

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

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



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ



**«Αποτύπωση Απαιτήσεων Ασφάλειας και Ιδιωτικότητας
Ad-hoc Δικτύων »**

Παπαγιαννακόπουλος Παναγιώτης

M3030027

ΑΘΗΝΑ, ΔΕΚΕΜΒΡΙΟΣ 2004



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

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ



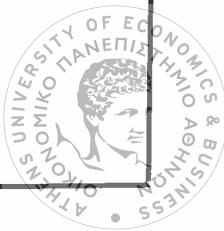
**«Αποτύπωση Απαιτήσεων Ασφάλειας και Ιδιωτικότητας
Ad-hoc Δικτύων»**

**Παπαγιαννακόπουλος Παναγιώτης
M3030027**

**Επιβλέπων Καθηγητής: Καθ. Δημήτρης Γκρίτζαλης
Εξωτερικός Κριτής: Λέκτ. Γεώργιος Ξυλωμένος**

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

ΑΘΗΝΑ, ΔΕΚΕΜΒΡΙΟΣ 2004



ΠΕΡΙΛΗΨΗ ΕΡΓΑΣΙΑΣ

Η ασφάλεια αποτελεί ένα από τα κυρίαρχα ζητήματα σε μεγάλα, αλλά και μικρά, υπολογιστικά συστήματα. Η πολυπλοκότητα των υπολογιστικών συστημάτων σε συνδυασμό με την αλληλεπίδρασή τους μέσω δικτύων και του Παγκόσμιου Ιστού, καθιστούν την ασφάλεια ένα κρίσιμο παράγοντα για τους σύγχρονους οργανισμούς. Παράλληλα η εξάπλωση των ad-hoc δικτύων, εισάγει νέες προκλήσεις στο κομμάτι τόσο της διαχείρισης όσο και της ασφάλειας αυτών. Επιπρόσθετα, το διαφορετικό επιστημονικό υπόβαθρο αλλά και η διαφορετική κουλτούρα που χαρακτηρίζει τους εμπλεκόμενους στο κομμάτι της ασφάλειας δημιουργούν καινοφανή προβλήματα στην διαχείριση ασφάλειας των δικτύων, που εντείνονται από την μεταβαλλόμενη φύση των εν λόγω δικτύων.

Σκοπός της διατριβής αυτής είναι η δημιουργία μίας μεθόδου που θα έχει σαν στόχο την τυπική αποτύπωση των απαιτήσεων ασφάλειας και ιδιωτικότητας των ad-hoc δικτύων. Επιπλέον η μέθοδος αυτή θα μπορεί να προσαρμόζεται συνεχώς στο μεταβαλλόμενο περιβάλλον τους και θα μπορεί με σαφήνεια και χωρίς παρερμηνείες να αποτυπώνει τις απαιτήσεις ασφάλειας.

Η μέθοδος αποτελείται από δύο βασικά στάδια. Πρώτο στάδιο αποτελεί η δημιουργία μίας οντολογίας ασφάλειας. Μέσω αυτής είναι δυνατή η τυπική απεικόνιση όλων των απαραίτητων πληροφοριών/εννοιών με ενιαίο τρόπο. Επόμενο στάδιο αποτελεί η εξαγωγή της γνώσης από διάφορες πηγές πληροφόρησης και η πλήρωση της οντολογίας βάση των πηγών αυτών. Αρχικά μέσω εργαλείων τοπολογικής αναγνώρισης, εντοπίζονται τα αγαθά του δικτύου. Στη συνέχεια από τις πολιτικές ασφάλειας που έχουν προκύψει από αναλύσεις επικινδυνότητας, εξάγεται πληροφορία που αφορά στα αντίμετρα που πρέπει να εφαρμοστούν στο εκάστοτε αγαθό. Η εξαγωγή της γνώσης επιτυγχάνεται μέσω τεχνικών επεξεργασίας φυσικής γλώσσας.

Τα εργαλεία που χρησιμοποιήθηκαν για την ανάπτυξη της μεθόδου είναι το GATE (General Architecture for Text Engineering) και το Protégé. Το πρώτο αποτελεί περιβάλλον επεξεργασίας φυσικής γλώσσας. Παρέχει γραφική διεπαφή, γεγονός που το καθιστά εύκολο στην χρήση του. Είσοδος του προγράμματος αποτελούν λεκτικές οντότητες όπως κείμενα, λεξικά, οντολογίες και έξοδος αυτού

είναι οι οντότητες που ενδιαφέρουν την εκάστοτε εκτέλεση όπως για παράδειγμα τοποθεσίες, άτομα, οργανισμοί κ.α. Το Protégé αποτελεί περιβάλλον διαχείρισης οντολογιών. Το τελευταίο παρέχει ένα εύχρηστο γραφικό περιβάλλον διαχείρισης οντολογιών. Τέλος και τα δύο λογισμικά παρέχουν προγραμματιστική διεπαφή (Java API) μέσω της οποία είναι εφικτή η δημιουργία αυτόνομων εφαρμογών τόσο στο κομμάτι της διαχείρισης της γνώσης ενός πεδίου όσο και στην εξαγωγή αυτής.

ABSTRACT

Security has become a very important aspect in all kinds of information systems regarding the size of them. The complexity of these information systems in combination with their interaction via networks and World Web, render their security a crucial factor for the successful operation of modern organisations. At the same time, the wide adoption of ad-hoc networks arises new challenges both in managing security and security itself. In addition, the different scientific background and culture that characterizes people who are involved in the security of IS, create new and sometimes complex problems which are intensified by the altered nature of networks in question.

Aim of this thesis is the creation and presentation of a new method that will imprint all the security and privacy requirements of ad-hoc networks in a formal way. Moreover, this method has the ability to be adapted continuously in ad-hoc networks' altered environment and it imprints with clarity and without misinterpretations the security requirements.

This method is constituted by two basic stages. The first stage involves the creation of a security ontology. The latter will act as a container for the formal representation of all security concepts. The next stage involves the information extraction from several sources and the fulfillment of the security ontology with the concepts recognized by the information extraction method. Initially, the assets of the network are mapped, via software that recognizes a network's topology. Secondly, information is being extracted from the high level security policies (resulted from risk analysis methods). The above information concerns the security countermeasures for each asset that has been mapped previously. Information extraction is feasible through natural language processing techniques.

The tools, utilized for the development of the method described above, are GATE (General Architecture for Text Engineering) and Protégé. The first one is a tool or framework for natural language processing. It provides a graphical user interface that facilitates its use. The input of this software is verbal entities such as text, lexicons, ontologies and other. The output is a set of entities that describe concepts like places, organizations, individuals or others that the user might define

during the processing of the verbal entities. Protégé is a mean for creating and managing ontologies. It also provides a graphical user interface for the ease of use. Finally, both programs mentioned above provide an application programming interface (JAVA API) which makes feasible the creation of autonomous application in the fields of knowledge management and natural language processing.

Πίνακας Περιεχομένων

1. ΕΙΣΑΓΩΓΗ	9
1.1. ΑΠΟΤΥΠΩΣΗ ΑΠΑΙΤΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	9
1.1.1. Γιατί απαιτείται η τυπική αποτύπωση ασφάλειας και ιδιωτικότητας .	9
1.1.2. Επισκόπηση Υπαρχόντων Προσεγγίσεων	11
1.1.3. Χαρακτηριστικά και ιδιαιτερότητες ad-hoc δικτύων.....	15
1.1.4. Ανάγκη Υπαρξης Νέας Προσέγγισης και Συμβάσεις Αυτής	17
1.1.4.1. Συμβάσεις για τα δεδομένα εισόδου.....	18
1.1.4.2. Συμβάσεις για την επεξεργασία των δεδομένων εισόδου	19
1.2. ΒΑΣΙΚΕΣ ΈΝΝΟΙΕΣ	21
1.2.1. Οντολογίες.....	21
1.2.2. Τεχνικές αποτύπωσης οντολογιών.....	25
1.2.3. Επεξεργασία Φυσικής Γλώσσας (NLP) και Εξαγωγή Πληροφοριών (IE)	29
2. ΜΕΘΟΔΟΛΟΓΙΑ ΠΡΟΣΕΓΓΙΣΗΣ	32
2.1. ΕΝΝΟΙΟΛΟΓΙΚΟ ΜΟΝΤΕΛΟ	32
2.2. ΟΡΙΣΜΟΣ ΜΟΝΤΕΛΟΥ ΟΝΤΟΛΟΓΙΑΣ ΑΣΦΑΛΕΙΑΣ	35
2.2.1. Οντολογία Ασφάλειας	35
2.2.2. Λεξιλόγιο Πεδίου Ορισμού Ασφάλειας	47
2.2.3. Αποτύπωση Σχέσεων μεταξύ των Εννοιών.....	57
2.3. ΠΑΡΟΥΣΙΑΣΗ ΜΕΘΟΔΟΥ ΤΥΠΙΚΗΣ ΑΠΟΤΥΠΩΣΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΑΠΑΙΤΗΣΕΩΝ ΑΣΦΑΛΕΙΑΣ AD-HOC ΔΙΚΤΥΩΝ	59
2.4. ΕΡΓΑΛΕΙΑ	66
2.4.1. Επεξεργαστής οντολογιών Protégé.....	68
2.4.2. Εξαγωγή Πληροφοριών, Gate	71
3. ΕΦΑΡΜΟΓΗ ΚΑΙ ΑΞΙΟΛΟΓΗΣΗ ΜΕΘΟΔΟΥ	76
3.1. ΕΦΑΡΜΟΓΗ ΜΕΘΟΔΟΥ	76
3.1.1. Παρουσίαση Στοιχείων Εισόδου	76
3.1.2. Επεξεργασία εισόδου με την βοήθεια του GATE	81
3.1.3. Προσδιορισμός Απαιτήσεων Ασφάλειας βάσει των αποτελεσμάτων του GATE και της οντολογίας στο Protégé.....	85
3.2. ΑΞΙΟΛΟΓΗΣΗ ΑΠΟΤΕΛΕΣΜΑΤΩΝ	91
3.2.1. Σύγκριση αποτελεσμάτων με τα επιθυμητά αποτελέσματα.....	91
3.2.2. Κριτική επισκόπηση των αποτελεσμάτων της τυπικής αποτύπωσης	96
4. ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΈΡΕΥΝΑ	99
5. ΒΙΒΛΙΟΓΡΑΦΙΑ	101
6. ΠΑΡΑΡΤΗΜΑΤΑ	106
6.1. GATE.....	106
6.2. ΠΑΡΑΘΕΣΗ ΠΗΓΑΙΟΥ ΚΩΔΙΚΑ JAVA	112
6.3. PROTEGE – ΟΝΤΟΛΟΓΙΑ ΑΣΦΑΛΕΙΑΣ	124



Ευρετήριο Εικόνων

Εικόνα 1 : Παράδειγμα εφαρμογής οντολογίας	24
Εικόνα 2 : Εννοιολογικό Πλαίσιο Μεθοδολογίας	34
Εικόνα 3 : Αναπαράσταση του μοντέλου CIM	37
Εικόνα 4 : CIM Meta Schema	38
Εικόνα 5 : Βασικές θεματικές ενότητες του Core Model	39
Εικόνα 6 : Plan-Do-Check-Act Model (PDCA)	43
Εικόνα 7 : Αρχικό Μοντέλο Οντολογίας Ασφάλειας	44
Εικόνα 8 : Εκλεπτυσμένο Μοντέλο	45
Εικόνα 9 : Τελικό Μοντέλο Risk Assessment	46
Εικόνα 10 : Υπομοντέλο Asset	48
Εικόνα 11 : Computer Equipment	49
Εικόνα 12 : Network Equipment	51
Εικόνα 13 : Software	52
Εικόνα 14 : Countermeasure (Security Countermeasure)	55
Εικόνα 15 : Απειλή (Threat)	56
Εικόνα 16 : Εννοιολογικό Μοντέλο	60
Εικόνα 17 : Τελικό μοντέλο Risk Assesment	63
Εικόνα 18 : Περιγραφή Γνωρίσματος Threats[]	64
Εικόνα 19 : Επίπεδα τυπικής αποτύπωσης γνώσης	66
Εικόνα 20 : Κατηγοριοποίηση τεχνικών αποτύπωσης γνώσης	67
Εικόνα 21 : Protege, επεξεργαστής οντολογιών	70
Εικόνα 22 : Γραφική απεικόνιση της οντολογίας ασφάλειας	80
Εικόνα 23 : Εμφάνιση αποτελεσμάτων CM_Group	86
Εικόνα 24 : Εμφάνιση αποτελεσμάτων Target	87
Εικόνα 25 : Εμφάνιση αποτελεσμάτων Pattern	88

1. Εισαγωγή

1.1. Αποτύπωση απαιτήσεων ασφάλειας και ιδιωτικότητας

1.1.1. Γιατί απαιτείται η τυπική αποτύπωση ασφάλειας και ιδιωτικότητας

Η έννοια της ασφάλειας αποτελεί πλέον ένα από τα κυρίαρχα ζητήματα σε μεγάλα, αλλά και μικρά, υπολογιστικά συστήματα. Όπως και με τους υπόλοιπους κλάδους της επιστήμης, έτσι και με την επιστήμη των υπολογιστών, επίβουλοι ευνοούνται των τεράστιων δυνατοτήτων των υπολογιστών για κακόβουλα έργα. Οι κίνδυνοι που ελλοχεύουν είναι ποικίλοι και σε συνδυασμό με το γεγονός ότι τα συστήματα γίνονται όλο και πιο πολύπλοκα, καθιστούν το κομμάτι της ασφάλειας ακόμα πιο δύσκολο. Παράλληλα η αλληλεπίδραση μεταξύ των υπολογιστικών συστημάτων μέσω δικτύων (είτε τοπικών και ενδο-εταιρικών είτε μέσω του Παγκόσμιου Ιστού) εισάγουν επιπλέον προβλήματα προς επίλυση.

Μία μικρή σε μέγεθος επιχείρηση ή ένας απλός χρήστης των υπολογιστών μπορούν με βασικές διαδικασίες να ασφαλίσουν το υπολογιστικό τους σύστημα ικανοποιητικά. Αντίθετα, τα πληροφοριακά συστήματα μεγάλων εταιριών απαιτούν πολύπλοκες μεθόδους λόγω της υψηλής τους πολυπλοκότητας. Ταυτόχρονα απαιτούν λύσεις οι οποίες θα είναι ευέλικτες και ευπροσάρμοστες σε διαδικασίες διαχείρισης (management). Είναι απαραίτητο να μπορεί δυναμικά να προσαρμόζεται η πολιτική ασφάλειας στις καινούργιες ανάγκες και στους καινούργιους κινδύνους που μπορεί να παρουσιαστούν, χωρίς δηλαδή να απαιτείται η διακοπή της λειτουργίας του πληροφοριακού συστήματος για την εφαρμογή των νέων πολιτικών ασφαλείας.

Ταυτόχρονα η είσοδος τεχνολογιών που επιτρέπουν την αλλαγή τοπολογίας ενός δικτύου σε πραγματικό χρόνο, δυσκολεύουν το έργο των υπεύθυνων ασφαλείας. Ασύρματα δίκτυα που αλλάζουν συνεχώς «όψεις» απαιτούν λύσεις και πολιτικές ασφάλειας οι οποίες θα είναι ευέλικτες έτσι ώστε να προσαρμόζονται εύκολα στις ανάγκες τους εκάστοτε δικτύου.

Επιπλέον, ένα από τα σημαντικότερα προβλήματα που υπάρχουν στο τομέα της ασφάλειας των υπολογιστικών αλλά και πληροφοριακών συστημάτων είναι το διαφορετικό γνωστικό υπόβαθρο που υπάρχει μεταξύ των εμπλεκομένων στον τομέα αυτό. Συχνά είναι τα φαινόμενα κατά τα οποία η ίδια λέξη γίνεται κατανοητή με διαφορετικό τρόπο από διαφορετικά άτομα. Αν φανταστούμε έναν μικρό οργανισμό

τότε το πρόβλημα αυτό είναι μηδαμινό μιας και οι εμπλεκόμενοι στον τομέα της ασφάλειας είναι λίγοι (Τις περισσότερες φορές μόνο ένας). Σε περιπτώσεις όμως όπου πολλά άτομα συνεργάζονται στον τομέα αυτό το πρόβλημα αποτελεί τροχοπέδη για την επίτευξη του τελικού στόχου, της ικανοποιητικής εξασφάλισης του εκάστοτε πληροφοριακού συστήματος.

Για να γίνει πιο κατανοητό το πρόβλημα παραθέτουμε το εξής παράδειγμα. Οι λέξεις security, safety, insurance, assurance, police, fuse μεταφράζονται στα ελληνικά με την λέξη ασφάλεια. Είναι όμως σαφές ότι η ερμηνεία αυτών των λέξεων είναι διαφορετική για κάποιον του οποίου η μητρική γλώσσα είναι τα αγγλικά. Επιπλέον αν θελήσουμε να ορίσουμε την έννοια της ασφάλειας θα διαπιστώσουμε ότι και εκεί υπάρχουν διαφορετικοί ορισμοί. Το αγγλικό διάσημο λεξικό Oxford [4] προσδίδει στην έννοια ασφάλεια τον εξής ορισμό : *Freedom of danger or anxiety*. Το ελληνικό λεξικό του καθηγητή κ.Μπαμπινιώτη [3] ορίζει την ασφάλεια ως *η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου αισθάνεται κανείς ότι δεν απειλείται αλλά και ως η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας*. Τέλος ένα ακόμη παράδειγμα είναι οι έννοιες δεδομένα και πληροφορία, οι οποίες συγχέονται συχνά. Με τον όρο δεδομένα εννοούμε ένα σύνολο από σύμβολα τα οποία έχουν καταγραφεί. Με τον όρο πληροφορία εννοούμε τα δεδομένα τα οποία συνοδεύονται από την σημασία (έννοιά) τους. Είναι λοιπόν προφανές ότι στην πολύ γενική φράση «*Τα δεδομένα της εταιρείας πρέπει να προστατευτούν*», οι ερμηνείες που μπορούν να αποδοθούν είναι πολλές.

Για όλους τους παραπάνω λόγους, κρίνεται αναγκαία η τυπική αποτύπωση των απαιτήσεων ασφάλειας και ιδιωτικότητας. Με τον τρόπο αυτό ασάφειες που οφείλονται σε παρερμηνείες όρων αλλά και σε διαφορές σχετικά με το γνωστικό υπόβαθρο των εμπλεκομένων στο κομμάτι της ασφάλειας θα μπορέσουν να εκλείψουν. Η παροχή μίας κοινής γλώσσας για τη συζήτηση των ζητημάτων ασφάλειας πληροφοριών αποτελεί βασική προϋπόθεση για μία επιτυχημένη προσπάθεια «ασφάλισης»¹ ενός πληροφοριακού συστήματος. Η εννοιολογική θεμελίωση των όρων αποτελεί βασικό συστατικό της επιτυχίας.

¹ Ο όρος ασφάλιση τοποθετήθηκε σκοπίμως σε εισαγωγικά. Μιας και ο όρος δεν έχει αποτυπωθεί τυπικά, ο εκάστοτε αναγνώστης τον αντιλαμβάνεται με διαφορετικό τρόπο.

1.1.2. Επισκόπηση Υπαρχόντων Προσεγγίσεων

Τα τελευταία χρόνια έχει δοθεί ιδιαίτερο βάρος στα διαχείριση της ασφάλειας. Η τυπική αποτύπωση των απαιτήσεων ασφάλειας αποτελεί μείζον θέμα, ιδίως στην περίοδο της συνεχούς αυξανόμενης κλίμακας τόσο των ενδο-εταιρικών δικτύων όσο και του Παγκόσμιου Ιστού γενικότερα. Παρόλα αυτά, μπορεί να διαπιστώσει κανείς ότι υπάρχει σχετικά μικρή πρόοδος στον τομέα αυτό, είτε λόγω της ιδιαιτερότητας του έργου, είτε διότι η έννοια της ασφάλειας δεν αποτελεί πρωτεύον ζήτημα για πολλές εταιρίες και οργανισμούς. Στην παράγραφο αυτή παρουσιάζονται μερικές από τις σημαντικότερες προσπάθειες στον τομέα αυτό.

Μία από τις κυριότερες ωθήσεις στο χώρο αποτελεί η προσπάθεια για προτυποποίηση που έγινε από το IETF Policy Group (<http://www.ietf.org/html.charters/ipsecp-charter.html>)². Η ομάδα αυτή θεώρησε την διαχείριση της πολιτικής ασφάλειας ως μία ακόμα service-oriented εργασία. Έτσι ένας πελάτης (για παράδειγμα ένας router) κάνει μία αίτηση για κανόνες πολιτικής ασφάλειας σε ένα κεντρικό server, ο οποίος με την σειρά του παίρνει τα αντικείμενα που του έστειλε ο πελάτης, τα διερμηνεύει και αποστέλλει αποφάσεις εφαρμογής πολιτικών ασφάλειας για τα συγκεκριμένα αντικείμενα. Για παράδειγμα ο router δεν ξέρει αν πρέπει να επιτρέπει την εγκαθίδρυση συνδέσεων τύπου ftp ή όχι. Αποστέλλει λοιπόν μία αίτηση στον server και εκείνος βάση του μοντέλου που έχει δημιουργηθεί απαντά αν μπορεί ή όχι να δημιουργήσει τέτοιου τύπου συνδέσεις. Η IETF ορίζει ένα policy framework το οποίο μπορεί να χρησιμοποιηθεί για ιεράρχηση των ροών των πακέτων και για εξουσιοδότηση (authorization) χρήστης υπηρεσιών και «αγαθών» του δικτύου.

Στο [23], παρουσιάζεται μία μέθοδος η οποία προτείνει την δημιουργία μίας γλώσσας ημι-τυπικής αποτύπωσης των απαιτήσεων ασφάλειας και ονομάζεται Ponder. Η γλώσσα Ponder περιέχει δομές με στόχο την περιγραφή των ακόλουθων βασικών τύπων πολιτικής ασφάλειας (policy types) :

- Authorization Policies, οι οποίες ορίζουν επιτρεπτές πράξεις και χρησιμοποιούνται για να προσδιορίσουν το access control.
- Event-triggered Obligation Policies, οι οποίες ορίζουν ενέργειες που πρέπει να γίνουν από πράκτορες διαχείρισης (manager agents). Πρόκειται για κανόνες

² Το group αυτό δεν υπάρχει πλέον. Πλέον η πλησιέστερη ομάδα που εργάζεται στον τομέα αυτό είναι το IP Security Policy Group, από όπου και το link που αναφέρουμε.

που ενεργοποιούνται μόλις λάβει χώρα ένα γεγονός, για παράδειγμα μία παραβίαση του δικτύου. Τότε, ενεργοποιούνται οι manager agents όπου θέτουν σε εφαρμογή τις συγκεκριμένες πολιτικές ασφάλειας.

- Refrain Policies, οι οποίες ορίζουν ενέργειες που τα υποκείμενα του δικτύου πρέπει να αποφεύγουν ή δεν επιτρέπεται να κάνουν. Για παράδειγμα, δεν πρέπει κανένας χρήστης να «ανοίξει» τις πόρτες 20 και 21 (FTP data port και flow control port αντίστοιχα) στον υπολογιστή του.
- Delegation Policies, οι οποίες αφορούν σε μεταβίβαση αρμοδιοτήτων από ένα χρήστη/υπολογιστή σε άλλο. Για παράδειγμα δικαίωμα εγγραφής σε ένα αρχείο από ένα υψηλόβαθμο στέλεχος σε ένα χαμηλότερου βαθμού.

Για την δημιουργία των κανόνων που θα αποτυπώνουν την πολιτική ασφάλειας τυπικά έχουν οριστεί κάποιες δομές δεδομένων. Αυτές είναι τα Groups, τα οποία αποτελούν ένα σύνολο από αντικείμενα στα οποία εφαρμόζεται μία κοινή πολιτική ασφάλειας, για παράδειγμα όλοι οι τελικοί υπολογιστές (hosts), οι Roles, οι οποίοι ορίζουν ένα group από policies που αφορά σε κοινές θέσεις στο εργασιακό περιβάλλον, για παράδειγμα ο ρόλος του προγραμματιστή που αναφέρεται σε όλους τους προγραμματιστές μίας εταιρίας, τα Relationships που ορίζουν ένα group από policies που αναφέρεται στις σχέσεις μεταξύ των αντικειμένων και των υποκειμένων του δικτύου και τέλος τα Constraints τα οποία αφορούν σε τυχόν περιορισμούς που υπάρχουν στην εφαρμογή των κανόνων της πολιτικής ασφάλειας. Ένα μικρό παράδειγμα κανόνα (για αναλυτικότερη παρουσίαση της μεθόδου βλέπε [24], [25], [26]) είναι το ακόλουθο :

```
type auth+ profileAccessT(subject administrators, target<userProfile> users) {
    action modify(), remove();}
```

Το συγκεκριμένο παράδειγμα μίας authorization policy που ονομάζεται profileAccessT και ορίζει ότι οι administrators (ένα group) μπορούν (σύμβολο +) να αλλάξουν (modify()) και να αφαιρέσουν (remove()) αντικείμενα τύπου userProfile που ανήκουν στο group των users.

Αντίστοιχη πρόταση αποτελεί το [33]. Στην συγκεκριμένη μέθοδο χρησιμοποιήθηκε η τυπική γλώσσα Event Calculus [34], με την μορφή που αυτή παρουσιάστηκε στο [35], σε συνδυασμό με την μέθοδο KAOS. Στην συγκεκριμένη μορφή το Event Calculus, αποτελείται από i) ένα set από σημεία χρόνου (time points), ii) ένα set από ιδιότητες που μπορούν να αλλάξουν τιμή με την πάροδο του χρόνου και



ονομάζονται fluents και iii) ένα set από κατηγορίες γεγονότων (event types). Το KAOS αποτελεί μέθοδο εκλέπτυνσης ασαφών και αφηρημένων στόχων σε ποιο ειδικούς και καλά ορισμένους. Χρησιμοποιώντας το KAOS προσδιορίζονται σαφείς στόχοι, οι οποίοι στην συνέχεια εκφράζονται τυπικά με την βοήθεια του Event Calculus.

Μία ακόμη προσπάθεια προς την κατεύθυνση της τυπικής αποτύπωσης απαιτήσεων ασφάλειας είναι αυτή των Moffet και Sloman [27][28]. Οι τελευταίοι προσδιορίζουν την εξάλειψη των ασαφειών της φυσικής γλώσσας και την εύρεση των κύριων εννοιών που ενδιαφέρουν τον χρήστη, ως τις κυριότερες προκλήσεις στον τομέα του policy refinement (διώλιση, εκλέπτυνση). Με τον όρο Policy refinement εννοούμε την διαδικασία μετατροπής των high-level policies σε low-level policies. Η διαδικασία αυτή περιλαμβάνει τρία στάδια :

- Προσδιορισμός των πόρων που απαιτούνται για να ικανοποιήσουν τα requirements των policies.
- Μετάφραση των high-level policies σε operational-level, τέτοιες που να μπορεί το σύστημα να εφαρμόσει (χωρίς ασάφειες)
- Επαλήθευση ότι οι απαιτήσεις που προέκυψαν από το βήμα δύο ταυτίζονται με τις απαιτήσεις που περιγράφονται στα high-level policies.

Δημιούργησαν έτσι μία μέθοδο βασισμένη σε Prolog η οποία μετατρέπει τις υψηλού επιπέδου πολιτικές (high-level policies) σε χαμηλού επιπέδου (low-level), ικανά για εφαρμογή από ένα υπολογιστικό σύστημα. Βέβαια, όπως τονίζουν, σε οποιαδήποτε μέθοδο απαιτείται και ανθρώπινη παρέμβαση για σωστά αποτελέσματα.

Μία ακόμα προσέγγιση στον τομέα της τυπικής αποτύπωσης των απαιτήσεων ασφάλειας είναι το NLIPT tool. Οι ερευνητική ομάδα στο [29] δημιούργησαν ένα πρωτότυπο εργαλείο το οποίο επεξεργάζεται κείμενα σε φυσική γλώσσα και προσπαθεί να εξάγει πληροφορίες που αφορούν στο θέμα, στα αντικείμενα που περιλαμβάνει και στις ενέργειες που προβλέπει ένα αντίμετρο (security countermeasure).

Ο Ortalo [30], περιγράφει μία γλώσσα για να εκφράσει τις πολιτικές ασφάλειας στα πληροφοριακά συστήματα, η οποία στηρίζεται στην λογική των “permissions and obligation” (επιτρεπτές ενέργειες και υποχρεώσεων). Η λογική αυτή ονομάζεται deontic logic. Το βασικό αξίωμα της συγκεκριμένης προσέγγισης είναι ο κανόνας



$$Pp = \neg O \neg p$$

δηλαδή “Permitted p is equivalent to not p obliged”. Η προσέγγιση αυτή δεν είναι κατάλληλη για την για την μοντελοποίηση των obligation policies και authorization policies. Ενίσχυση της παραπάνω άποψης αποτελεί και το [31], στο οποία αναφέρονται αρκετά παράδοξα της παραπάνω θεωρίας.

Τέλος, το LaSCO αποτελεί μία γραφική προσέγγιση για τον προσδιορισμό των security constraints στα αντικείμενα, στην οποία γίνεται η θεώρηση ότι μία πολιτική απαρτίζεται από δύο μέρη : το domain (υποθέσεις σχετικά με το σύστημα) και την απαίτηση («τι» είναι επιτρεπτό να λάβει χώρα στο εκάστοτε domain). Οι πολιτικές που εμφανίζονται στο LaSCO έχουν την μορφή προτάσεων με συνθήκη για access control. Η συγκεκριμένη προσέγγιση είναι πολύ περιορισμένη και δεν μπορεί να ικανοποιήσει το σύνθετο έργο της διαχείρισης των πολιτικών ασφάλειας με τυπικό τρόπο.

1.1.3. Χαρακτηριστικά και ιδιαιτερότητες ad-hoc δικτύων

Σύμφωνα με τους Imrich Chlamtac, Marco Conti και Jennifer J. -N. Liu [37] ένα mobile ad-hoc network ορίζεται ως εξής :

«Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, "ad-hoc" network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g., disaster recovery environments.»

Από τον ορισμό γίνεται σαφές ότι τα ad-hoc δίκτυα, ενώ χρίζουν μεγάλης ευκολίας, διακρίνονται από ιδιαίτερα γνωρίσματα που τα καθιστούν δύσκολα στην διαχείρισή τους. Μερικά από τα χαρακτηριστικά που τα διαφοροποιούν από τα κοινά, σταθερής τοπολογίας δίκτυα, είναι τα ακόλουθα :

- Autonomous Terminal : Στα MANET, κάθε κινητός κόμβος αποτελεί και έναν αυτόνομο κόμβο, ο οποίος μπορεί να διαδραματίσει είτε τον ρόλο του host είτε τον ρόλο του router. Έτσι, οι όροι τερματικός υπολογιστής και δρομολογητής επικαλύπτουν ο ένας τον άλλο.
- Distributed Operation : Από την στιγμή που δεν υπάρχει ένα δίκτυο κορμού (backbone network) για την κεντρική διαχείριση των λειτουργιών του δικτύου, τόσο ο έλεγχος όσο και η διαχείριση του δικτύου είναι κατανεμημένη μεταξύ των τερματικών κόμβων. Οι κόμβοι πρέπει να «συνεργάζονται» για να επιτευχθεί σωστή δρομολόγηση και ασφάλεια στο ad-hoc δίκτυο.
- Dynamic Network Topology : Εφόσον οι κόμβοι που συμμετέχουν σε ένα ad-hoc δίκτυο είναι κινητοί, η τοπολογία του δικτύου μπορεί να αλλάζει τακτικά και ασταθώς. Έτσι, κύριο χαρακτηριστικό των MANET είναι η γρήγορη προσαρμογή και αναδιάρθρωση της τοπολογίας του δικτύου.
- Fluctuating Link Capacity : Το μέσο που χρησιμοποιείται για την μετάδοση των δεδομένων (ασύρματες ζεύξεις) από την φύση έχει ορισμένα ιδιαίτερα χαρακτηριστικά. Έτσι τα ad-hoc δίκτυα είναι επιρρεπή στον θόρυβο, στο fading («ξεθώριασμα» του σήματος), και στην παρεμβολή κακόβουλων ωτακουστών.

