελεσματικότερη προστασία του. ***Patterns***, είναι τα δείγματα που προκύπτουν από την εκτενή παρακολούθηση και μελέτη ενός συνόλου δραστηριοτήτων και την παρουσίασή τους με την μορφή **προτύπων** που εκφράζουν την δραστηριότητα στο σύνολό της.

3.4 ΕΙΔΗ ΤΩΝ IDSs

Σήμερα υπάρχουν διάφοροι τύποι IDSs, τα οποία χαρακτηρίζονται από διαφορετικές προσεγγίσεις στον τρόπο που το καθένα υλοποιεί την διαδικασία της παρακολούθησης και της ανάλυσης των γεγονότων, για την ανίχνευση επιθέσεων. Η κατηγοριοποίηση των IDSs μπορεί να επιτευχθεί εξετάζοντας διαφορετικούς παράγοντες κάθε φορά. Οι παράγοντες που εξετάζονται προκύπτουν από ένα γενικό μοντέλο, το οποίο περιγράφει τις λειτουργίες των IDSs. Τα περισσότερα IDSs επιτελούν τρεις θεμελιώδεις λειτουργίες και ο διαχωρισμός των IDSs προκύπτει από τον τρόπο που κάθε ένα υλοποιεί τις λειτουργίες αυτές :

Πηγές Πληροφορίας (*Information Sources*)
Είναι οι πηγές που χρησιμοποιεί το IDS ώστε να συλλέξει την κατάλληλη πληροφορία, την οποία θα αναλύσει για να καθορίσει αν έχει πραγματοποιηθεί μία επίθεση. Οι πιο συνήθεις πηγές πληροφορίας μπορεί να είναι σε επίπεδο παρακολούθησης *συστήματος (Host)* και *δικτύου (Network)*.

Ανάλυση (*Analysis*)
Ο τρόπος με τον οποίο το IDS οργανώνει και επεξεργάζεται τα γεγονότα που προκύπτουν από τις *Πηγές Πληροφορίας* και αποφασίζει ποια από αυτά μπορεί να αποτελούν μία επίθεση. Οι πιο γνωστές μέθοδοι *Ανάλυσης* είναι η *Misuse Detection* , η *Anomaly Detection* και η *Protocol Anomaly Detection*.

Απόκριση (*Response*)
Είναι το σύνολο των ενεργειών που θα εκτελέσει το IDS, όταν ανιχνεύσει μία επίθεση. Υπάρχουν δύο είδη τέτοιων ενεργειών, οι *Παθητικές (Passive)* και οι *Ενεργητικές (Active)*. Τα *Passive Responses* συνήθως καταγράφουν το γεγονός της επίθεσης και ενημερώνουν με κάποιο τρόπο τους υπεύθυνους, ώστε αυτοί να πάρουν τα κατάλληλα μέτρα. Τα *Active Responses* έχουν να κάνουν με αυτοματοποιημένη αντιμετώπιση της επίθεσης από το ίδιο το IDS. Στη συνέχεια περιγράφονται αναλυτικότερα οι παραπάνω λειτουργίες και παρουσιάζονται τα είδη των IDSs που προκύπτουν, ανάλογα με το πως το κάθε ένα τις υλοποιεί.

3.4.1 INFORMATION SOURCES (Πηγές Πληροφορίας)

Ο πιο συνήθης τρόπος κατηγοριοποίησης των IDSs, είναι λαμβάνοντας υπόψη τις πηγές της πληροφορίας που χρησιμοποιούν, από τις οποίες προκύπτουν τα γεγονότα που θα αναλυθούν σε επόμενο στάδιο, ώστε να ανιχνευθεί μία επίθεση. Κάποια IDSs για την ανίχνευση των επιθέσεων, παρακολουθούν και αναλύουν πακέτα που ανήκουν στο traffic ενός δικτύου, το οποίο μπορεί να είναι ένα δίκτυο κορμού (Backbone) ή ένα τμήμα (segment) ενός τοπικού δικτύου (LAN). Κάποια άλλα IDSs παρακολουθούν και αναλύουν πληροφορία που εξάγεται από το Λειτουργικό Σύστημα (Λ.Σ) ή από τις εφαρμογές ενός συστήματος. Έτσι τα IDSs ανάλογα με την πηγή της πληροφορίας, χωρίζονται σε δύο κατηγορίες, με τα δικά της πλεονεκτήματα και μειονεκτήματα η κάθε μία :

3.4.1.1 NETWORK IDSs (NIDS)

Τέτοιου είδους είναι τα IDSs που κατά κύριο λόγο χρησιμοποιούνται σήμερα. Τα NIDSs παρακολουθούν και αναλύουν κάθε πακέτο που ανήκει στο traffic ενός δικτύου. Ένα NIDS που έχει εγκατασταθεί σε ένα segment ή ένα switch ενός δικτύου, επεξεργάζεται κάθε πακέτο που περνάει από αυτό το σημείο, προστατεύοντας κάθε σύστημα που είναι συνδεδεμένο στο δίκτυο. Τα NIDS συνήθως αποτελούνται από συστήματα (*Sensors*), τα οποία τοποθετούνται σε διάφορα σημεία ενός δικτύου. Ο *Sensor* εκτελεί όλες τις λειτουργίες του NIDS και είναι ένα σύστημα αφιερωμένο μόνο για αυτές. Οι *Sensors* παρακολουθούν το traffic του δικτύου, αναλύουν τοπικά τα πακέτα σε πραγματικό χρόνο και καταγράφουν τα αποτελέσματά τους τοπικά ή/και απομακρυσμένα σε ένα κεντρικό σύστημα. Επίσης οι *Sensors* έχουν την δυνατότητα να κάνουν κρυφή την παρουσία τους (Stealth Mode), έτσι ώστε να μην είναι δυνατό για τον επιτιθέμενο να αντιληφθεί την θέση τους ή και την ύπαρξή τους.

Πλεονεκτήματα των NIDS

- Ελάχιστοι μόνο *Sensors* μπορούν να προστατέψουν ένα πολύ μεγάλο δίκτυο.
- Η υλοποίηση και η εφαρμογή ενός NIDS σε ένα δίκτυο επηρεάζει ελάχιστα την λειτουργία του δικτύου.

Οι *Sensors* στους οποίους εκτελούνται οι λειτουργίες του NIDS, είναι συνήθως παθητικές συσκευές που απλά παρακολουθούν και επεξεργάζονται το traffic του δικτύου, χωρίς να παρεμβάλλονται στην κανονική λειτουργία του. Έτσι είναι σχετικά εύκολο το να προστεθεί ένας *Sensor* σε ένα δίκτυο.

- Τα NIDS μπορούν να είναι αρκετά ασφαλή, όσο αναφορά τις επιθέσεις που μπορεί να έχουν αυτά ως στόχο, καθώς έχουν την δυνατότητα να κρύβουν την παρουσία τους από τους επιτιθέμενους.

Μειονεκτήματα των NIDS

Τα NIDSs μπορούν να παρουσιάσουν προβλήματα σε δίκτυα όπου υπάρχει πολύ μεγάλο traffic. Τα προβλήματα προκύπτουν όταν σε περιόδους που το traffic ενός τέτοιου δικτύου κυμαίνεται σε πολύ υψηλά επίπεδα, το NIDS δεν έχει τους πόρους να επεξεργαστεί όλα πακέτα, με αποτέλεσμα να αγνοήσει κάποια από αυτά, κάτι που μπορεί να οδηγήσει στην αποτυχία αναγνώρισης μίας επίθεσης. Για τον λόγο αυτό γίνονται προσπάθειες έτσι ώστε να παραχθούν NIDSs τα οποία θα έχουν την μορφή Hardware, κάτι που θα τα κάνει πιο γρήγορα και πιο ανθεκτικά, αλλά συγχρόνως πιο ακριβά και λιγότερο ευέλικτα.

- Τα NIDS δεν μπορούν αναλύσουν πληροφορία σε κρυπτογραφημένη μορφή και αυτό είναι ένα πρόβλημα που συναντάται συχνά σήμερα με την χρήση των Virtual Private Networks (VPNs) .
- Τα περισσότερα NIDSs δεν μπορούν να καθορίσουν αν μία επίθεση ήταν επιτυχής. Αυτό που κάνουν είναι απλά να επισημάνουν το γεγονός της εμφάνισης μίας επίθεσης και των συστημάτων που είχε στόχο και στην συνέχεια είναι στην αρμοδιότητα του υπεύθυνου για αυτό το σκοπό ατόμου, να εξετάσει κάθε ένα από αυτά τα συστήματα για να εντοπίσει αν η επίθεση πέτυχε.

3.4.1.2 HOST IDSs (HIDS)

Τα HIDSs λειτουργούν με την πληροφορία που συλλέγεται από ένα και μόνο σύστημα το οποίο και προστατεύουν. Αυτό δίνει την δυνατότητα στα HIDS να προσφέρουν λεπτομερή πληροφόρηση για μία επίθεση, δίνοντας πληροφορίες για τις διαδικασίες (processes) και τους χρήστες που έλαβαν μέρος στην συγκεκριμένη επίθεση στο σύστημα που προστατεύουν. Η πληροφορία που κυρίως ελέγχουν τα HIDSs είναι τα αρχεία καταγραφής του συστήματος. Επίσης τα HIDSs έχουν την δυνατότητα να ελέγξουν το αποτέλεσμα μίας επίθεσης, καθώς έχουν άμεση πρόσβαση, για παρακολούθηση των αρχείων και των διαδικασιών του συστήματος, που συχνά στοχεύουν οι επιτιθέμενοι. Κάποια HIDSs προσφέρουν την δυνατότητα χρήσης μίας κοινής κονσόλας διαχείρισης και ελέγχου πολλών συστημάτων, κάνοντας έτσι πιο εύκολη την χρήση τους.

Πλεονεκτήματα των HIDSs

- Τα HIDSs καθώς λειτουργούν τοπικά στο σύστημα που προστατεύουν, έχουν την ικανότητα να ανιχνεύσουν επιθέσεις που δεν ανιχνεύονται από τα NIDS.
- Μπορούν να λειτουργήσουν σε περιβάλλοντα που η επικοινωνία μεταξύ των συστημάτων γίνεται σε κρυπτογραφημένη μορφή (VPNs), καθώς εξετάζουν την πληροφορία πριν αυτή κρυπτογραφηθεί από το σύστημα αποστολέα και αφού αυτή αποκρυπτογραφηθεί από το σύστημα παραλήπτη.
- Τα HIDSs έχουν την δυνατότητα να ελέγξουν και να επιβεβαιώσουν το αποτέλεσμα μίας επίθεσης στο σύστημα που προστατεύουν.

Μειονεκτήματα των HIDSs

- Τα HIDSs είναι δύσκολα στην διαχείρισή τους, καθώς πρέπει να ρυθμιστούν ξεχωριστά για κάθε σύστημα που παρακολουθείται.
- Τα HIDSs είναι επιρρεπή σε επιθέσεις που έχουν στόχο το σύστημα που προστατεύουν. Καθώς το HIDS υλοποιείται τοπικά στο σύστημα που προστατεύει, αν ο επιτιθέμενος καταφέρει να παραβιάσει το σύστημα αυτό, τότε έχει την δυνατότητα να απενεργοποιήσει και το HIDS και να συνεχίσει ανενόχλητος.
- Τα HIDSs δεν μπορούν να εντοπίσουν διάφορες αναγνωριστικές ενέργειες του επιτιθέμενου, όπως τα scans που πραγματοποιεί σε ολόκληρο το δίκτυο.
- Τα HIDSs είναι επιρρεπή σε κάποιες Denial Of Service (DoS) επιθέσεις, οι οποίες μπορεί να προκαλέσουν την διακοπή της λειτουργίας τους.
- Τα HIDSs επηρεάζουν αρνητικά την απόδοση του συστήματος που προστατεύουν, καθώς χρησιμοποιούν τους πόρους του για να εκτελέσουν τις λειτουργίες τους.