- Light – Weight Terminals : Τέλος, στις περισσότερες των περιπτώσεων, οι κόμβοι που συμμετέχουν σε ένα τέτοιο δίκτυο υστερούν σε τεχνικές προδιαγραφές (CPU, Memory, Network Card), γεγονός που μπορεί να εισάγει επιπλέον προβλήματα λόγω της υπερφόρτωσης ενός κόμβου από αρμοδιότητες και λειτουργίες.

Τα ad-hoc δίκτυα υποφέρουν από τις ίδιες ευπάθειες που υποφέρουν και τα ενσύρματα δίκτυα, όπως denial of service, man in the middle κα. Είναι φανερό ότι τα παραπάνω χαρακτηριστικά εγείρουν νέες προκλήσεις στον τομέα της ασφάλειας τόσο των υπολογιστών όσο και των δικτύων. Αρχικά, όπως προαναφέρθηκε τα ad-hoc δίκτυα χαρακτηρίζονται από την αδόμητη τοπολογία τους, μιας και οι κόμβοι που συμμετέχουν σε ένα τέτοιο δίκτυο είναι ελεύθεροι να συμμετέχουν και να αποχωρούν από αυτό ανά πάσα στιγμή. Απόρροια αυτού είναι ότι τα δίκτυα αυτά δεν έχουν σαφή όρια εισόδου δηλαδή κάποιον κόμβο μέσω του οποίου όλοι οι υπόλοιποι επικοινωνούν με τον υπόλοιπο κόσμο. Στην περίπτωση των ενσύρματων δικτύων η εγκατάσταση ενός firewall στο σημείο εισόδου μπορεί να αντιμετωπίσει θέματα που αφορούν στο access control ικανοποιητικά. Κάτι τέτοιο δεν είναι εφικτό και στην περίπτωση των ad-hoc δικτύων.

Επιπλέον τα ad-hoc δίκτυα είναι εκτεθειμένα σε κινδύνους που αφορούν τόσο στην δρομολόγηση όσο και στην φυσική προστασία. Αναφορικά με το πρώτο, παρατηρούμε ότι η δρομολόγηση σε ad-hoc δίκτυα πραγματοποιείται με την συνεργασία όλων των κόμβων. Ο κάθε κόμβος «διαφημίζει» τους κόμβους στους οποίους μπορεί να μεταδώσει πακέτα. Δημιουργείται έτσι μία σχέση εμπιστοσύνης (trust) μεταξύ των κόμβων. Αν ένας κόμβος αρνείται να μεταφέρει πακέτα ή αν διαφημίζει εσκεμμένα λανθασμένες διαδρομές τότε το δίκτυο υπολειτουργεί ή δεν λειτουργεί καθόλου. Επιπλέον μπορεί να τροποποιεί τα πακέτα δημιουργώντας έτσι υπερφόρτωση στο δίκτυο μιας και ο τελικός κόμβος που λαμβάνει τα πακέτα ζητά την επανάληψή τους συνεχώς. Τέλος στον τομέα της φυσικής προστασίας των κόμβων, είναι φανερό ότι απαιτούνται επιπλέον μέτρα μιας και οι κόμβοι είναι κινητοί. Τέλος, ένα ακραίο σενάριο αλλά υπαρκτό, είναι αυτό του “sleep deprivation torture”. Μιας και πολλοί κόμβοι στηρίζονται ενεργειακά σε μπαταρίες, κάποιος μπορεί στέλνοντας συνεχώς πακέτα σε έναν κόμβο να «αδειάσει» την ενεργειακή πηγή του.

1.1.4. Ανάγκη Ύπαρξης Νέας Προσέγγισης και Συμβάσεις Αυτής

Στις προηγούμενες παραγράφους παρουσιάσαμε τις κυριότερες προσπάθειες της επιστημονικής κοινότητας στον τομέα της τυπικής αποτύπωσης των απαιτήσεων ασφάλειας καθώς και τα ιδιαίτερα χαρακτηριστικά, τόσο τα γενικά όσο και τα security ειδικά, των ad-hoc δικτύων. Οι περισσότερες από τις μεθόδους που παρουσιάστηκαν, μεταφράζουν τις πολιτικές υψηλού επιπέδου (high-level policies) που συνήθως εκφράζονται σε φυσικό λόγο (natural language statements) σε μία τυπική γλώσσα αποτύπωσης των απαιτήσεων ασφάλειας (security requirements). Όμως, οι πολιτικές ασφάλειας που έχουν δημιουργηθεί εστιάζουν κατά κύριο λόγο την προσοχή τους σε δίκτυα που έχουν σταθερή υποδομή. Στις περιπτώσεις των ad-hoc δικτύων, στα οποία η τοπολογία δεν είναι σταθερή αλλά διαμορφώνεται συνεχώς, οι παραπάνω μέθοδοι δεν είναι αξιόπιστη. Η διαδικασία μετάφρασης είναι αρκετά χρονοβόρα είτε αυτή γίνεται μέσω ατόμων είτε μέσω υπολογιστικών συστημάτων.

Είναι προφανές ότι οι υπάρχουσες προσεγγίσεις είναι δύσκολο να εφαρμοστούν και να ανταπεξέλθουν με επιτυχία στις απαιτήσεις των ad-hoc δικτύων. Κρίνεται λοιπόν αναγκαία η ύπαρξη μίας νέες μεθόδου η οποία θα μπορεί να ανταπεξέλθει στο δύσκολο έργο της διαχείρισης ασφάλειας των δικτύων και ιδίως των ad-hoc. Η μέθοδος αυτή θα εστιάζει την προσοχή της σε τρία σημεία i) Σωστή εξαγωγή γνώσης από τα high-level policies και αναπαράσταση αυτής με τυπικό τρόπο, ii) μείωση κατά το δυνατόν του χρόνου εξαγωγής της γνώσης, και iii) μέθοδος που λαμβάνει υπόψη της τα ιδιαίτερα χαρακτηριστικά των ad-hoc δικτύων.

Για να μείνει η προσέγγιση σε ένα επίπεδο απλό αλλά και διαχειρήσιμο κρίνεται υποχρεωτικός ο ορισμός μερικών συμβάσεων. Οι συμβάσεις αυτές παρουσιάζονται στις επόμενες παραγράφους, και χωρίζονται σε δύο ενότητες, συμβάσεις που αφορούν στα δεδομένα εισόδου και συμβάσεις που αφορούν στην επεξεργασία των δεδομένων.

1.1.4.1. Συμβάσεις για τα δεδομένα εισόδου

Στην παράγραφο αυτή, παρουσιάζονται ορισμένες συμβάσεις που αφορούν στα δεδομένα εισόδου. Οι τελευταίες οριοθετούν το πρόβλημα αυστηρότερα με στόχο την απλοποίησή του.

- Τα policy statements πρέπει να συγκεντρωθούν από παραδείγματα πολιτικών, όπως αυτά στο [38].
- Οι πολιτικές ασφάλειας τις οποίες πρόκειται να επεξεργαστούμε δεν είναι ολοκληρωμένες, αλλά αφορούν μόνο στο κομμάτι των αντιμέτρων. Πεδία και ενότητες των πολιτικών όπως εισαγωγή, συγγραφέας και άλλα ξεφεύγουν από το εύρος της μελέτης.
- Οι πολιτικές ασφάλειας αφορούν μόνο σε θέματα τεχνικά, τα οποία μπορούν να έχουν απευθείας εφαρμογή στις υποκείμενες συσκευές. Πολιτικές ασφάλειας οι οποίες αφορούν σε διαδικαστικά (procedural), ή αντίστοιχα θέματα είναι εκτός της οπτικής γωνίας της συγκεκριμένης μεθόδου.
- Η Οντολογία δεν είναι πλήρης. Η τυπική αποτύπωση της γνώσης γίνεται με την βοήθεια μίας Security Ontology. Σκοπός της μεθόδου δεν είναι η δημιουργία μίας οντολογίας ικανής να αναπαραστήσει οποιαδήποτε έννοια στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Για τον λόγο αυτό, η οντολογία αναπαριστά ένα κομμάτι της περιοχής αυτής. Η δημιουργία της έχει στηριχθεί σε βέλτιστες πρακτικές (best practices) στον τομέα της ασφάλειας και σε κοινά αποδεκτά πρότυπα (standards).
- Πληροφορίες που απαιτούνται από τη μέθοδο εκτός από τα αντίμετρα (π.χ. πληροφορία που αφορά στην τοπολογία του δικτύου), θεωρείται δεδομένη και ακριβής. Η πληροφορία απεικονίζεται σε τελική μορφή χωρίς να χρειάζεται περαιτέρω επεξεργασία.
- Τέλος τα αντίμετρα (countermeasures) που επεξεργάζομαστε δεν περιέχουν ασάφειες. Με τον όρο αυτό εννοούμε προτάσεις όπου δεν απαιτείται «ανθρώπινη» σκέψη για εξαγωγή της γνώσης, δηλαδή συνδυασμό

υπονοούμενης γνώσης (*implicit*). Επιπλέον τα αντίμετρα προς επεξεργασία αποτελούν ένα δείγμα αντιμέτρων που χρησιμοποιεί η CRAMM³.

1.1.4.2. Συμβάσεις για την επεξεργασία των δεδομένων εισόδου

Τέλος, στην παράγραφο αυτή παρουσιάζονται συμβάσεις που αφορούν στην επεξεργασία των δεδομένων εισόδου. Έχουν υιοθετηθεί κάποιες απλές ευρετικές αρχές (*heuristics*) σχετικά με την εξαγωγή της γνώσης, όπως:

- Όποιο πληροφοριακό αγαθό δεν μπορεί να εντοπιστεί ρητώς με τους κανόνες που έχουν θεσπιστεί, πχ σαφής αναφορά σε εξυπηρετητές δρομολογητές κτλ, θα θεωρείται ότι αναφέρεται στην πληροφορία ως αγαθό που χρήζει προστασίας. Μια βελτιωμένη έκδοση της άνω σύμβασης είναι ο εντοπισμός του πληροφοριακού αγαθού το οποίο περιέχει την εν λόγω πληροφορία (λ.χ., για το αντίμετρο «Use asymmetric algorithms for signatures», το πληροφοριακό αγαθό θα είναι η πληροφορία σε μορφή μηνύματος, ενώ ο περιέχων πόρος της πληροφορίας (*information container*) θα εννοείται ο πελάτης / εξυπηρετητής από τον οποίο μεταδίδεται η πληροφορία).
- Επιπλέον όταν δεν ορίζεται σαφώς ποιο είναι το υποκείμενο που υλοποιεί το αντίμετρο, τότε θα θεωρείται ότι το αντίμετρο εφαρμόζεται από κάποιο εξουσιοδοτημένο πρόσωπο/ρόλο, όπως για παράδειγμα οι διαχειριστές του δικτύου. Για παράδειγμα στην πρόταση «Passwords to be at least 6 characters long», υποθέτουμε ότι το υποκείμενο που θα εφαρμόσει το αντίμετρο είναι οι διαχειριστές του δικτύου (*administrators*). Ταυτόχρονα όταν δεν είναι εφικτός ο προσδιορισμός των τυχών περιορισμών που μπορεί να έχει ένα αντίμετρο τότε θεωρείται ότι δεν υπάρχει κανένας περιορισμός στην εφαρμογή του.
- Παρατηρώντας την δομή του συνόλου των αντιμέτρων που χρησιμοποιήθηκαν από την μέθοδο CRAMM, μπορεί να συμπεράνει κανείς ότι ακολουθούν κάποιο κοινό πρότυπο στον τρόπο γραφής τους (*pattern*). Η εξαγωγή της γνώσης στηρίζεται στα πρότυπα αυτά αν και πολλές φορές υπάρχουν εξαιρέσεις που δυσχεραίνουν το έργο της εξαγωγής. Υποθέτουμε ότι δεν

³ Η CRAMM αποτελεί ένα πρόγραμμα που υλοποιεί την ομάνυμη μέθοδο ανάλυσης επικινδυνότητας και είναι συμβατή, εκτός των άλλων, με το πρότυπο BS 7799. Τα αρχικά σημαίνουν CCTA (Central Computer and Telecommunication Agency) Risk Analysis and Manage Method.

υπάρχουν προτάσεις που να αντιβαίνουν στα αναγνωρισμένα πρότυπα. Για να γίνει ποιο κατανοητή η έννοια του προτύπου (pattern) παρατίθεται το ακόλουθο πρότυπο:

<Something1> to <Verb> <Something2>

Παράδειγμα πρότασης που ακολουθεί το πρότυπο αυτό είναι το αντίμετρο :

«Passwords to be at least six characters long»

Έτσι στις προτάσεις αυτής της μορφής μπορούμε να συμπεράνουμε ότι η λέξη/φράση <Something1> είναι το πληροφοριακό αγαθό και η φράση <Verb><Something2> είναι το ΤΙ πρέπει να γίνει/υλοποιηθεί.

1.2. Βασικές Έννοιες

1.2.1. Οντολογίες

Ο διαμοιρασμός της γνώσης αποτελεί βασικό παράγοντα στην εξέλιξη των επιστημών αλλά και στην ανάπτυξη των οργανισμών. Πολλά συστήματα έχουν δημιουργηθεί για να επιτύχουν τον στόχο αυτό, χωρίς όμως τα ανάλογα αποτελέσματα. Τα συστήματα διαμοιρασμού γνώσης (knowledge-based systems), όπως και τα κοινά λογισμικά, αντιμετωπίζουν προβλήματα ετερογένειας σε πολλούς τομείς όπως πλατφόρμες υλοποίησης, γλώσσες προγραμματισμού και το πιο σημαντικό από όλα, ετερογένεια στον τρόπο αναπαράστασης της γνώσης. Στην πραγματικότητα λοιπόν ο διαμοιρασμός της γνώσης δεν είναι καθολικός μιας και η ανταλλαγή αυτής (της γνώσης) μέσω διαφορετικών συστημάτων, ακόμη και διαφορετικών επιστημονικών ομάδων, καθίσταται δύσκολη.

Το βασικό συστατικό μίας τυπικά αποτυπωμένης γνώσης βασίζεται στην αντιληπτικότητα (*conceptualization*), στα αντικείμενα, στις έννοιες και στις οντότητες που υπάρχουν σε ένα πεδίο ορισμού καθώς και στις σχέσεις αυτών. Με τον όρο αντιληπτικότητα εννοούμε την «εικόνα» που έχουμε για το κομμάτι του κόσμου που θέλουμε να αναπαραστήσουμε. Ορίζοντας την αντιληπτικότητα αυστηρά ο διαμοιρασμός της γνώσης μπορεί να πραγματοποιηθεί ευκολότερα. Σύμφωνα λοιπόν με τον T. Gruber “*Ontology is an formal, explicit specification of a shared conceptualization.*” (Gruber 1993). Ο όρος είναι δανεισμένος από την φιλοσοφία, όπου μία Οντολογία είναι η συστηματική περιγραφή μίας ύπαρξης. Μία οντολογία αποτελείται από ένα λεξιλόγιο όρων, μία ερμηνεία αυτών (πιθανά ορισμοί) καθώς και από την αποτύπωση των σχέσεων μεταξύ των όρων αυτών.

Οι οντολογίες χωρίζονται σε τέσσερις μεγάλες κατηγορίες. Ακολουθούν με σειρά γενικού προς ειδικό:

- **Top-level ontologies**: Ασχολούνται με έννοιες όπως ο χώρος, ο χρόνος, γεγονότα (στην αφηρημένη έννοιά τους). Σκοπός τους είναι η μοντελοποίηση των εννοιών αυτών έτσι ώστε να χρησιμοποιούνται σε διαφορετικά πεδία ορισμού (domains) με τον ίδιο τρόπο. (π.χ. ANSI X3T2 Ad Hoc Group on Ontology).
- **Domain ontologies**: Οι συγκεκριμένες οντολογίες όπως είναι φανερό και από το όνομά τους, χρησιμοποιούνται για να περιγράψουν τυπικά τα αντικείμενα



και τις σχέσεις τους σε ένα πεδίο εφαρμογής (ή αλλιώς σε ένα κομμάτι του πραγματικού κόσμου). Παραδείγματα τέτοιων πεδίων εφαρμογής είναι η ζωγραφική, η αρχαιολογία, η μοριακή βιολογία κ.α. Συνήθως αποτελούν μία προέκταση των top-level ontologies.

- **Task ontologies**: Οι task ontologies ασχολούνται με τις διεργασίες που λαμβάνουν χώρα σε ένα συγκεκριμένο πεδίο εφαρμογής. Μετακίνησης, δανεισμού, συντήρησης, διαγραφής, εισαγωγής αντικειμένων. Και αυτές με την σειρά τους αποτελούν προέκταση των top-level ontologies, χρησιμοποιώντας τις domain ontologies για αναφορές στα αντικείμενα που διαπραγματεύονται .
- **Application ontologies**: Η τελευταία κατηγορία οντολογιών είναι στην ουσία η εξειδίκευση όλων των παραπάνω κατά τέτοιο τρόπο έτσι ώστε να λύσει τυχόν προβλήματα επικοινωνίας σε μία συγκεκριμένη ομάδα ανθρώπων. Χρησιμοποιείται κατά κύριο λόγο ως «ενδιάμεσος» μεταξύ ανομοιογενών λογισμικών, που όμως ασχολούνται με το ίδιο πεδίο ορισμού.

Έτσι αν θελήσουμε να απαντήσουμε στο γενικό ερώτημα γιατί να θέλει κάποιος να δημιουργήσει μία οντολογία; θα μπορούσαμε να επισημάνουμε τα εξής :

1. Για τον διαμοιρασμό μίας κοινής αντίληψης που υπάρχει μεταξύ ανθρώπων με διαφορετική κουλτούρα αλλά και μεταξύ διαφορετικών συστημάτων.
2. Για την επαναχρησιμοποίηση γνώσης.
3. Για να μην υπάρχουν ασάφειες σχετικά με τους όρους ασφάλειας που έχουν νόημα σε ένα πεδίο εφαρμογής (domain)
4. Για να υπάρχει μία κοινή ανάλυση της γνώσης και εξαγωγή κοινών συμπερασμάτων από διαφορετικές ομάδες χρηστών.

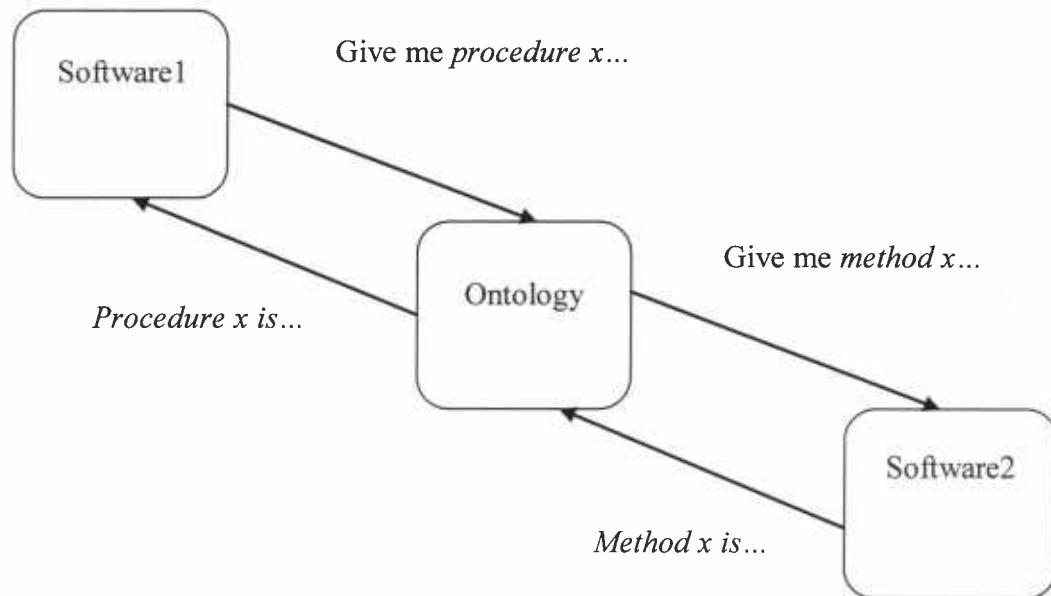
Για να γίνει περισσότερο κατανοητή η έννοια της οντολογίας ας δούμε μερικές εφαρμογές της όπως αυτές μπορούν να προκύψουν από τα παραπάνω. Στο τέλος της παραγράφου αυτής παρουσιάζεται και ένα παράδειγμα εφαρμογής οντολογίας. Οι κυριότερες εφαρμογές είναι (Grüniger 1996):

- **Επικοινωνία**: είτε μεταξύ μεμονωμένων ατόμων είτε μεταξύ οργανισμών

- Διαδραστικότητα μεταξύ συστημάτων υπολογιστών: μετάφραση των μεθόδων μοντελοποίησης, κωδικοποίηση πληροφοριών από το ένα σύστημα στο άλλο κ.α.
- Τεχνολογία Λογισμικού: Στον τομέα της επαναχρησιμοποίησης κώδικα όπου τυπικές αποτυπώσεις μεθόδων και εργαλείων μπορούν εύκολα να υιοθετηθούν από καινούργιες ομάδες προγραμματιστών, στον τομέα της αξιοπιστίας όπου έλεγχοι συνέπειας αλλά και συνοχής του κώδικα μπορούν να γίνουν ευκολότερα, αλλά και στον τομέα των απαιτήσεων όπου μπορούν να βοηθήσουν τον αναλυτή να αποτυπώσει τις απαιτήσεις σε μία τυπική μορφή απολύτως κατανοητή και χωρίς ασάφειες για τον προγραμματιστή.

Ας υποθέσουμε ότι δύο Ελληνικά πανεπιστήμια ασχολούνται με δομή του ατόμου όπως την βλέπει η κβαντοχημεία. Τα ξένα συγγράμματα περιγράφουν με την λέξη “*orbital*” το χώρο στον οποίο υπάρχει σημαντική πιθανότητα (μεγαλύτερη του 0.95) να βρεθεί κάποια χρονική στιγμή τ ένα ηλεκτρόνιο. Η λέξη αυτή στα ελληνικά αποδόθηκε με τον όρο *τροχιακό* από το ένα πανεπιστήμιο και με τον όρο *τροχιώδες* από το άλλο. Υποθέτοντας ότι τα δύο αυτά πανεπιστήμια θέλουν να ανταλλάσουν πληροφορίες για τα αποτελέσματα των πειραμάτων τους θα πρέπει η κάθε επιστημονική ομάδα να αποκωδικοποίησε τις έννοιες που χρησιμοποιεί η άλλη σε μορφή κατανοητή για αυτούς. Αυτό συνεπάγεται απώλεια χρόνου και για τις δύο ομάδες. Με την προσθήκη μίας οντολογίας, η οποία θα αποτυπώνει τυπικά τις έννοιες αυτές, οι δύο επιστημονικές ομάδες θα μπορούν να ανταλλάξουν δεδομένα χωρίς προβλήματα ερμηνείας των εννοιών.

Τέλος ένα ακόμη παράδειγμα είναι η ενοποίηση δύο λογισμικών. Ο όρος μέθοδος, αποτυπώνεται από το ένα πρόγραμμα με την λέξη *procedure* ενώ από το άλλο με την λέξη *method*. Αν το ένα πρόγραμμα από τα δύο ζητήσει την *procedure x* τότε το άλλο δεν θα καταλάβει ότι πρόκειται για την *method x*. Η βοήθεια της οντολογίας μπορεί να παρασταθεί σχηματικά ως εξής :



Εικόνα 1 : Παράδειγμα εφαρμογής οντολογίας

Η λύση αυτή μπορεί να επεκταθεί για περισσότερα από ένα κομμάτια λογισμικού χωρίς κανένα επιπλέον κόστος. Είναι φανερό ότι περίπτωση δημιουργίας κάποιου software agent, μπορεί η ανταλλαγή της συγκεκριμένης πληροφορίας να γινόταν ικανοποιητικά αλλά η λύση δεν θα ήταν ευέλικτη και δυναμική. Στην περίπτωση κατά την οποία τα δύο λογισμικά θελήσουν να ανταλλάξουν διαφορετικού είδους πληροφορία (πχ κάποιο δεδομένο x), τότε η επέκταση του πράκτορα λογισμικού θα είναι δυσκολότερη σε σχέση με την απλή επέκταση της οντολογίας για υποστήριξη και τέτοιου είδους αντικειμένων.

1.2.2. Τεχνικές αποτύπωσης οντολογιών

Με την στροφή της επιστημονικής κοινότητας στον τομέα της αναπαράστασης της γνώσης, πολλές «γλώσσες» αποτύπωσης οντολογιών έχουν βγει στο προσκήνιο. Στην παράγραφο αυτή περιγράφουμε την εξέλιξη των σημαντικότερων τεχνικών, τα πλεονεκτήματα και τα μειονεκτήματα που παρουσιάζει η κάθε μία και επισημαίνουμε μερικές από τις σχεδιαστές αρχές για κάθε γλώσσα. Τα πλεονεκτήματα και τα μειονεκτήματα εστιάζονται κατά κύριο λόγο στα σχεδιαστικά κριτήρια που έχει προτείνει η W3C, τα οποία είναι ο Διαμοιρασμός Οντολογιών (Ontology Sharing), Διαχείριση Εκδόσεων (Versioning⁴), η Διαλειτουργικότητα (Interoperability), Συμπερασματικοί Μηχανισμοί (Reasoning support), η Ευκολία στην Χρήση (Ease of Use), η Συμβατότητα με Πρότυπα (Compatibility with standards), και η Διεθνοποίηση – Υποστήριξη πολλών γλωσσών (Internationalization) (Heflin, et. al, 2002).

Οι πιο διαδεδομένες γλώσσες του σημασιολογικού ιστού (Semantic Web) είναι η RDF, η RDFS, η OIL, η DAML+OIL, και η OWL. Οι γλώσσες αυτές δεν είναι ανεξάρτητες μεταξύ τους, αλλά υπάρχει μία αρχιτεκτονική στρωμάτων. Στο κατώτερο επίπεδο βρίσκεται η XML [4] η οποία χρησιμοποιείται για το συντακτικό της. Πάνω από την XML υπάρχει η RDF (Resource Description Framework) [11], μία απλή γλώσσα για μεταδεδομένα. Η RDF χρησιμοποιείται για annotation⁵ σκοπούς πηγών του Web. Αμέσως μετά βρίσκεται η RDFS (RDF Schema) [6], η οποία, όπως αναφέρει και το όνομά της, μπορεί να χρησιμοποιηθεί για δημιουργία σχημάτων που ορίζουν έννοιες καθώς και τις πιθανές σχέσεις που υπάρχουν μεταξύ των εννοιών. Ένα επίπεδο πιο πάνω (από το επίπεδο αυτό και στη συνέχεια αναφερόμαστε στις “λογικές” γλώσσες οντολογιών) βρίσκεται η OIL [8][9] και η DAML. Η OIL (Ontology Inference Layer) αποτελεί μία γλώσσα με ισχυρή εκφραστική δύναμη για την δημιουργία οντολογιών. Η OIL αποτελεί μία προσπάθεια της αγγλικής επιστημονικής κοινότητας. Ταυτόχρονα, η αμερικανική επιστημονική κοινότητα παρουσίασε την DAML (DARPA Agent Markup Language). Η τελευταία έκδοση και των δύο γλωσσών είναι η DAML+OIL [12], η συνένωση των δύο γλωσσών σε μία προσπάθεια δημιουργίας μίας ισχυρής γλώσσας που εκμεταλλεύεται τα

⁴ Οι εκδόσεις βοηθούν στην περίπτωση αλλαγής της οντολογίας τα υπάρχοντα δεδομένα να μην χαθούν αλλά ταυτόχρονα να ξέρουν οι ενδιαφερόμενοι σε ποια έκδοση της οντολογίας αναφέρονται.

⁵ Η λέξη annotation μεταφράζεται ως σχολιάζω, προσδίων νόημα. Θεωρήθηκε καλύτερη η αναφορά της αγγλικής λέξης παρά η μετάφρασή της στα ελληνικά.

πλεονεκτήματα των δύο γλωσσών. Τέλος, στο τελευταίο επίπεδο βρίσκεται η OWL [7] – ίσως η ισχυρότερη μεταξύ των γλωσσών. Παρακάτω ακολουθεί μία ανάλυση για την κάθε γλώσσα ξεχωριστά.

RDF (S) : Το επόμενο βήμα στην προσπάθεια αποτύπωσης της γνώσης ήταν η RDF (Resource Description Framework) [2]. Η RDF αποτελεί στην ουσία επέκταση της XML. Η εκφραστική δύναμή της είναι αρκετά περιορισμένη και οι αιτιολογικές της ικανότητες δεν είναι οι ισχυρότερες μεταξύ των διαφορετικών γλωσσών, παρέχοντας έτσι έναν περιορισμένο αιτιολογικό μηχανισμό κατάλληλο μόνο για ελέγχους περιορισμών (constraint checking). Η RDF εξελίχθηκε στην RDF-S η οποία παρέχει δυνατότητας αποτύπωσης ενός σχήματος, κάτι το οποίο δεν υπήρχε στην απλή RDF. Το γεγονός αυτό και σε συνδυασμό με την πληθώρα εργαλείων και παραδειγμάτων που βρίσκονται διαθέσιμα στο κοινό, καθιστούν την γλώσσα πολύ διαδεδομένη. Όσον αφορά στην «διεθνοποίηση» υποστηρίζει πολλές φυσικές γλώσσες και είναι συμβατή με την HTML, της οποίας θεωρείται ότι είναι υπερσύνολο (superset). Η επιστημονική κοινότητα ασχολείται με την περαιτέρω ανάπτυξη και βελτίωσή της.

OIL : Η εκφραστική δύναμη της OIL αποτελεί ισχυρό πλεονέκτημα για αυτή έναντι της RDFS. Οι αιτιολογικές ικανότητες που προσφέρει, παρέχουν ελέγχους συνέπειας για τα αντικείμενα της οντολογίας, ευκολία στην διασύνδεση ξεχωριστών οντολογιών καθώς και εντοπισμό τυχόν υπονοούμενων σχέσεων μεταξύ των αντικειμένων. Η OIL επιτρέπει μερικώς την δημιουργία κανόνων απεικόνισης⁶ των αντικειμένων. Επιπλέον, υποστηρίζει διάφορες φυσικές γλώσσες γεγονός που την καθιστά φιλική και εύχρηστη για τον χρήστη. Ακόμη, υπάρχουν αρκετά εργαλεία που υποστηρίζουν την γλώσσα αυτή, καθώς και αρκετό υλικό με πλούσια παραδείγματα που μπορούν να βοηθήσουν τους νέους χρήστες. Όσον αφορά στην συμβατότητα η OIL είναι βασισμένη στα Description Logics όσο και στα F-Logics. Τα Description Logics περιγράφουν τις σχέσεις που μπορεί να υπάρχουν μεταξύ instances (στιγμιότυπα) των τάξεων μίας οντολογίας. Τα F-Logics (Frame Based Logics) αποτελούν στην ουσία μεταφορά των αρχών του αντικειμενοστραφούς προγραμματισμού στο κομμάτι των οντολογιών. Ελέγχουν δηλαδή την κληρονομικότητα καθώς και την ιεραρχία των τάξεων. Κάτι που αξίζει να σημειωθεί είναι το γεγονός ότι το βασικό τμήμα της OIL

⁶ Οι κανόνες απεικόνισης, βοηθούν στην αντιστοίχηση εννοιών του πραγματικού κόσμου (έννοιες από ένα λεξικό, από μία βάση δεδομένων κ.ο.κ.) με τις τάξεις της οντολογίας.



συμπίπτει με αυτό της RDFS εκτός από την δυνατότητα αναπαράστασης αφηρημένων κλάσεων που παρέχει η RDFS. Τέλος η OIL δεν βρίσκεται πλέον υπό ανάπτυξη.

DAML + OIL : Οι μηχανισμοί αιτιολόγησης (inference mechanisms) που παρέχει είναι αρκετά χρήσιμοι σε περιπτώσεις κοινής χρήσης οντολογιών. Όσον αφορά στην διαλειτουργικότητα, επιτρέπει δημιουργία κανόνων αποτύπωσης, όχι όμως σε μεγάλο βαθμό. Οι μηχανισμοί αιτιολόγησης στηρίζονται περισσότερο στα Description Logics. Η εκφραστική της δύναμη, είναι αρκετά βελτιωμένη σε σχέση με τους πρόγονούς της. Είναι αρκετά εύκολη στην χρήση και αναφορικά με την συμβατότητα μπορούμε να πούμε ότι παρέχει σημαντικές ευκολίες μιας και υποστηρίζει πλήρως XML και RDF σχήματα.

OWL : Η OWL, όπως προαναφέρθηκε, αποτελεί την πιο πρόσφατη γλώσσα σημασιολογικού ιστού. Υπάρχουν τρεις εκδόσεις της γλώσσας αυτής [12] ανάλογα με τις απαιτήσεις του εκάστοτε μοντέλου.

- *OWL Lite* : Η μικρότερη έκδοση από τις τρεις συνολικά της OWL. Ο OWL Lite υποστηρίζει μία απλή δημιουργία ιεραρχίας τάξεων καθώς και τον προσδιορισμό των μεταξύ τους σχέσεων. Επιπλέον μπορούν να οριστούν περιορισμοί μόνο όσον αφορά στο κομμάτι του πλήθους των στιγμιότυπων των τάξεων (πλήθος 0 ή 1). Η έκδοση αυτή χρησιμοποιείται κατά κύριο λόγο σε συστήματα όπου το μέγεθος της οντολογίας δεν είναι μεγάλο, καθώς και σε απλές ταξινομίες αλλά και θησαυρούς.
- *OWL DL* : Ίσως η πιο διαδεδομένη έκδοση της OWL. Υποστηρίζει πιο απαιτητικούς χρήστες οι οποίοι θέλουν να εκμεταλλευτούν στο μέγιστο την εκφραστική δύναμη της OWL, χωρίς όμως να θυσιάσουν την υπολογιστική πληρότητα (όλες οι συνεπαγωγές είναι εγγυημένο ότι μπορούν να υπολογιστούν) και την πολυπλοκότητα (όλες οι υπολογισμοί θα τελειώσουν σε κάποιο πεπερασμένο διάστημα χρόνου) των μηχανισμών αιτιολόγησης. Τα Η συγκεκριμένη έκδοση της OWL είναι «χτισμένη» στην αρχή των Description Logics, εξ ου και τα αρχικά DL.
- *OWL Full* : Η τελευταία έκδοση της OWL αποτελεί το πληρέστερο αλλά και συνάμα πιο πολύπλοκο κομμάτι της. Είναι προορισμένη για απαιτητικούς χρήστες οι οποίοι απαιτούν ισχυρή εκφραστική δύναμη και ταυτόχρονα την

πλήρη συντακτική ελευθερία της RDF (όπως ήδη έχει αναφερθεί η OWL έχει δημιουργηθεί βάση του συντακτικού της RDF). Το μεγάλο της μειονέκτημα έγκειται στο γεγονός ότι δεν παρέχει υπολογιστικές εγγυήσεις. Συνήθως χρησιμοποιείται για μεγάλου μεγέθους οντολογίες, όπως οι top-level ontologies είτε domain ontologies (όπως αυτές ορίστηκαν στην παράγραφο 1.2.1) όταν το πεδίο περιγραφής είναι αρκετά μεγάλο.

Το βασικό μειονέκτημα της OWL είναι το γεγονός ότι βρίσκεται ακόμα υπό ανάπτυξη. Το γεγονός αυτό και σε συνδυασμό με την πλούσια εκφραστική δύναμη της OWL (και κατά κύριο λόγο της OWL Full) καθιστά δύσκολη την εύρεση ενός αιτιολογικού λογισμικού που θα μπορεί να υποστηρίξει πλήρως τις δυνατότητες της OWL. Κάθε μία από τις παραπάνω κατηγοριοποιήσεις αποτελεί προέκταση του προγόνου της. Έτσι, η OWL Full αποτελεί υπερσύνολο της OWL DL, η οποία με την σειρά της αποτελεί υπερσύνολο της OWL Lite.

1.2.3. Επεξεργασία Φυσικής Γλώσσας (NLP) και Εξαγωγή Πληροφοριών (IE)

Όπως προαναφέρθηκε και σε προηγούμενη παράγραφο, η μέθοδος που παρουσιάζεται χρησιμοποιεί τεχνικές από δύο μεγάλους κλάδους της επιστήμης των υπολογιστών, της επεξεργασίας φυσικής γλώσσας (natural language processing, NLP) και της εξαγωγής πληροφοριών (information extraction, IE).

Με τον όρο φυσική γλώσσα εννοούμε το σύνολο των λέξεων ή φράσεων που χρησιμοποιούνται από τους ανθρώπους για την προφορική ή γραπτή τους επικοινωνία. Η επεξεργασία φυσικής γλώσσας ορίζεται ως η χρήση των υπολογιστών για επεξεργασία προφορικής ή γραπτής γλώσσας για κάποιο πρακτικό λόγο, όπως μετάφραση κειμένου, εξαγωγή πληροφοριών από τον Παγκόσμιο Ιστό, διεξαγωγή διαλόγων είτε με ανθρώπους είτε με μηχανές και πολλά άλλα. Τα παραπάνω παραδείγματα αποτελούν μερικά παραδείγματα βασικών εφαρμογών στον τομέα αυτό. Πιο εξειδικευμένες εφαρμογές περιλαμβάνουν για παράδειγμα την απόφαση ενός υπολογιστή για το αν δύο άρθρα σε διαφορετικές εφημερίδες είναι το ένα αντιγραφή του άλλου. Σε αυτές τις περιπτώσεις ο υπολογιστής πρέπει να μπορεί να κατανοήσει (με κάποιο τρόπο) το νόημα του κειμένου, διαδικασία πιο σύνθετη από τις προαναφερθείσες.

Πιο αναλυτικά ο τομέας του NLP περιλαμβάνει :

- **Σύνθεση ομιλίας :** Η σύνθεση ομιλίας αποτελεί ένα από τους βασικούς τομείς του NLP. Οι περιπτώσεις όπου ο στόχος είναι απλά η δημιουργία προτάσεων που να έχουν νόημα για τους ανθρώπους θεωρούνται σχετικά απλές. Όμως σε καταστάσεις όπου πρέπει να δημιουργηθούν προτάσεις βάση κάποιας προηγούμενης έτσι ώστε να υπάρχει νόημα θεωρούνται εξαιρετικά δύσκολες λόγω της μεγάλης πολυπλοκότητας της ανθρώπινης γλώσσας αλλά και της ανθρώπινης σκέψης (μεταφορές, ιδιωματισμοί κ.α.).
- **Αναγνώριση ομιλίας :** Στην ουσία ο διαχωρισμός ενός συνεχόμενου κύματος ήχου σε λέξεις. Ίσως ο πιο προχωρημένος τομέας στον κλάδο της επεξεργασίας φυσικής γλώσσας. Πολλά πακέτα φωνητικής πληκτρολόγησης διατίθενται ήδη στο εμπόριο. Τα συστήματα αυτά μπορούν να διαχωριστούν ανάλογα με το αν απαιτούν εκπαίδευση από τον χρήστη ή αν είναι ανεξάρτητα από την εκάστοτε φωνή.

- Κατανόηση ομιλίας :** Πολλοί είναι αυτοί που συγχέουν την αναγνώριση ομιλίας με την κατανόηση ομιλίας. Στόχος του τομέα αυτού είναι η σωστή νοηματοδότηση των λέξεων και όχι η απλή μετατροπή των λέξεων από κάποιο ηχητικό σήμα σε μία άλλη μορφή όπως είναι στην αναγνώριση φωνής. Ο υπολογιστής πρέπει να είναι σε θέση ανάλογα με την δομή της πρότασης αλλά και ανάλογα με την χρήση των λέξεων να αντιλαμβάνεται μεταφορές, ιδιωματισμούς και άλλα.
- Ανάκτηση πληροφοριών :** Η Ανάκτηση Πληροφοριών (Information Retrieval – IR) είναι ο κλάδος του NLP που ασχολείται με την αναζήτηση πληροφοριών σε έγγραφα, με αυτούσιων εγγράφων σχετικά με ένα θέμα και με την αναζήτηση μεταδεδομένων⁷. Επιπλέον ασχολείται με την αναζήτηση πληροφοριών σε βάσεις δεδομένων που περιεχόμενά τους μπορεί να είναι εικόνες, ήχος, ή και κείμενα.
- Εξαγωγή πληροφοριών :** Η Εξαγωγή Πληροφοριών (Information Extraction – IE) είναι ένας κλάδος της Ανάκτησης Πληροφοριών (IR). Στόχος της είναι η αυτόματη εξαγωγή δομημένων ή ημιδομημένων πληροφοριών από κείμενα αναγνώσιμα από υπολογιστές. Μία πολύ βασική εφαρμογή του IE είναι η σάρωση πλήθους εγγράφων σε φυσική γλώσσα και η αποθήκευση των εξαγομένων πληροφοριών σε βάση δεδομένων. Η Εξαγωγή Πληροφοριών είναι και ο κλάδος που θα μας βοηθήσει στην ανάπτυξη της μεθόδου που παρουσιάστηκε πιο πάνω.

Πιο αναλυτικά μπορούμε να πούμε ότι η IR απλά βρίσκει κείμενα που μας ενδιαφέρουν από διάφορες πηγές και τα παρουσιάζει στον χρήστη. Οι τυπικές IE εφαρμογές αναλύουν ένα κείμενο και παρουσιάζουν μόνο τις πληροφορίες που θέλει να δει ο χρήστης. Σύμφωνα με τον H.Cunningham [1] το IE ορίζεται ως η διαδικασία είσοδος της οποίας είναι κείμενα σε φυσική γλώσσα και έξοδός της είναι δεδομένα σε συγκεκριμένη μορφή και μη-διφορούμενα. Τα δεδομένα αυτά μπορούν απευθείας να παρουσιαστούν για επίδειξη στον χρήστη ή μπορούν να αποθηκευτούν για περαιτέρω ανάλυση ή να χρησιμοποιηθούν για ευρετηριακούς λόγους σε Information Retrieval εφαρμογές.

⁷ Με μία ελεύθερη απόδοση μπορούμε να περιγράψουμε τα μεταδεδομένα ως δεδομένα που περιγράφουν άλλα δεδομένα – π.χ. μεταδεδομένα για ένα σύνολο από έγγραφα αποτελούν ο συγγραφέας, ο τίτλος και άλλα.

Υπάρχουν πέντε είδη εξαγωγής πληροφοριών που βρίσκονται υπό έρευνα (όπως αυτά καθορίστηκαν από το μεγαλύτερο forum στον τομέα αυτό, το Message Understanding Forum):

- **Named Entity Recognition (NE)** : (Αναγνώριση Οντοτήτων) Βρίσκει και ταξινομεί ονόματα, τοποθεσίες και άλλα.
- **Coreference Resolution (CO)** : Αναγνωρίζει τις σχέσεις μεταξύ των οντοτήτων που βρέθηκαν από την NE.
- **Template Element Construction (TE)** : Προσθέτει περιγραφικές πληροφορίες σχετικά στα αποτελέσματα της NE (χρησιμοποιώντας την CO).
- **Template Relation Construction (TR)** : Βρίσκει τις σχέσεις μεταξύ των οντοτήτων του TE.
- **Scenario Template Production (ST)** : «Ταιριάζει» τα αποτελέσματα του TE και TR σε συγκεκριμένα σενάρια γεγονότων.

Ένα ολοκληρωμένο παράδειγμα που θα μας βοηθήσει να κατανοήσουμε τα παραπάνω καλύτερα είναι το ακόλουθο.

Το πανύψηλο κτήριο εγκαινιάστηκε την Τρίτη. Αυτό είναι «παιδί» του αρχιτέκτονα KLM. Ο KLM εργάζεται στην εταιρία XYZ Inc.

Με την αναγνώριση οντοτήτων (NE) οι οντότητες που θα αναγνωριστούν είναι το κτήριο, η Τρίτη, ο KLM και η XYZ Inc. Η CO διαπιστώνει ότι η λέξη *Aυτό* αναφέρεται στην έννοια κτήριο. Η TE διαπιστώνει ότι το κτήριο είναι πανύψηλο και ότι είναι «παιδί» του KLM. Η TR βρίσκει ότι ο KLM δουλεύει στην εταιρία XYZ και τέλος η ST ανακαλύπτει ότι πραγματοποιήθηκε κάποια γεγονός εγκαινίασης στο οποίο εμπλέκονται οι διάφορες οντότητες.

Από όλα τα παραπάνω, εμείς θα ασχοληθούμε κατά κύριο λόγο με το Name Entity Recognition, με το Coreference Resolution και με το Template Element Construction. Μέσα από τα αντίμετρα θα προσπαθήσουμε να εντοπίσουμε τις κεντρικές έννοιες που αφορούν στο αντίμετρο αυτό καθώς και τις πιθανές σχέσεις μεταξύ των οντοτήτων αυτών.

2. Μεθοδολογία Προσέγγισης

2.1. Εννοιολογικό Μοντέλο

Στην ενότητα που ακολουθεί παρουσιάζουμε την μέθοδο που προτείνουμε για την τυπική αποτύπωση των απαιτήσεων ασφάλειας ενός ad-hoc δικτύου. Η μέθοδος που παρουσιάζεται μπορεί να εφαρμοστεί και σε κοινά δίκτυα σταθερής τοπολογίας. Στην παράγραφο αυτή, δίνουμε μία πρώτη εικόνα της μεθόδου παρουσιάζοντας το εννοιολογικό πλαίσιο αυτής. Στην συνέχεια, ορίζουμε την οντολογία, η οποία και θα είναι το τελικό «προϊόν» της μεθόδου αυτής, το λεξιλόγιο των όρων της και τις σχέσεις που έχουν οι όροι μεταξύ τους. Η επόμενη παράγραφος περιγράφει αναλυτικά τα βήματα της μεθόδου όπως αυτά παρουσιάστηκαν σε αυτή την παράγραφο. Τέλος, μιας και για την υλοποίηση της μεθόδου χρησιμοποιήθηκαν δύο εργαλεία, το GATE και το Protege, στις τελευταίες δύο παραγράφους αναλύουμε την αρχιτεκτονική των εργαλείων αυτών.

Οι πηγές των πληροφοριών που μπορεί να έχει ο κάθε ενδιαφερόμενος στο τομέα της ασφάλειας των πληροφοριακών συστημάτων ποικίλουν. Για να δημιουργηθεί μία ικανοποιητική πολιτική ασφάλειας αλλά και για να μπορεί να η ασφάλεια στη συνέχεια να είναι διαχειρήσιμη, κρίνεται αναγκαία η λεπτομερής εξέταση όλων των διαθέσιμων πηγών. Οι πηγές αυτές ονομαστικά είναι :

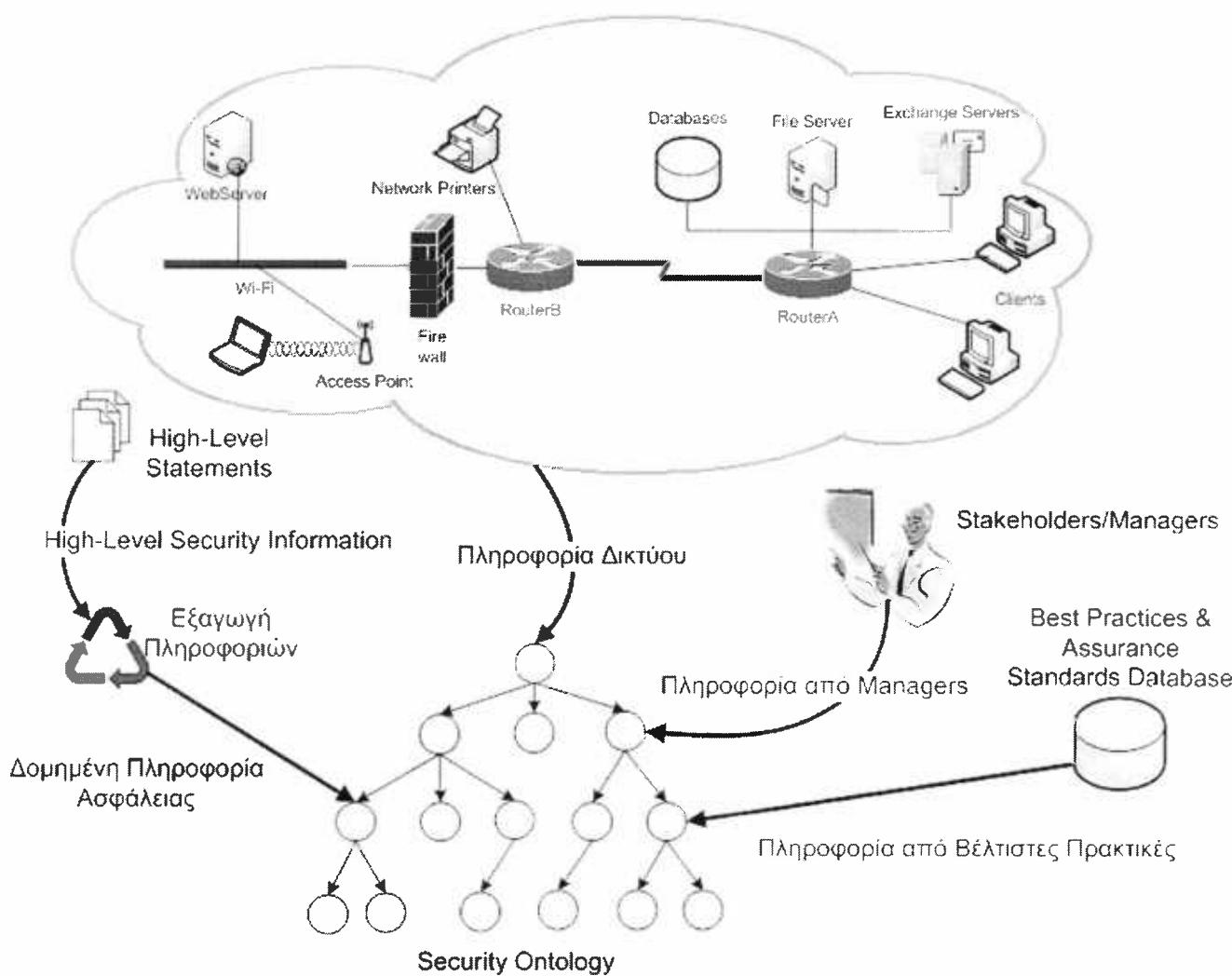
- Πληροφορία δικτύου. Με τον όρο αυτό εννοούμε πληροφορία σχετικά με την τοπολογία του δικτύου. Πόσοι servers υπάρχουν, πόσοι clients, τι λειτουργικά συστήματα έχουν ο καθένας, ποιες πόρτες είναι ανοιχτές στον κάθε υπολογιστή και γενικώς παρόμοιες πληροφορίες που είναι απαραίτητες. Για την εξαγωγή της πληροφορίας δικτύου, υπάρχουν αρκετά εργαλεία διαθέσιμα, όπως το Nmap [40], το Netstumbler [41] και το GFILANGuard [42].
- Πληροφορία από το επίπεδο διαχείρισης. Τις περισσότερες φορές, ανάλογα με τις ιδιαιτερότητες της κάθε εταιρείας/οργανισμού, οι πολιτικές ασφάλειας διαμορφώνονται από τους Managers έτσι ώστε να επιτευχθούν οι επιχειρησιακοί στόχοι. Συνήθως η πληροφορία περιλαμβάνει εξαιρέσεις που πρέπει να ληφθούν υπόψη, όπως υπηρεσίες που είναι γενικά απαγορευτικές στο σύνολο των υπολογιστών, για παράδειγμα ftp, αλλά σε συγκεκριμένους

υπολογιστές είναι επιτρεπτές. Σε αυτές τις περιπτώσεις οι εξαιρέσεις παρέχονται σε μορφή κατάλληλη προς επεξεργασία και όχι σε high-level statements.

- Πληροφορία από τα high-level policies. Οι πολιτικές που συγκροτούνται αποτυπώνουν τα αγαθά που η εκάστοτε εταιρία θεωρεί ότι πρέπει να προφυλάξει και περιγράφει εκείνες τις ενέργειες που απαιτούνται για να μειώσουν κατά το δυνατόν τον κίνδυνο απώλειας του κάθε αγαθού. Οι πληροφορία αυτή μπορεί να μετασχηματιστεί σε μία τυπική μορφή χρησιμοποιώντας τεχνικές επεξεργασίας φυσικής γλώσσας, όπως για παράδειγμα το GATE [18]. Στην παράγραφο 2.4.2, παρουσιάζουμε τα βασικά συστατικά της αρχιτεκτονικής του GATE.
- Πληροφορία από κοινά αποδεκτά standards. Οι κοινές πρακτικές (best practices) σε θέματα ασφάλειας πληροφοριακών συστημάτων βοηθούν τους υπεύθυνους ασφαλείας είτε ως ένα σημείο αναφοράς για την δημιουργία πολιτικής ασφάλειας είτε ως επικουρική λύση σε δύσκολες καταστάσεις όπου η λύση δεν είναι προφανής. Πλέον υπάρχουν διαθέσιμες στο κοινό βάσεις δεδομένων που έχουν κοινές πρακτικές για τα πιο συνηθισμένα προβλήματα και ανάλογα με το αγαθό το οποίο χρήζει προστασίας.

Όλες οι παραπάνω πηγές πληροφοριών μπορούν, αλλά και είναι αναγκαίο να αξιοποιηθούν κατάλληλα για την τυπική αποτύπωση των απαιτήσεων ασφάλειας. Το μέσο το οποίο θα χρησιμοποιηθεί για την αποθήκευση των πληροφοριών σε τυπική μορφή είναι μία οντολογίας ασφάλειας, για τους λόγους που αναφέρθηκαν στην παράγραφο 1.2.1⁸. Η τελευταία αποτυπώνει κεντρικές ιδέες και έννοιες στον τομέα της ασφάλειας καθώς και τις σχέσεις μεταξύ των εννοιών αυτών.

⁸ Επιπλέον παρέχεται μία αναλυτικότερη επεξήγηση των πλεονεκτημάτων των οντολογιών έναντι των υπόλοιπων μοντέλων απεικόνισης γνώσης στην παράγραφο 2.4



Εικόνα 2 : Εννοιολογικό Πλαίσιο Μεθοδολογίας

Όπως απεικονίζεται και στο παραπάνω σχήμα, το κάθε είδος πληροφορίας συμβάλλει στην δημιουργία της οντολογίας ασφάλειας (Security Ontology, SO). Με την κατάλληλη επεξεργασία των πληροφοριών μπορούμε να βρούμε την χρυσή τομή αυτών και να την αποτυπώσουμε στην οντολογία. Αναλυτικά τα βήματα της προσέγγισης που παρουσιάζεται, αλλά και η μέθοδος δημιουργίας μίας SO, η οποία στηρίχθηκε σε κοινά αποδεκτές προτάσεις, παρουσιάζονται στις επόμενες παραγράφους.

2.2. Ορισμός Μοντέλου Οντολογίας Ασφάλειας

2.2.1. Οντολογία Ασφάλειας

Όπως παρουσιάστηκε στην παράγραφο 1.2.1 η οντολογία αποτελεί ένα καλό μέσο αναπαράστασης της γνώσης. Συγκεκριμένα στον τομέα της ασφάλειας αρκετές προσπάθειες έχουν γίνει με στόχο τόσο την τυπική αποτύπωση των απαιτήσεων της ασφάλειας ενός πληροφοριακού συστήματος όσο και με την διαχείριση αυτής (ενότητα 1.1.2). Οι προτάσεις που υπάρχουν δεν είναι αρκετά ευέλικτες. Οι περισσότερες από αυτές απαιτούν την εκμάθηση μίας εξειδικευμένης γλώσσας με αποτέλεσμα να δημιουργείται χάσμα μεταξύ αυτών που τελικά θα χειριστούν την μέθοδο της τυπικής αποτύπωσης και των υπεύθυνων ασφαλείας. Επιπλέον αν θελήσουμε να χρησιμοποιήσουμε κάποια από τις παραπάνω μεθόδους για την τυπική αποτύπωση των απαιτήσεων ασφάλειας ad-hoc δικτύων, πιθανά να αντιμετωπίσουμε προβλήματα. Τα ad-hoc δίκτυα, όπως προαναφέρθηκε, αλλάζουν δυναμικά με αποτέλεσμα να απαιτείται μία μέθοδος η οποία θα είναι σε θέση να προσαρμόζει τις απαιτήσεις ασφάλειας γρήγορα και δυναμικά. Κάτι τέτοιο δεν είναι εφικτό, εφόσον οι μέθοδοι που παρουσιάστηκαν απαιτούν επεξεργασία από ανθρώπους, κάτι αρκετά χρονοβόρο.

Πριν ξεκινήσουμε την αναλυτική παρουσίαση της μεθόδου, θα ορίσουμε την οντολογία ασφάλειας – τις έννοιες/τάξεις που ορίσαμε, τις σχέσεις μεταξύ των τάξεων και τέλος το λεξιλόγιο των όρων της οντολογίας για την αποφυγή παρερμηνειών – αλλά και την μέθοδο που ακολουθήσαμε για να την δημιουργήσουμε.

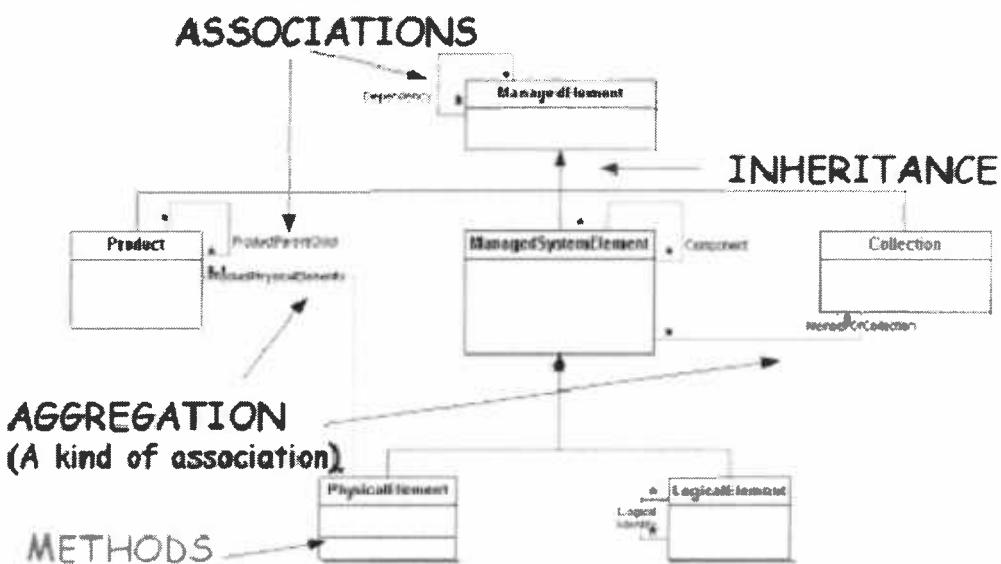
Οσον αφορά στη δημιουργία της SO δεν υπάρχει κάποια τυπική μέθοδος η οποία με συγκεκριμένα αλγορίθμικά βήματα παράγει σαν αποτέλεσμα μία βέλτιστη οντολογία για ένα πεδίο εφαρμογής [42]. Η μέθοδος που ακολουθήθηκε είναι η συνεργατική μέθοδος όπως αυτή περιγράφεται στο [44]. Η κεντρική ιδέα της μεθόδου αυτής είναι η δημιουργία της οντολογίας από μία ομάδα ανθρώπων οι οποία συνεργατικά και επαναληπτικά βελτιώνουν τις αρχικές τους σκέψεις για την αποτύπωση των εννοιών ενός πεδίου εφαρμογής. Η μέθοδος αυτή στηρίζεται σε μεγάλο βαθμό στα σχεδιαστικά κριτήρια και στα Πρότυπα Ασφάλειας (security standards) όπως αυτά αναφέρονται στο [45]. Τα βήματα για την δημιουργία μίας SO αναλυτικά είναι :

- 1) Υιοθέτηση βασικών σχεδιαστικών αρχών οντολογιών ασφάλειας [45], οι οποίες θα λειτουργήσουν και ως ένα πλαίσιο (framework) για την περαιτέρω πορεία.
- 2) Εύρεση των κύριων εννοιών ασφάλειας από τα πρότυπα ασφάλειας και από τις κοινές πρακτικές (security standards and best practices). Υπάρχει πλήθος βιβλιογραφίας από την οποία μπορούμε να εντοπίσουμε τις κύριες έννοιες όπως το ISO/IEC [45], το British Standard 7799 Part 2 [46] και το Common Criteria framework [47]. Παραδείγματα εννοιών που συναντά κανείς είναι οι απειλές (threats), το ρίσκο (risk), τα αγαθά (assets), και οι επιπτώσεις (impact).
- 3) Κανονικοποίηση του λεξιλογίου της οντολογίας. Από τις προαναφερθείσες πηγές υπάρχει ο κίνδυνος παρερμηνειών των εννοιών. Κάθε πηγή μπορεί να ορίζει μία έννοια κατά διαφορετικό τρόπο, όπως για παράδειγμα η έννοια ευπάθεια (vulnerability) όπου στο μεν Australian Standard Handbook of Information Security Risk Management [48], υπάρχει απευθείας σύνδεση με την έννοια αγαθό (asset), ενώ στα Common Criteria η έννοια της ευπάθειας συνδέεται έμμεσα με την έννοια αγαθό μέσω της έννοιας ρίσκο (risk).
- 4) Δημιουργία εννοιο-κεντρικών οντολογιών. Στο συγκεκριμένο βήμα γίνεται μία προσπάθεια για δημιουργία επιμέρους οντολογιών η οποίες θα έχουν ως κεντρική τάξη μία έννοια. Τέτοιες οντολογίες μπορεί να δημιουργηθούν για παράδειγμα για τις έννοιες αγαθό και ευπάθεια.
- 5) Έχοντας καταλήξει από προηγούμενα βήματα στις σχέσεις μεταξύ των εννοιών μπορούμε στην συνέχεια να διασυνδέσουμε τις επιμέρους οντολογίες της έννοιας ευπάθεια και της έννοιας αγαθό σε μίας κεντρική Security Ontology επεκτείνοντάς την ταυτόχρονα όπου αυτό απαιτείται.
- 6) Ελέγχουμε και διορθώνουμε το λεξιλόγιο για τυχόν παραλείψεις στις ιδιότητες των εννοιών, στις σχέσεις μεταξύ των ή ακόμα και σε παραλείψεις κεντρικών εννοιών.
- 7) Τέλος το τελικό μοντέλο της SO ελέγχεται για τις πραγματικές δυνατότητες απεικόνισης των απαιτήσεων ασφάλειας μέσω του διαλόγου. Σε περίπτωση που η SO δεν καλύπτει τις ανάγκες μας επιστρέφουμε στο βήμα 2.