3.4.2 ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ (Analysis)

Υπάρχουν κυρίως τρεις προσεγγίσεις για την ανάλυση των συμβάντων προς ανίχνευση των επιθέσεων. Η πρώτη είναι η τεχνική του *Misuse Detection* η οποία χρησιμοποιείται και από τα περισσότερα IDSs και η οποία προσπαθεί να εντοπίσει κάτι που θεωρείται ‘ύποπτο’, με την έννοια ότι υπάρχει γνώση χρήσης του, σε επιθέσεις που έχουν επαναληφθεί. Η δεύτερη είναι η τεχνική του *Anomaly Detection,* η οποία προσπαθεί να εντοπίσει patterns δραστηριότητας που δεν θεωρούνται φυσιολογικά και η οποία βρίσκεται σε ερευνητικό στάδιο μέχρι σήμερα. Η τελευταία είναι η τεχνική του *Protocol Anomaly Detection,* η οποία στην ουσία αποτελεί μία παραλλαγή της *Anomaly Detection,* με την διαφορά ότι ελέγχει την δραστηριότητα που έχει σχέση με την λανθασμένη, μη φυσιολογική χρήση των πρωτοκόλλων επικοινωνίας.
Τα IDSs που χρησιμοποιούν μόνο την τεχνική του *Anomaly Detection* είναι ελάχιστα, καθώς τα περισσότερα ανιχνεύουν επιθέσεις με την τεχνική του *Misuse Detection* και του *Protocol Anomaly Detection*. Κάθε μία από αυτές τις τεχνικές έχει τα πλεονεκτήματα και τα μειονεκτήματά της, ενώ η καλύτερη προσέγγιση είναι αυτή στην οποία χρησιμοποιείται κατά κύριο λόγο η τεχνική του *Misuse Detection,* η οποία συνδυάζεται με τα αποτελέσματα του *Protocol Anomaly Detection* και κάποιες έξυπνες μεθόδους του *Anomaly Detection*.

3.4.2.1 MISUSE DETECTION

Με την τεχνική του *Misuse Detection* ελέγχεται η δραστηριότητα ενός δικτύου για να εντοπιστούν γεγονότα που μπορεί να ταιριάζουν με κάποια προκαθορισμένα πρότυπα γεγονότων που περιγράφουν μία γνωστή επίθεση. Τα πρότυπα αυτά ονομάζονται *Signatures* (υπογραφές) και για αυτό το λόγο η τεχνική αυτή ονομάζεται και *Signature-based detection*.

Ένα *signature* μπορεί για παράδειγμα να περιγράφει κάποια χαρακτηριστικά ενός πακέτου, όπως η εμφάνιση στα data του, ενός συγκεκριμένου λεκτικού που χρησιμοποιείται για μία επίθεση. Συνήθως για κάθε επίθεση ορίζεται και ξεχωριστό *signature*, αλλά υπάρχουν και προσεγγίσεις όπου ένα signature μπορεί να περιγράφει μία ομάδα από επιθέσεις. Η τεχνική ονομάζεται *Statebased detection*.

Πλεονεκτήματα

- Η τεχνική του *Misuse Detection* έχει την ικανότητα να ανιχνεύει επιθέσεις χωρίς να παράγει πολύ μεγάλο αριθμό από False Positives.
- Με την τεχνική αυτή είναι δυνατό να καθοριστεί γρήγορα και αρκετά αξιόπιστα το εργαλείο που χρησιμοποιήθηκε για να υλοποιηθεί η επίθεση.

Μειονεκτήματα

- Με την τεχνική του *Misuse Detection* μπορούν να ανιχνευτούν μόνο γνωστές επιθέσεις και για αυτό το λόγο πρέπει τα *signatures* να ανανεώνονται τακτικά ώστε να καλύπτουν νέες επιθέσεις που εμφανίζονται.
- Η αξιοπιστία της *Misuse Detection* τεχνικής στηρίζεται στην ποιότητα και την σωστή δημιουργία των *signatures* που χρησιμοποιεί. Πολλά IDSs χρησιμοποιούν *signatures* που περιγράφουν αυστηρά μία συγκεκριμένη επίθεση και δεν έχουν την δυνατότητα να ανιχνεύουν διάφορες παραλλαγές αυτής. Η *state-based* τεχνική σε πολλές περιπτώσεις καταφέρνει να ξεπεράσει αυτό το πρόβλημα.

3.4.2.2 ANOMALY DETECTION

Η τεχνική του *Anomaly Detection* προσπαθεί να εντοπίσει μη φυσιολογική, ασυνήθιστη συμπεριφορά ενός δικτύου ή ενός συστήματος. Λειτουργεί με την υπόθεση ότι η δραστηριότητα που παράγεται με την εμφάνιση μίας επίθεσης, παρουσιάζει διαφορές από την φυσιολογική (νόμιμη) δραστηριότητα και για αυτό υπάρχει η δυνατότητα να ανιχνευτούν τυχόν επιθέσεις, από συστήματα που μπορούν να εντοπίσουν αυτές τις διαφορές.
Αρχικά με την μέθοδο του *Anomaly Detection* δημιουργούνται πρότυπα (patterns) που αντιπροσωπεύουν την φυσιολογική συμπεριφορά των χρηστών ή των συστημάτων ή του traffic ενός δικτύου. Τα πρότυπα αυτά χτίζονται από δεδομένα που συλλέγονται κατά την κανονική λειτουργία και αποτελούν το δείγμα φυσιολογικής δραστηριότητας. Η δημιουργία των patterns είναι το πιο δύσκολο κομμάτι της τεχνικής του *Anomaly Detection* καθώς η δραστηριότητα ενός δικτύου ή ενός συστήματος παρουσιάζει πολλές διακυμάνσεις και δεν είναι εύκολο να μοντελοποιηθεί.
Στη συνέχεια συλλέγονται δεδομένα από τα γεγονότα που συμβαίνουν και με διάφορες μεθόδους εξετάζεται κατά πόσο αυτά διαφέρουν από τα patterns της φυσιολογικής δραστηριότητας. Μερικές από τις μεθόδους που χρησιμοποιούνται στην τεχνική του *Anomaly Detection* για να γίνει η δημιουργία των patterns και η σύγκριση των γεγονότων με αυτά είναι :

3.4.2.2.1 THRESHOLD DETECTION

Με αυτή την μέθοδο καταμετρούνται κάποια χαρακτηριστικά της συμπεριφοράς του χρήστη και του συστήματος και ελέγχεται το πλήθος τους, σε σχέση με κάποιο ανώτατο όριο που θεωρείται το επιτρεπτό. Τέτοιου είδους χαρακτηριστικά συμπεριφοράς μπορεί να είναι ο αριθμός των αρχείων στα οποία είχε πρόσβαση ένας χρήστης μέσα σε συγκεκριμένη χρονική περίοδο, το πλήθος των αποτυχημένων προσπαθειών κάποιου χρήστη να κάνει login σε ένα σύστημα, το ποσοστό της CPU που κάνει χρήση ένα process κ.α. Το ανώτατο επιτρεπτό όριο μπορεί να έχει μία στατική τιμή ή να μεταλλάσσεται δυναμικά, προσαρμόζοντας την τιμή του, σύμφωνα με τις τιμές που παρατηρούνται στη διάρκεια του χρόνου και θεωρούνται φυσιολογικές.

3.4.2.2.2 ΣΤΑΤΙΣΤΙΚΕΣ ΜΕΘΟΔΟΙ

Οι *Στατιστικές Μέθοδοι* μπορεί να είναι *Παραμετρικές*, στις οποίες η φυσιολογική δραστηριότητα εκφράζεται με αριθμητικά ποσοστά τα οποία δημιουργούνται από προκαθορισμένα patterns, και *Μη-Παραμετρικές* στις οποίες η φυσιολογική δραστηριότητα εκφράζεται με αριθμητικά ποσοστά, τα οποία δημιουργούνται δυναμικά παρατηρώντας την δραστηριότητα με το πέρασμα του χρόνου.

3.4.2.2.3. RULE BASED

Η μέθοδος αυτή είναι παρόμοια με την *Μη-Παραμετρική Στατιστική* μέθοδο με την έννοια ότι τα patterns της φυσιολογικής δραστηριότητας, δημιουργούνται από δεδομένα που παρατηρούνται με το πέρασμα του χρόνου, αλλά διαφέρει στο ότι αυτά τα patterns δεν εκφράζονται με αριθμητικές ποσότητες αλλά με κάποιους κανόνες (rules).

3.4.2.2.4. ΑΛΛΕΣ ΜΕΘΟΔΟΙ

Έχουν να κάνουν με την χρήση *νευρωνικών δικτύων* και *γενετικών αλγορίθμων*. Τα συστήματα που χρησιμοποιούν αυτές τις μεθόδους, εκπαιδεύονται με ένα μεγάλο σύνολο από δεδομένα, κανόνες και σχέσεις μεταξύ πληροφοριών, ώστε να δημιουργήσουν τα patterns που θα ορίσουν την φυσιολογική δραστηριότητα.
Δυστυχώς τα IDSs που χρησιμοποιούν την τεχνική του *Anomaly Detection* δεν είναι αρκετά αξιόπιστα και παρουσιάζουν πολλά συμπτώματα από False Positives και False Negatives, καθώς τα πρότυπα που εκφράζουν την φυσιολογική δραστηριότητα μπορούν να έχουν πολλές παραλλαγές.

Παρόλα αυτά με την τεχνική του *Anomaly Detection* μπορούν να ανιχνευτούν νέες, άγνωστες επιθέσεις, όπως επίσης τα αποτελέσματά τους μπορούν να χρησιμοποιηθούν σαν πηγές πληροφορίας σε IDSs που χρησιμοποιούν την τεχνική του *Misuse Detection*. Σήμερα είναι ελάχιστα τα IDSs που κάνουν χρήση μόνο του *Anomaly Detection* και η εφαρμογή της τεχνικής αυτής είναι κυρίως για την ανίχνευση των Network και Port scans.

Το *Anomaly Detection* αποτελεί ένα καθαρά ερευνητικό αντικείμενο με πολλά ελπιδοφόρα μηνύματα για το μέλλον.

Πλεονεκτήματα

- Η τεχνική του *Anomaly Detection* μπορεί να εντοπίσει κάποια ασυνήθιστη δραστηριότητα και για αυτό το λόγο μπορεί να ανιχνεύσει συμπτώματα μίας επίθεσης, χωρίς να απαιτείται η γνώση λεπτομερειών για αυτή.
- Μπορεί να ανιχνεύσει επιθέσεις που δεν έχουν επαναληφθεί και γενικότερα δεν υπάρχει προηγούμενη γνώση για αυτές.
- Μπορεί να εξάγει πληροφορίες οι οποίες στην συνέχεια να χρησιμοποιηθούν σαν είσοδο σε IDSs που κάνουν χρήση της τεχνικής του *Misuse Detection*.

Μειονεκτήματα

- Η τεχνική αυτή παρουσιάζει πολλά συμπτώματα από False Positives και False Negatives, καθώς δεν μπορούν να δημιουργηθούν αξιόπιστα και αποδοτικά patterns, λόγω της απρόβλεπτης συμπεριφοράς των χρηστών και των δικτύων.
- Για να δημιουργηθούν τα patterns της φυσιολογικής δραστηριότητας συνήθως απαιτούνται εκτεταμένα εκπαιδευτικά σύνολα που θα χρησιμοποιηθούν ως παράδειγμα.

3.4.2.3. PROTOCOL ANOMALY DETECTION

Η τεχνική αυτή έχει εμφανιστεί τα τελευταία χρόνια στο χώρο των IDSs και στην ουσία είναι μία παραλλαγή της τεχνικής του *Anomaly Detection*. Η διαφορά τους βρίσκεται στο ότι η *Protocol Anomaly Detection* ελέγχει την δραστηριότητα του δικτύου όσο αναφορά την σωστή χρήση των πρωτοκόλλων επικοινωνίας και κυρίως εκείνων που ανήκουν στην οικογένεια του TCP/IP. Τα πρωτόκολλα επικοινωνίας είναι σύνολα από αρχές και κανόνες που ορίζουν τον τρόπο με τον οποίο επιτυγχάνεται η επικοινωνία μεταξύ δύο διασυνδεδεμένων συστημάτων. Είναι γεγονός ότι ένα πολύ μεγάλο ποσοστό των επιθέσεων που λαμβάνουν χώρα στο Internet υλοποιούνται με την μη φυσιολογική χρήση των πρωτοκόλλων επικοινωνίας. Η θεωρητική χρήση των πρωτοκόλλων ορίζεται σε επίσημα, ευρέως αποδεκτά έγγραφα τα RFCs (Request For Comments) τα οποία περιγράφουν τα standards, που κάθε πρωτόκολλο πρέπει να ακολουθεί κατά την υλοποίησή του.