Όπως αναφέρεται στο βήμα δύο, είναι απαραίτητο να οριστούν οι βασικές έννοιες/τάξεις του μοντέλου. Για το σκοπό αυτό, χρησιμοποιήσαμε το πρότυπο ασφάλειας British Standard 7799 (BS7799) και το μοντέλο Common Information

Model (CIM). Το CIM είναι ένα πληροφοριακό μοντέλο, μια εννοιολογική όψη του περιβάλλοντος, που χρησιμοποιείται για την περιγραφή και διαχείριση υπολογιστικών και επιχειρησιακών οντοτήτων σε εταιρικά και μη περιβάλλοντα. Έχει δημιουργηθεί από την DMTF (Distributed Management Task Force) [50]. Για να επιτύχει το στόχο του, στηρίζεται στις αρχές της αντικειμενοστραφούς θεωρίας. Το μοντέλο CIM χωρίζεται σε τρία μεγάλα τμήματα, το Specification (προδιαγραφή), το Meta-Schema (μετά-σχήμα) και το Schema (Σχήμα).

Το specification κομμάτι ορίζει το συντακτικό και τους κανόνες που χρησιμοποιούνται για την απεικόνιση της γνώσης. Περιγράφει ένα αντικειμενοστραφές μετά-μοντέλο, το οποίο στηρίζεται στην Unified Modeling Language (UML). Το μοντέλο αυτό περιλαμβάνει εκφράσεις για τα κυριότερα στοιχεία (common elements) τα οποία πρέπει να παρουσιάζονται ξεκάθαρα και διαφανώς σε εφαρμογές διαχείρισης. Τέτοια στοιχεία μπορεί να είναι οι κλάσεις (classes), οι ιδιότητες των αντικειμένων (properties of classes) και οι μέθοδοι (methods). Στην παρακάτω εικόνα απεικονίζεται η δομή του μοντέλου CIM. Οι συνδέσεις με κόκκινο χρώμα δηλώνουν την συσχέτιση μεταξύ των αντικειμένων, με μπλε χρώμα την κληρονομικότητα και με πράσινο χρώμα σχέσεις συνόλου⁹.

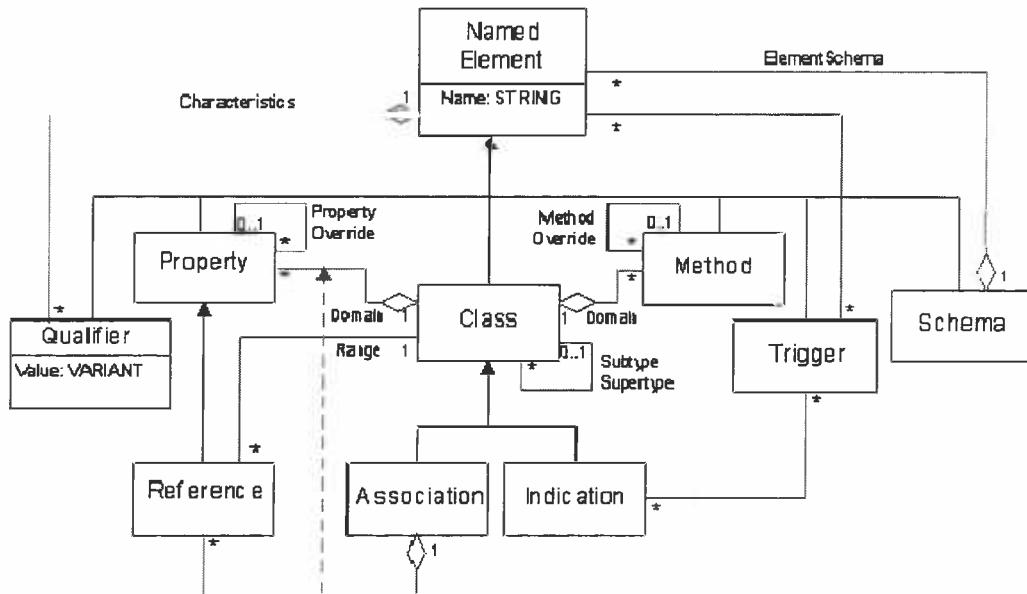


Εικόνα 3 : Αναπαράσταση του μοντέλου CIM

Το επόμενο τμήμα του CIM μοντέλου είναι το μετά-Σχήμα. Το τελευταίο αποτελεί τον ορισμό του πληροφοριακού μοντέλου CIM. Καθορίζει τους όρους που

⁹ Η επεξήγηση των χρωμάτων είναι απαραίτητη μιας και θα χρησιμοποιηθεί κατόπιν.

χρησιμοποιούνται στο μοντέλο καθώς και τις μεταξύ τους σχέσεις. Στην παρακάτω εικόνα φαίνεται το μέτα-Σχήμα.



Εικόνα 4 : CIM Meta Schema

Τα συστατικά του είναι τα Σχήματα (Schemas), οι Κλάσεις (Classes), οι Ιδιότητες (Properties), και οι Μέθοδοι (Methods).

To Schema με την σειρά του αποτελείται από δύο βασικά τμήματα, το Core Model, το Common Model. Επέκτασή του είναι το Extension Model. Είναι δομημένο με τέτοιο τρόπο ώστε το περιβάλλον διαχείρισης να αντιμετωπίζεται ως μία συλλογή από επιμέρους συσχετιζόμενα συστήματα. Το CIM Schema παρέχει ένα σύνολο από κλάσεις, ιδιότητες αυτών καθώς και τις σχέσεις μεταξύ των κλάσεων. Μέσω αυτού του σχήματος καθίσταται δυνατή η διαχείριση της πληροφορίας. Αναφορικά με τα τρία μοντέλα έχουμε :

- **Core Model** : Το συγκεκριμένο μοντέλο περιλαμβάνει τις έννοιες που είναι εφαρμόσιμες σε όλες τις περιοχές της διαχείρισης των πληροφοριακών συστημάτων. Το Core Model είναι ένα σύνολο από τάξεις, σχέσεις μεταξύ αυτών και ιδιοτήτων αυτών, και παρέχει ένα βασικό λεξιλόγιο των τάξεων αυτών.



Εικόνα 5 : Βασικές θεματικές ενότητες του Core Model

- Common Model : Γύρω από το Core Model (Εικόνα 5) υπάρχουν τα common models. Τα μοντέλα αυτά είναι πληροφοριακά μοντέλα που καταγράφουν έννοιες σχετικές με ένα αγαθό προς διαχείριση, ανεξάρτητες (έννοιες) όμως από οποιαδήποτε τεχνολογία ή υλοποίηση. Παραδείγματα τέτοιων μοντέλων, όπως αυτά απεικονίζονται και στην παραπάνω εικόνα είναι τα Systems, Applications, User και άλλα.

Τέλος, προέκταση του CIM Schema (Core model + Common Model) αποτελεί το Extension Schema. Το τελευταίο αντιπροσωπεύει προεκτάσεις του μοντέλου που εμπίπτουν σε κάποια συγκεκριμένη τεχνολογία. Τα σχήματα αυτά είναι συγκεκριμένα ανάλογα με το περιβάλλον στο οποίο εφαρμόζονται όπως για παράδειγμα τα λειτουργικά συστήματα των προς εξέταση υπολογιστών ενός δικτύου.

Συμπερασματικά λοιπόν το CIM αποτελεί μία καλή αρχή για την δημιουργία της οντολογίας ασφάλειας. Οι έννοιες που περιγράφει και αναπαριστά αποτελούν μεγάλο μέρος των σύγχρονων πληροφοριακών συστημάτων, επιτρέποντας έτσι την πλήρη περιγραφή ενός επιχειρησιακού/οργανωσιακού περιβάλλοντος. Παρέχει ένα δομημένο τρόπο αναπαράστασης της γνώσης περί στοιχείων διαχείρισης ενός πληροφοριακού συστήματος, μεταξύ των οποίων και της έννοιας της ασφάλειας. Επιπλέον αποτελεί κοινά αποδεκτό μοντέλο γεγονός που καθιστά εύκολη την επέκτασή του και την ενσωμάτωσή του με άλλα μοντέλα. Ακόμη το CIM είναι γραμμένο σε γλώσσα MOF η οποία μπορεί πολύ εύκολα να ενσωματωθεί σε όλες τις γλώσσες οντολογιών όπως αυτές παρουσιάστηκαν στην ενότητα 1.2.2.

Όπως προαναφέρθηκε το CIM αποτελεί ένα πληροφοριακό μοντέλο περιγραφής και διαχείρισης υπολογιστικών και επιχειρησιακών οντοτήτων σε εταιρικά και μη περιβάλλοντα. Το αρχικό σχήμα του CIM δίνει τις κατευθυντήριες γραμμές για κάποιον ο οποίος προσπαθεί να αναπαραστήσει τυπικά τις έννοιες ενός ολοκληρωμένου πληροφοριακού συστήματος. Οι θεματικές ενότητες του Common Model που απεικονίζονται στην Εικόνα 5 δεν υπεισέρχονται σε βάθος σε θέματα διαχείρισης ασφάλειας. Συνεπώς για την δημιουργία μίας ολοκληρωμένης οντολογίας ασφάλειας απαιτείται η εξέταση και ενός προτύπου για την διαχείριση της ασφάλειας των πληροφοριακών συστημάτων, όπως το British Standard 7799, το οποίο προαναφέρθηκε στην αρχή της παραγράφου 2.2.1.

Το πρότυπο BS7799 χωρίζεται σε δύο μέρη, το *BS 7799-1 Information Technology* και το *BS 7799-2 Information Security Management Systems*:

- *BS 7799-1 Information Technology*. Κώδικας Πρακτικών για τη Διαχείριση Ασφάλειας των Πληροφοριών (Code of practice for information security management). Το πρώτο μέρος είναι επίσης γνωστό ως BS ISO/IEC 17799,
- *BS 7799-2 Information security management systems*. Συστήματα Διαχείρισης Ασφάλειας Πληροφορίας. Το δεύτερο μέρος χρησιμοποιείται για σκοπούς ελέγχου και πιστοποίησης.

Αναφορικά με το πρώτο μέρος, αυτό παρέχει ένα σύνολο από κατευθυντήριες γραμμές για υλοποίηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών ή όπως ονομάζεται ISMS (Information Security Management System). Μετά την υιοθέτησή του από αρκετές εταιρίες και οργανισμούς, στο τέλος του 2000 το μοντέλο αυτό προτυποποιήθηκε με την ονομασία ISO/IEC 17799. Στην ουσία το ISO/IEC 17799 έχει σαν στόχο την παροχή μίας κοινής βάσης για την ανάπτυξη οργανωσιακών προτύπων στον τομέα της ασφάλειας και την αποτελεσματική διαχείριση των πολιτικών ασφαλείας. Επιπλέον η πρόθεσή του είναι ο ορισμός των κυριότερων θεματικών ενοτήτων που πρέπει μία εταιρία να εστιάσει την προσοχή της και όχι η εισήγηση συγκεκριμένων λύσεων σε μία θεματική περιοχή, για παράδειγμα πρόταση ειδικού αλγορίθμου κρυπτογράφησης. Κάθε οργανισμός που σκοπεύει να χρησιμοποιήσει το πρότυπο αυτό, πρέπει να ορίσει τις απαιτήσεις ασφάλειας που θέλει να έχει. Οι πηγές από όπου μπορεί και πρέπει να αντλήσει πληροφορία για τον σκοπό αυτό, ανεξάρτητα από οποιοδήποτε πρότυπο είναι η αποτίμηση των κινδύνων



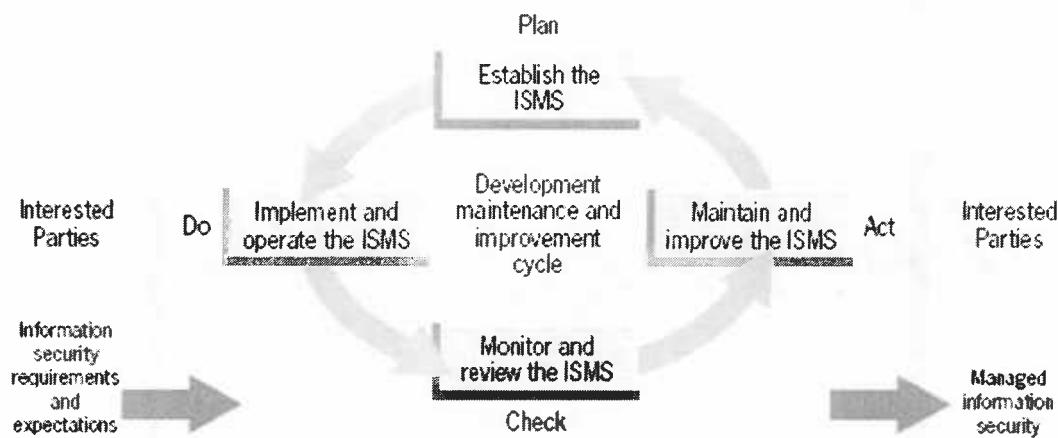
ενός οργανισμού, οι νομικές και ρυθμιστικές απαιτήσεις και τέλος ένα σύνολο από αρχές και απαιτήσεις για οποιαδήποτε μορφής πληροφορία αποτελεί ιδιοκτησία της εταιρίας. Το BS 7799 Part-1 είναι δομημένο κατά τέτοιο τρόπο ώστε να καλύπτει τις προαναφερθείσες πηγές. Παρέχει ένα σύνολο από ελέγχους για κάθε θεματική ενότητα. Από το σύνολο των ελέγχων που παρέχονται, η εταιρία που εφαρμόζει το πρότυπο αυτό επιλέγει εκείνους που θα την οδηγήσουν σε ένα ικανοποιητικό επίπεδο ασφάλειας σε όλους τους τομείς. Οι θεματικές ενότητες που καλύπτει το BS 7799 Part-1 είναι οι ακόλουθες [48], [50]:

- Security Policy (Πολιτική Ασφάλειας) : Σε αυτή την θεματική ενότητα περιλαμβάνεται η εξέταση της πολιτικής ασφάλειας των πληροφοριών. Στόχος του ελέγχου είναι η υποστήριξη και η καθοδήγηση του Οργανισμού/Εταιρίας στο κομμάτι της ασφάλειας πληροφοριών.
- Security Organization (Ασφάλεια Οργανισμού) : Περιλαμβάνονται η υποδομή ασφάλειας πληροφοριών, η ασφάλεια πρόσβασης εξωτερικών συνεργατών και τέλος ασφάλεια σε θέματα outsourcing¹⁰. Αντίστοιχα, οι στόχοι που τίθενται είναι η διαχείριση της ασφάλειας της πληροφορίας από άτομα του ίδιου οργανισμού, από τρίτους που έχουν πρόσβαση σε αυτή και τέλος όταν η επεξεργασία της πληροφορίας έχει ανατεθεί σε τρίτους.
- Asset Classification and Control (Κατηγοριοποίηση και Έλεγχος Πόρων) : Στην συγκεκριμένη θεματική ενότητα περιλαμβάνονται οι έλεγχοι για την διατήρηση της προστασίας των εταιρικών πόρων (Accountability for Assets) καθώς και ελέγχους διαβεβαίωσης ότι οι πληροφοριακοί πόροι τυγχάνουν κατάλληλα επίπεδα προστασίας (Information Classification).
- Personnel Security (Ασφάλεια Προσωπικού) : Η συγκεκριμένη θεματική ενότητα περιλαμβάνει ελέγχους που αφορούν στο κατά πόσο οι υπάλληλοι της εταιρίας έχουν εκπαιδευτεί για την αντιμετώπιση συμβάντων παραβίασης της ασφάλειας. Επιπλέον ένας ακόμη στόχος είναι η διαβεβαίωση των κινδύνων που οφείλονται σε ανθρώπινα λάθη, εσκεμμένα και μη, καθώς και έλεγχοι που αφορούν στην διαβεβαίωση ότι οι χρήστες γνωρίζουν τους πιθανούς κινδύνους σχετικά με τις απειλές των πληροφορικών πόρων.

¹⁰ Outsource : Η διαδικασία κατά την οποία μια οντότητα αναθέτει σε τρίτο να παράξει ένα κομμάτι της εργασίας της. Για παράδειγμα στην διαδικασία παραγωγής ενός αυτοκινήτου, το ρόλο που πιθανά να ενσωματωθεί στον πίνακα ελέγχου να μην έχει κατασκευαστεί από την ίδια εταιρία.

- Physical and Environmental Security (Φυσική και Περιβαλλοντική Ασφάλεια): Σε αυτή την θεματική ενότητα υπάρχουν οι εξής περιοχές προς έλεγχο, οι ασφαλής περιοχές (Secure Areas), η ασφάλεια εξοπλισμού (Equipment Security) και οι γενικοί έλεγχοι. Οι στόχοι είναι οι προληπτικές ενέργειες για την αποφυγή της μη-εξουσιοδοτημένης πρόσβασης, η πρόληψη απώλειας ή ζημιάς και η πρόληψη έκθεσης σε κίνδυνο (σε οποιαδήποτε μορφή του) της πληροφορίας, αντίστοιχα.
- Communication and Operations Management (Διαχείριση Επικοινωνιών και Λειτουργιών) : Μία από τις μεγαλύτερες θεματικές ενότητες. Μερικοί από τους στόχους είναι η μείωση του κινδύνου βλάβης του συστήματος, η προστασία της ακεραιότητας του συστήματος, η σωστή διαχείριση των δικτύων και η διαβεβαίωση της ορθής λειτουργίας των επιχειρησιακών διαδικασιών.
- Access Control (Ελεγχος Πρόσβασης) : Μία ακόμη εκτενής θεματική ενότητα. Σε αυτή περιλαμβάνονται στόχοι όπως αποφυγή μη-εξουσιοδοτημένης πρόσβασης στους πόρους ενός πληροφορικού συστήματος, όπως οι χρήστες, η εφαρμογές, οι υπολογιστές κ.α., η προστασία των δικτυακών πόρων και ο εντοπισμός της μη-εξουσιοδοτημένης πρόσβασης.
- System Development and Maintenance (Ανάπτυξη και Συντήρηση Συστημάτων) : Στόχοι της συγκεκριμένης θεματικής ενότητας είναι η αποφυγή απώλειας ή αλλαγής των δεδομένων των χρηστών σε συστήματα εφαρμογών, η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών που επεξεργάζονται και ανταλλάσσουν οι χρήστες στο εταιρικό περιβάλλον, και γενικότερα η διασφάλιση ότι τα έργα πληροφορικής και οι υποστηρικτικές διαδικασίες λαμβάνουν χώρα ασφαλώς.
- Business Continuity Management (Διαχείριση Επιχειρησιακής Συνέχειας) : Βασικός στόχος της θεματικής ενότητας είναι η κατά το δυνατόν εξάλειψη των διακοπών στην ροή των επιχειρησιακών διεργασιών και η προστασία των κρίσιμων δραστηριοτήτων της εταιρίας.
- Compliance (Συμμόρφωση) : Στην τελευταία θεματική ενότητα περιλαμβάνονται στόχοι όπως η διαβεβαίωση της συμβατότητας των συστημάτων με τις πολιτικές ασφάλειας που έχουν καθοριστεί και η αποφυγή παραβιάσουν των νομικών καθεστώτων και συμβάσεων, που ισχύουν στην έδρα της εταιρίας, για τις απαιτήσεις ασφάλειας.

Το δεύτερο τμήμα του British Standard (BS 7799 Part-2), παρέχει μία βασική υποδομή για εξωτερικό έλεγχο και από το 2002 και μετά εναρμονίζεται και με τα υπόλοιπα πρότυπα διαχείρισης συστημάτων όπως το ISO 9001. Βασικό στοιχείο του τμήματος αυτού είναι η εισαγωγή του μοντέλου Plan-Do-Check-Act (PDCA) ως προσέγγιση για την διαχείριση, ανάπτυξη, βελτίωση και συντήρηση συστημάτων ISMS (Information Security Management System) τα οποία εμφανίζονται στο πρώτο κομμάτι του British Standard 7799.



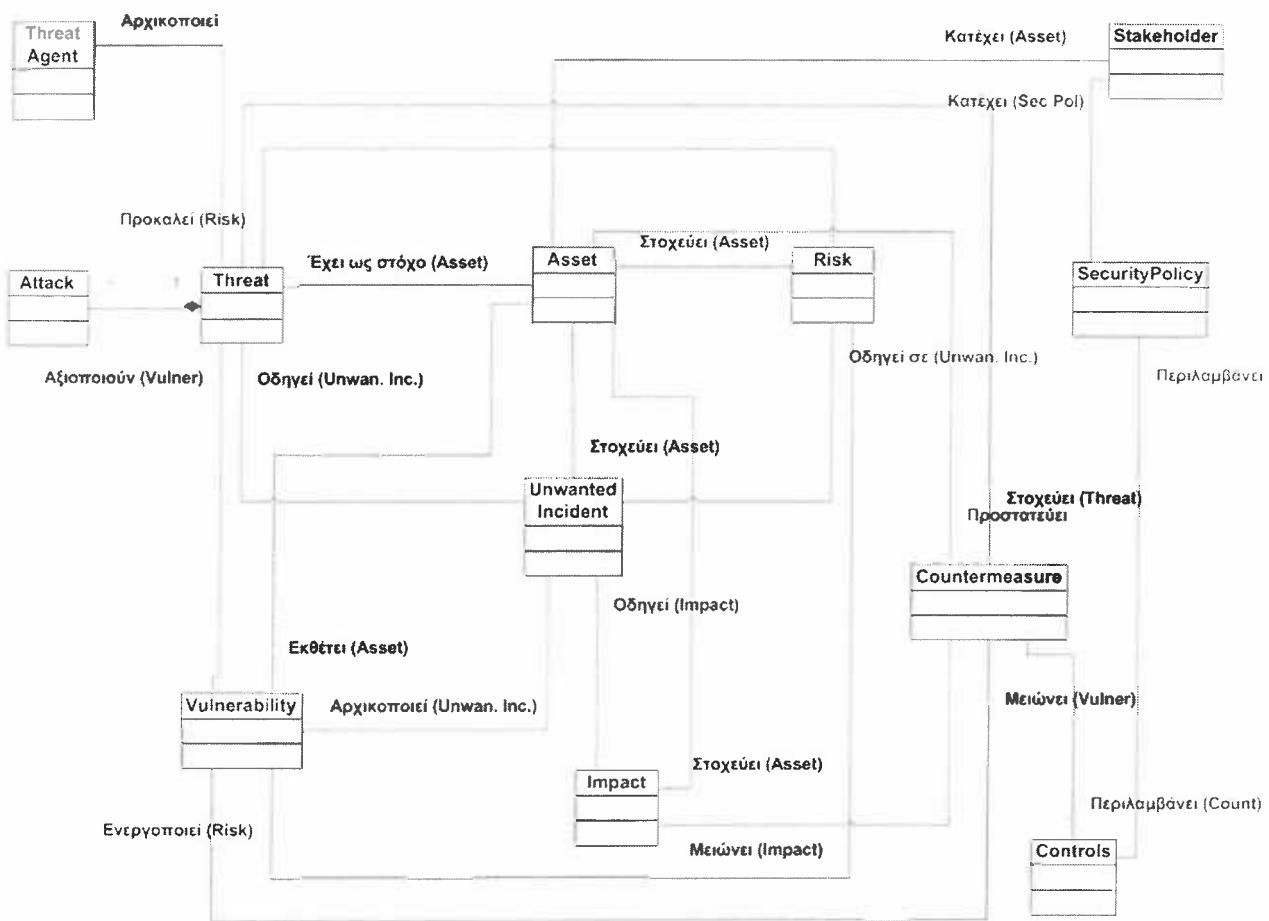
Εικόνα 6 : Plan-Do-Check-Act Model (PDCA)

Τα βασικά βήματα του μοντέλου αυτού, όπως αυτά διακρίνονται και από την Εικόνα 6, είναι τα εξής :

- Βήμα 1 (Plan) : Εγκατάσταση ενός ISMS συστήματος
- Βήμα 2 (Do) : Η υλοποίηση και η λειτουργία του ISMS
- Βήμα 3 (Check) : Ο έλεγχος και η επανεξέταση του συστήματος
- Βήμα 4 (Act) : Συντήρηση και βελτίωση του ISMS.

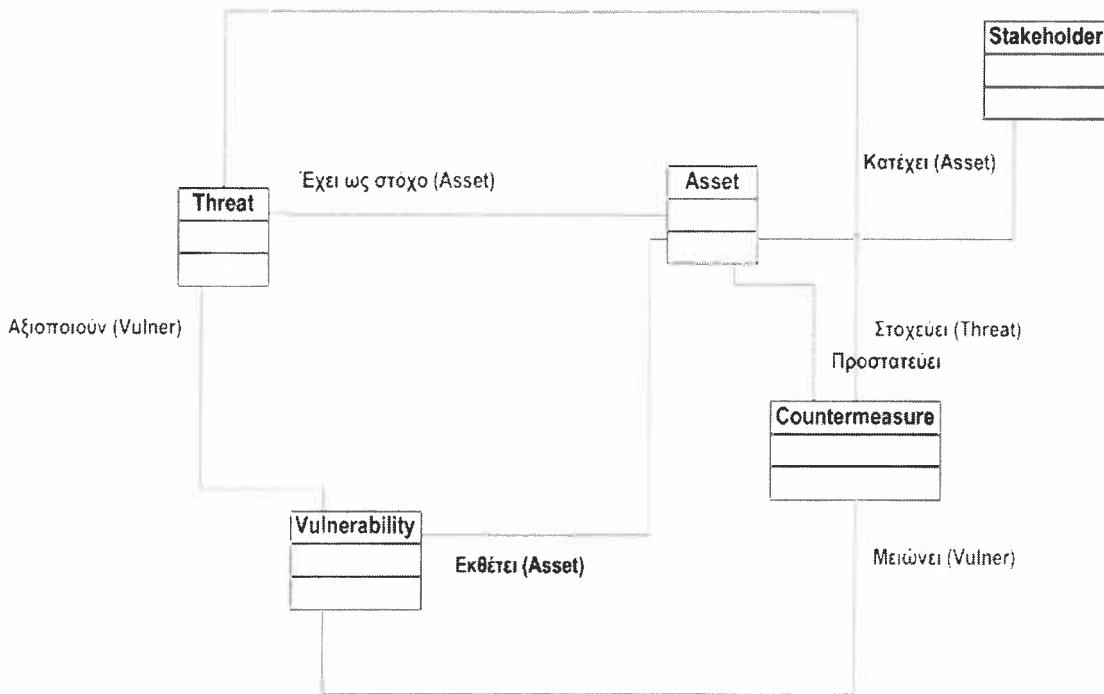
Από το πρότυπο BS 7799, θα εστιάσουμε την προσοχή μας στο πρώτο τμήμα αυτού, μιας και το δεύτερο αφορά στη δημιουργία και συντήρηση ενός ISMS συστήματος, που είναι εκτός του εύρους της συγκεκριμένης εργασίας. Στη συνέχεια της παραγράφου παρουσιάζουμε την οντολογία ασφάλειας που στηρίζεται στις δύο προαναφερθείσες πηγές, το πρότυπο BS 7799 Part-1 (ISO/IEC 17799) και το μοντέλο CIM (Common Information Model) από την DMTF.

Στην παρακάτω εικόνα παρουσιάζουμε τις κεντρικές έννοιες που αποτυπώνονται στην οντολογία. Στην ουσία πρόκειται για ένα μοντέλο αποτίμησης της επικινδυνότητας με χρήση εννοιών όπως αυτές ορίζεται από το πρότυπο BS 7799 Part-1. Συγκεκριμένα η αποτίμηση της επικινδυνότητας ορίζεται ως η αποτίμηση των απειλών, των επιπτώσεων και των αδυναμιών των πληροφοριών, και η πιθανότητα εμφάνισής τους. Το αρχικό μοντέλο απεικονίζεται παρακάτω.



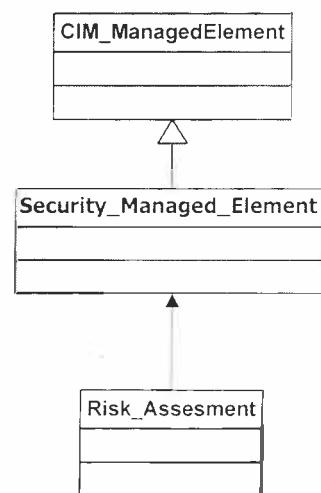
Εικόνα 7 : Αρχικό Μοντέλο Οντολογίας Ασφάλειας

Στην παρούσα εργασία ενδιαφερόμαστε μόνο για μερικές από τις παραπάνω έννοιες. Οι έννοιες που μας αφορούν είναι το Asset (Αγαθό), ο Stakeholder (Ιδιοκτήτης), το Vulnerability (Ευπάθεια), το Countermeasure (Αντίμετρο) και το Threat (Απειλή). Έτσι για λόγους απλότητας από το αρχικό μοντέλο καταλήγουμε στο απλούστερο στην Εικόνα 8. Οι χρωματισμοί των συνδέσεων των τάξεων και στο αρχικό μοντέλο αλλά και στο εκλεπτυσμένο ακολουθούν το μοντέλο CIM (Εικόνα 3).