Οι επιθέσεις που στηρίζονται στην μη φυσιολογική χρήση των πρωτοκόλλων, αποβλέπουν στο γεγονός ότι τέτοιου είδους ενέργειες έχουν παραβλεφθεί από τα RFCs ή στην κακή υλοποίηση και εφαρμογή των κανόνων που περιγράφονται στα RFCs, από διάφορους κατασκευαστές λειτουργικών συστημάτων και λογισμικών γενικότερα.

Με την τεχνική του *Protocol Anomaly Detection* παρακολουθείται και αναλύεται η δραστηριότητα που έχει σχέση με την χρήση των πρωτοκόλλων και ελέγχεται για το αν αυτή συμφωνεί με κάποια patterns τα οποία περιγράφουν την φυσιολογική, νόμιμη χρήση των πρωτοκόλλων. Η δημιουργία των patterns είναι πιο εύκολη υπόθεση σε σχέση με αυτή στην τεχνική του *Anomaly Detection,* καθώς σε αυτήν την περίπτωση τα patterns αποτελούνται από τους προκαθορισμένους κανόνες που περιγράφονται από τα RFCs και όχι από κανόνες που περιγράφουν την φυσιολογική δραστηριότητα ενός δικτύου ή ενός συστήματος που μπορεί να παρουσιάζει πολλές διακυμάνσεις.

Πλεονεκτήματα

- Η τεχνική του *Protocol Anomaly Detection* μπορεί να εντοπίσει κάποια ασυνήθιστη δραστηριότητα που αφορά μη φυσιολογική χρήση κάποιου πρωτοκόλλου και για αυτό το λόγο μπορεί να ανιχνεύσει συμπτώματα μίας επίθεσης χωρίς να απαιτείται η γνώση λεπτομερειών για αυτή.
- Μπορεί να ανιχνεύσει επιθέσεις που δεν έχουν επαναληφθεί και γενικότερα δεν υπάρχει προηγούμενη γνώση για αυτές.
- Μπορεί να εξάγει πληροφορίες οι οποίες στην συνέχεια να χρησιμοποιηθούν σαν είσοδο σε IDSs που κάνουν χρήση της τεχνικής του *Misuse Detection*.

Μειονεκτήματα

- Η δημιουργία των patterns δεν μπορεί πάντα να ακολουθεί πιστά στους κανόνες που ορίζονται από τα RFCs, καθώς δεν συμβαίνει το ίδιο και από τα λειτουργικά συστήματα και τα άλλα λογισμικά που κάνουν χρήση των πρωτοκόλλων. Τα patterns που δημιουργούνται πρέπει να λαμβάνουν το γεγονός αυτό υπόψη τους.
- Δεν μπορούν να ανιχνεύσουν επιθέσεις που δεν στηρίζονται στην μη φυσιολογική χρήση των πρωτοκόλλων.
- Όταν ανιχνευτεί μία επίθεση με την τεχνική αυτή, συνήθως δεν προσφέρονται πληροφορίες που να περιγράφουν επαρκώς το είδος της και απαιτείται η συμμετοχή εξειδικευμένων ατόμων που να μπορούν να ερμηνεύσουν τα αποτελέσματα που παράγονται.

3.4.3 RESPONSES

Μετά το στάδιο της συλλογής των δεδομένων και της επεξεργασίας τους, τα IDSs πρέπει με κάποιο τρόπο να γνωστοποιήσουν τα αποτελέσματά τους, αναφέροντας τα γεγονότα που υποδεικνύουν πιθανές περιπτώσεις επιθέσεων ή και να δράσουν προς αντιμετώπιση αυτών. Η λειτουργία αυτή των IDSs είναι πολύ σημαντική, καθώς αυτή θα αποτελέσει την βάση για να ληφθούν τα κατάλληλα μέτρα προστασίας γρήγορα και αποτελεσματικά.

Τα είδη των Responses μπορούν να διαχωριστούν σε *Active Responses*, *Passive Responses* ή *Mixed Responses*. Τα τελευταία είναι συνδυασμός των δύο προηγούμενων και δεν θα γίνει εκτενέστερη αναφορά σε αυτά.

3.4.3.1 ACTIVE RESPONSES

Τα *Active Responses* είναι αυτοματοποιημένες ενέργειες που εκτελούνται από το IDS, όταν ανιχνεύσει συγκεκριμένους τύπους επιθέσεων. Υπάρχουν τρεις κατηγορίες των *Active Responses*:

3.4.3.1.1. ΣΥΛΛΟΓΗ ΕΠΙΠΡΟΣΘΕΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Αυτή είναι ίσως η λιγότερο ενεργητική αντίδραση αλλά σε ορισμένες περιπτώσεις η πιο παραγωγική. Η λειτουργία της είναι να συλλεχτούν περισσότερες πληροφορίες για μία πιθανή επίθεση που εντοπίστηκε, οι οποίες θα ξεκαθαρίσουν περισσότερο την κατάσταση, ώστε να ληφθεί η κατάλληλη απόφαση για το αν πρέπει να παρθούν κάποια παραπέρα μέτρα προστασίας. Έτσι κάποιο IDS όταν εντοπίσει μία πιθανή επίθεση, μπορεί για παράδειγμα να αυξήσει το επίπεδο ευαισθησίας των *Information Sources* που χρησιμοποιεί (πχ. να ρυθμίσει κάποιον *Sensor* να καταγράφει όλα τα πακέτα ενός δικτύου και όχι αυτά που αφορούν συγκεκριμένα συστήματα ή πόρτες). Με την συλλογή της επιπρόσθετης πληροφορίας γίνεται δυνατό να συλλεχθούν περισσότερα στοιχεία για μία πιθανή επίθεση, τα οποία εξυπηρετούν τόσο στην αποφυγή λανθασμένων συμπερασμάτων που μπορεί να προκύψουν διαφορετικά, όσο και στον εντοπισμό και την ποινική δίωξη του επιτιθέμενου.

3.4.3.1.2 ΠΑΡΕΜΠΟΔΣΗ ΤΟΥ ΕΠΙΤΙΘΕΜΕΝΟΥ

Ένας άλλος τύπος του *Active Response,* είναι η αναχαίτιση της επίθεσης την ώρα που πραγματοποιείται και στη συνέχεια ή παρεμπόδιση της παραπέρα πρόσβασης του επιτιθέμενου στο προστατευόμενο σύστημα ή δίκτυο. Στην ουσία το IDS εμποδίζει τα πακέτα που έχουν IP διεύθυνση, από την οποία φαίνεται ότι προέρχεται ο επιτιθέμενος και όχι τον ίδιο τον επιτιθέμενο προσωπικά. Πολλές φορές αυτό δεν αποτελεί αξιόπιστη λύση, καθώς οι πιο έμπειροι επιτιθέμενοι χρησιμοποιούν ψεύτικες IP διευθύνσεις.
Παρόλα αυτά με τέτοιου είδους ενέργειες είναι δυνατό να εμποδιστούν οι πιο αρχάριοι και να αποθαρρυνθούν οι πιο έμπειροι, που υλοποιούν μία επίθεση. Τέτοιες ενέργειες περιλαμβάνουν :

- Να σταλούν πακέτα (με ενεργοποιημένο το RST flag στον TCP header) τα οποία θα τερματίσουν οποιαδήποτε σύνδεση του επιτιθέμενου με το σύστημα – στόχο.
- Να ρυθμιστούν οι routers και τα firewall του δικτύου, ώστε να μην επιτρέπουν την διέλευση οποιουδήποτε πακέτου, το οποίο έχει διεύθυνση αποστολέα ή παραλήπτη, την IP διεύθυνση την οποία χρησιμοποιεί ο επιτιθέμενος στα πακέτα που στέλνει.
- Να ρυθμιστούν οι routers και τα firewall του δικτύου, ώστε να μην είναι δυνατή πρόσβαση σε πόρτες υπηρεσίες και πρωτόκολλα που κάνει χρήση ο επιτιθέμενος.

3.4.3.1.3. ΔΡΑΣΗ ΕΝΑΝΤΙΟΝΤΟΥ ΕΠΙΤΙΘΕΜΕΝΟΥ

Υπάρχουν πολλές σκέψεις για το αν είναι σωστό κατά την ανίχνευση μίας επίθεσης να παρθούν μέτρα που συμπεριλαμβάνουν την δράση εναντίον του επιτιθέμενου. Στην πιο ακραία μορφή της αυτή η δράση θα μπορούσε να είναι η υλοποίηση επίθεσης με στόχο τον επιτιθέμενο ή η συλλογή πληροφοριών για το δίκτυό του. Παρόλο που αυτή η αντιμετώπιση μοιάζει αρκετά αποτελεσματική και δίκαιη, κρύβει πολλούς κινδύνους. Κατά πρώτο λόγο αυτού του είδους η δράση μπορεί να είναι παράνομη. Επιπρόσθετα καθώς πολλοί επιτιθέμενοι χρησιμοποιούν ψεύτικες IP διευθύνσεις όταν εξαπολύουν μία επίθεση, τέτοιου είδους δράση θα μπορούσε να προκαλέσει ζημιές σε λάθος χρήστες ή και δίκτυα. Τέλος κάτι τέτοιο θα μπορούσε να προκαλέσει περισσότερο τον επιτιθέμενο και αυτός να αντιδράσει εξαπολύοντας μία επίθεση που θα μπορούσε να έχει καταστροφικά αποτελέσματα.
Τέτοιου είδους δράση εναντίον του επιτιθέμενου πρέπει να γίνεται με πολύ προσοχή και πριν κάποιος αποφασίσει να υιοθετήσει αυτήν την τεχνική, καλό είναι να έχει συμβουλευτεί κάποιον ειδικό για τα νομικά θέματα που προκύπτουν.

3.4.3.2 PASSIVE RESPONSES

Τα *Passive Responses* είναι η μέθοδος με την οποία το IDS απλά προμηθεύουν τους αρμόδιους χρήστες, με τις πληροφορίες που αφορούν την ανίχνευση μίας επίθεσης. Στη συνέχεια είναι στην ευθύνη των αρμοδίων να δράσουν κατάλληλα, εκμεταλλευόμενοι τις πληροφορίες αυτές. Αυτού του είδους η αντίδραση είναι και η πιο συνήθης από τα περισσότερα IDSs. Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί ένα IDS να γνωστοποιήσει τα αποτελέσματά του στους αρμόδιους χρήστες.

3.4.3.2.1 ΑΝΑΚΟΙΝΩΣΗ ΤΩΝ ALERTS

Αυτή η τεχνική έχει να κάνει με τον τρόπο που ένα IDS ανακοινώνει και παρουσιάζει στους αρμόδιους χρήστες, τις επισημάνσεις του για μία επίθεση. Μία επισήμανση για την ανίχνευση κάποιας επίθεσης, συνήθως ονομάζεται *alert*. Τα περισσότερα IDSs δίνουν την δυνατότητα στον χρήστη να καθορίσει με σχετική ευχέρεια, την στιγμή και την μορφή που θα παράγονται τα *alerts* και σε ποιους χρήστες θα παρουσιάζονται. Ένα IDS είναι δυνατόν να ρυθμιστεί ώστε τα *alerts* να εμφανίζονται σε πραγματικό χρόνο, την ώρα που εντοπίζεται μία επίθεση, όπως για παράδειγμα με αναδυόμενα παράθυρα στην οθόνη ή μπορεί να ρυθμιστεί ώστε να καταγράφει τα *alerts* σε κάποιο αρχείο για μετέπειτα εξέταση. Η μορφή που θα παράγεται ένα *alert* από το IDS, μπορεί να είναι από μία απλή αναφορά στο είδος της επίθεσης με έναν τίτλο, στον επιτιθέμενο και στο θύμα αυτής, μέχρι και αναλυτική αναφορά που θα περιέχει και πληροφορίες για το πακέτο που οδήγησε στον εντοπισμό της επίθεσης, κάνοντας λεπτομερή περιγραφή του ή αναφορά στο εργαλείο που χρησιμοποιήθηκε για την υλοποίησή της.
Επίσης κάποια IDSs έχουν την δυνατότητα να πληροφορούν με *alerts* απομακρυσμένα τους εξουσιοδοτημένους χρήστες, είτε με αποστολή e-mail σε αυτούς, είτε ακόμα μέσω κλήσεων ή αποστολή γραπτών μηνυμάτων σε κινητά τηλέφωνα που ανήκουν σε αυτούς.

3.4.3.2.2. SNMP TRAPS

Κάποια IDSs έχουν την δυνατότητα να αναφέρουν τα *alerts* που παράγουν, σε ένα κεντρικό σύστημα διαχείρισης του δικτύου με την χρήση SNMP Traps. Έτσι με την αποστολή σε ένα κεντρικό σύστημα, των *alerts* που παράγονται από διάφορα IDSs ενός δικτύου, καθώς και άλλων πληροφοριών που εξάγονται από άλλους μηχανισμούς ασφάλειας, όπως Firewalls, είναι δυνατό να γίνει ευκολότερα συσχετισμός μεταξύ των αποτελεσμάτων που έχουν προκύψει από διαφορετικές πηγές και να σχηματιστεί μία πιο σαφής και λεπτομερής εικόνα των γεγονότων.

3.5 ΤΟ ΓΕΝΙΚΟ ΜΟΝΤΕΛΟ ΠΑΙΓΝΙΟΥ ΜΕΤΑΞΥ ΧΡΗΣΤΗ ΚΑΙ IDS

Θα παρουσιάσουμε ένα μοντέλο παιγνίου για το Intrusion Detection μεταξύ του χρήστη και ενός IDS σε εκτεταμένη μορφή. Η περιγραφή αυτού του μοντέλου αποκαλύπτει τα στοιχεία του, πώς παίζεται, και πώς θα μπορούσε να ενταχθεί ως ένας μηχανισμός στο IDS. Επειδή το παίγνιο αυτό είναι επαναλαμβανόμενο, διαχωρίζονται τα τμήματά του, ώστε να να καθοριστεί η δομή του. Με βάση τα παραπάνω, κατασκευάζεται ένα παίγνιο δύο παικτών (μεταξύ του internal attacker και του IDS), που δε συνεργάζονται μεταξύ τους, το οποίο αναλύεται και επιλύεται για να τονίσει τη λειτουργικότητα του μοντέλου και τη σκοπιμότητα της υλοποίησής του.
Επειδή το μοντέλο είναι γενικής χρήσης, επιτρέπει την ευελιξία της εφαρμογής της σε πολλές και διαφορετικές περιπτώσεις για την κατασκευή ενός ολόκληρου παιγνίου που βασίζεται στο μηχανισμό του Intrusion Detection που πρέπει να ενσωματωθούν σε μια IDS. Λόγω της δυναμικής φύσης των αλληλεπιδράσεων μεταξύ ενός χρήστη και ενός IDS και επειδή τα μοντέλα θεωρίας παιγνίων δυναμικών αλληλεπιδράσεων χρησιμοποιούν την εκτεταμένη μορφή αναπαράστασης, θα παρουσιαστεί το Intrusion Detection ως μια εκτεταμένη μορφή παιγνίου.

3.5.1 ΠΑΙΧΤΕΣ

Για να διαμορφώσουμε μια εκτεταμένη μορφή παιγνίου ανάμεσα σε ένα Intrusion Detection System (IDS) και σε ένα χρήστη που προτίθεται να χρησιμοποιήσει ένα Target System (TS) που βρίσκεται πίσω από το IDS, πρέπει να αναφερθούν πέντε στοιχεία: οι παίκτες, οι πιθανές δράσεις, ενέργειες και αποφάσεις των παικτών, τί γνωρίζουν οι παίκτες πριν πάρουν μια απόφαση, οι προδιαγραφές για το πώς οι δράσεις των παικτών οδηγούν σε αποτελέσματα, και η προδιαγραφές των προτιμήσεων των παικτών πάνω σε αυτά τα αποτελέσματα. Αυτό το παίγνιο έχει δύο παίκτες, το IDS που θα το ονομάζουμε I και τον χρήστη που θα τον ονομάζουμε U. Ο παίκτης U μπορεί να είναι ένα κανονικός χρήστης ή ένας εισβολέας.

Ακόμη και αν είναι κανονικός χρήστης θα μπορούσε να βλάψει ακούσια το TS. Συνεπώς, ο παίκτης U θεωρείται ως ένα γενικός χρήστης και δεν χρειάζεται περαιτέρω κατηγοριοποίηση πριν ενεργήσει.

3.5.2 ΔΡΑΣΕΙΣ / ΚΙΝΗΣΕΙΣ

Κάθε παίκτης έχει μια σειρά από πιθανές ενέργειες να εξετάσει. Ο παίκτης I επιλέγοντας C, επιτρέπει στον παίκτη U να χρησιμοποιεί το TS, εφόσον ο Παίκτης U ακολουθεί νόμιμες ενέργειες. Αντίθετα, ο παίκτης I επιλέγοντας P αποφεύγει πρόσθετες ζημιές στο TS, εφόσον κρίνει ότι ο παίκτης U ακολουθεί παράνομες ενέργειες. Με λίγα λόγια, σε αυτό το παίγνιο ο παίκτης I έχει δύο επιλογές:

Με την επιλογή C επιτρέπει στον παίκτη U να συνεχίσει να χρησιμοποιεί το TS και με την επιλογή P αποτρέπει τον παίκτη U να επιτεθεί ή να κάνει περεταίρω ζημιά στο TS. Σε πραγματικές περιπτώσεις, αυτή η δυαδική προσέγγιση αντικατοπτρίζει το γεγονός ότι παίκτης U αιτείται μιας υπηρεσίας ή ενός πόρου από το TS, και ο παίκτης I είτε δέχεται να εκπληρώσει το αίτημα (επιλογή C) ή το απορρίπτει (επιλογή P).

Η ερμηνεία είναι η ίδια και σε άλλες προσεγγίσεις που ενδεχομένως φαίνεται να περιλαμβάνουν περισσότερες από δύο επιλογές για τον παίκτη I. Ομοίως, ο παίκτης U έχει τρεις πιθανές ενέργειες: L όταν ενεργεί νόμιμα, A όταν ενεργεί παράνομα δημιουργώντας επιθέσεις, και E όταν αποφασίζει να βγει από το TS.

3.5.3 ΔΙΑΔΟΧΙΚΕΣ ΚΑΙ ΤΑΥΤΟΧΡΟΝΕΣ ΚΙΝΗΣΕΙΣ

Στη συνέχεια, το βασικό ερώτημα που πρέπει να απαντηθεί για αυτό το παίγνιο είναι πώς αυτό το παίγνιο θα παιχτεί με ταυτόχρονες ή διαδοχικές κινήσεις. Το καθοριστικό κριτήριο για την απάντηση σε αυτό το θέμα είναι να ληφθεί υπόψη κατ 'αρχάς, ότι με τη χρήση του TS και ζητώντας μια υπηρεσία από αυτό, ο χρήστης περιμένει μια απάντηση, αν και τις περισσότερες φορές δεν το συνειδητοποιεί. Στη συνέχεια ο χρήστης κάνει ένα νέο αίτημα , και ούτω καθεξής. Έτσι, έχουμε μια αλληλεπίδραση διαδοχικών κινήσεων, όπως αυτή που λαμβάνει χώρα ανάμεσα σε δύο παίκτες σε μια παρτίδα σκάκι. Ωστόσο, όταν το TS προστατεύεται από ένα IDS, ο χρήστης αλληλεπιδρά με το TS αλλά επίσης αλληλεπιδρά και με το IDS. Στο τελευταίο είδος αλληλεπίδρασης, ο χρήστης ενεργεί και την ίδια στιγμή το IDS συλλέγει τα δεδομένα που σχετίζονται με τη δράση αυτή, τα φιλτράρει και σε περίπτωση επίθεσης, αποφασίζει για την αντιμετώπισή της .

Η παιγνιοθεωρητική προσέγγιση της παραπάνω αλληλεπίδρασης ,δείχνει ότι στο Intrusion Detection ο εισβολέας σχεδιάζει τις κινήσεις του πριν τις πράξει και υπολογίσει μελλοντικές συνέπειες.

Έως αυτό το σημείο το παίγνιο είναι επαναλαμβανόμενο και διαδοχικό, αλλά όταν ο εισβολέας ξεκινήσει την εφαρμογή αυτού του σχεδίου και αντιμετωπίσει την ύπαρξη του IDS προστατεύοντας το TS από την επίθεση, τότε θα προσπαθήσει να ανακαλύψει ποια θα είναι είναι η επόμενη κίνηση του IDS. Τα τελευταία δείχνουν ότι το παίγνιο περιλαμβάνει επίσης ταυτόχρονες κινήσεις. Ωστόσο, το IDS έχει σχεδιαστεί να υλοποιεί μία ή περισσότερες τεχνικές για το που οδηγούν σε ένα προκαθορισμένο σχέδιο για κινήσεις του ID, υπολογίζοντας τις μελλοντικές συνέπειες που αφορούν τις μελλοντικές συνέπειες για την προστασία του TS. Μέχρι το σημείο αυτό και πάλι το παίγνιο είναι για δεύτερη φορά ένα παίγνιο διαδοχικών κινήσεων, αλλά όταν ένας χρήστης μπαίνει στο σύστημα, το IDS παρατηρεί τις κινήσεις του για να αποφασίσει αν είναι ένας εισβολέας ή όχι, και σύμφωνα με το σχεδιασμό, να καταλάβει τις κινήσεις του εισβολέα. Το συμπέρασμα είναι ότι για άλλη μια φορά το παίγνιο περιλαμβάνει επίσης ταυτόχρονες κινήσεις. Κατά συνέπεια, το Intrusion Detection στο IT Security είναι ένα παίγνιο που συνδυάζει διαδοχικές και ταυτόχρονες κινήσεις.

3.5.4 ΓΕΝΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΠΑΙΓΝΙΟΥ

Ας σκεφτούμε την εκτεταμένη μορφή του παιγνίου για το Intrusion Detection που απεικονίζεται στο σχήμα. 1. Ένας χρήστης (παίκτης U) επιχειρεί να εισαχτεί σε ένα TS που προστατεύεται από το IDS (παίκτης I). Ο χρήστης ενδέχεται να συνδεθεί με επιτυχία στο TS ή όχι (π.χ. λόγω τυπογραφικού λάθους στο password). Ακόμη και αν αποκτήσει πρόσβαση στο TS θα μπορούσε να είναι ήδη σε «μαύρη λίστα». Ως εκ τούτου, ο παίκτης I παίζει πρώτος στον αρχικό κόμβο του παιγνίου που παριστάνεται από έναν ανοιχτό κύκλο, όταν παίκτης U προσπαθεί να εισέλθει στο TS. Στη συνέχεια, ο παίκτης I, εξετάζοντας αυτήν την προσπάθεια, έχει δύο επιλογές, να επιτρέψει τη συνέχιση του χρήστη (επιλογή C) ή να αποτρέψει τον χρήστη να χρησιμοποιήσει το TS (επιλογή P) και να τελειώσει το παίγνιο. Στην τελευταία αυτή περίπτωση, είναι δεδομένο ότι παίκτης θα έχει επιτύχει να εντοπίσει πραγματικά τον εισβολέα και δεν προκάλεσε ψεύτικο συναγερμό. Ως εκ τούτου, το αποτέλεσμα στο τέλος του παιγνίου είναι το διάνυσμα (ανίχνευση, απόπειρα επίθεσης) για τον παίκτη I και τον παίκτη U αντίστοιχα.