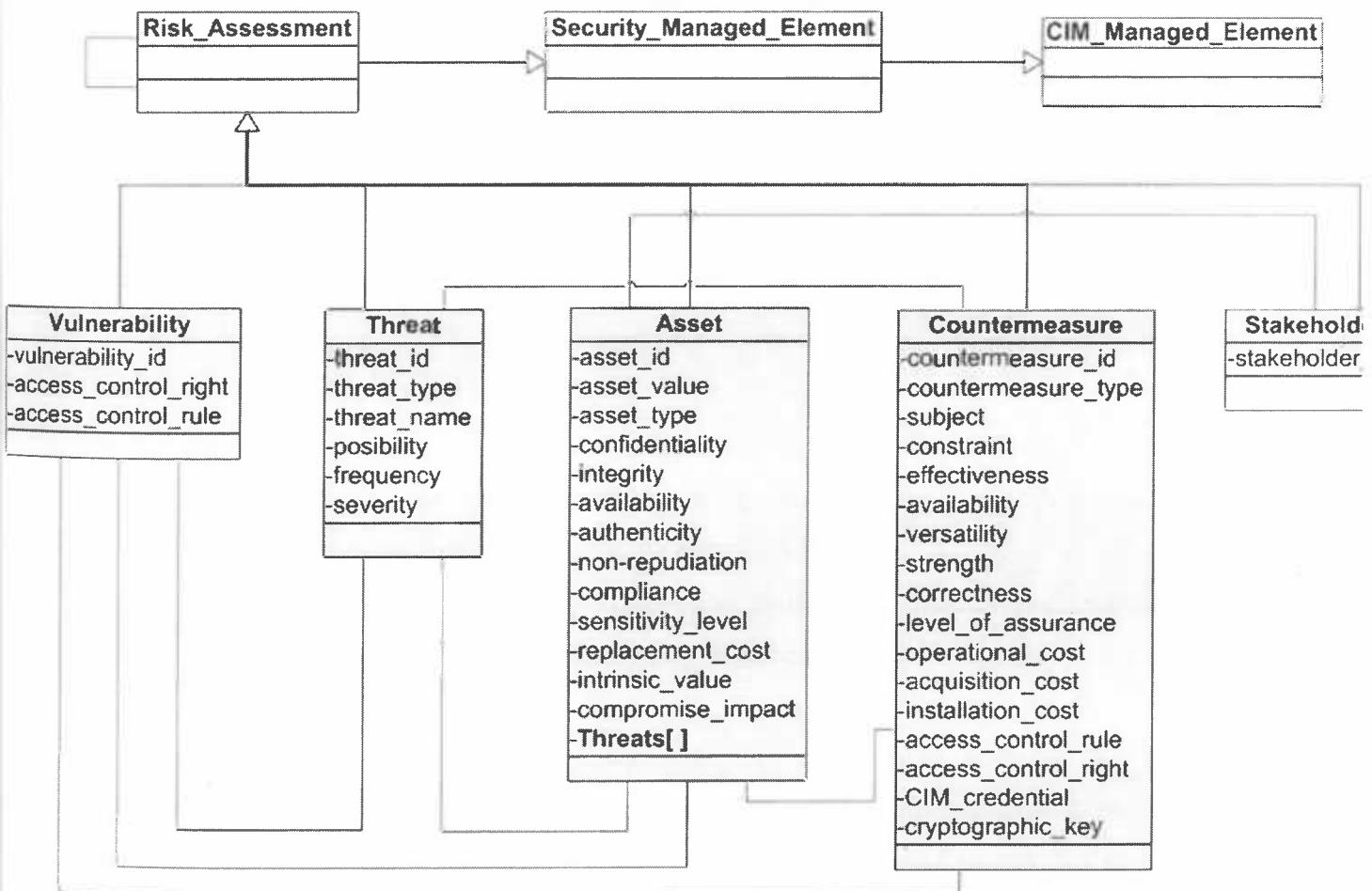


Εικόνα 8 : Εκλεπτυσμένο Μοντέλο

Όπως ήδη έχει αναφερθεί, μία από τις πηγές για την δημιουργία της οντολογίας είναι το μοντέλο CIM. Η οντολογία που παρουσιάζεται στην Εικόνα 8 μπορεί να ενσωματωθεί σε ένα κομμάτι του μοντέλου αυτού. Στο μοντέλο CIM, και συγκεκριμένα στα Core Model, υπάρχει η έννοια του *CIM_ManagedElement*. Το τελευταίο αποτελεί μία βασική τάξη η οποία περιγράφει όλες τις έννοιες που μπορούν να αναπαρασταθούν στον τομέα της διαχείρισης πληροφοριακών συστημάτων. Σκοπός μας είναι η ένταξη του μοντέλου που δημιουργήθηκε για την διαχείριση της ασφάλειας κάτω από αυτή την τάξη. Για το λόγο αυτό δημιουργήσαμε μία επιπλέον τάξη την *Security_Managed_Element* η οποία είναι υποκλάση της *CIM_ManagedElement* και υπερκλάση όλων των έννοιών που εισήγαμε παραπάνω. Η έννοια *Security_Managed_Element* περιγράφει τις έννοιες που αφορούν στην διαχείριση της ασφάλειας. Επιπλέον δημιουργήθηκε μία τάξη *Risk_Assessment* η οποία συμβολίζει την έννοια της αποτίμησης της ασφάλειας. Κάτω από αυτή υπάρχουν οι τάξεις Asset, Threat, Vulnerability, Countermeasure και Stakeholder.



Συνεπώς όλες οι τάξεις του μοντέλου κληρονομούν τις ιδιότητες της τάξης Risk_Asessment, η οποία με την σειρά της κληρονομεί τις ιδιότητες της τάξης Security_Managed_Element η οποία κληρονομεί τις ιδιότητες της κλάσης CIM_ManagedElement. Στις ακόλουθες παραγγάφους θα περιγράψουμε αναλυτικότερα την σύνδεση του μοντέλο με το μοντέλο CIM. Για λόγους ευκρίνειας οι τάξεις που προέρχονται από το μοντέλο CIM έχουν σαν πρώτο συνθετικό την συμβιολοσειρά “CIM_”. Το τελικό στάδιο στην δημιουργία της οντολογίας είναι η εισαγωγή των ιδιοτήτων για κάθε κλάση. Αυτές (οι ιδιότητες) προέρχονται από το πρότυπο BS 7799 Part-1 και από τα [53] [55]. Έτσι το μοντέλο διαμορφώνεται ως εξής :



Εικόνα 9 : Τελικό Μοντέλο Risk Assessment

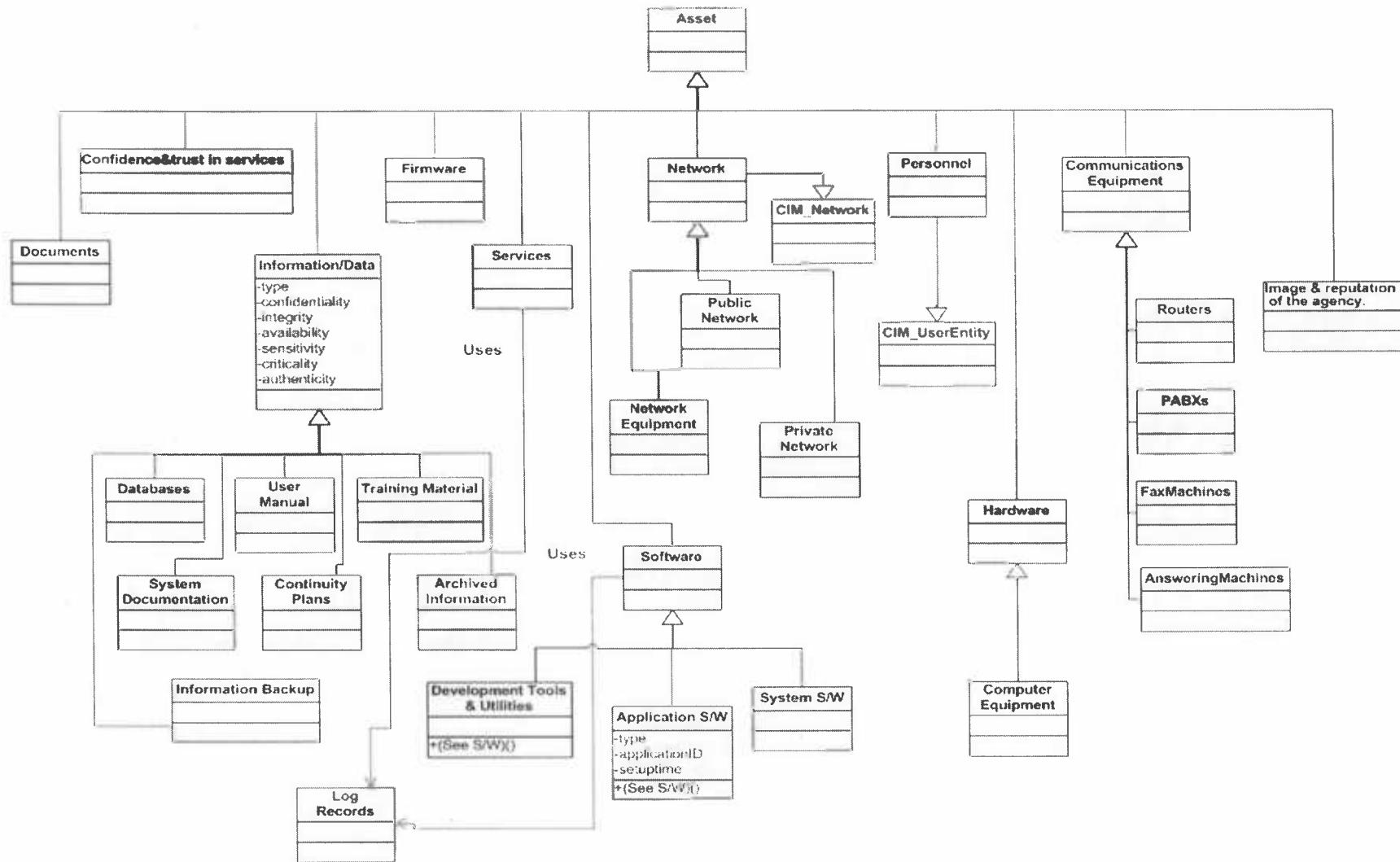
2.2.2. Λεξιλόγιο Πεδίου Ορισμού Ασφάλειας

Οι κλάσεις που παρουσιάστηκαν στην Εικόνα 9 προέκυψαν από την μελέτη του προτύπου ασφαλείας BS 7799 Part-1. Για να μπορούμε όμως να μιλήσουμε για οντολογία θα πρέπει να ορίσουμε το λεξικό των όρων που χρησιμοποιούμε στην οντολογία καθώς και τις σχέσεις μεταξύ των όρων. Στην παράγραφο αυτή παρουσιάζουμε το λεξιλόγιο και εμπλουτίζουμε την οντολογία με επιμέρους οντολογίες που αφορούν στον κάθε όρο ξεχωριστά.

Από την μελέτη των [53] και [52] αλλά και από την προσωπική αντίληψη των πραγμάτων προκύπτουν οι παρακάτω βασικοί όροι :

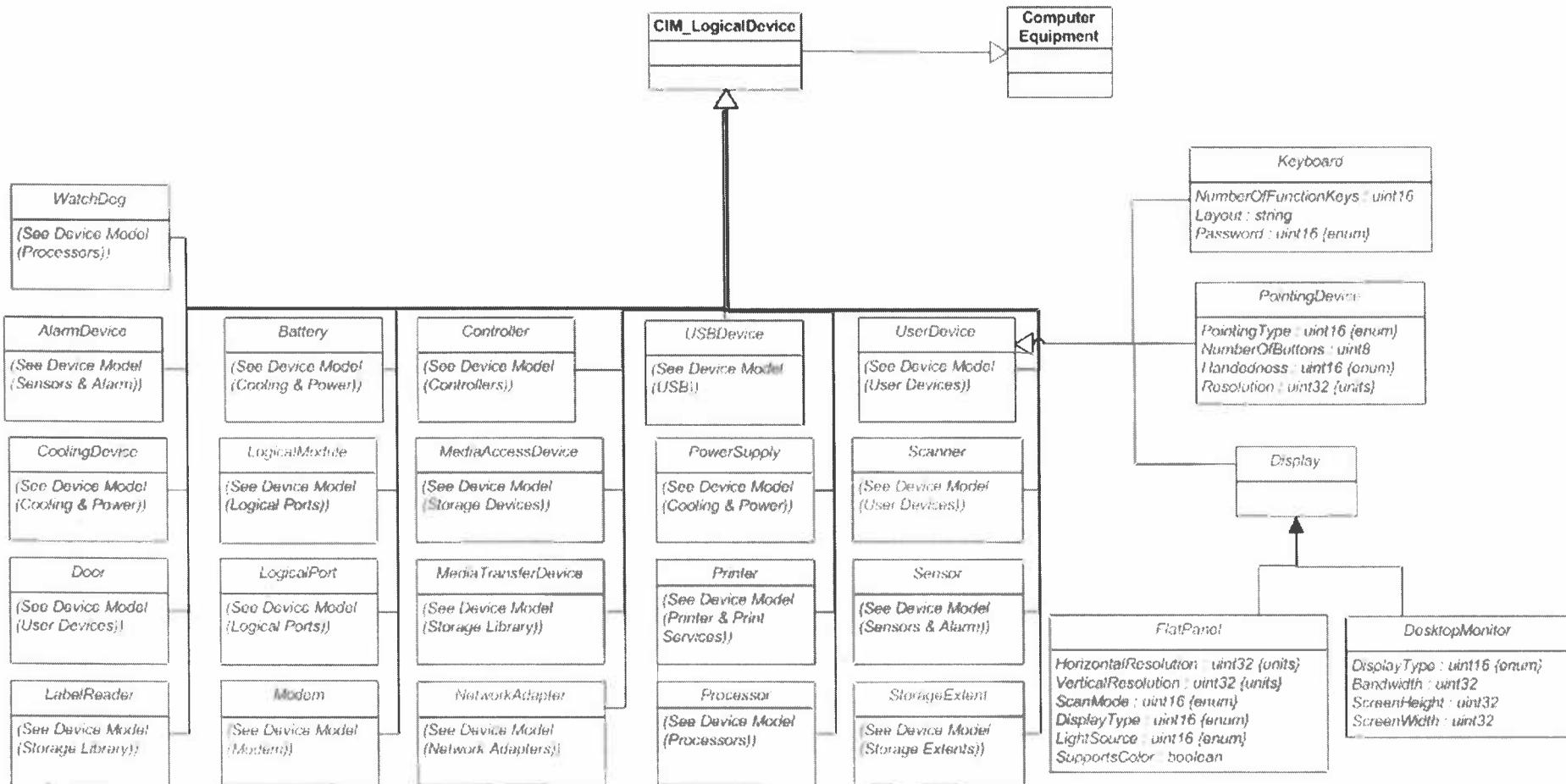
- *Αγαθό (Asset)* : Οτιδήποτε έχει αξία και αξίζει προστασίας. Μπορεί να είναι δεδομένα, μέθοδοι, υπολογιστικοί πόροι κ.α.
- *Ιδιοκτήτης (Stakeholder)* : Φυσικό ή νομικό πρόσωπο που κατέχει ή χρησιμοποιεί, αντίστοιχα, ένα αγαθό.
- *Αδυναμία (Vulnerability)* : Οποιαδήποτε αδυναμία, ευπάθεια στον σχεδιασμό, την υλοποίηση, την χρήση του πληροφοριακού συστήματος αυξάνει την πιθανότητα παραβίασης σε αυτό, η οποία προσβάλει μία από τις ιδιότητες της Ασφάλειας – Αυθεντικότητα, Διαθεσιμότητα, Εμπιστευτικότητα, Ακεραιότητα και Εγκυρότητα.
- *Απειλή (Threat)* : Πιθανή ενέργεια που εκμεταλλεύεται μία αδυναμία και μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων χαρακτηριστικών της ασφάλειας ενός πληροφοριακού συστήματος.
- *Αντίμετρο (Countermeasure)* : Ενέργειες, συσκευές, λογισμικό που έχουν ως στόχο την μείωση των αδυναμιών ενός πληροφοριακού συστήματος.

Για να γίνει πληρέστερη η οντολογία απαιτείται να αναλύσουμε περαιτέρω μερικές από τις έννοιες που υπάρχουν στο κεντρικό μοντέλο. Στην συνέχεια ακολουθούν οι επιμέρους οντολογίες για το κάθε στοιχείο ξεχωριστά. Αναφορικά με την έννοια του αγαθού, παρατηρούμε ότι αυτό μπορεί να είναι κείμενα, πληροφορία, δεδομένα, λογισμικό, υπηρεσίες κ.α. όπως αυτά φαίνονται παρακάτω.



Εικόνα 10 : Υπομοντέλο Asset

Από το παραπάνω μοντέλο διακρίνονται οι τάξεις CIM_Network και CIM_UserNetwork, στις οποίες συνδέεται το προτεινόμενο μοντέλο. Το παραπάνω μοντέλο χωρίζεται στα εξής υπομοντέλα : Computer Equipment, Network Equipment και Software. Τα τελευταία είναι :



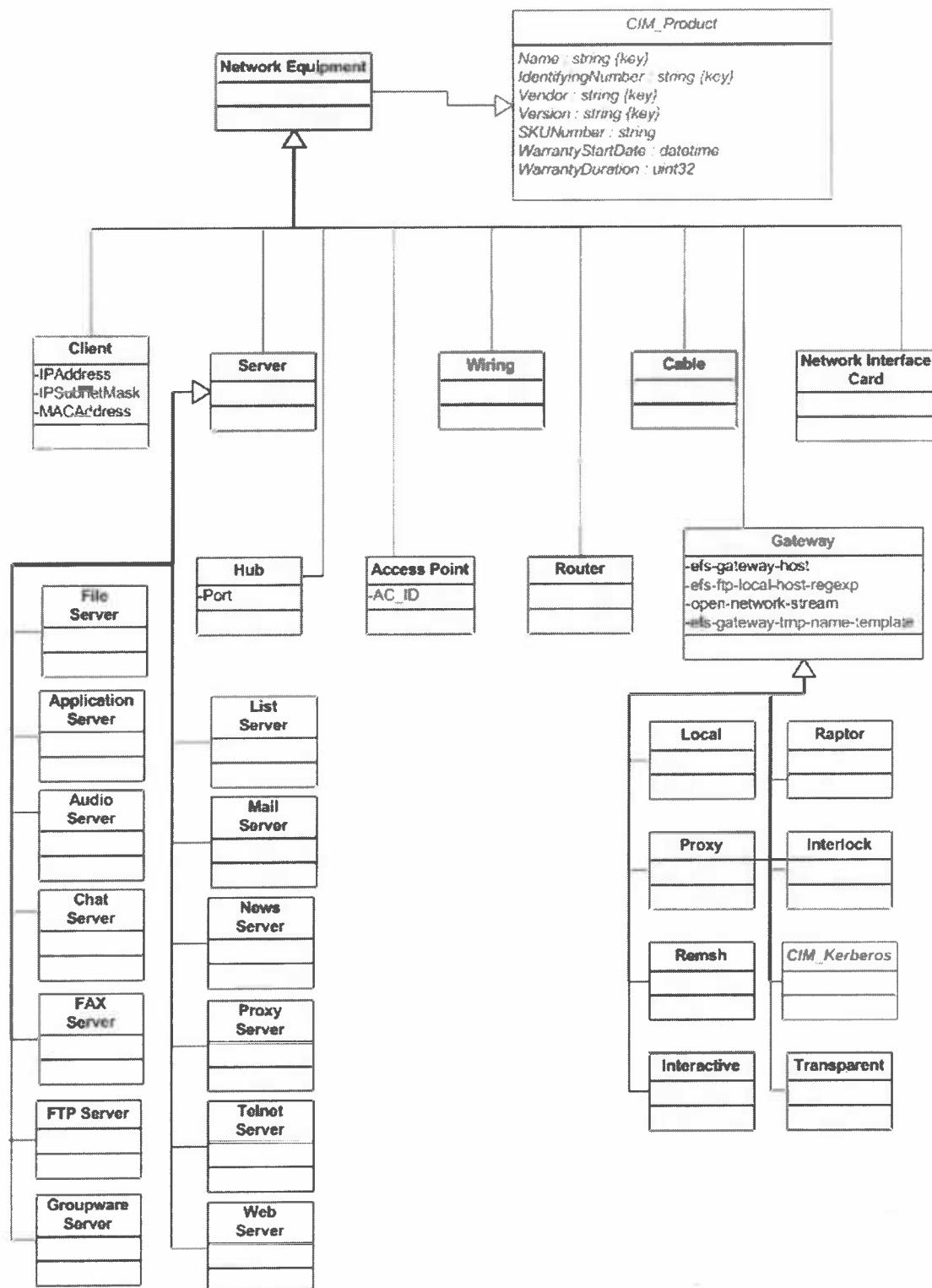
Εικόνα 11 : Computer Equipment

Στην Εικόνα 11 παρουσιάζεται η σχέση της τάξης Computer Equipment με την κλάση CIM_LogicalDevice. Η τελευταία ανήκει στο ‘Device’ common model του μοντέλου CIM. Κάτω από αυτή βρίσκονται κλάσεις όπως Modem, Network Adapter (προσαρμογέας δικτύου), Logical Port («Λογική Πόρτα»), Printer (Εκτυπωτής) και άλλα. Συνεπώς όλες αυτές οι κλάσεις αποτελούν υποκλάσεις της αρχικής κλάσης Computer Equipment.

Στη συνέχεια παρουσιάζεται το υπομοντέλο Network Equipment. Η ομώνυμη κλάση αποτελεί υποκλάση της CIM_Product, η οποία ανήκει στο core model του μοντέλου CIM. Οι βασικές κλάσης της τάξης Network Equipment είναι :

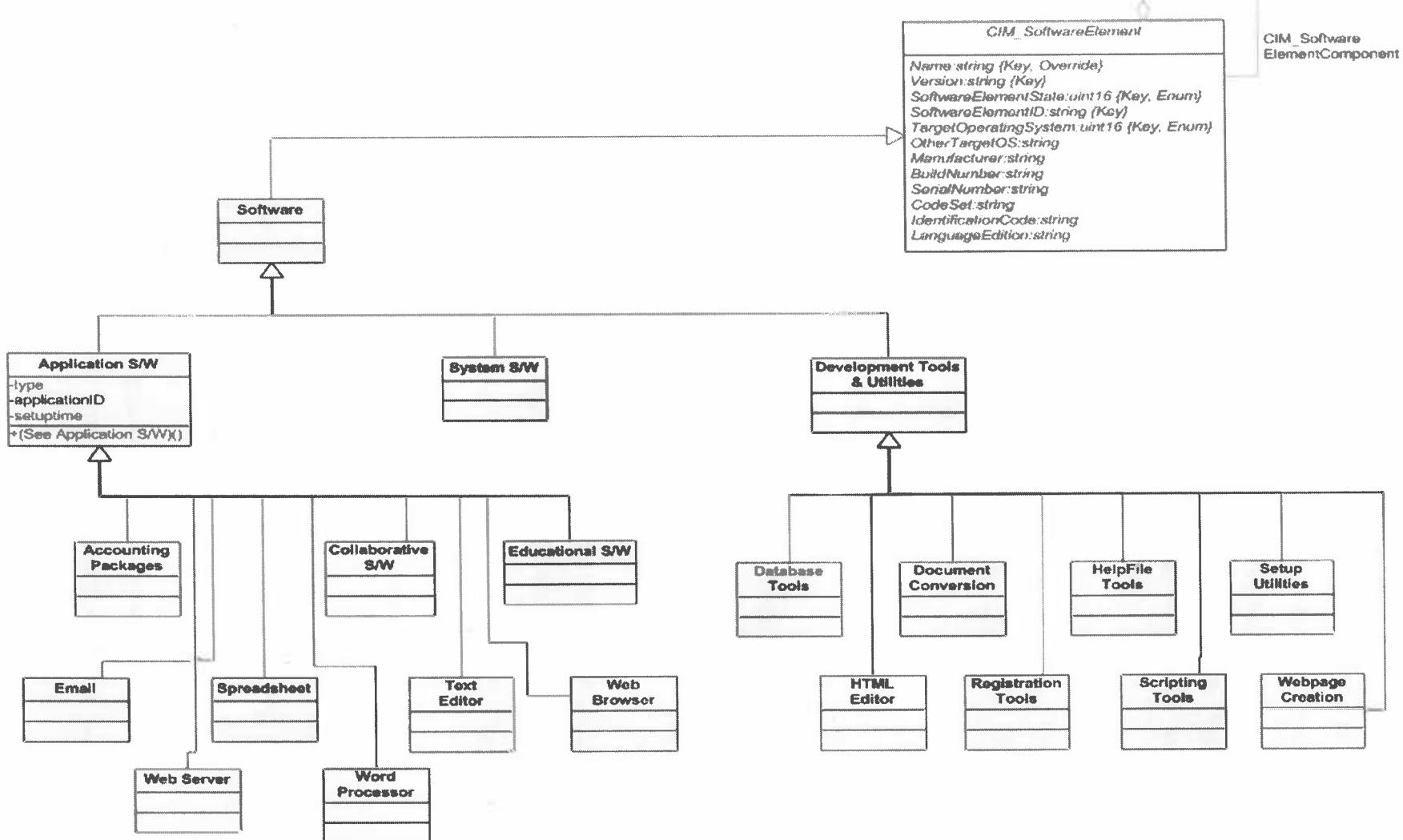
- Εξυπηρετητής (Server), ο οποίος χωρίζεται σε επιμέρους τάξεις ανάλογα με το είδος της εξυπηρέτησης που παρέχει – File Server, Mail Server κτλ.
- Access Point, σημείο πρόσβασης ασύρματων κόμβων στο δίκτυο
- Καλωδίωση (Wiring)
- Δρομολογητές (Routers), υπεύθυνοι για τις σωστές δρομολογήσεις πακέτων που ανταλλάσσονται από τους διάφορους κόμβους του δικτύου
- Gateways, «πύλες» που συνδέουν το ενδοεταιρικό δίκτυο με τον εξωτερικό κόσμο, είτε ένα άλλο εταιρικό δίκτυο είτε τον Παγκόσμιο Ιστό.
- Δικτυακές Κάρτες Υπολογιστών (Network Interface Card).

Τα παραπάνω παρουσιάζονται στην ακόλουθη εικόνα :



Εικόνα 12 : Network Equipment

Στη συνέχεια παρουσιάζεται το υπομοντέλο του Software.



Εικόνα 13 : Software

Όπως φαίνεται και από το σχήμα η κλάση Software είναι υποκλάση της CIM_SoftwareElement, η οποία προέρχεται από το “Application” common model του CIM. Η τάξη Software χωρίζεται σε τρεις βασικές υποκλάσεις, την Application Software, την System Software και την Development Tools and Utilities.

Αναφορικά με την πρώτη, αυτή χωρίζεται σε επιμέρους τάξεις όπως τα Accounting Packages, το Collaborative S/W, το Educational S/W, το Email, τα Spreadsheet, ο Text Editor, ο Web Browser, ο Web Server, ο Word Processor. Επιπλέον η τάξη Development Tools and Utilities χωρίζεται στις εξής υποκλάσεις, τα Database Tools, τα Document Conversion, τα HTML Editor, τα Registration Tools, τα Scripting Tools, τα Webpage Creation, τα Help file Tools και τα Setup Utilities.

Όσον αφορά στους τυπικούς ορισμούς των εννοιών που εμφανίζονται στο υπομοντέλο Software αυτοί έχουν ως εξής :

- Application S/W: Λογισμικό Εφαρμογών
- Spreadsheet: Λογιστικό φύλλο
- Word Processor: Επεξεργαστής κειμένου
- Text Editor: Επεξεργαστής κειμένου
- Web Browser: Φυλλομετρητής διαδικτυακών ιστοσελίδων
- Educational S/W: Εκπαιδευτικό λογισμικό, κ.λπ.
- Development Tools & Utilities: Εργαλεία και Εφαρμογές ανάπτυξης λογισμικού
- Database Tools: Εργαλεία δημιουργίας και διαχείρισης βάσεων δεδομένων
- HTML Editor: Εργαλεία δημιουργίας και επεξεργασίας HTML κώδικα
- Help File Tools: Εργαλεία δημιουργίας βοηθητικών αρχείων
- Scripting Tools: Εργαλεία δημιουργίας script κώδικα
- Webpage Creation: Εργαλεία δημιουργίας ιστοσελίδων, κ.λπ

Μία επιπλέον κλάση που αναλύεται περισσότερο είναι η Countermeasure. Τα αντίμετρα που μπορεί να εφαρμόσει κανείς σε ένα πληροφοριακό σύστημα χωρίζονται στις εξής μεγάλες κατηγορίες,

- Intrusion Detection Systems : Τα συγκεκριμένα συστήματα αποτελούν Συστήματα Αναγνώρισης Εισβολής. Για να επιτύχουν τον σκοπό αυτό εντοπίζουν τυχόν ανωμαλίες στο πληροφοριακό σύστημα καθώς και τον



εκάστοτε χρήστη που προκαλεί μία αλλαγή σε ένα αγαθό του πληροφοριακού συστήματος.

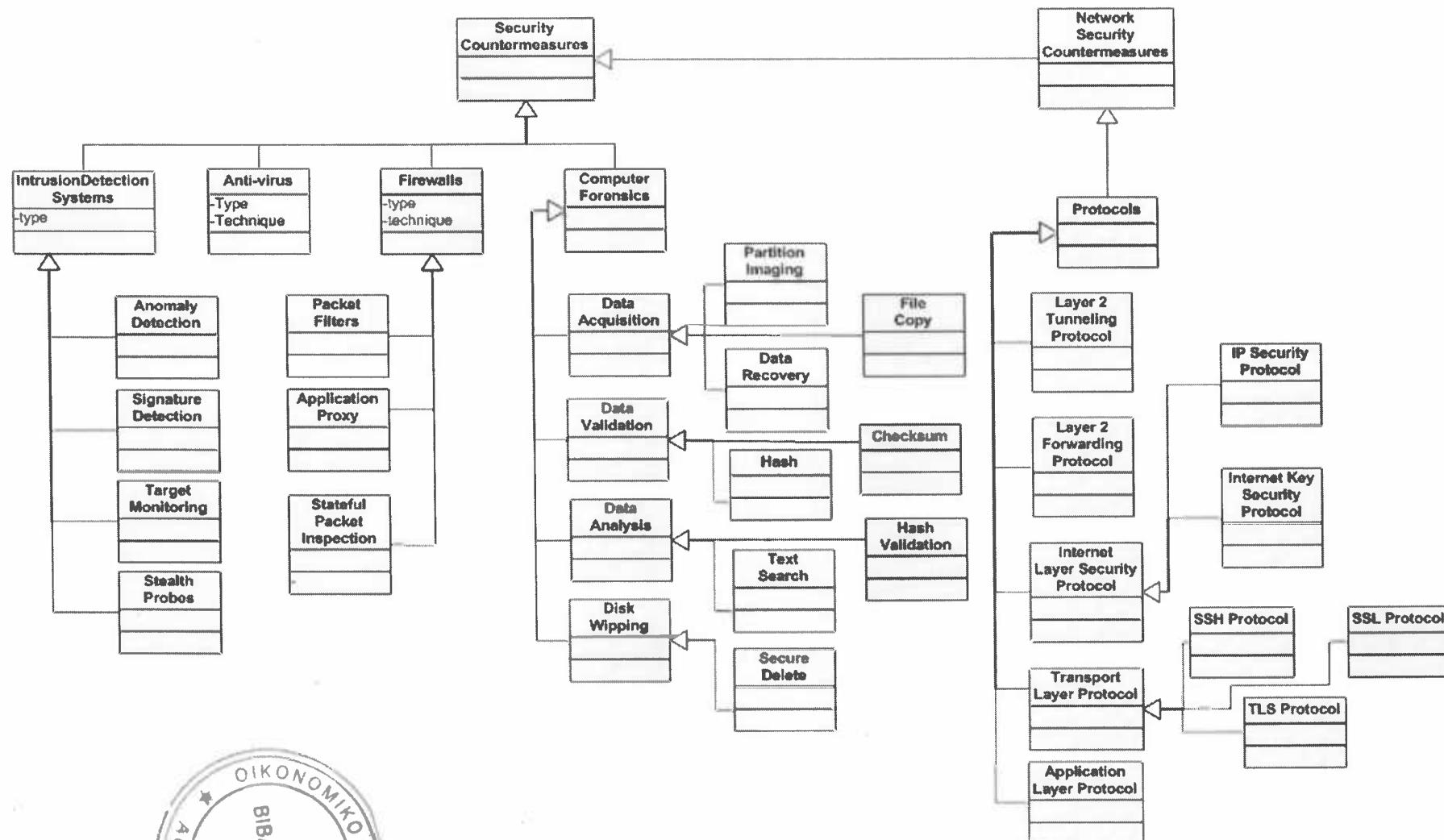
- Firewalls : Τοίχος Προστασίας. Τα firewall είναι είτε λογισμικό, είτε υλικό το οποίο απαγορεύει μη εξουσιοδοτημένη πρόσβαση σε πόρους και αγαθά του συστήματος.
- Computer Forensics : Εργαλεία και υλοποιήσεις που απαιτούνται για την κρυπτογράφηση των δεδομένων, την δημιουργία αντιγράφων ασφαλείας και συναφείς ενέργειες.
- Antivirus : Αντιβιοτικά. Λογισμικό το οποίο προστατεύει τους υπολογιστές από ιομορφικά λογισμικά.
- Network Security Countermeasures : Αντίμετρα που αφορούν στην υποδομή του δικτύου. Για κάθε επίπεδο της αρχιτεκτονικής OSI (εφτά επίπεδα) υπάρχουν τα αντίμετρα που μπορούν να εφαρμοστούν με στόχο την προστασία του κάθε επιπέδου ξεχωριστά. Για παράδειγμα, tunneling protocols επιπέδου 2, forwarding protocols επιπέδου 2, πρωτόκολλα ασφαλείας στο επίπεδο εφαρμογής, στο επίπεδο TCP/IP κ.ο.κ.