Αν ο παίκτης I επιλέξει C, τότε ο παίκτης U έχει τρεις επιλογές: να διενεργήσει νομικές διαδικασίες (επιλογή L), να επιτεθεί στο TS (επιλογή A), ή να φύγει από το TS (επιλογή E). Αν ο παίκτης U φύγει από το TS, τότε το παίγνιο τελειώνει με το αποτέλεσμα (δεν υπήρξε ανίχνευση, προσπάθεια επίθεσης). Ο λόγος γι' αυτά τα τελικά αποτελέσματα είναι:

1. Ο χρήστης έχει επιτύχει να μπει στο TS και το IDS δεν εντόπισε κάποια επίθεση ακόμα και αν ήταν κρυφή, και φαίνεται ως διείσδυση.

Ο χρήστης δεν κάνει επίθεση στο TS, ακόμα και αν έχει τις δυνατότητες (γνωρίζει το username και το password), αλλά απλώς τις ελέγχει στο TS προκειμένου να επιτεθεί μια άλλη φορά στο μέλλον.

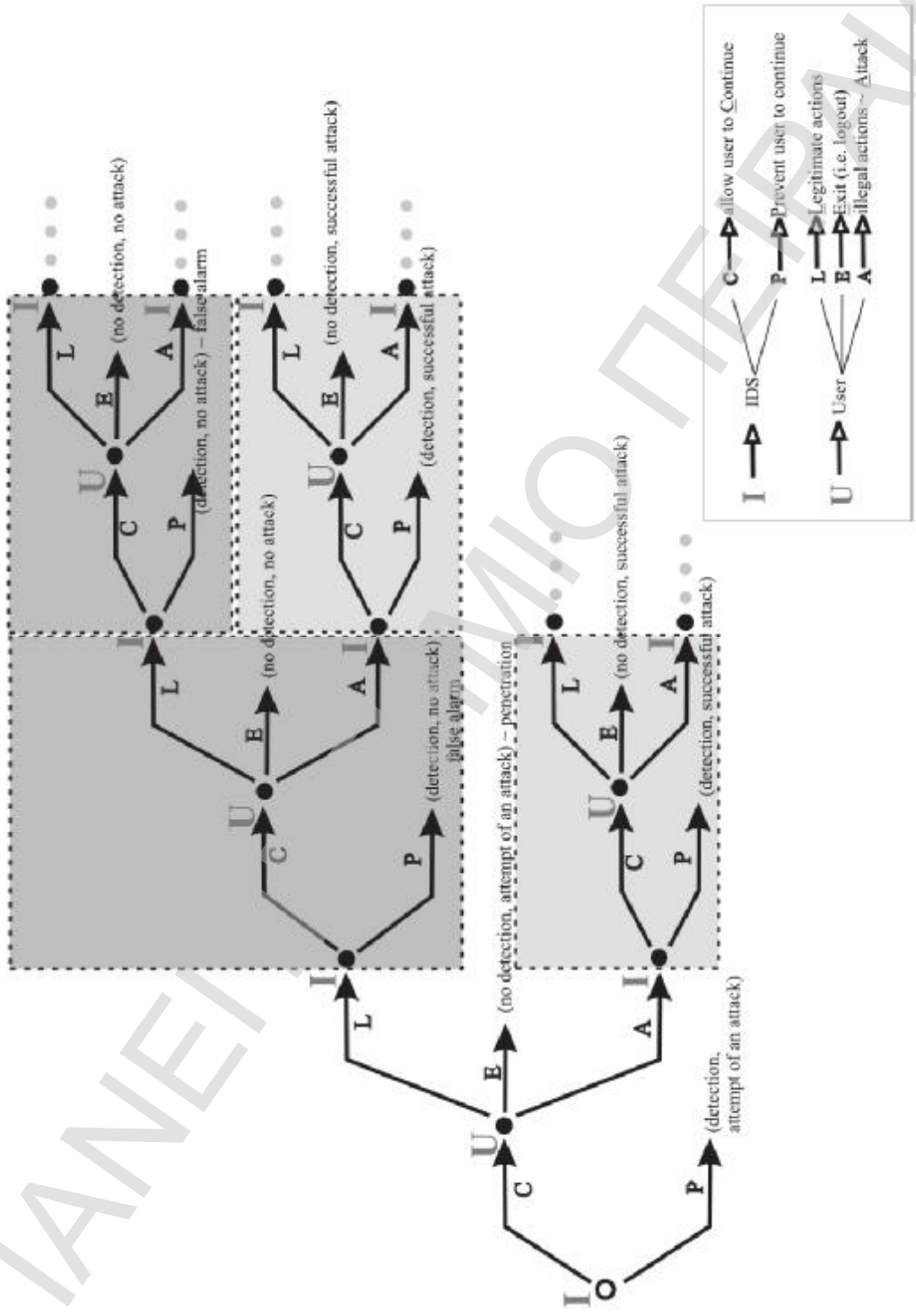


Fig. 1. Intrusion Detection as an extensive form game

Το παίγνιο συνεχίζεται με τον παίκτη U να επιλέγει μια νομική ενέργεια για το TS ή να επιτίθεται στο TS. Και στις δύο περιπτώσεις, ο παίκτης I στη αναλύει την κίνηση του αντιπάλου και αποφασίζει εάν αυτός ενεργεί νόμιμα ή όχι. Εάν παίκτης I επιλέξει P, τότε τα τελικά πιθανά αποτελέσματα του παιγνίου είναι δύο. Ειδικότερα, αν ο παίκτης U κάνει επίθεση (επιλογή A), τότε τα τελικά αποτελέσματα είναι (ανίχνευση, επιτυχημένη επίθεση), αλλιώς (επιλογή L), τα τελικά αποτελέσματα είναι (ανίχνευση, μη επίθεση) όπου έχουμε ψεύτικο συναγερμό. Εναλλακτικά, όταν παίκτης I επιτρέπει στον παίκτη U συνέχιση της συνεργασίας με το TS (επιλογή C), εφόσον ο δεύτερος ενεργεί νόμιμα, τότε ο παίκτης U μπορεί να προχωρήσει με νόμιμες ενέργειες (επιλογή L), ή με μια επίθεση (επιλογή A), ή να αποφασίζει για την έξοδο από το TS (επιλογή E) τερματίζοντας το παίγνιο. Αυτό το παίγνιο έχει ως τελικό αποτέλεσμα (μη ανίχνευση, μη επίθεση). Το περιγραφόμενο στάδιο του παιγνίου, περιβάλλεται από ένα διακεκομμένο παραλληλόγραμμο, όπως φαίνεται στο Σχήμα. 1 και είναι μια επαναλαμβανόμενη διαίρεση του παιγνίου η οποία οδηγεί στο τέλος αυτού, όταν παίκτης U επιλέξει E. Διερευνώντας περαιτέρω την εκτεταμένη μορφή του ID παιγνίου για επανειλημμένες διαιρέσεις, εντοπίζουμε δύο μέρη, όπου το ένα έχει σχέση με νόμιμες ενέργειες και το άλλο με τις επιθέσεις. Η εκτεταμένη μορφή του ανωτέρω παιγνίου εξηγείται λεπτομερώς στο Σχήμα 2, όπου εμφανίζονται δύο ξεχωριστά τμήματα με τις επαναλήψεις τους. Παρά το γεγονός ότι το παίγνιο ID φαίνεται να μην τελειώνει ποτέ, κάθε μία από τις επαναλαμβανόμενες διαιρέσεις σίγουρα έχει μία εναλλακτική οδό στην οποία το παίγνιο τελειώνει, και έτσι έχουμε ένα πεπερασμένο παίγνιο.

3.5.5 ΄ΕΛΕΓΧΟΣ ΤΗΣ ΕΚΤΕΤΑΜΕΝΗΣ ΜΟΡΦΗΣ

Εκτεταμένης μορφής παίγνια θα πρέπει να δίνουν την εικόνα ενός δένδρου. Δύο είναι οι κανόνες που πρέπει να εξασφαλισθούν για αυτή τη μορφή:

- Πρώτα, από τον αριθμό των κατευθύνσεων, τουλάχιστον η μία πρέπει να επισημάνει έναν κόμβο και να δείχνει το πολύ έναν.
- Και το δεύτερο, να εντοπίσει ξανά το δέντρο με τέτοιο τρόπο ώστε ο κόμβος εκκίνησης να μην κάνει κύκλο, αλλά στην πραγματικότητα ο αρχικός κόμβος θα πρέπει να είναι το τέλος αυτού του εντοπισμού.

Ο πρώτος κανόνας σημαίνει ότι ένας παίκτης, όταν είναι η σειρά του να παίξει, μετά από μία πράξη άλλου παίκτη, έχει τουλάχιστον μια δράση για την εκτέλεση, είτε κάποιος άλλος παίκτης έχει σειρά να παίξει, αλλιώς το παίγνιο τελειώνει και δίνει συγκεκριμένο αποτέλεσμα.

Ο δεύτερος κανόνας αποσκοπεί στην επίλυση των παιγνίων σε εκτεταμένη μορφή, χρησιμοποιώντας την μέθοδο του εντοπισμού, δεδομένου ότι έχουν τη μορφή ενός δένδρου.