Τέλος στο υπομοντέλο που αφορά στις απειλές παρατηρούμε τα ακόλουθα όσον αφορά την κατηγοριοποίηση των τελευταίων:

- Σκόπιμη Απειλή : Αφορά σε απειλές που προέρχονται από κακόβουλους για την διατάραξη της λειτουργίας του πληροφοριακού συστήματος. Μερικές από αυτές είναι η Denial of Service, η Eavesdropping, IoI, Ιομορφικό λογισμικό, Δούρειοι Ίπποι κ.α.
- Συμπωματική Απειλή : Άλλιώς μπορούν να ονομαστούν και ως τυχαίες απειλές. Παραδείγματα τέτοιων απειλών είναι τα προγραμματιστικά λάθη, σφάλματα που οφείλονται στο υλικό, λάθη κατά την μετάδοση δεδομένων, λάθος δρομολογήσεις πακέτων, λάθη που οφείλονται στην λειτουργία των συνεργατών της εταιρίας (πχ χρεοκοπία τρίτου).
- Περιβαλλοντική Απειλή : Αναλύεται στα εξής τμήματα, τις φυσικές καταστροφές όπως πλημμύρες, σεισμούς, καταιγίδες και στις γενικότερες περιβαλλοντικές συνθήκες όπως είναι η διακοπή ρεύματος (που οφείλεται στον τοπικό παροχέα, στην θερμοκρασία του περιβάλλοντος, στην υγρασία κ.α.

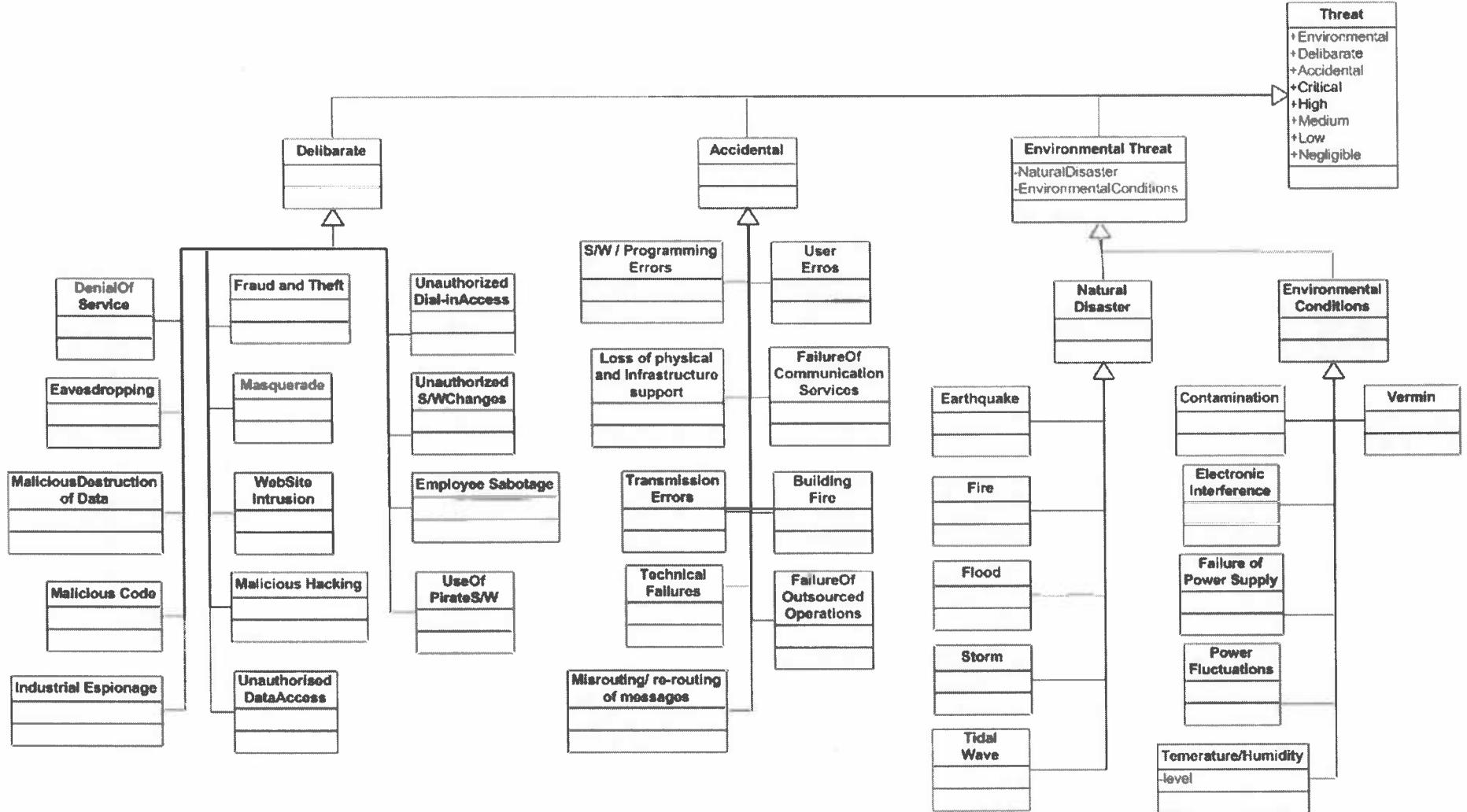


Παρακάτω απεικονίζονται τα προαναφερθέντα μοντέλα :



Εικόνα 14 : Countermeasure (Security Countermeasure)





Εικόνα 15 : Απειλή (Threat)

2.2.3. Αποτύπωση Σχέσεων μεταξύ των Εννοιών

Έχοντας παρουσιάσει το μοντέλο της οντολογίας, παρέχοντας ταυτόχρονα και το λεξικό των όρων για την αποσαφήνιση των όρων, θα παρουσιάσουμε τις σχέσεις που υπάρχουν μεταξύ των εννοιών. Αρχικά αποτυπώνουμε τις σχέσεις μεταξύ των όρων που δημιουργήσαμε και στη συνέχεια παρουσιάζουμε τις σχέσεις των όρων με τις υπάρχουσες κλάσεις του μοντέλου CIM. Αναλυτικότερα έχουμε :

Κλάση Threat (Απειλή) :

- 1) Εκμεταλλεύεται μία Ευπάθεια (Exploits a Vulnerability)
- 2) Στοχεύει ένα Αγαθό (Targets an Asset)

Κλάση Vulnerability (Ευπάθεια) :

- 1) Εκθέτει ένα Αγαθό (Exposes an Asset)

Κλάση Countermeasure (Αντίμετρο) :

- 1) Προστατεύει ένα Αγαθό (Protects an Asset)
- 2) Μειώνει τις Ευπάθειες (Vulnerabilities)
- 3) Στοχεύει μία Απειλή (Targets an Asset)

Κλάση Stakeholder (Ιδιοκτήτης) :

- 1) Κατέχει ένα Αγαθό

Η ενοποίηση της οντολογίας με το μοντέλο του CIM πραγματοποιήθηκε με τις εξής συνδέσεις :

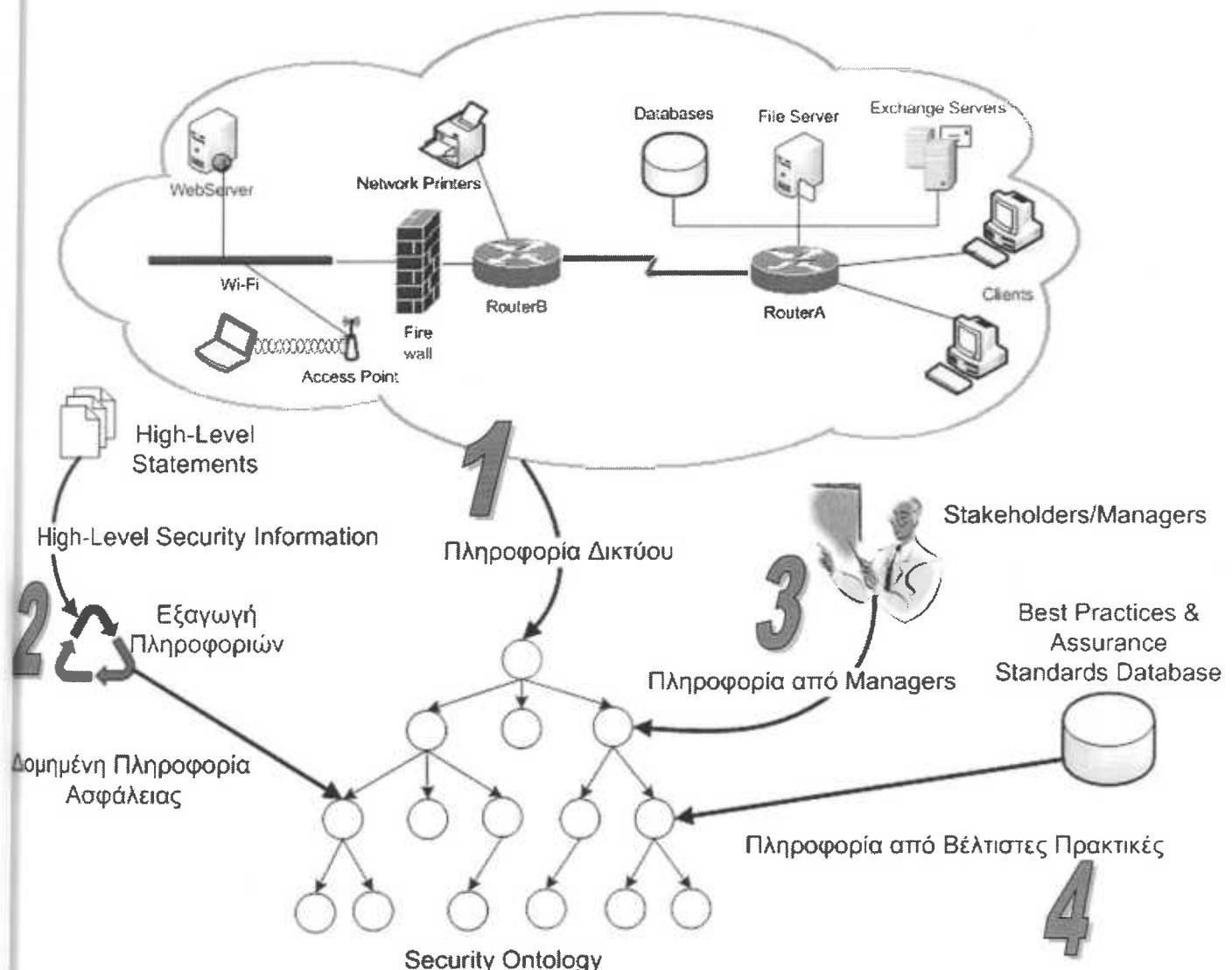
- 1) CIM_ManagedElement : Όλη η οντολογία κρέμεται κάτω από την τάξη Security_Managed_Element η οποία με την σειρά της κρέμεται κάτω από την CIM_ManagedElement
- 2) CIM_Network : Στην ανάλυση του Asset, υποκλάση της τάξης Network είναι η κλάση CIM_Network. Στην τελευταία περιλαμβάνονται πληροφορίες για το δίκτυο, όπως πρωτόκολλα επικοινωνίας και άλλα.



- 3) CIM_Logical_Device : Αποτελεί υποκλάση της τάξης Computer Equipment (Εικόνα 11). Συνεπώς κάτω από την υποκλάσεις της τάξης Computer Equipment είναι όλες οι υποκλάσεις της τάξης CIM_Logical_Device
- 4) CIM_Product : Υποκλάση αυτής αποτελεί η κλάση Network Equipment (Εικόνα 12)
- 5) CIM_Software_Element : Η κλάση Software κληρονομεί όλα τα γνωρίσματα της τάξης CIM_Software_Element μιας και αποτελεί υποκλάση αυτής.

2.3. Παρουσίαση Μεθόδου τυπικής αποτύπωσης ιδιωτικότητας και απαιτήσεων ασφάλειας ad-hoc δικτύων

Έχοντας ολοκληρώσει στις προηγούμενες παραγράφους την παρουσίαση της ολοκληρωμένης, για της ανάγκες της υπάρχουσας εργασίας, οντολογίας, σε αυτή την παράγραφο αναλύουμε την μεθόδου για την τυπική αποτύπωση των απαιτήσεων ασφάλειας και ιδιωτικότητας ad-hoc δικτύων. Αξίζει να σημειωθεί ότι, ενώ στα επόμενα θα περιγραφεί η μέθοδος της προσέγγισης στην πληρότητά της, το πρακτικό μέρος της εργασίας υλοποιεί ένα μέρος από την εν λόγω προσέγγιση. Όπως παρουσιάστηκε στην ενότητα 2.1, το εννοιολογικό μοντέλο της μεθόδου είναι το ακόλουθο :



Εικόνα 16 : Εννοιολογικό Μοντέλο

Όπως ήδη έχει αναφερθεί και σε προηγούμενες παραγράφους σκοπός της μεθόδου είναι η τυπική αποτύπωση των απαιτήσεων ασφάλειας ενός ad-hoc δικτύου. Στην ουσία η πληροφορία η οποία θα αποτυπώνεται στην οντολογία θα αφορά στο “ΤΙ” και όχι στο “ΠΩΣ” των απαιτήσεων ασφάλειας. Για να καταστεί δυνατή η τυπική αποτύπωση πρέπει να ορίσουμε μία δομή, στην οποία θα αποθηκεύουμε την αναγκαία πληροφορία έτσι ώστε να ορίσουμε κατά το δυνατόν πληρέστερα και ακριβέστερα το “ΤΙ” των απαιτήσεων ασφάλειας.

Ένα πρώτο στοιχείο που πρέπει να υπάρχει σε μία τέτοια δομή είναι το *subject* ή αλλιώς το *υποκείμενο* που θα εφαρμόσει το αντίμετρο. Το υποκείμενο μπορεί να είναι κάποιος ρόλος, όπως για παράδειγμα ο διαχειριστής του δικτύου ή κάποιος δαίμονας ο οποίος εκτελείται ανά τακτά χρονικά διαστήματα. Κάθε αντίμετρο περιγράφεται

από ένα θέμα (CM_Group) το οποίο βοηθά στην εύρεση κοινών πρακτικών για την εφαρμογή του. Στην μέθοδο που παρουσιάζουμε δανειστήκαμε τις ομάδες αντιμέτρων της CRAMM¹¹. Έτσι ένα αντίμετρο μπορεί να αφορά σε δικτυακό Έλεγχο Πρόσβασης (*Network Access Controls*), σε ακεραιότητα των δεδομένων πάνω στο δίκτυο (*Data Integrity over Network*), σε *Anagνώριση και Αυθεντικοποίηση* (*Integrity and Authentication*) και σε πολλά άλλα. Το επόμενο δεδομένο που πρέπει να εξάγουμε και να αποτυπώσουμε είναι ο στόχος (*target*) του αντίμετρου. Με τον όρο target εννοούμε την οντότητα εκείνη για την οποία εφαρμόζεται το αντίμετρο. Αν για παράδειγμα ένα αντίμετρο είχε την εξής μορφή

“Configure routers to only accept packets from defined external sources”

τότε το target αυτού του αντίμετρου είναι όλοι οι δρομολογητές ή διαφορετικά όλα τα στιγμιότυπα της τάξης δρομολογητής (routers) της οντολογίας. Στα παραπάνω πεδία κρίνεται απαραίτητη η προσθήκη ενός πεδίου *Ενέργεια* (*Action*). Αποτελεί το βασικό τμήμα της δομής αυτής μιας και περιγράφει το “ΤΙ” του αντίμετρου, δηλαδή τις απαραίτητες ενέργειες για την εφαρμογή του αντίμετρου ασφάλειας. Τέλος υπάρχουν περιπτώσεις κατά τις οποίες η εφαρμογή ενός αντίμετρου δεν είναι καθολική, αλλά υπάρχουν περιορισμοί είτε στο πεδίο εφαρμογής είτε στην έννοια του χρόνου, είτε του χώρου. Έτσι το αντίμετρο

“Configure filtering routers so that it is not possible for external hosts to communicate with internal hosts, except mail servers and web servers.”

δεν θα εφαρμοστεί συνολικά αλλά θα υπάρξει η εξαίρεση των εξυπηρετητών αλληλογραφίας (mail servers) και των εξυπηρετητών ιστού (web servers).

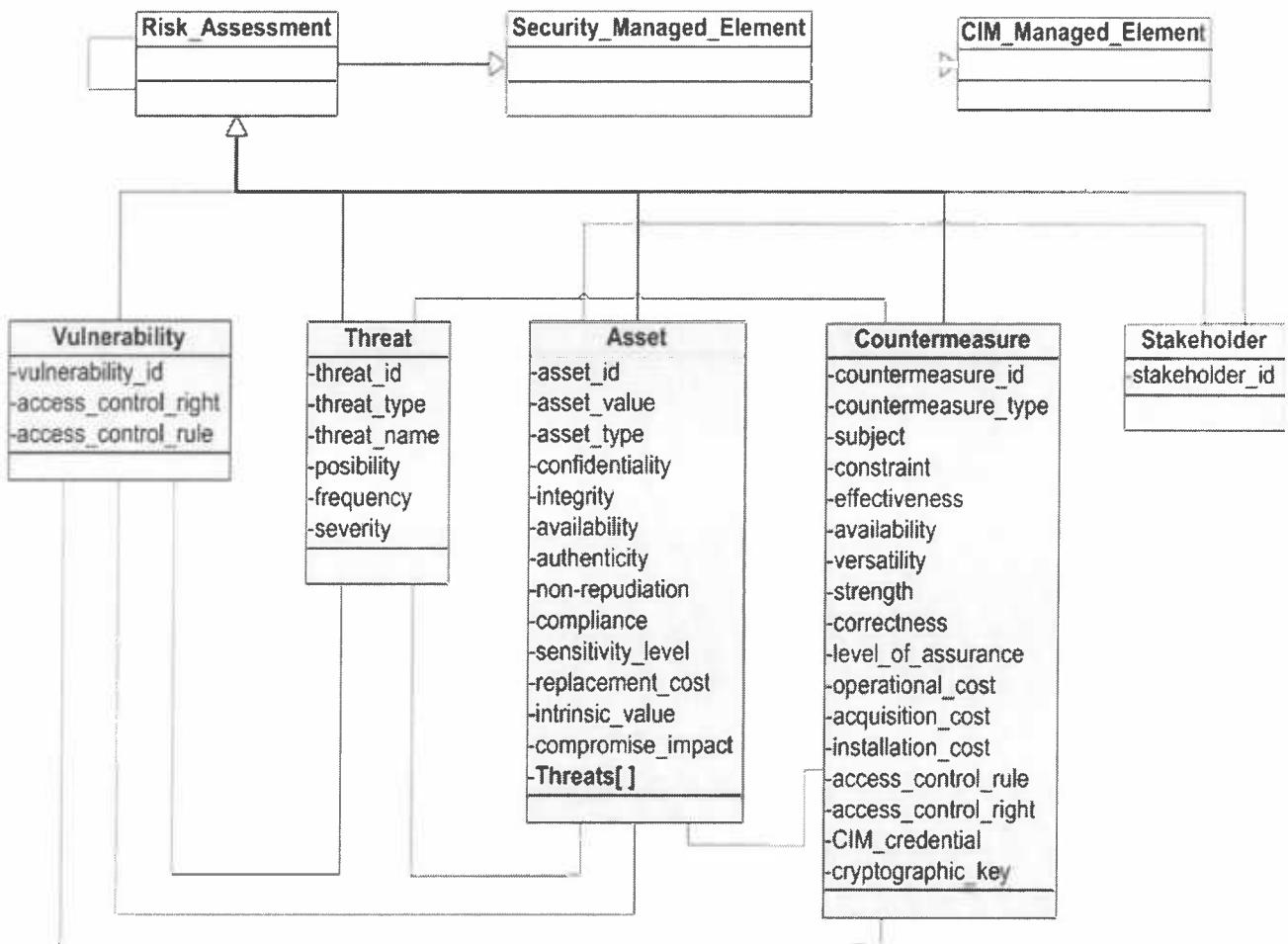
Έτσι λοιπόν η ολοκληρωμένη δομή του αντίμετρου που θα πρέπει να εξάγουμε από τις διαθέσιμες πηγές είναι :

¹¹ Η CRAMM αποτελεί ένα πρόγραμμα που υλοποιεί την ομώνυμη μέθοδο ανάλυσης επικινδυνότητας και είναι συμβατή, εκτός των άλλων, με το πρότυπο BS 7799. Τα αρχικά σημαίνουν CCTA (Central Computer and Telecommunication Agency) Risk Analysis and Manage Method.

Δομή Αντίμετρου (Countermeasure – CM)	
Subject (Υποκείμενο)	Περιγράφει το υποκείμενο που θα υλοποιήσει/εφαρμόσει το αντίμετρο.
CM_Group (Θέμα)	Αφορά στην κατηγοριοποίηση του αντίμετρου σε κάποιο ομάδα κοινών αντιμέτρων. Οι ομάδες έχουν προκύψει από την CRAMM.
Στόχος (Target)	Περιγράφει το που θα εφαρμοστεί το αντίμετρο.
Action (Ενέργεια)	Το πεδίο αυτό περιγράφει την ενέργεια που αποτυπώνεται στο αντίμετρο.
Constraints (Περιορισμοί)	Αφορά σε τυχόν περιορισμούς που μπορεί να έχει η εφαρμογή του αντίμετρου σε θέματα τοποθεσίας (πχ πρόσβαση μόνο εντός δικτύου), χρονικά (εντός εργασιακών ορών) και ρόλων (και μπορεί να το εφαρμόσει μόνο ο διαχειριστής του δικτύου).

Πίνακας 1 : Δομή Τυπικής Αποτύπωσης Αντίμετρου

Στην συνέχεια της παρουσίασης, θα αναλύσουμε τον τρόπο με τον οποίο θα αποθηκεύσουμε την δομή στην οντολογία και συνεπώς σε όλα τα στιγμιότυπα του εκάστοτε δικτύου. Το ανώτερο επίπεδο της οντολογίας όπως αυτό παρουσιάστηκε στην προηγούμενη παράγραφο είναι το ακόλουθο :



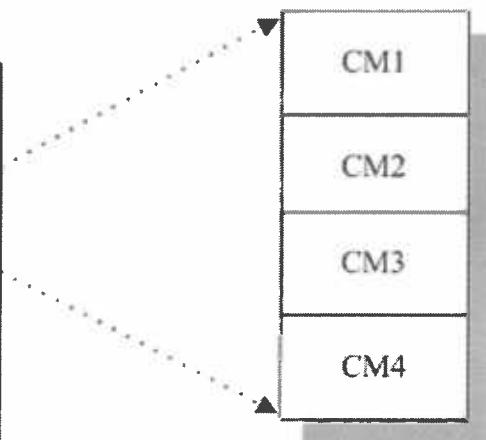
Εικόνα 17 : Τελικό μοντέλο Risk Assesment

Βασικό σημείο που απαιτεί επιπλέον ανάλυση αποτελεί η ιδιότητα Threats[], η οποία εντοπίζεται στην τάξη Asset. Από τις ιδιότητες της κληρονομικότητας η ιδιότητα αυτή θα μεταφερθεί σε όλες τις υποκλάσεις της τάξης αυτής. Για παράδειγμα, σε όλα τα στιγμιότυπα της τάξης Web Server που απεικονίζεται στο υπομοντέλο Software (Εικόνα 13) θα περιέχεται και η ιδιότητα Threats[].

Είναι εύκολα κατανοητό ότι κάθε αγαθό ανάλογα με την κατηγορία στην οποία ανήκει (για παράδειγμα φυσικό ή λογικό αγαθό) έχει και κάποιες απειλές. Στόχος λοιπόν του πεδίου αυτού είναι η καταγραφή των απειλών για κάθε αγαθό. Στην συνέχεια στόχος της μεθόδου είναι η τυπική αποτύπωση όλων εκείνων των αντίμετρων που στοχεύουν στο εκάστοτε αντίμετρο. Έτσι λοιπόν σε κάθε γραμμή του πίνακα Threats υπάρχει και ένας μονοδιάστατος πίνακας ο οποίος έχει σαν στοιχεία του την δομή του Counter Measure το οποίο αναφέρθηκε παραπάνω. Για να γίνει πιο κατανοητή η δομή του γνωρίσματος Threats[] παραθέτουμε το ακόλουθο σχήμα:

Πίνακας Threats

Threat1	CMs
Threat2	CMs
Threat3	CMs
Threat4	CMs



Εικόνα 18 : Περιγραφή Γνωρίσματος Threats[]

Επόμενο βήμα στην ανάλυσή μας αποτελεί η περιγραφή της εξαγωγής της γνώσης από τις βασικές πηγές εισόδου όπως απεικονίζονται στην Εικόνα 17 (αριθμοί 1 ~ 4). Σε πρώτο στάδιο πρέπει να εξάγουμε πληροφορία που αφορά στην τοπολογία του δικτύου (“1” από Εικόνα 16). Χρησιμοποιώντας ένα εργαλείο σάρωσης δικτύου, όπως για παράδειγμα το NetStumbler [41] ή το Nmap [40], παράγουμε ένα αρχείο plain text¹². Μετά την επεξεργασία του κειμένου η διαθέσιμη πληροφορία θα αφορά σε χαρακτηριστικά τις εκάστοτε συσκευής που συμμετέχει στο δίκτυο. Παραδείγματα τέτοιων χαρακτηριστικών αποτελούν το λειτουργικό σύστημα, ο τύπος της συσκευής, τυχόν αναβαθμίσεις του λειτουργικού συστήματος, οι IP διευθύνσεις και άλλα. Άρα λοιπόν σαν πρώτο στάδιο συμπλήρωσης της οντολογίας έχουμε την δημιουργία των απαραίτητων στιγμιότυπων (instances), καθώς και την «συμπλήρωση» των χαρακτηριστικών τους γνωρισμάτων.

Το επόμενο στάδιο αφορά αποκλειστικά στην δημιουργία εγγραφών για τον πίνακα Threats[] του κάθε στιγμιότυπου. Για να γίνει αυτό εφικτό πρέπει να αναλύσουμε την πληροφορία που έχουμε από τα high-level statements (“2” από Εικόνα 16). Έχοντας εντοπίσει τις κύριες οντότητες του προς εξέταση δικτύου μπορούμε να συμπληρώσουμε για κάθε μία από αυτές τις γνωστές απειλές ασφάλειας που έχει. Γνωστές, μιας και αυτές προϋπάρχουν στην οντολογία πριν ακόμα αναγνωρίσουμε τις οντότητες του δικτύου. Οι απειλές αυτές έχουν προκύψει από την Ανάλυση Επικινδυνότητας και/ή την μελέτη προτύπων και μοντέλων ασφαλείας και έχουν εισαχθεί στην οντολογία ως στιγμιότυπα της τάξης Threats (βλ. ενότητα 1.1.4).

¹² Plain text αρχεία είναι αυτά που περιέχουν μόνο κείμενο χωρίς καμία μορφοποίηση των περιεχομένων του. Συνήθης κατάληξη είναι η “.txt”

για τις συμβάσεις που υιοθετήθηκαν). Στη συνέχεια χρησιμοποιώντας τεχνικές επεξεργασίας φυσικής γλώσσας, εξάγουμε πληροφορία που αφορά στα αντίμετρα. Το είδος της πληροφορίας που μας ενδιαφέρει παρουσιάστηκε παραπάνω (Πίνακας 1). Κατόπιν, πρέπει το κάθε αντίμετρο που βρέθηκε και αναγνωρίστηκε επιτυχώς, να ταξινομηθεί σε κάθε απειλή που μπορεί να βρει εφαρμογή (βλ. ενότητα 1.1.4 για τις συμβάσεις που υιοθετήθηκαν). Για τον σκοπό αυτό, χρησιμοποιούμε το πεδίο CM_Group για να εντάξουμε το αντίμετρο σε μία ομάδα αντιμέτρων και να αποφανθούμε σε ποιες ακριβώς απειλές έχει εφαρμογή. Έτσι, για παράδειγμα, είναι φανερό ότι αν το αντίμετρο έχει χαρακτηριστεί ότι ανήκει στην ομάδα Identification and Authentication (Ταυτοποίηση και Αυθεντικοποίηση), δεν μπορεί να χρησιμοποιηθεί π.χ. για τη λογιστική χρέωση των χρηστών για ένα αγαθό όπως PrinterA (Εκτυπωτής A).

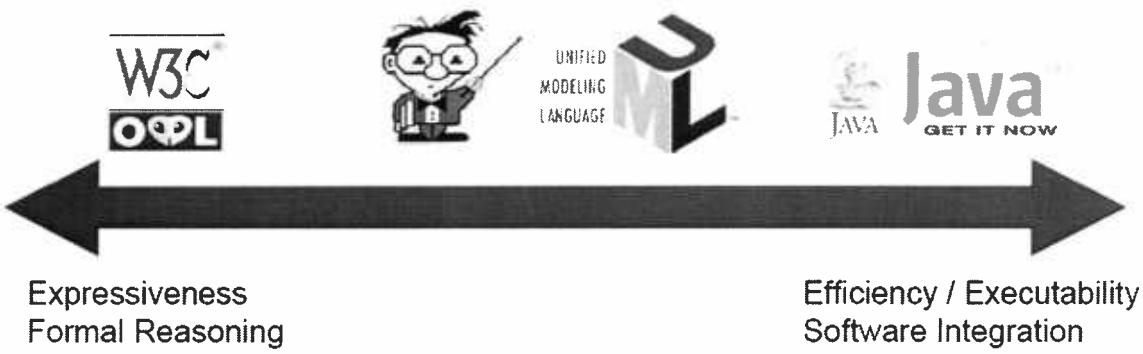
Το επόμενο στάδιο αφορά στην διαχειριστική πληροφορία που προέρχεται από τα επιχειρησιακά στελέχη (“3” από Εικόνα 16). Σε αρκετές περιπτώσεις, μετά την ολοκλήρωση των διαδικασιών για την δημιουργία ενός Security Policy μιας εταιρείας, πραγματοποιούνται αρκετά στάδια εκλέπτυνσης αυτών έως ότου «συμμορφωθεί» πλήρως με τις ανάγκες τις εταιρίας. Η πληροφορία αυτή είναι αδύνατον να συλλεχθεί με οποιονδήποτε άλλο τρόπο εκτός από διαλογικές διαδικασίες. Συνεπώς η πληροφορία αυτή θα ενταχθεί στην οντολογία με μη-αυτόματο τρόπο.

Τέλος υπάρχουν περιπτώσεις όπου για λόγους ελλιπούς ανάλυσης επικινδυνότητας για πολλά αγαθά δεν υπάρχουν αντίμετρα. Έτσι λοιπόν, στο τελευταίο βήμα επεξεργασίας των πηγών εισόδου (“4” από Εικόνα 16) εντοπίζουμε για την κάθε απειλή ενός αγαθού βέλτιστες πολιτικές ασφάλειας και κοινές πρακτικές από κοινά αποδεκτές βάσεις δεδομένων και ενσωματώνουμε την πληροφορία αυτή στο εκάστοτε πεδίο CM του πίνακα Threats []. Ολοκληρώνοντας και το στάδιο αυτό έχουμε δημιουργήσει το μοντέλο της οντολογίας με την απαραίτητη πληροφορία για την τυπική αποτύπωση των απαιτήσεων ασφάλειας του δικτύου μας.

2.4. Εργαλεία

Από τις προηγούμενες παραγράφους όπου παρουσιάστηκε η μέθοδος τυπικής αποτύπωσης των απαιτήσεων ασφάλειας και ιδιωτικότητας, γίνεται φανερό ότι για να καταστεί δυνατή η υλοποίηση της μεθόδου απαιτούνται δύο βασικά εργαλεία, το ένα αφορά στην επεξεργασία οντολογιών και το άλλο στην επεξεργασία φυσικής γλώσσας. Πριν αναφερθούμε στα δύο αυτά εργαλεία ακολουθεί μία σύντομη παρουσίαση των πλεονεκτημάτων των οντολογιών έναντι των υπόλοιπων τεχνικών για την τυπική αποτύπωση γνώσης.

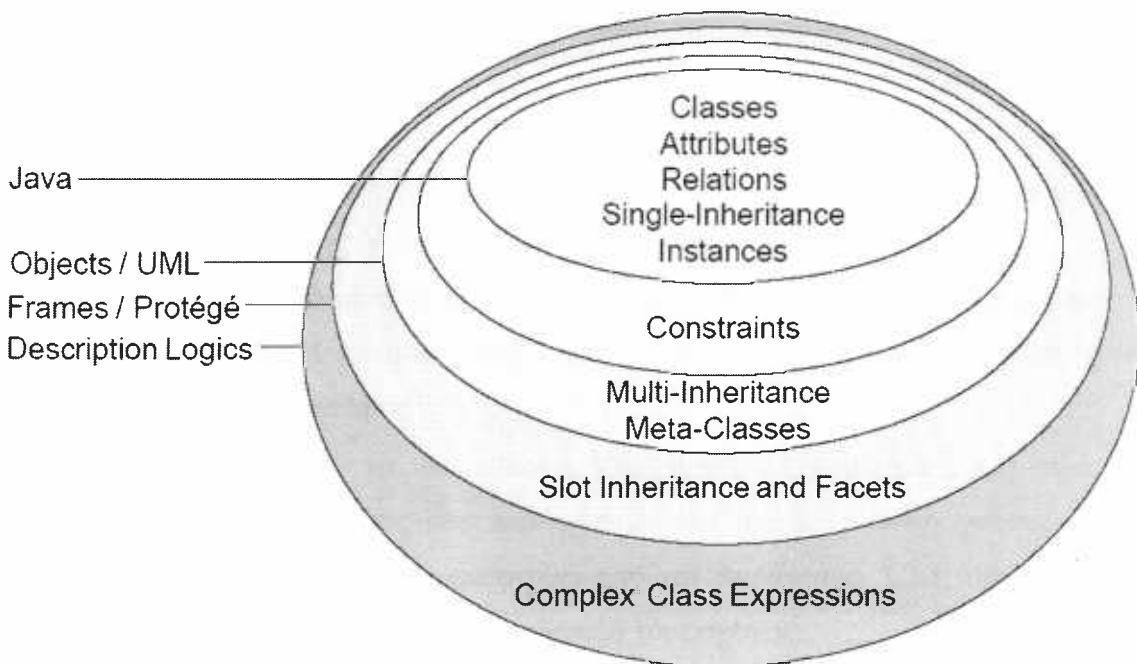
Θέλοντας να ταξινομήσουμε κατά μία έννοια τις διάφορες μορφές τυπικής αποτύπωσης της γνώσης θα μπορούσαμε να πούμε ότι υπάρχουν τρία επίπεδα τα οποία απεικονίζονται στο ακόλουθο σχήμα:



Εικόνα 19 : Επίπεδα τυπικής αποτύπωσης γνώσης

Στα χαμηλότερα επίπεδα με την βοήθεια της JAVA και άλλων γλωσσών αντικειμενοστραφούς προγραμματισμού μπορούν να οριστούν τάξεις καθώς και οι μεταξύ τους σχέσεις. Όμως ένα μειονέκτημα των αντικειμενοστραφών γλωσσών προγραμματισμού είναι το γεγονός ότι δεν μπορούν να αναπαρασταθούν πολύπλοκες σχέσεις μεταξύ των εννοιών καθώς και συνθήκες που πιθανά να ισχύουν μεταξύ των κλάσεων όπως για παράδειγμα συνθήκες ικανού και αναγκαίου. Στο επόμενο στάδιο βρίσκεται η UML (Unified Modeling Language) η οποία αποτελεί γλώσσα κατασκευής μοντέλων του πραγματικού κόσμου. Αν και η UML παρέχει μεγαλύτερη ευελιξία στην δημιουργία και τον ορισμό τόσο των τάξεων όσο και των μεταξύ τους σχέσεων, συνήθως προορίζεται για αναπαράσταση των δεδομένων μίας συγκεκριμένης εφαρμογής και όχι του συνόλου των εφαρμογών που μπορούν να χρησιμοποιηθούν οι έννοιες προς αναπαράσταση. Έτσι αν δύο βιβλιοπωλεία

στηρίχθηκαν στην UML για την ανάπτυξη των εφαρμογών τους, σε μία πιθανή ενοποίηση αυτών, πιθανά να αντιμετωπίσουν προβλήματα μιας και η μία εφαρμογή μπορεί να απεικονίζει την έννοια περιοδικό με την κλάση “μηνιαίος τύπος” ενώ η άλλη με την κλάση “περιοδικά”. Τέλος, οι οντολογίες, όπως έχει αναφερθεί στην παράγραφο 1.2.1, αποτελούν την τυπική αποτύπωση της αντιληπτικότητας για ένα πεδίο του πραγματικού κόσμου. Με τις οντολογίες συνθήκες που προαναφέρθηκαν (όπως συνθήκες ικανού και αναγκαίου) μπορούν να ορισθούν. Επιπλέον οι οντολογίες παρέχουν αιτιολογικές μηχανισμούς (reasoning) που ελέγχουν αν η οντολογία είναι συνεπής. Με τον όρο συνεπής εννοούμε τον έλεγχο των σχέσεων μεταξύ των εννοιών καθώς και διάφορες παράμετροι της κάθε έννοιας ζεχωριστά. Έτσι μία κατηγοριοποίηση των τεχνικών αναπαράστασης της γνώσης είναι αυτή στην ακόλουθη εικόνα:



Εικόνα 20 : Κατηγοριοποίηση τεχνικών αποτύπωσης γνώσης

Είναι φανερό λοιπόν ότι για λόγους πληρότητας αλλά και σαφέστερου ορισμού των εννοιών που περιλαμβάνονται στον τομέα της ασφάλειας των πληροφοριακών συστημάτων κρίνεται σκόπιμη η χρήση των οντολογιών.

Τέλος στις επόμενες παραγράφους θα παρουσιαστούν τα δύο βασικά εργαλεία που χρησιμοποιήθηκαν με σκοπό την υλοποίηση της μεθόδου που προαναφέρθηκε. Το GATE (A General Architecture for Text Engineering) και το Protégé αποτελούν

προϊόν επιστημονικής έρευνας στα πανεπιστήμια του Sheffield και Stanford, αντίστοιχα. Το πρώτο αφορά σε επεξεργασία φυσικής γλώσσας, ενώ το δεύτερο σε επεξεργασία οντολογιών. Παρακάτω ακολουθεί μία βασική περιγραφή και των δύο εργαλείων.

2.4.1. Επεξεργαστής οντολογιών Protégé

Το Protégé δημιουργήθηκε κυρίως για ιατρικούς λόγους. Στόχος του επιστημονικού αυτού προγράμματος ήταν η δημιουργία ενός λογισμικού που θα μπορεί να διαχειρίζεται ιατρικές δεδομένα και να μπορεί να παρέχει απαντήσεις σε ερωτήματα που του ανατίθενται, όπως για παράδειγμα διάγνωση ασθένειας με συγκεκριμένα συμπτώματα. Ταυτόχρονα όμως η αποτύπωση της τυπικής γνώσης έπρεπε να γίνει κατά τέτοιο τρόπο ώστε να μπορεί να υπάρξει ένα κοινό πλαίσιο ορισμών ύστοι ώστε να είναι δυνατή η επέκταση της μοντέλου από οποιονδήποτε ενδιαφερόμενο. Τα χαρακτηριστικά αυτά όπως αναφέρθηκε και σε προηγούμενες παραγράφους παρέχονται από τις οντολογίες. Προφανώς, επειδή η διαχείριση των οντολογιών είναι ανεξάρτητη από το πεδίο το οποίο περιγράφουν, το Protégé άρχισε να χρησιμοποιείται για την δημιουργία και επεξεργασία λοιπών οντολογιών.

Το Protégé διαθέτει γραφική διεπαφή η οποία καθιστά την χρήση του ακόμα πιο εύκολη στον χρήστη. Η γραφική διεπαφή είναι βασισμένη στις καρτέλες (tabs) η οποία επιτρέπει στον χρήστη να :

- δημιουργήσει και να διαχειριστεί ένα μοντέλο οντολογίας, το οποίο αποτελείται από τάξεις που περιγράφουν ένα ορισμένο πεδίο γνώσης. Η οντολογία όπως ήδη έχει αναφερθεί από την παράγραφο 1.2.1, ορίζει ένα σύνολο από έννοιες καθώς και τις μεταξύ τους σχέσεις,
- να δημιουργήσει ένα εργαλείο για την διαχείριση της γνώσης που αφορά στο συγκεκριμένο πεδίο εφαρμογής. Το εργαλείο αυτό βοηθά τους ειδικούς μίας περιοχής γνώσης να εισάγουν και να διαμοιράζουν την γνώση τους εύκολα. Οι ειδικοί εισάγουν στιγμιότυπα των τάξεων / εννοιών στην οντολογία τα οποία στην συνέχεια μπορούν να χρησιμοποιηθούν για την επίλυση προβλημάτων.

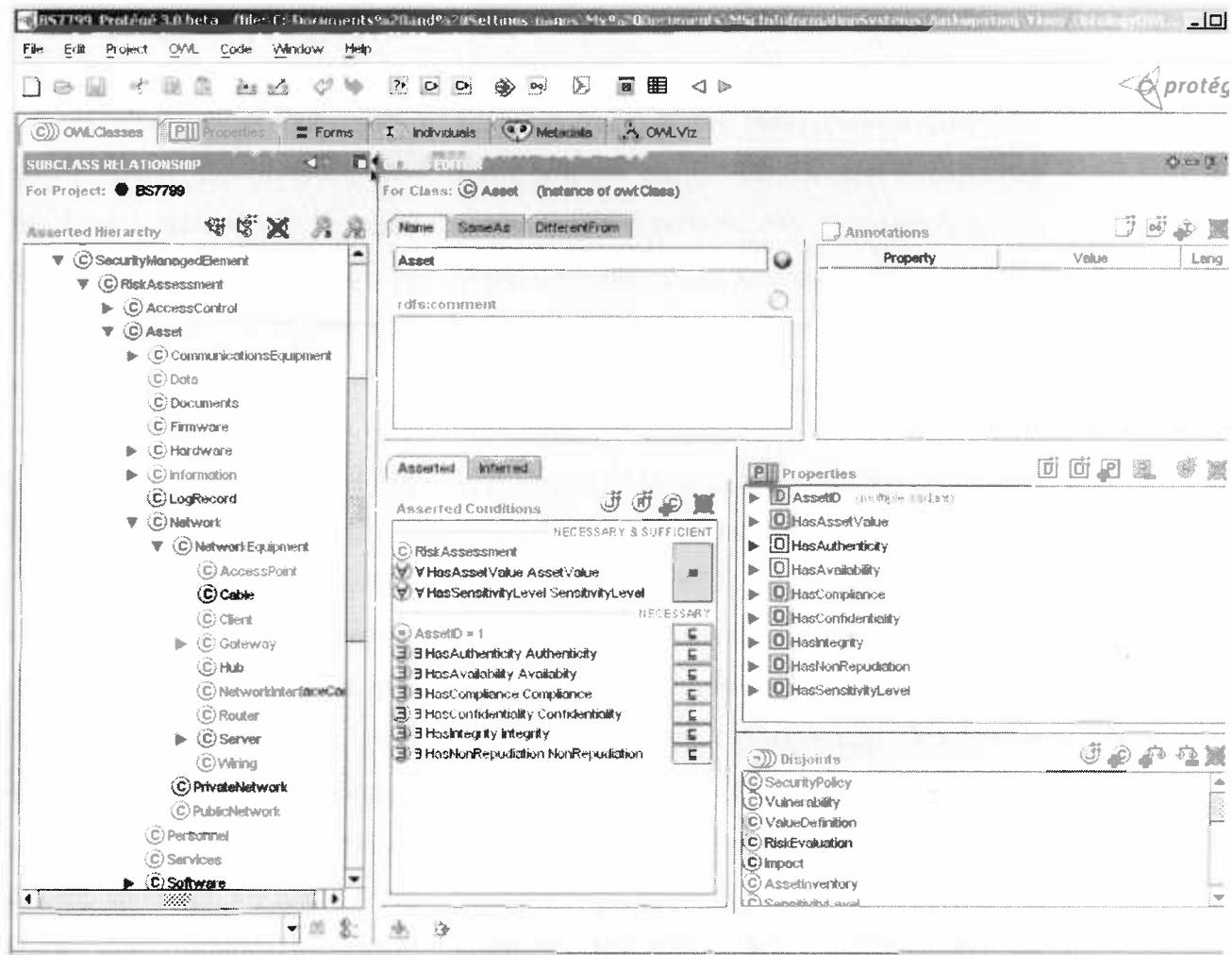
- να δημιουργήσει και να εκτελέσει εφαρμογές, οι οποίες αποτελούν και το τελικό προϊόν που δημιουργείται όταν η οντολογία χρησιμοποιείται για την επίλυση προβλημάτων, για την δημιουργία έμπειρων συστημάτων κ.α.

Ένα ακόμη μεγάλο πλεονέκτημα του Protégé είναι το γεγονός ότι είναι ανεξάρτητο από συγκεκριμένες πλατφόρμες. Έχει υλοποιηθεί σε JAVA και είναι ανοιχτού κώδικα. Το τελευταίο χαρακτηριστικό προσδίδει στο Protégé μία ακόμη λειτουργικότητα, ίσως την πιο σημαντική, την επεκτασιμότητα από τον εκάστοτε χρήστη. Εύκολα λοιπόν μπορεί κανένας να προσθέσει λειτουργικότητα με την συγγραφή κώδικα και την ενσωμάτωσή του στο Protégé (plugins). Ταυτόχρονα το Protégé, παρέχει προγραμματιστική διεπαφή γεγονός που το καθιστά εύκολο και στην ενσωμάτωσή του από άλλες εφαρμογές (API – Application Programming Interface). Έτσι ενώ αρχικά η αποτύπωση των οντολογιών γινόταν μόνο σε μία μορφή (συγκεκριμένη μορφή του πυρήνα του Protégé), τώρα είναι δυνατή η αποτύπωση οντολογιών σε RDF, XML αλλά και OWL (λεπτομέρειες για τους τρόπους αναπαράστασης οντολογιών βλέπε παράγραφο 1.2.2).

Για την υλοποίηση της μεθόδου χρησιμοποιήσαμε την έκδοση 3.0 του Protégé (build 120) σε συνδυασμό με το OWL plug-in (version 2.0). Η γραφική διεπαφή του Protégé χρησιμοποιήθηκε για την δημιουργία της οντολογίας, ενώ στην συνέχεια μέσω της προγραμματιστικής διεπαφής (API), τόσο του Protégé όσο και του OWL plug-in, κατέστη δυνατή η ένωση του GATE¹³ με το Protégé.

Στην συνέχεια ακολουθεί μία εικόνα από την γραφική διεπαφή του Protégé.

¹³ Λεπτομέρειες για το GATE ακολουθούν στις επόμενες παραγράφους.



Εικόνα 21 : Protege, επεξεργαστής οντολογιών

Στο πάνω μέρος της διεπαφής παρατηρεί κανένας την καρτελοειδή μορφή του Protégé (tabs). Η πρώτη καρτέλα αφορά στις δημιουργημένες κλάσεις / έννοιες (OWL Classes). Η καρτέλα αυτή έχει προκύψει από την εισαγωγή του OWL Plug-in. Οι κλάσεις παρουσιάζονται σε δενδροειδή μορφή έτσι ώστε να είναι εύκολη η παρουσίαση των υπερκλάσεων αλλά και των υποκλάσεων. Επιπλέον στην καρτέλα αυτή ορίζονται πιθανές συνθήκες ικανού και αναγκαίου αλλά και μόνο αναγκαίου (asserted conditions) που πιθανά να υπάρχουν καθώς και οι ιδιότητες (properties) των τάξεων. Αξίζει να σημειωθεί ότι υπάρχουν δύο είδη ιδιοτήτων, τα object properties και τα datatype properties. Τα πρώτα υλοποιούν τις σχέσεις μεταξύ δύο εννοιών, έτσι για παράδειγμα μεταξύ των τάξεων Asset και AssetValue υπάρχει η σχέση “has”, η οποία υλοποιείται με ένα object property. Τέλος τα datatype properties αφορούν σε βασικές δομές δεδομένων (primitive types) όπως για παράδειγμα Συμβολοσειρές (Strings), Αριθμούς (Integers, Doubles κ.α.), κ.α.

2.4.2. Εξαγωγή Πληροφοριών, Gate

Η εξαγωγή πληροφοριών από τα γραπτά κείμενα που αναφέρθηκαν στις προηγούμενες παραγράφους έγινε με την βοήθεια του GATE (General Architecture for Text Engineering). Η ανάπτυξη του GATE ξεκίνησε στο Πανεπιστήμιο του Sheffield το 1995 και από τότε έχει χρησιμοποιηθεί σε ένα πλήθος ερευνών αλλά και έργων [16]. Η πρώτη έκδοση του GATE βγήκε σε κυκλοφορία το 1996 και χρησιμοποιήθηκε σε αρκετές εφαρμογές λεκτικής ανάλυσης αλλά κυρίως σε εφαρμογές εξαγωγής γνώσης (Information Extraction) [1],[17].

Όπως αναφέρεται στο [18], το GATE είναι μία αρχιτεκτονική, ένα *framework* (πλαίσιο εργασίας), και ένα περιβάλλον ανάπτυξης. Μία αρχιτεκτονική γιατί ορίζει την δομή και λειτουργία ενός προγράμματος γλωσσικής επεξεργασίας και αναθέτει στα διάφορα συστατικά του προγράμματος τις δραστηριότητες που πρέπει το κάθε ένα να φέρει εις πέρας. Framework, γιατί παρέχει επαναχρησιμοποιήσιμες βιβλιοθήκες για προγράμματα τύπου LE (Language Engineering), βοηθώντας έτσι τους προγραμματιστές να χρησιμοποιήσουν έτοιμο κώδικα, να τον βελτιώσουν αλλά και να τον ενσωματώσουν σε μεγαλύτερες εφαρμογές όπου ένα κομμάτι τους είναι το LE. Ακόμη, το GATE είναι ένα περιβάλλον ανάπτυξης (development environment) διότι βοηθά τους χρήστες να ελαχιστοποιήσουν τον χρόνο που ξοδεύουν στο να τροποποιήσουν υπάρχοντα components ή να δημιουργήσουν καινούργια παρέχοντας τεχνικές αποσφαλμάτωσης (debugging) αλλά και εργαλεία χρήσιμα στην συγγραφή κώδικα.

Ένα βασικό του πλεονέκτημα είναι το γεγονός ότι τα διάφορα κομμάτια του GATE (components) μπορούν να εφαρμοστούν σε οποιαδήποτε γλώσσα προγραμματισμού και σε οποιαδήποτε βάση δεδομένων. Σε κάθε περίπτωση η αρχιτεκτονική του GATE «φαίνεται» στον χρήστη ως μία JAVA class η οποία μπορεί να καλέσει το πρόγραμμα που έχουμε δημιουργήσει ή αντίστροφα να «καλεστεί» (import) στο δικό μας πρόγραμμα. Όσον αφορά στις βάσεις δεδομένων το GATE παρέχει συνδεσιμότητα με τρεις βάσεις δεδομένων : με Oracle, με Java serialization (απλά αρχεία που χρησιμοποιούνται για την αποθήκευση δεδομένων με την χρήση βιβλιοθηκών της JAVA), αλλά και με PostgreSQL. Βέβαια ο χρήστης μπορεί να δημιουργήσει ένα δικό του component όπου θα μπορεί να αποθηκεύει τις πληροφορίες του σε όποια βάση δεδομένων θέλει. Τέλος το GATE έχει

ενσωματωμένο GUI (Graphic User Interface) γεγονός που καθιστά ακόμα πιο εύκολη την χρήση του¹⁴.

Στο σημείο αυτό θα εμβαθύνουμε την παρουσίασή μας στο GATE, παρουσιάζοντας τις τρεις βασικές κατηγορίες των τμημάτων του :

- **Language Resources (LRs)** : Αντιπροσωπεύουν έννοιες όπως λεξικά, κείμενα, συλλογές από έγγραφα αλλά και οντολογίες. Γενικά με τον όρο LR περιγράφουμε τα λεκτικά δεδομένα προς επεξεργασία.
- **Processing Resources (PRs)** : Αντιπροσωπεύουν οντότητες οι οποίες είναι κατά κύριο λόγο αλγόριθμοι. Μερικά παραδείγματα είναι οι parsers (σαρωτές κειμένου), αναλυτές γραμματικής, συνωνύμων και άλλα. Γενικά PR ονομάζονται τα στοιχεία εκείνα με την βοήθεια των οποίων επεξεργαζόμαστε τα LR.
- **Visual Resources (VRs)** : Τα Visual Resources αποτελούν κομμάτια του γραφικού τρόπου αλληλεπίδρασης του GATE (GUI). Δεν προσθέτουν λειτουργικότητα στην αρχιτεκτονική του GATE απλά είναι ένας εύχρηστος τρόπος χρησιμοποίησης των PRs.

Όλα τα παραπάνω components μπορούν να βρίσκονται είτε τοπικά σε έναν υπολογιστή είτε δικτυακά (διαθέσιμων μέσω HTTP πρωτοκόλλου). Ο κατανεμημένος τρόπος λειτουργίας του, προσθέτει άλλο ένα πλεονέκτημα στην χρήση του. Επιπλέον ένα ακόμη σημαντικό πλεονέκτημα είναι η ο διαχωρισμός των components όπως αυτός αναλύθηκε παραπάνω. Τόσο οι αλγόριθμοι (PRs) όσο και τα λεκτικά δεδομένα (LRs) μπορούν να αναπτυχθούν ξεχωριστά από διαφορετικές ομάδες ανθρώπων, όπως προγραμματιστές και γλωσσολόγοι αντίστοιχα. Επιπλέον διαχωρίζοντας το γραφικό περιβάλλον από τα υπόλοιπα components καθίσταται εύκολη η βελτίωση ακόμη και η δημιουργία νέων αλγορίθμων χωρίς να απαιτείται από τον χρήστη να τροποποιήσει το GUI αλλά και το αντίστροφο.

Στη συνέχεια της παραγράφου παρουσιάζουμε ένα set από Processing Resources το οποίο έρχεται ενσωματωμένο με την έκδοση του GATE και τα οποία χρησιμεύουν για τις κυριότερες NLP (Natural Language Processing) εφαρμογές. Προφανώς κανένα από τα PRs δεν είναι υποχρεωτικά στην χρήση τους. Ο κάθε χρήστης μπορεί να επιλέξει ποια του είναι χρήσιμα αλλά και να αντικαταστήσει όποια θέλει με δικά του

¹⁴ Το GATE είναι διαθέσιμο στην διεύθυνση <http://gate.ac.uk>

components. Τα παραπάνω PR σχηματίζουν την ANNIE – A Nearly-New Information Extraction system, μπορούν όμως να χρησιμοποιηθούν ανεξάρτητα από το πακέτο αυτό.

Η ANNIE απαρτίζεται από τα εξής βασικά κομμάτια (PRs): τον tokenizer, τον sentence splitter, τον POS tagger, τον gazetteer, τον semantic tagger ή αλλιώς Named Entity Transducer, και τον orthomatcher¹⁵. Ο tokenizer χωρίζει το κείμενο σε απλά tokens, όπως αριθμοί, σύμβολα στίξης και λέξεις. Η πρώτη ενέργεια που πρέπει να γίνει σε οποιοδήποτε κείμενο που θα υποστεί κάποιου είδους λεκτική ανάλυση, είναι ο χωρισμός του κειμένου σε tokens. Το βάρος της ανάλυσης μπορεί να δοθεί στην συνέχεια σε κάποιο component που κάνει γραμματική ανάλυση χωρίς να επιβαρυνθεί και με το χωρισμό των tokens. Οι τύποι των tokens που παράγει ο tokenizer μπορεί να είναι :

- Word (Λέξη) : Λέξη ορίζεται μία σειρά από σύμβολα, είτε κεφαλαία είτε μικρά, τα οποία περιέχουν τουλάχιστον ένα φωνήν.
- Number (Αριθμός) : Αριθμός είναι ένας οποιοσδήποτε συνδυασμός από συνεχόμενα ψηφία.
- Symbol (Σύμβολο) : Τα σύμβολα χωρίζονται σε δύο κατηγορίες, οικονομικά σύμβολα (π.χ. €, \$) και στα γενικά σύμβολα (π.χ. *, &, #, @).
- Punctuation (Στίξη) : Το GATE χωρίζει τα σύμβολα της στίξης σε τρεις κατηγορίες. Στίξη έναρξης, για παράδειγμα (, «, Στίξη τέλους, για παράδειγμα), !, ., » και σε γενικά σύμβολα στίξης όπως :, ;.
- Space Token (Κενός χαρακτήρας) : Οι κενοί χαρακτήρες χωρίζονται σε δύο κατηγορίες. Η πρώτη αφορά στα κενά μεταξύ των λέξεων και η δεύτερη αφορά στους χαρακτήρες Control όπως είναι για παράδειγμα ο χαρακτήρας αλλαγής γραμμής.

Ο sentence splitter χωρίζει το κείμενο σε προτάσεις, όπως άλλωστε φανερώνει και το όνομά του. Το συγκεκριμένο module είναι απαραίτητο για τον POS tagger ο οποίος παρουσιάζεται παρακάτω. Πρόταση θεωρείται μία σειρά από tokens η οποία τερματίζει με ένα σύμβολο όπως η τελεία, αλλά και από πολλαπλά σύμβολα στίξης όπως ?!?!?!

¹⁵ σ.σ.: Οποιαδήποτε μετάφραση στους όρους αυτούς θα ήταν μάλλον ατυχής.

Ο POS (Part-of-Speech) tagger είναι προϊόν του [19]. Αποτελεί το module που είναι υπεύθυνο για την γραμματική ανάλυση ενός κειμένου. Με την βοήθεια του sentence splitter το κείμενο χωρίζεται σε προτάσεις. Στην συνέχεια ο POS tagger αναλύει την κάθε πρόταση στα βασικά συστατικά που αποτελούν μία πρόταση όπως ρήματα, ουσιαστικά, επιρρήματα και άλλα. Το module αυτό χρησιμοποιεί ένα λεξικό (lexicon) και ένα σύνολο από γραμματικούς κανόνες. Τόσο το λεξικό όσο και οι κανόνες έχουν προκύψει από την ανάλυση εκατοντάδων κειμένων της Wall Street Journal. Και τα δύο συστατικά μπορούν να αλλάξουν αν ο χρήστης το επιθυμεί.

Ο Gazetteer αποτελείται από λίστες ονομάτων τα οποία είναι χωρισμένα ανάλογα με μία κοινή τους ιδιότητα. Έτσι για παράδειγμα υπάρχει μία λίστα η οποία έχει ονόματα πόλεων όπως Paris, Athens, New York, μία λίστα με ονόματα οργανισμών όπως Microsoft, AMD, Intel αλλά και λίστες από ονόματα ανθρώπων όπως John, Paul, Nick κ.ο.κ. Μετά την ανάλυση ενός κειμένου με τον Gazetteer οι λέξεις υπομνηματίζονται (annotated) από την ιδιότητά τους ως πόλεις, οργανισμοί, άτομα κ.α.