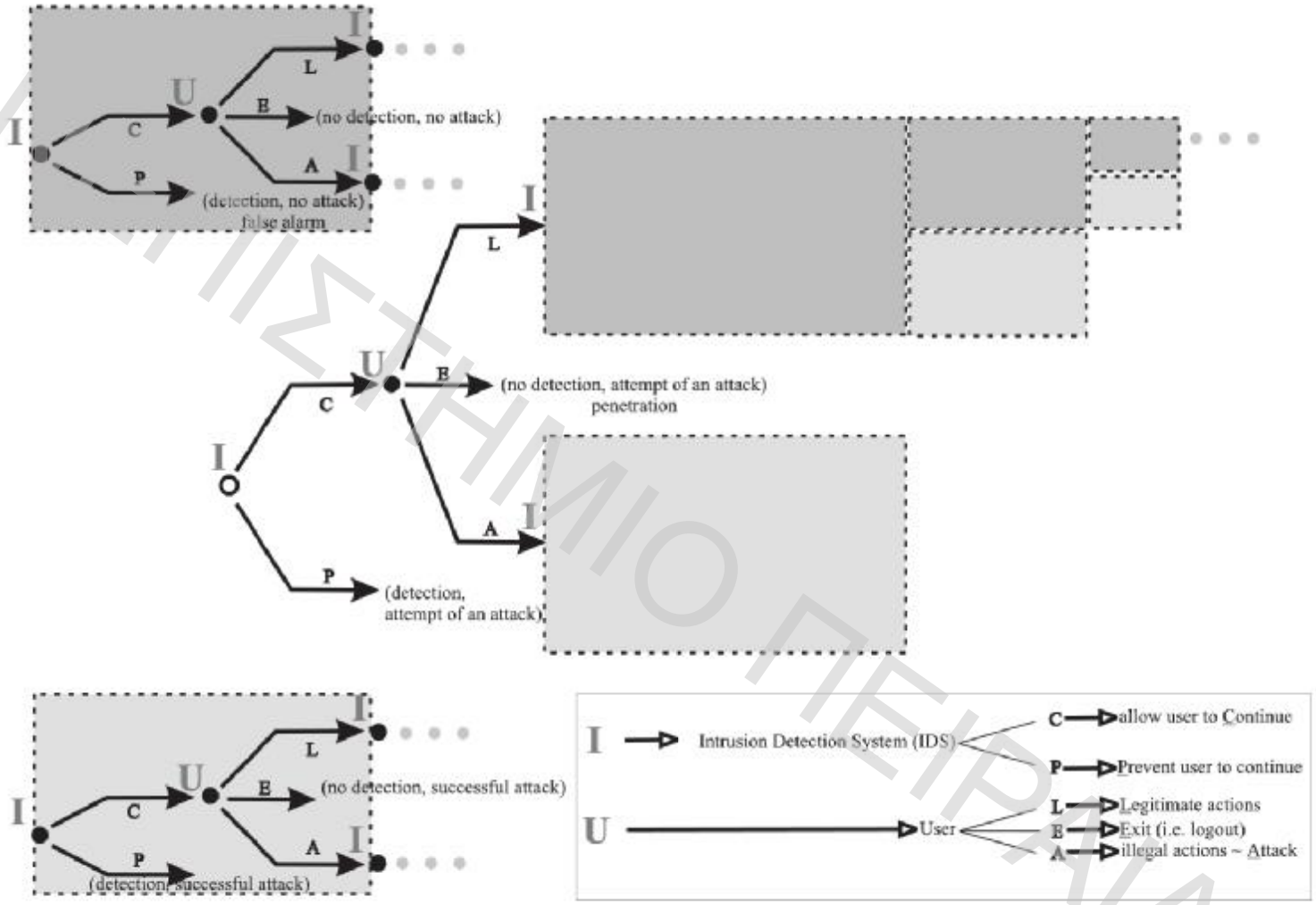


Fig. 2. Intrusion Detection and the repeated divisions of the game

Το παίγνιο Intrusion Detection που περιγράφεται παραπάνω έχει μοντελοποιηθεί με τη μορφή ενός δέντρου. Για τον έλεγχο του παιγνίου κατά τον πρώτο κανόνα, είναι προφανές ότι ο αριθμός των κατευθύνσεων τόσο σε κάθε κόμβο, όσο και σε ένα συγκεκριμένο κόμβο, θα πρέπει να ικανοποιούν τον κανόνα αυτό. Επίσης, εξετάζοντας την αξιοπιστία του εντοπισμού από κάθε κόμβο προς τον αρχικό κόμβο του παιγνίου, δεν θα πρέπει να σχηματιστεί κύκλος και ο αρχικός κόμβος θα πρέπει να τερματιστεί επιτυχώς.

3.5.6 ΠΑΙΖΟΝΤΑΣ ΤΟ ΠΑΙΓΝΙΟ ΜΕ ΕΝΑΝ ΕΣΩΤΕΡΙΚΟ ΕΙΣΒΟΛΕΑ

Για την επικύρωση του μοντέλου που αναφέραμε παραπάνω, θα κατασκευάσουμε ένα παίγνιο που θα είναι μεταξύ του IDS και του χρήστη TS πίσω από αυτό το IDS. Επιπλέον, θα υποτεθεί ότι ο χρήστης επίσης είναι ένας εσωτερικός εισβολέας. Βέβαια είναι δύσκολο να εντοπιστεί ένας εισβολέας λόγω των πλεονεκτημάτων που έχει για να τον προστατεύουν αρκετά. Μια τέτοια προσπάθεια δημιουργεί ένα μεγάλο αριθμό λανθασμένων στοιχείων και αυτό έχει ως αποτέλεσμα την ενεργοποίηση θετικών alarm, με ένα ανάλογο αριθμό των αρνητικών alarm.

Το παίγνιο έχει δύο παίκτες, τον εσωτερικό εισβολέα U και τον IDS I. Με απλά λόγια, το γενικό μοντέλο παιγνίου φαίνεται ως μια μαύρη και άσπρη αναπαράσταση, δείχνοντας έτσι την δράση του κάθε παίκτη. Φαίνεται ότι ένας εσωτερικός εισβολέας ενός οργανισμού που πράττει κανονικά σύμφωνα με τις δεσμεύσεις και τις υποχρεώσεις του, κατά καιρούς κάνει και λάθη, επίσης δρα μεθοδολογικά για να προετοιμάσει επιθέσεις και τέλος εκτελεί αυτές τις επιθέσεις όπως τις σχεδίασε.

Το IDS ακολουθεί μια κατεύθυνση, την κατεύθυνση της συνεργασίας και αποφασίζει μεταξύ τεσσάρων εναλλακτικών λύσεων. Πρώτον, επιτρέπει στο χρήστη να συνεχίσει αν δεν παρατηρηθεί τίποτα ύποπτο, δεύτερον κάνει μια σύσταση κάθε φορά που προκύπτουν ελαφρές αποκλίσεις, τρίτον θέτει μια προειδοποίηση για να υπενθυμίσει στον χρήστη να είναι συνεπής με τους κανονισμούς χρησιμοποιώντας το TS, και τέταρτον να σταματήσει το χρήστη όταν διαπιστωθεί παραβίαση. Συνοψίζοντας, ο παίκτης U έχει τέσσερις στρατηγικές , Κανονική, Λάθος, προ- επίθεση, επίθεση, και ο παίκτης IDS έχει τέσσερις στρατηγικές, Συνέχεια, Επισήμανση, Προειδοποίηση, Stop. Προφανώς, για τον παίκτη U η πρώτη στρατηγική N αντιστοιχεί σε νόμιμες ενέργειες, ενώ οι υπόλοιπες στρατηγικές ισοδυναμούν με παράνομες ενέργειες. Ομοίως, για τον παίκτη I οι τρεις πρώτες στρατηγικές έχουν την άδεια να συνεχίσουν, ενώ η δεύτερη, η S όχι.

Η μεταφορά των εν λόγω παιγνίου από την εκτεταμένη μορφή σε ένα παίγνιο στρατηγικής μας δίνει τον εξής 4x4 πίνακα, όπως παρουσιάζεται στον Πίνακα 1. Η σειρά αναφέρεται στον παίκτη (U) και η στήλη στο IDS (I). Τα αποτελέσματα του παιγνίου έχουν αποτιμηθεί αρχικά από τις προτιμήσεις, και στη συνέχεια, υπολογίζονται με τη χρησιμοποίηση της συνάρτησης του von Neumann-Morgenstern.

Ειδικότερα, η ιεράρχηση των προτιμήσεών της κάθε στρατηγικής του χρήστη, από τη λιγότερο προτιμητέα (PS) στην πλέον προτιμητέα (AC), έχει ως εξής:

PSU ≺ MSU ~ PWU ≺ PRU ~ MWU ≺ MRU ~ ARU ≺ AWU ~ NSU ≺ ASU ~ NWU ≺ NRU ≺ MCU ≺ PCU ≺ NCU ≺ ACU

Στη συνέχεια, εκχωρούνται αριθμοί που αντικατοπτρίζουν τις προτιμήσεις σύμφωνα με την συνάρτηση του Neumann-Morgenstern. Θέτουμε 0 την στρατηγική του PS και 1 την στρατηγική του AC. Σύμφωνα με την παραπάνω ιεραρχία ορίζουμε έναν αριθμό σε κάθε στρατηγική. Στη συνέχεια έχουμε τις τιμές χωρίς κλάσματα, μετά τον πολλαπλασιασμό τους με τον κοινό παράγοντα. Τα τελικά αποτελέσματα του χρήστη δίνονται από τον πρώτο αριθμό του κάθε ζεύγους των αποτελεσμάτων, όπως εμφανίζεται στον Πίνακα 1.

		I **C**	**R**	**W**	**S**
U	**N**	(13,17)	(9,5)	(8,4)	(7,2)
	M	(10,3)	(6,6)	(5,7)	(4,14)
	P	(12,1)	(5,8)	(4,9)	(3,15)
	A	(19,0)	(6,10)	(7,11)	(8,16)

Πίνακας 1. Ένα παίγνιο μεταξύ εσωτερικού εισβολέα με τον IDS

Μετά τα ίδια βήματα για την κατάταξη των προτιμήσεων του IDS, έχουμε την εξής ιεράρχηση:

ACIDS ≺ PCIDS ≺ NSIDS ≺ MCIDS ≺ NWIDS ≺ NRIDS ≺ MRIDS ≺ MWIDS ≺ PRIDS ≺ PWIDS ≺ ARIDS ≺ AWIDS ≺ MSIDS ≺ PSIDS ≺ ASIDS ≺ NCIDS

Τέλος, η εκχώρηση αριθμών για την ποσοτικοποίηση των σχέσεων μεταξύ των προτιμήσεων του IDS μας δίνει τα τελικά αποτελέσματα που δίνονται από τον δεύτερο αριθμό του κάθε ζεύγους των αποτελεσμάτων, όπως εμφανίζεται στον Πίνακα 1.

3.5.6.1 ΛΥΝΟΝΤΑΣ ΤΟ ΠΑΙΓΝΙΟ

Καθώς έχουμε περιγράψει το Intrusion Detection ως ένα παίγνιο με 2 παίχτες που δεν συνεργάζονται μεταξύ τους, προχωρήσαμε στην επίλυσή του, χρησιμοποιώντας την ανάλυση της ισορροπίας. Μια ισορροπία σε ένα παίγνιο είναι ένα σύνολο αποφάσεων των παικτών που οδηγεί σε ένα αποτέλεσμα, έτσι ώστε, ο παίκτης να μην αποκλίνει για κανένα λόγο από τις επιλογές του, δεδομένου ότι όλοι οι παίκτες κάνουν το ίδιο. Ο John Nash απέδειξε ότι κάθε παίγνιο μη συνεργασίας έχει τουλάχιστον ένα σημείο ισορροπίας Nash (NE). Η έννοια της NE είναι η πιο συχνά χρησιμοποιούμενη λύση στην έννοια των παιγνίων μη συνεργασίας.

Εμείς υπολογίσαμε τη λύση αυτού του παιγνίου εξετάζοντας τις καλύτερες απαντήσεις των παικτών. Υπάρχει μια μοναδική Ισορροπία Nash (NE), η οποία αντιστοιχεί στον συνδυασμό AS (8,16). Επιπλέον, έχουμε χρησιμοποιήσει το εργαλείο Gambit ώστε να εξακριβωθεί η λύση μας και να πάρουμε το ίδιο αποτέλεσμα που βρήκαμε. Η θεωρία NE είναι τέλεια όταν αποκαλύπτει την πρόθεση της εσωτερικής εισβολής στο σύστημα και όταν το IDS αντιδρά σταματώντας την εισβολή αυτή. Είναι ενδιαφέρον, που υπάρχει και ένα άλλο ζεύγος στρατηγικών, με στρατηγικό προφίλ NC, τελικών αποτελεσμάτων (13,17) που είναι μεγαλύτερο από το αντίστοιχο της NE. Εκτός αυτού, τα τελικά αποτελέσματα (13,17) είναι τα υψηλότερα που μπορεί να πάρει ο κάθε παίκτης σε αυτό το παίγνιο. Στην πραγματικότητα, η στρατηγική NC του Pareto δεσπόζει στην στρατηγική της NE, και επειδή τα αντίστοιχα τελικά αποτελέσματα είναι τα υψηλότερα, η στρατηγική αυτή είναι η πιο αποτελεσματική. Με άλλα λόγια, κάθε παίκτης μεταξύ των δύο παικτών μπορεί να αυξήσει το αποτέλεσμα ακόμα και αν αποκλίνει από την οδό της ισορροπίας, επιλέγοντας την αποτελεσματική στρατηγική NC του Pareto.

Στο παίγνιο μιας φοράς, που παρουσιάστηκε σε κανονική μορφή, με πραγματικές συνθήκες δεν μπορέσαμε να το απεικονίσουμε αφού δεν το εξετάσαμε σε βάθος, με αποτέλεσμα να μην βρούμε ρεαλιστικές λύσεις. Πράγματι, οι παίκτες παίζουν επανειλημμένα και άπειρες φορές, ειδικά σε αυτό το παίγνιο. Ο λόγος είναι ότι, ο χρήστης δεν είναι ένας τυχαίος εισβολέας, αλλά ένας εσωτερικός χρήστης του συστήματος, που ξοδεύει πολύ χρόνο κάθε μέρα μέσα σε αυτό.

Το γενικό μοντέλο που περιγράφει το παίγνιο στο προηγούμενο κεφάλαιο, αποδεικνύει ότι τα τμήματα των επαναλαμβανόμενων διαιρέσεων έχουν ήδη εντοπιστεί. Για να επιλύσουμε αυτό το επαναλαμβανόμενο παίγνιο ακολουθήσαμε τη διαδικασία του DK Levine βήμα προς βήμα. Πρώτα, αποφασίσαμε να χρησιμοποιήσουμε το μέσο όρο της παρούσας μεθόδου για τα συνολικά αποτελέσματα που λάβαμε μεταξύ διαφορετικών περιόδων. Εναλλακτικές λύσεις θα ήταν να προσθέσουμε τα τελικά αποτελέσματα μαζί, να βρούμε το μέσο όρο τους, ή να πάρουμε την παρούσα αξία. Δεύτερον, διευκρινίσαμε ότι αυτό το παίγνιο μπορεί να επαναληφθεί άπειρες φορές, όπως αναφέρεται στην προηγούμενη παράγραφο. Τέλος, όσον αφορά την μείωση του συντελεστή δ που δείχνει πόσο πολύ ανυπόμονος είναι ο παίκτης, θα καθορίσουμε ένα συντελεστή ανυπομονησίας και για τους δύο παίκτες. Ο συντελεστής δ ποικίλλει μεταξύ μηδέν και ένα, με το μηδέν να ταιριάζει σε έναν παίκτη ανυπόμονο και με το ένα σε έναν υπομονετικό.

Στη δική μας περίπτωση, ο εσωτερικός εισβολέας είναι ένας υπομονετικός παίκτης, επειδή έχει πολύ χρόνο να οργανώσει και να εκτελέσει μια επίθεση. Επιπλέον, στο IDS είναι έμφυτο το γεγονός του υπομονετικού παίκτη, επειδή παίζει πολύ με έναν χρήστη του TS, αν και δεν γνωρίζουμε ότι είναι ένας εσωτερικός εισβολέας.

Ένα από τα πράγματα που εξετάσαμε ήταν οι δύσκολες στρατηγικές ισορροπίας. Θεωρώντας την περίπτωση στην οποία ο εσωτερικός εισβολέας παίζει μια συγκεκριμένη στρατηγική σε κάθε περίοδο, εξετάσθηκαν οι συνθήκες υπό τις οποίες απέκλιναν από αυτή την ισορροπημένη διαδρομή, στην οποία θα μπορούσε να έπαιζε άλλη στρατηγική. Αλλά το IDS θα έπρεπε να αντιδράσει επιλέγοντας μια στρατηγική «τιμωρίας» ενάντια στην εν λόγω απόκλιση, που είναι γνωστή ως σκληρή στρατηγική. Εξετάσαμε ειδικότερα το εξής σενάριο:

Υπόθεση 1. Ο εσωτερικός εισβολέας που ενεργεί νόμιμα ξεκινάει να παίζει το παίγνιο, επιλέγοντας την στρατηγική N. Το IDS απαντά παίζοντας με τη στρατηγική *C*. Αυτό ισχύει και για κάθε περίοδο όσο αναπαράγονται οι NC στρατηγικές. Αλλά τότε, υπό ποιές συνθήκες ο εσωτερικό εισβολέας θα διαπράξει μια επίθεση, δηλαδή, να αποκλίνει από την παρούσα ισορροπημένη διαδρομή; Ψάχνουμε για τον συντελεστή δ που θα παρακινήσει τον εσωτερικό εισβολέα να το κάνει διότι το όφελος θα είναι πολύ μεγαλύτερο.

Λύση: Υπολογίζουμε το μέσο όρο της παρούσας αξίας (ΠΑ) για κάθε παίκτη της ισορροπημένης διαδρομής με τον ακόλουθο τύπο και την σχετική ταυτότητα,

$$(\mathbf{1}-\boldsymbol{\delta})\cdot(\boldsymbol{u1}\ +\ \boldsymbol{\delta u2}+\boldsymbol{\delta^2 u3}+\boldsymbol{\delta^3 u4}+\cdots). \qquad \textbf{(1)}$$

όπου *ui, i* = 1, 2, 3 ..., είναι το τελικό αποτέλεσμα ενός παίκτη που λαμβάνει στο διάστημα i και δ είναι ο κοινός συντελεστής.

$$\mathbf{1}+\boldsymbol{\delta}+\boldsymbol{\delta^2}+\boldsymbol{\delta^3}+\cdots=\frac{\mathbf{1}}{\mathbf{1}-\boldsymbol{\delta}} \qquad \textbf{(2)}$$

Βρήκαμε *APVU* = 13 και *APVI* = 17, αντίστοιχα, όπως αναμένεται, επειδή οι ίδιες στρατηγικές παίζονται σε κάθε περίοδο. Μετά από αυτό, εξετάσαμε τις καλύτερες απαντήσεις των παικτών όταν ο αντίπαλος ακολουθεί την επιλεγμένη ισορροπημένη διαδρομή.

Όταν ο εσωτερικός εισβολέας ακολουθεί την στρατηγική *N*, τότε η καλύτερη απάντηση του IDS είναι η στρατηγική C. Όταν όμως το IDS ακολουθεί την στρατηγική C, τότε η καλύτερη απάντηση του εσωτερικού εισβολέα είναι η στρατηγική *A*, διότι το μεγαλύτερο δυνατό αποτέλεσμα είναι το 19.

Στη συνέχεια, υπολογίσαμε το APV για κάθε παίκτη αν κάθε ένας ακολουθούσε την διαδρομή ισορροπίας κατά την πρώτη περίοδο, αλλά στη συνέχεια και οι δύο απέκλιναν και συνέχιζαν να παίζουν το NE, όπως υπολογίστηκε. Τα αποτελέσματα είναι *APVI* = 17 − *δ* και *APVU* = 19 − 11 · *δ*. Τέλος, συγκρίναμε την παρούσα αξία του μέσου όρου στην που μας υπενθυμίζει την διαδρομή ισορροπίας με εκείνη που αφορά την αποκλίνουσα.

Με άλλα λόγια, προσδιορίσαμε το συντελεστή δ για τον οποίο ένας παίκτης θα παραμένει στην πρώτη του επιλογή και δεν θα αλλάζει μετά από την επίθεση του TS.

Ο συντελεστής δ πρέπει να είναι μεγαλύτερος ή ίσος με 6/11, το οποίο είναι λογικό για το είδος αυτού του εισβολέα. Το γεγονός είναι ότι, ο εσωτερικός εισβολέας συμπεριφέρεται όπως ένας υπομονετικός παίκτης όταν έχει αρκετό χρόνο στη διάθεσή του για να ολοκληρώσει μια επίθεση αλλά είναι αρκετά ανυπόμονος όταν ο χρόνος τον πιέζει για να τελειώσει τις παράνομες ενέργειες του. Το αποτέλεσμα μπορεί να επαληθεύεται από τον υπολογισμό του ορίου του μέσου όρου της παρούσας αξίας όταν το δ, τείνει να είναι κοντά στο 1, δηλαδή, όταν οι παίκτες είναι υπομονετικοί.

$$\lim_{\delta \to 1} (17 - \delta) = 16 \qquad (3)$$

$$\lim_{\delta \to 1} (19 - 11 \cdot \delta) = 8 \qquad (4)$$

Προφανώς από τα (3) και (4), προκύπτουν οι συμπληρωματικοί τύποι για τον μέσο όρο της παρούσας αξίας και για τους δύο παίκτες, καθώς μας δίνουν τα τελικά αποτελέσματα από την στατική ΝΕ, όταν το δ τείνει στο 1.

3.6 ΙΣΧΥΡΑ ΚΑΙ ΑΔΥΝΑΜΑ ΣΗΜΕΙΑ ΤΩΝ IDSs

Παρόλο που τα IDSs θεωρούνται μία πολύτιμη προσθήκη στην πολιτική ασφάλειας ενός δικτύου, υπάρχουν κάποιες λειτουργίες τις οποίες εκτελούν ικανοποιητικά και άλλες για τις οποίες δεν θεωρούνται επαρκή. Σε καμία περίπτωση δεν πρέπει να ανατίθεται σε ένα IDS να εκτελέσει λειτουργίες, τις οποίες εκτελούν άλλοι τύποι μηχανισμών ασφάλειας, πιο ολοκληρωμένα και πιο αποδοτικά. Μερικές από τις λειτουργίες που επιτελούνται με επιτυχία από τα IDSs είναι :

- Η παρακολούθηση και η ανάλυση των δραστηριοτήτων σε ένα σύστημα και της συμπεριφοράς των χρηστών.
- Μοντελοποίηση της φυσιολογικής, συνήθους δραστηριότητας ενός συστήματος ή ενός δικτύου και στην συνέχεια παρακολούθηση για διακυμάνσεις και αλλαγές που μπορεί να προκύψουν στη δραστηριότητα αυτή.
- Αναγνώριση των συμβάντων που αντιστοιχούν σε μία γνωστή επίθεση.
- Ειδοποίηση των αρμόδιων υπευθύνων, με το κατάλληλο τρόπο, όταν εντοπιστεί μία επίθεση.
- Επιτρέπουν σε άτομα που δεν θεωρούνται ειδικοί σε θέματα ασφάλειας δικτύων, να εκτελούν σημαντικές λειτουργίες παρακολούθησης του δικτύου για πιθανές επιθέσεις.

Μερικές από τις λειτουργίες που τα IDSs δεν μπορούν να εκτελέσουν ικανοποιητικά είναι :

- Να αναπληρώσουν άλλους, ανύπαρκτους ή κακώς ρυθμισμένους μηχανισμούς ασφάλειας. Τέτοιοι μπορεί να είναι firewalls, μηχανισμοί αυθεντικοποίησης και ταυτοποίησης, μηχανισμοί ελέγχου πρόσβασης, ανίχνευση και αντιμετώπιση ιών, κρυπτογραφημένη διασύνδεση μεταξύ συστημάτων.
- Άμεσα να ανιχνεύσουν, να ειδοποιήσουν και να αντιδράσουν σε μία επίθεση, σε μεγάλα δίκτυα με πολύ αυξημένο traffic ή σε συστήματα με λίγους ελεύθερους πόρους.
- Να ανιχνεύσουν νέα είδη επιθέσεων ή παραλλαγές παλαιοτέρων.

- Να δράσουν αποτελεσματικά σε επιθέσεις που υλοποιούνται από εξειδικευμένους και έμπειρους επιτιθέμενους και ειδικά στην περίπτωση που αυτοί έχουν αντιληφθεί την ύπαρξή τους και γνωρίζουν τρόπους να τα παρακάμψουν.
- Αυτοματοποιημένα να ερευνήσουν και να αναλύσουν μία επίθεση, χωρίς την ανθρώπινη συμμετοχή.
- Παρουσιάζουν πρόβλημα σε δίκτυα που διασυνδέονται με switches, καθώς αυτά δεν τους επιτρέπουν να έχουν παθητικά πρόσβαση σε όλο το traffic του δικτύου.
- Παρουσιάζουν συμπτώματα από *False Positives* και *False Negatives,* ιδιαίτερα στην περίπτωση που δεν έχουν ρυθμιστεί σωστά, και αυτό είναι κάτι που μειώνει την αξιοπιστία τους.

3.7 ΠΡΑΚΤΙΚΗ ΧΡΗΣΗΣ ΤΩΝ IDSs

Ο τρόπος με τον οποίο ένας οργανισμός θα σχεδιάσει την στρατηγική χρήσης και υλοποίησης IDSs, ώστε να προστατέψει αποτελεσματικά το δίκτυό του και κατ' επέκταση τα συστήματα που συνδέονται σε αυτό και τις πληροφορίες που περιέχουν, έχει άμεση σχέση με την τοπολογία του δικτύου και το είδος της πληροφορίας που πρέπει να διαφυλαχτεί. Σε κάθε περίπτωση οι εφαρμογές IDSs, για να καλύψουν με επιτυχία τις ανάγκες για προστασία ενός δικτύου, απαιτείται μελέτη και σχεδιασμός, καθώς και εξειδικευμένο προσωπικό, ώστε να διαχειρίζεται και να επιβλέπει συνεχώς την λειτουργία τους και να δρα αποτελεσματικά και υπεύθυνα στην περίπτωση εμφάνισης μίας επίθεσης.
Στις περισσότερες περιπτώσεις η πιο αποδοτική και προτεινόμενη πρακτική για την πληρέστερη προστασία ενός μεγάλου δικτύου, είναι η χρήση NIDSs και HIDSs σε συνδυασμό μεταξύ τους.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα τελευταία χρόνια με την ραγδαία ανάπτυξη του Internet, παρατηρείται και το φαινόμενο της αύξησης των επιθέσεων, που έχουν στόχο τα δικτυωμένα συστήματα που το αποτελούν. Το γεγονός αυτό οδήγησε στην ανάγκη παρακολούθησης και ανάλυσης των επιθέσεων αυτών, με σκοπό την έγκαιρη ανίχνευσή και αποτελεσματική αντιμετώπιση τους. Καθώς οι ήδη υπάρχοντες μηχανισμοί ασφάλειας δεν φαίνεται να επαρκούν για τον σκοπό αυτό, προέκυψε η εμφάνιση των *Intrusion Detection Systems,* τα οποία πλέον θεωρούνται μία απαραίτητη προσθήκη στην πολιτική ασφάλειας κάθε δικτύου και κατέχουν ένα πρωταγωνιστικό ρόλο στην προστασία από δικτυακές επιθέσεις παρόλο που τα IDSs δεν αποτελούν μία ολοκληρωμένη λύση για την πλήρη προστασία ενός δικτύου, ο συνδυασμός των αποτελεσμάτων τους με τα αποτελέσματα των κλασσικών μηχανισμών ασφάλειας, όπως τα Firewalls, μπορεί να οδηγήσει στον σχηματισμό μιας πιο ολοκληρωμένης εικόνας των κινδύνων που προκύπτουν από διάφορες δικτυακές απειλές και να συντελέσει στον σχεδιασμό πιο αποτελεσματικών μέτρων ασφάλειας ενός δικτύου.
Τα IDSs βρίσκονται υπό συνεχή εξέλιξη που κυρίως έχει να κάνει με την βελτίωση της αποδοτικότητάς τους και την εξάλειψη των συμπτωμάτων από *False Positives* και *False Negatives* που παρουσιάζουν. Κάθε IDS υλοποιεί τρεις θεμελιώδεις λειτουργίες, που έχουν να κάνουν με τις *Πηγές της Πληροφορίας* από τις οποίες συλλέγει τα γεγονότα που θα εξετάσει για την ανίχνευση μίας επίθεσης, τις *Τεχνικές Ανάλυσης* που χρησιμοποιεί για να εξετάσει τα γεγονότα αυτά και τον τρόπο που αντιδρά (*Responses*) όταν ανιχνεύσει μία πιθανή επίθεση. Η κατηγοριοποίηση των IDSs προκύπτει από τον διαχωρισμό τους, σύμφωνα με τον τρόπο που το κάθε ένα προσεγγίζει τις παραπάνω λειτουργίες. Τα IDSs που κυρίως χρησιμοποιούνται σήμερα, είναι αυτά που λειτουργούν σε επίπεδο δικτύου (NIDS) και χρησιμοποιούν για την ανάλυση των γεγονότων που εξετάζουν την τεχνική του *Misuse Detection*, η οποία συνήθως συνδυάζεται κατά κύριο λόγο με την τεχνική του *Protocol Anomaly Detection* και ίσως με κάποια αποτελέσματα της *Anomaly Detection*.

Το γενικό μοντέλο παιγνίου στον τομέα του Intrusion Detection του δικτύου ασφαλείας έχει κατασκευαστεί, παρουσιαστεί και εξεταστεί ενδελεχώς. Το παίγνιο έχει απεικονιστεί ως μια εκτεταμένη μορφή, και έχουν εντοπιστεί μέρη αυτών των επαναλαμβανόμενων διασπάσεων. Αποτελείται από διαδοχικές και ταυτόχρονες κινήσεις, και ακολουθεί κανόνες που διασφαλίζουν την εκτεταμένη μορφή του παιγνίου, και εγγυάται μια λύση του. Στη συνέχεια, αποδεικνύεται και εξηγείται ότι το στιγμιότυπο αυτού της γενικού μοντέλου παιγνίου έχει απομονωθεί και είναι ένα παίγνιο μεταξύ του εσωτερικού εισβολέα και του IDS. Επιλύσαμε πρώτα, το παίγνιο ως στατικό και ύστερα, ως ένα απείρως επαναλαμβανόμενο παίγνιο. Τα αποτελέσματα δείχνουν τις δυνατότητες της εφαρμογής ενός τέτοιου πλαισίου μέσα στο οποίο το IDS και ο χρήστης θα αλληλεπιδρούν με ασφαλή τρόπο για τη διαφύλαξη των συμφερόντων τους. Στο μέλλον, μια προσομοίωση του προτεινόμενου μοντέλου θα πρέπει να δημιουργηθεί για να διευκολύνει τη βελτιστοποίησή του καθώς και να επεκτείνει την προτεινόμενη προσέγγιση για την κάλυψη όσο το δυνατόν περισσότερο περιπτώσεων.

REFERNCES

1. Denning, P.: Is Computer Science Science? Communication of the ACM 48(4), 27–31 (2005)

2. Skyrms, B., Vanderschraaf, P.: Game theory. In: Gabbay, D.M., Smets, P. (eds.) Handbook of Defeasible Reasoning and Uncertainty Management Systems, pp. 391–439. Kluwer Academic Publishers, Dordrecht (1998)

3. Ho, Y., Zhao, Q., Pepyne, D.: The No Free Lunch Theorems: Complexity and Security. IEEE Transactions on Automatic Control 48(5), 783–793 (2003)

4. Cavusoglu, H., Raghunathan, S.: Configuration of Intrusion Detection System: A Comparison of Decision and Game Theoretic Approaches. In: Proc. of the 24th International Conference on Information Systems, pp. 692–705 (December 2003)

5. Alpcan, T., Basar, T.: A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection. In: Proc. of the 42rd IEEE Conference on Decision and Control (CDC), Maki, HI, pp. 2595–2600 (December 2003)

6. Alpcan, T., Basar, T.: A Game Theoretic Analysis of Intrusion Detection in Access Control Systems. In: Proc. of the 43rd IEEE Conference on Decision and Control (CDC), Paradise Island, Bahamas, pp. 1568–1573 (December 2004)

7. Lye, K., Wing, J.: Game Strategies in Network Security. In: Proc. of the Foundations of Computer Security Workshop, Copenhagen, Denmark (July 2003)

8. Kodialam, M., Lakshman, T.: Detecting Network Intrusions via Sampling: A Game Theoretic Approach. In: Proc. of the IEEE INFOCOM 2003, San Fransisco (March 2003)

9. Patcha, A., Park, J.: A Game Theoretic Approach to Modeling Intrusion Detection in Mobile Ad Hoc Networks. In: Proc. of the 2004 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, pp. 280–284 (June 2004)

10. Patcha, A., Park, J.: A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks. International Journal of Network Security 2(2), 131–137 (2006)

11. Agah, A., Das, S.K.: Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach. International Journal of Network Security 5(2), 145–153 (2007)

12. Kreps, D.: Game Theory and Economic Modelling. Oxford University Press, Oxford (2003)

13. Dixit, A., Skeath, S.: Games of Strategy. W. W. Norton & Company, Inc. (1999)

14. McKelvey, R.D., McLennan, A.M., Turocy, T.L.: Gambit: Software Tools for Game Theory, version 0.2007.01.30 (January 2007) (accessed May 20, 2008), http://gambit.sourceforge.net

15. Osborne, M.J.: An Introduction to Game Theory. Oxford University Press, New York (2004)

16. Levine, D.K.: Repeated Games Step-by-Step (May 2002) (accessed March 1, 2008), http://www.dklevine.com/econ101/repeated-step.pfd

17. Watching the Watchers: Intrusion Detection by Greg Shipley
http://www.networkcomputing.com/1122/1122f3.html

18. Network vs Host-based Intrusion Detection; A guide to Intrusion Detection Technology http://secinf.net/info/ids/nvh_ids/

19. Intrusion Detection: Challenges and myths by Marcus J. Ranum
http://secinf.net/info/ids/ids_mythe.html

20. State of the Practice of Intrusion Detection Technologies
http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028esum.html

21. Protect your network with an Intrusion Detection system, Gartner Research
http://www.techrepublic.com/article.jhtml?src=search&id=r00520010209ggr0

22. FAQ: Network Intrusion Detection Systems by Robert Graham
http://www.ticm.com/kb/faq/idsfaq.html

23. Limitations of Network Intrusion Detection by Steve Schupp
http://www.sans.org/infosecFAQ/intrusion/net_id.htm

24. [Anderson80] Anderson, J.P. “Computer Security Threat Monitoring and Surveillance.” Technical Report, James P. Anderson Co., Fort Washington, Pennsylvania, April 1980.

25. [Anderson93] Anderson, D. T. Lunt, H. Javitz, A. Tamaru, and A. Valdes. “Safeguard Final Report: Detecting Unusual Program Behavior Using the NIDES Statistical Component.” *SRI International Computer Science Laboratory Technical Report*, December 1993.

26. [Anderson95a] Anderson, D., T. Lunt, H. Javitz, A. Tamaru and A. Valdes. “Detecting Unusual Program Behavior Using the Statistical Component of the Next-generation Intrusion Detection Expert System (NIDES).” *SRI International Computer Science Laboratory Technical Report SRI-CSL-95-06*, May 1995.

27. [Anderson95b] Anderson, D., T. Frivold and A. Valdes. “Next-generation Intrusion Detection Expert System (NIDES): A Summary.” *SRI International Computer Science Laboratory Technical Report SRI-CSL-95-07*, May 1995.

28. [Cannady96] Cannady, J. and J. Harrell. “A Comparative Analysis of Current Intrusion Detection Technologies.” *4th Technology for Information Security Conference (TISC’96)*, May 1996.

29. [Combs98] Combs, Brownell. “The Pseudo-Internal Intruder; a new Access Oriented Intruder Category.” University of Virginia Technical Report, 1999.

30. [Cotrozzi93] Cotrozzi, M. and D. Vincenzetti. “ATP – Anti-Tampering Program.” *UNIX Security IV Symposium (USENIX)*, October 1993.

31. [Debar92] Debar, H., M. Becker and D. Siboni. “A Neural Network Component for and Intrusion Detection System.” *Proceedings of the IEEE Symposium on Research in Computer Security and Privacy*, 1992.

32. [Denning87] Denning, D. “An Intrusion Detection Model.” *IEEE Transactions on Software Engineering*, 13.2 (1987) 222.

33.[Farmer94] Farmer, D. and E. Spafford. “The COPS Security Checker Systems.” *Purdue Technical Report CSD-TR-993*, January 1994.

34. [Forrest94] Forrest, S., L. Allen, A.S. Perelson, and R. Cherukuri. “Self-Nonself Discrimination in a Computer.” *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy*, 1994.

35. [Garvey91] Garvey, T.D. and T.F. Lunt. “Model-Based Intrusion Detection.” *Proceedings of the 14th National Computer Security Conference*, October 1991.

36. [Hochberg93] Hochberg, J., K. Jackson, C.Stallings, J.F. McClary, D. DuBois, and J. Ford. “NADIR: An Automated System for Detecting Network Intrusion and Misuse.” *Computers and Security*, 12.3 (1993) 235-248, http://nadir.lanl.gov/libLA-UR-93-137.html.

37. [Hofmeyer97] Hofmeyer, S.A., S. Forrest, and A. Somayaji. “Intrusion Detection using Sequences of System Calls.” Revised: December 17, 1997. http://www.cs.unm.edu/~steveah/publications/ids.ps.gz.

38. [Ilgun93] Ilgun, K. “USTAT: A Real-Time Intrusion Detection System for UNIX.” *Proceedings*
of the IEEE Symposium on Research in Security and Privacy, May 1993.

39. A Generic Intrusion Detection Game Model in IT Security (Ioanna Kantzavelou and Sokratis Katsikas).

40.«Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων» (Τζικόπουλος Παναγιώτης)