Ο Semantic tagger ή αλλιώς NE Transducer, αποτελείται από κανόνες, οι οποίοι είναι γραμμένοι σε JAPE (Java Annotation Pattern Engine). Οι κανόνες αυτοί έχουν βασιστεί στο CPSL (Common Pattern Specification Language) [20]. Με την βοήθεια των κανόνων αυτών, μπορούμε να προσδώσουμε ιδιότητες σε φράσεις που ταιριάζουν σε μία συγκεκριμένη μορφή. Ένα παράδειγμα που θα μας βοηθήσει να κατανοήσουμε καλύτερα την έννοια των κανόνων αυτών είναι η αναγνώριση μίας IP διεύθυνσης. Η τελευταία αποτελείται από τέσσερις αριθμούς και τρία σημεία στίξης. Με την βοήθεια των JAPE κανόνων μπορούμε να δηλώσουμε στην εφαρμογή μας ότι η ακολουθία *AΣΑΣΑΣΑ* αποτελεί μία διεύθυνση IP, όπου *A* είναι ένας αριθμός και *Σ* είναι η τελεία. Στους κανόνες αυτούς μπορούμε να χρησιμοποιήσουμε annotated (υπομνηματισμένες) λέξεις που έχουν βρεθεί από τον Gazetteer. Εάν τελευταίο παράδειγμα είναι η διεύθυνση e-mail. Χωρίς τους JAPE κανόνες μία διεύθυνση *john@microsoft.com* δεν θα αναγνωριζόταν συνολικά αλλά η λέξη *john* ως όνομα, η λέξη *microsoft* ως εταιρία, το *@* και η τελεία ως σύμβολα, και η λέξη *com* ως αρκτικόλεξο. Με τους JAPE κανόνες όλη η φράση θα αναγνωριστεί ως μία διεύθυνση ηλεκτρονικού ταχυδρομείου.

Ένα ακόμη component της ANNIE είναι ο Orthographic Coreference (orthomatcher). Ο τελευταίος αποτελεί προαιρετικό κομμάτι και κύριος σκοπός του είναι η προσθήκη σχέσεων μεταξύ των οντοτήτων που έχουν βρεθεί από τον semantic



tagger. Οι σχέσεις δημιουργούνται μεταξύ αντικειμένων που έχουν κοινό χαρακτηρισμό, για παράδειγμα *Οργανισμοί*, ή σε περίπτωση όπου μία από τις δύο έννοιες δεν έχει κάποιο χαρακτηρισμό (έχει χαρακτηριστεί ως unknown). Στην τελευταία περίπτωση, ο orthomatcher αλλάζει τον unknown σε X, όπου X είναι ο χαρακτηρισμός μίας άλλης έννοιας με την οποία υπάρχει σχέση. Ένα παράδειγμα είναι οι λέξεις *U.S.A.* και *U.S.* βρίσκονται στο κείμενό μας και για κάποιο λόγο η πρώτη έχει αναγνωριστεί ως τύπου Location ενώ η δεύτερη ως τύπου unknown. Τότε ο orthomatcher θα συσχετίσει τα δύο αντικείμενα ότι αναφέρονται στο ίδιο πράγμα και θα αναθέσει στην λέξη *U.S.* τον χαρακτηρισμό της λέξης *U.S.A.*, δηλαδή Location.

Στην μέθοδο που παρουσιάστηκε, χρησιμοποιήθηκε το σύστημα της ANNIE και συγκεκριμένα οι tokenizer, sentence splitter, POS tagger, gazetteer, Named Entity Transducer, και ο orthomatcher. Τα συγκεκριμένα εργαλεία τροποποιήθηκαν ανάλογα με τις απαιτήσεις της μεθόδου. Για περεταίρω ανάλυση της αρχιτεκτονικής του GATE βλέπε [21].

3. Εφαρμογή και Αξιολόγηση Μεθόδου

3.1. Εφαρμογή Μεθόδου

Στις επόμενες παραγράφους θα παρουσιαστεί αναλυτικότερα η υλοποίηση της μεθόδου για την τυπική αποτύπωση απαιτήσεων ασφάλειας και ιδιωτικότητας που παρουσιάστηκε στις προηγούμενες παραγράφους. Αρχικά εξετάζονται τα στοιχεία εισόδου της μεθόδου, στην συνέχεια παρουσιάζεται αναλυτικά η μέθοδος και τέλος παρατίθεται μία σύγκριση των αποτελεσμάτων που προέκυψαν μετά την εκτέλεση της μεθόδου, με την γνώση (αποτελέσματα) που θα εξαγόταν αν η επεξεργασία είχε ανθρώπινο χαρακτήρα δηλαδή πραγματοποιούταν από κάποιο ειδικό στον τομέα της ασφάλειας των Π.Σ. Στο τέλος της παραγράφου αυτής παρουσιάζουμε τις εμπειρίες που αποκομίστηκαν από την προσπάθεια υλοποίησης ενός τέτοιου εγχειρήματος καθώς και περαιτέρω έρευνα που μπορεί να πραγματοποιηθεί προς την κατεύθυνση αυτή.

3.1.1. Παρουσίαση Στοιχείων Εισόδου

Το πρώτο βήμα στην μέθοδο που παρουσιάστηκε είναι η συλλογή των απαραίτητων στοιχείων εισόδου. Ένα στοιχείο από αυτά είναι τα πληροφοριακά αγαθά σε επίπεδο υλικού που απαρτίζουν το δίκτυο προς εξέταση. Αν και η αποτύπωση των αγαθών αυτών θα μπορούσε να πραγματοποιηθεί και χειροκίνητα, εντούτοις υπάρχουν αρκετά εργαλεία διαθέσιμα στο εμπόριο τα οποία μπορούν να χαρτογραφήσουν το δίκτυο και επιπλέον να προσδώσουν πρόσθετα χαρακτηριστικά στον κάθε πόρο όπως για παράδειγμα λειτουργικό σύστημα, ενημερωμένες εκδόσεις κ.α. Τέτοια εργαλεία μπορεί να είναι τα [40], [41] και [42].

Τα τελευταία είναι σε θέση να παράγουν με απλές διαδικασίες αρχεία σε μορφή απλού κειμένου¹⁶, τα οποία περιέχουν την απαραίτητη πληροφορία για το δίκτυο. Παράδειγμα τέτοιας εξόδου προγράμματος αποτελεί το ακόλουθο απόσπασμα, το οποίο αποτελεί χαρτογράφηση τόσο ενσύρματου εξοπλισμού όσο και ασύρματου όπως άλλωστε μας ενδιαφέρει:

¹⁶ Τα αρχεία απλού κειμένου (Plain text) είναι αυτά που περιέχουν μόνο κείμενο χωρίς καμία μορφοποίηση των περιεχομένων του. Συνήθης κατάληξη είναι η “.txt”

Network: " " BSSID: "00:02:2D:00:34:57"

CDP Broadcast Device 1

Device ID : KENTPUR

Capability:

Interface : FastEthernet0

IP : 172.25.1.14

Platform : cisco 1720

Software : Cisco Internetwork Operating System Software

IOS (tm) C1700 Software (C1700-Y-M), Version 12.1(1), RELEASE SOFTWARE
(fc1)

Copyright (c) 1986-2000 by cisco Systems, Inc.

Compiled Tue 14-Mar-00 16:40 by cmong

CDP Broadcast Device 2

Device ID : Kent_County

Capability:

Interface : Ethernet0

IP : 172.25.1.5

Platform : cisco 2500

Software : Cisco Internetwork Operating System Software

IOS (tm) 3000 Software (IGS-J-L), Version 11.1(5), RELEASE SOFTWARE (fc1)

Copyright (c) 1986-1996 by cisco Systems, Inc.

Compiled Mon 05-Aug-96 11:48 by mkamson

CDP Broadcast Device 3

Device ID : Kentres

Capability:

Interface : Ethernet0

IP : 172.25.1.10

Platform : cisco 1602

Software : Cisco Internetwork Operating System Software

IOS (tm) 1600 Software (C1600-Y-M), Version 12.0(3), RELEASE SOFTWARE
(fc1)

Copyright (c) 1986-1999 by cisco Systems, Inc.

Compiled Mon 08-Feb-99 20:15 by phanguye

CDP Broadcast Device 4

Device ID : kent390

Capability:

Interface : Ethernet0

IP : 172.25.1.11

Platform : cisco 1604

Software : Cisco Internetwork Operating System Software

IOS (tm) 1600 Software (C1600-Y-L), Version 12.0(3), RELEASE SOFTWARE
(fc1)

Copyright (c) 1986-1999 by Cisco Systems, Inc.

Compiled Mon 08-Feb-99 19:32 by phanguye

Όπως φαίνεται και από την παραπάνω αναφορά, όλες οι συσκευές δικτυακού εξοπλισμού έχουν καταγραφεί με τα κύρια χαρακτηριστικά τους όπως διεύθυνση IP, λειτουργικό σύστημα, έκδοση λειτουργικού συστήματος κ.α. Από την παραπάνω αναφορά και με την βοήθεια απλών τεχνικών επεξεργασία φυσικής γλώσσας ή απλής λεκτικής ανάλυσης καθίσταται δυνατή η δημιουργία των απαραίτητων στιγμιότυπων των κλάσεων της οντολογίας ασφάλειας. Έτσι, βάσει του παραπάνω παραδείγματος, θα πρέπει να δημιουργηθούν κάτω από την κλάση Router τέσσερα νέα στιγμιότυπα, ένα για κάθε Router (Cisco 1604, 1602, 2500, 1720). Είναι προφανώς ότι μπορούν να εκτελεστούν πολλά εργαλεία ταυτόχρονα για την καλύτερη και ακριβέστερη αποτύπωση του δικτυακού εξοπλισμού. Μιας και η διαδικασία εξαγωγής των απαραίτητων στιγμιότυπων αποτελεί κάτι εύκολο προς υλοποίηση, η προσοχή μας εστιάστηκε στον τομέα της εξαγωγής γνώσης από τα αντίμετρα και συγκεκριμένα των πεδίων που θεωρούμε επαρκή για να τα περιγράψουν. Τα πεδία αυτά αναπτύχθηκαν αναλυτικότερα στην παράγραφο 2.3. Για τις ανάγκες τις παρουσίασης των αποτελεσμάτων υποθέτουμε ότι το δίκτυο αποτελείται από δύο μηχανές, ένα πελάτη και ένα εξυπηρετητή (client and server).

Ένα ακόμη στοιχείο εισόδου που πρέπει να τροφοδοτήσουμε την μέθοδο μας είναι η πολιτική ασφάλειας. Όπως ήδη έχει αναφερθεί και στην παράγραφο 1.1.4.1, στην ουσία δεν μας ενδιαφέρει συνολικά η πολιτική ασφάλειας αλλά ειδικότερα τα

αντίμετρα που περιλαμβάνονται σε αυτή. Ακριβέστερα λοιπόν το επόμενο στοιχείο εισόδου είναι τα αντίμετρα και όχι ολόκληρη η πολιτική ασφάλειας.

Τόσο η μορφή όσο και το περιεχόμενο των αντίμετρων δεν ακολουθεί κάποιο συγκεκριμένο πρότυπο. Και τα δύο είναι άμεσα συνδεδεμένα με τον συγγραφέα του αντίμετρου, είτε είναι κάποια φυσική οντότητα (διαχειριστής / αναλυτής ασφάλειας πληροφοριακών συστημάτων) είτε είναι κάποιο λογισμικό. Η μέθοδος που παρουσιάζεται στηρίζεται μόνο στα αντίμετρα τα οποία προκύπτουν από κάποιο λογισμικό και συγκεκριμένα από την CRAMM¹⁷. Με τον τρόπο αυτό μπορούμε να εφαρμόσουμε κάποια αλγορίθμική μέθοδο επάνω στα αντίμετρα με σκοπό την εκλέπτυνσή τους από υψηλού επιπέδου σε χαμηλού. Επιπλέον, η ευρεία διάδοση της CRAMM αποτέλεσε ένα ακόμα ισχυρό κίνητρο για την υιοθέτηση των αντιμέτρων που χρησιμοποιεί (για περισσότερες λεπτομέρειες σχετικά με τις συμβάσεις που υιοθετήθηκαν για τα αντίμετρα βλέπε την παράγραφο 1.1.4.1). Το κείμενο με τα αντίμετρα το οποίο χρησιμοποιήθηκε τελικώς είναι το ακόλουθο:

Countermeasures.txt

«Use asymmetric algorithms for signatures.

Use filters to restrict the level of access between internal and external hosts.

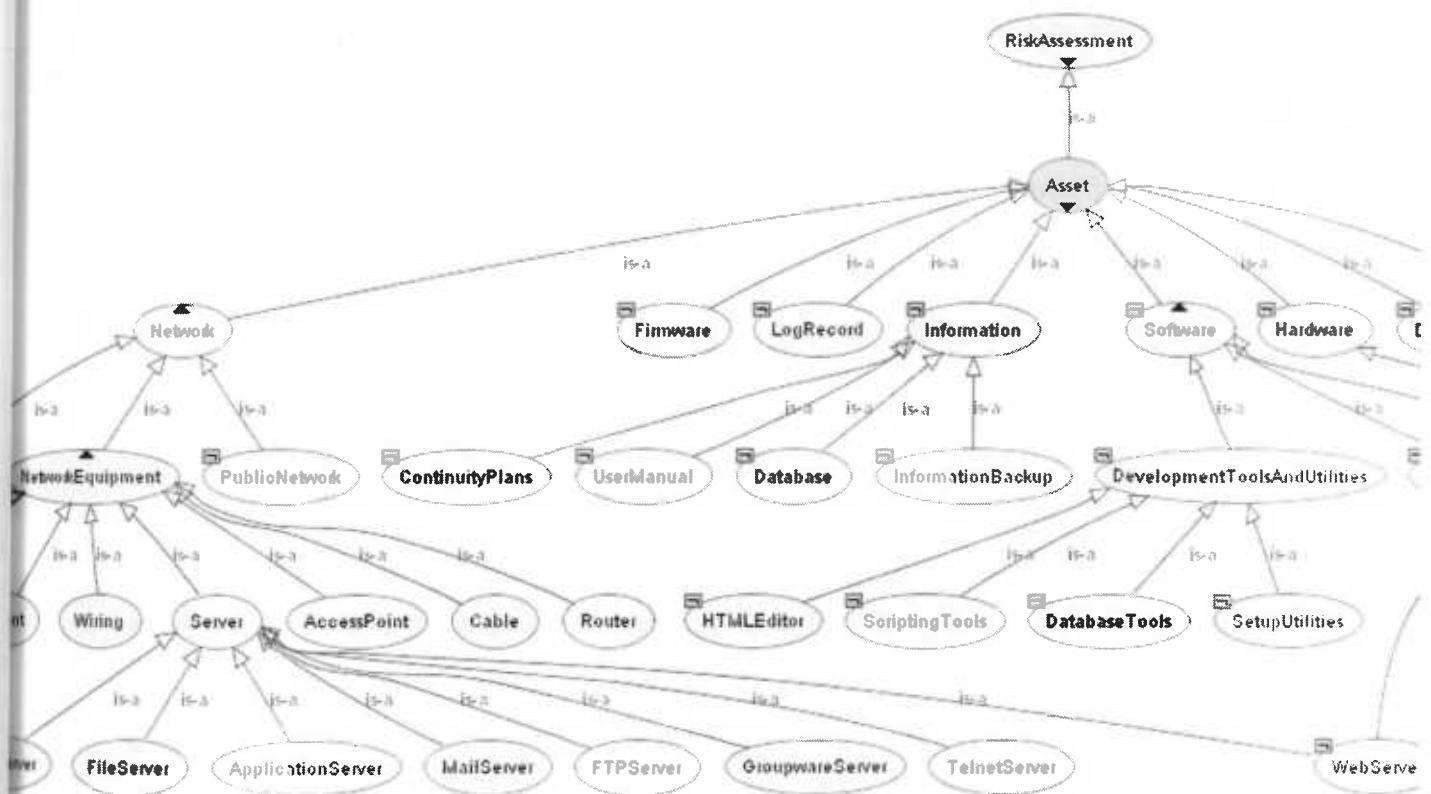
Use filters to control which systems are permitted connections with the Internet.

Passwords to be at least 6 characters long.»

Τέλος, το τελευταίο στοιχείο προς είσοδο στην εφαρμογή είναι η οντολογία ασφάλειας. Μετά την τελική επεξεργασία των αντίμετρων απαιτείται η σύνδεση των αντίμετρων με το κατάλληλο αντικείμενο της οντολογίας με απότερο σκοπό την πλήρωση του πεδίου **Threats** το οποίο αποτελεί πεδίο της τάξης Asset. Η οντολογία εισάγεται στην μέθοδο με την βοήθεια τόσο της προγραμματιστικής διεπαφής που παρέχει το Protégé αλλά και της προγραμματιστικής διεπαφής του OWL Plug-in. Παρακάτω ακολουθεί ένα μέρος της οντολογίας που χρησιμοποιείται (παρουσιάζεται

¹⁷ Βλέπε παράγραφο 1.1.4.1

μέρος της για λόγους οικονομίας χώρου – για ολόκληρη την οντολογία βλέπε παράρτημα 6.3) σε γραφική μορφή (φιλικότερη μορφή από την προγραμματιστική σε OWL). Η γραφική αποτύπωση της οντολογίας προέκυψε από την χρήση ενός επιπλέον plug-in του Protégé, το OWLViz.



Εικόνα 22 : Γραφική απεικόνιση της οντολογίας ασφάλειας

Έχοντας παρουσιάσει τα απαραίτητα στοιχεία εισόδου, στην επόμενη παράγραφο αναλύεται η μέθοδος τυπικής αποτύπωσης.

3.1.2. Επεξεργασία εισόδου με την βοήθεια του GATE

Στο σημείο αυτό παρουσιάζεται η μέθοδος καθώς και τα βασικά αλγορίθμικά βήματα τα οποία ακολουθήθηκαν με σκοπό την πλήρωση της οντολογίας. Η όλη διαδικασία στηρίχθηκε σε τεχνικές επεξεργασίας φυσικής γλώσσας. Ένα ερευνητικό πρόγραμμα σχετικά με την υλοποίηση πλατφόρμας που θα εξυπηρετεί σε τέτοιου είδους επεξεργασία είναι το GATE, a General Architecture for Text Engineering [13], το οποίο αναλύεται στην παράγραφο 2.4.2. Έχοντας λοιπόν αρωγό το εν λόγῳ λογισμικό θα προσπαθήσουμε να εξάγουμε από τα κείμενα των high-level policies (και πιο συγκεκριμένα από τα αντίμετρα που βρίσκονται σε αυτά) την απαραίτητη γνώση για κάθε οντότητα του δικτύου.

Όπως ήδη έχει αναφερθεί και στην παράγραφο 2.4.2 το GATE προσφέρει ενσωματωμένη μία σειρά διαδικασιών για επεξεργασία φυσικής γλώσσας, την ANNIE. Ένα από τα πρώτα στάδια της ANNIE είναι ο Gazetteer. Ο τελευταίος περιέχει αρχεία τα οποία με την σειρά τους περιέχουν λίστες από λέξεις / φράσεις (για συντομία λέξεις παρακάτω), μία ανά γραμμή. Τα κάθε αρχείο αντιπροσωπεύει ένα σύνολο από ονόματα, πόλεις, επαγγέλματα κ.α. Μόλις μία λέξη αναγνωριστεί από τον Gazetteer στο κείμενο, υπομνηματίζεται (annotated) με ένα προκαθορισμένο χαρακτηρισμό (Lookup) καθώς και με δύο επιπλέον χαρακτηριστικά όπου αυτά έχουν οριστεί. Τα τελευταία αποτελούν τον «μέγιστο τύπο» και τον «ελάχιστο τύπο» (majorType and minorType) της εκάστοτε λέξης. Οι τύποι αυτοί χρησιμοποιούνται για την περεταίρω επεξεργασία των λέξεων αυτών καθώς και τον τελικό υπομνηματισμό τους σε σύνολα Πόλεων, Οργανισμών, Επαγγελμάτων κ.α.

Στην μέθοδο που παρουσιάζεται το πρώτο στάδιο ήταν η δημιουργία τέτοιων αρχείων τα οποία θα περιγράφουν κοινές έννοιες. Εξετάζοντας τα αντίμετρα της CRAMM¹⁸, παρατηρούμε ότι υπάρχουν λέξεις που μας παραπέμπουν σε συγκεκριμένες κατηγορίες αντιμέτρων όπως για παράδειγμα η λέξη firewall (τείχος προστασίας), η οποία φανερώνει την κατηγορία που ανήκει το αντίμετρο. Ο Gazetteer βοηθά στην κατηγοριοποίηση του αντίμετρου, όπως για παράδειγμα αν αναγνωριστεί η λέξη firewall μέσα στο αντίμετρο τότε αυτό κατά ένα μεγάλο ποσοστό ανήκει στην κατηγορία «Network Access Controls» με υποκατηγορία «Firewalls». Τόσο οι κατηγορίες όσο και οι υποκατηγορίες των αντιμέτρων είναι δανεισμένες από την

¹⁸ Η συγκεκριμένη παρατήρηση έχει εφαρμογή σε οποιαδήποτε αντίμετρα και αν επεξεργαζόμασταν.

CRAMM. Συνεπώς μέσω αυτής της διαδικασίας αναγνώρισης λέξεων κλειδιών μπορούμε να κατηγοριοποιήσουμε το αντίμετρο (χαρακτηριστικό CM_Group από την δομή του αντίμετρου όπως αυτή παρουσιάστηκε στην παράγραφο 2.3.) Στο παράρτημα παρουσιάζονται όλες τα αρχεία τα οποία ορίστηκαν με σκοπό την αναγνώριση λέξεων ή φράσεων με κοινές ιδιότητες.

Το επόμενο στάδιο είναι η εύρεση του πεδίου target (δομή αντίμετρου). Παρόμοια με το προηγούμενο στάδιο, μέσω λεκτικής αναζήτησης, προσπαθούμε να αναγνωρίσουμε λέξεις κλειδιά οι οποίες θα φανερώνουν το πού θα εφαρμοστεί το αντίμετρο. Έτσι για παράδειγμα στην εύρεση λέξεων ή και φράσεων όπως server, application server κ.τ.λ., είναι πολύ πιθανό το αντίμετρο να εφαρμόζεται σε όλα τα στιγμιότυπα της κλάσης Server (ή μόνο σε αυτά της κλάσης Application Server αν αναγνωριστεί η φράση application server). Ταυτόχρονα απαιτείται ο ευρύτερος έλεγχος του πλαισίου στο οποίο γίνονται αναφορές σε τέτοιες λέξεις/φράσεις για να επιλυθούν προβλήματα όπως για παράδειγμα η αναφορά τόσο σε server όσο και σε clients. Σε προτάσεις αυτού του είδους απαιτείται περαιτέρω επεξεργασία και αναγνώριση κατά το δυνατόν του context της πρότασης για την τελική εξαγωγή του αντικειμένου εφαρμογής του αντίμετρου.

Τα στοιχεία που υπολείπονται για να «γεμίσουμε» την δομή των αντιμέτρων όπως αυτή έχει οριστεί είναι τα action (ενέργεια – ΤΙ πρέπει να γίνει), subject (υποκείμενο) και constraints (περιορισμοί). Η προσέγγιση που υιοθετούμε είναι με χρήση προτύπων γραφής, ή αλλιώς patterns, των αντιμέτρων. Μελετώντας τα αντίμετρα, παρατηρείται ότι είναι δυνατή η κατηγοριοποίηση αυτών με βάση την δομή της πρότασης. Για παράδειγμα οι προτάσεις

«Passwords to be changed at least once every 12 months»

«Passwords to be at least 6 characters long»

έχουν μία κοινή δομή. Ξεκινούν με ένα ουσιαστικό, το οποίο είναι και ο στόχος του αντίμετρου και συνεχίζουν με την λέξη «to» ακολουθούμενη από ένα ρήμα καθώς και κάποιες παραμέτρους. Στο άνωθεν παράδειγμα, το action που πρέπει να αποτυπωθεί είναι από το ρήμα και έπειτα (πχ to be at least 6 characters long), ενώ το target είναι το Passwords. Εκλεπτύνοντας περισσότερο την γνώση που αποκομίστηκε μπορούμε να ορίσουμε ότι τα Passwords αφορούν υπολογιστές και συνεπώς το target είναι όλα τα υπολογιστικά μηχανήματα. Η εύρεση των patterns πραγματοποιείται με την βοήθεια του POSTagger. Ο τελευταίος αποτελεί μια Υπολογιστική Οντότητα (Processing Resource, PR) ενσωματωμένη στην ANNIE. Είσοδό του έχει μία βάση με

λέξεις καθώς και τι μέρος του λόγου είναι η κάθε μια. Κατά την εκτέλεσή του αποθηκεύεται το μέρος του λόγου της κάθε λέξης σαν χαρακτηριστικό αυτής. Σε περίπτωση που μία λέξη μπορεί να είναι παραπάνω από ένα μέρος του λόγου, χρησιμοποιούνται patterns για να αναγνωρίσει τελικά τι είναι η εκάστοτε λέξη. Παράδειγμα τέτοιας λέξης είναι η λέξη *use*, η οποία μπορεί να είναι ουσιαστικό ή ρήμα. Σε περίπτωση εύρεσης της φράσης «*the use of*» τότε βάση του pattern <the> <verb> <of>, μπορεί να συμπεράνει ότι είναι ουσιαστικό.

Στη συνέχεια παρουσιάζονται τα patterns τα οποία χρησιμοποιούμε για την εξαγωγή της γνώσης. των παραπάνω πληροφοριών καθώς και το πώς αντιμετωπίζεται το κάθε pattern:

<Noun> <to> <Verb> <Something>

Στην περίπτωση αυτή το target είναι το noun και το action είναι το «<to> <Verb> <Something>». Το target μπορεί όμως να έχει οριστεί και από τον Gazetteer όπως αναφέρθηκε παραπάνω. Σε αυτή την περίπτωση τα δύο αντικείμενα εφαρμογής που βρέθηκαν συνδυάζονται για να προκύψει ένα ποιο ακριβές target. Τόσο το subject όσο και το constraints θεωρούνται τα προκαθορισμένα (βλέπε παράγραφο 1.1.4.2).

<Verb> <Something> <Preposition (πρόθεση)> <Something>

Σε αυτή την περίπτωση το action του αντίμετρου είναι το «<Verb> <Something>». Επίσης όσον αφορά στο υποκείμενο που θα εκτελέσει το αντίμετρο καθώς και στους περιορισμούς που μπορεί να έχει το αντίμετρο, το προαναφερθέν pattern δεν φανερώνει κάτι τέτοιο οπότε και θεωρούνται οι προκαθορισμένες τιμές και για τα δύο.

<Verb> <Something> <to> <Something> <Preposition (πρόθεση)><Something>

Το συγκεκριμένο πρότυπο, είναι ίσως και το πιο δύσκολο από τα προηγούμενα. Στην συγκεκριμένη περίπτωση το action θα είναι «<Verb> <Something>» και το subject το προκαθορισμένο. Όμως στην συγκεκριμένη περίπτωση υπάρχει άλλη μία πρόθεση στην πρόταση εκτός από την λέξη *to*. Η τελευταία τις περισσότερες φορές χρησιμοποιείται για να υποδηλώσει κάποιο περιορισμό στην εφαρμογή του αντιμέτρου. Για παράδειγμα μία πρόταση η οποία εμπίπτει στον κανόνα αυτό είναι η «*Use filters to restrict the level of access between internal and external hosts*». Το action «*Use filters*» δεν πρέπει να εφαρμοστεί σε όλους τους υπολογιστικούς πόρους αλλά μόνο σε εκείνους οι οποίοι συνδέονται με εξωτερικούς. Ακόμη ποιο

εκλεπτυσμένα, εγκατάσταση φίλτρων απαιτείται μόνο στους δρομολογητές εκείνους που δρομολογούν συνδέσεις μεταξύ εσωτερικών και εξωτερικών κόμβων. Άρα λοιπόν ο περιορισμός σε αυτές τις περιπτώσεις είναι το <Preposition (πρόθεση)><Something>.

Το τελευταίο πρότυπο που αναφέρθηκε παρουσιάζει μερικές ιδιαιτερότητες. Υπάρχουν περιπτώσεις στις οποίες το λήμμα <Preposition (πρόθεση)> χρησιμοποιείται απλά για διευκρινήσεις στην φράση <Something> που ακολουθεί την λέξη <to>. Σε αυτές τις περιπτώσεις δεν υπάρχει κανένας περιορισμός και ως εκ τούτου πρέπει να υπάρξει ένα διαχωρισμός μεταξύ των δύο περιπτώσεων. Μια πρόθεση που τις περισσότερες φορές, αν όχι όλες, υποδηλώνει κάποιο περιορισμό, είναι η λέξη between. Συνεπώς το παραπάνω πρότυπο εκλεπτύνεται περισσότερο και χωρίζεται σε δύο πρότυπα. Το πρώτο παραμένει το ίδιο με την μόνη διαφορά ότι ορίζεται μία λίστα από προθέσεις η οποία υποδηλώνει ύπαρξη περιορισμού και το δεύτερο το οποίο δεν ελέγχει την ύπαρξη πρόθεσης μιας και αυτή απλά διευκρινίζει προηγούμενες έννοιες. Σχηματικά λοιπόν είναι το επιπλέον πρότυπο έχει ως εξής:

<Verb> <Something> <to> <Something> <Λίστα από προθέσεις><Something>

<Verb> <Something> <to> <Something>

όπου στην «λίστα από προθέσεις» περιλαμβάνεται η λέξη between.

Αξίζει να σημειωθεί ότι τα συγκεκριμένα πρότυπα είναι απλά ένα δείγμα από το σύνολο των προτύπων που πιθανά να υπάρχουν και να προκύπτουν από την μελέτη του συνόλου των αντιμέτρων. Το αρχείο των αντιμέτρων περιέχει αντιπροσωπευτικά δείγματα από κάθε πρότυπο έτσι ώστε να γίνει κατανοητότερη η εφαρμογή των προτύπων επάνω στο κείμενο των αντιμέτρων.

Στην επόμενη παράγραφο εφαρμόζουμε τα παραπάνω στο αρχείο των αντιμέτρων και προσπαθούμε να εξάγουμε την απαραίτητη γνώση μέσω των κανόνων που ορίσαμε παραπάνω. Στο παράρτημα 6.2, παρατίθεται ο πηγαίος κώδικας σε JAVA ο οποίος υλοποιεί τα προαναφερθέντα.

3.1.3. Προσδιορισμός Απαιτήσεων Ασφάλειας βάσει των αποτελεσμάτων του GATE και της οντολογίας στο Protégé.

Στην παράγραφο αυτή θα προσπαθήσουμε να εφαρμόσουμε τις τεχνικές που αναφέρθηκαν παραπάνω στο αρχείο των αντίμετρων που παρουσιάστηκε στην παράγραφο 3.1.1. Μετά την εφαρμογή θα παρουσιάσουμε τα αποτελέσματα τα οποία προέκυψαν μετά την εφαρμογή της μεθόδου, τόσο στο γραφικό περιβάλλον του GATE (απλά για καλύτερη ανάγνωση αυτών) όσο και στο περιβάλλον κονσόλας¹⁹. Στο γραφικό περιβάλλον δεν απεικονίζεται η γνώση για κάθε πεδίο μιας αυτή προκύπτει από υλοποίηση σε κώδικα JAVA. Συγκεκριμένα στο γραφικό περιβάλλον παρουσιάζονται το CM_Group (κατηγοριοποίηση αντιμέτρου), πιθανά targets (αντικείμενο εφαρμογής), καθώς και ένας χαρακτηρισμός της πρότασης σχετικά με το ποιο πρότυπο ακολουθεί έτσι ώστε να είναι δυνατή η επεξεργασία της από το πρόγραμμα που δημιουργήθηκε.

¹⁹ Το περιβάλλον της κονσόλας προκύπτει από την εκτέλεση του προγράμματος που δημιουργήθηκε για τους σκοπούς της εργασίας και στηρίζεται στις κλήση API (Application Programming Interface) που παρέχει το GATE.

Annotations (0 selected)

Type	Set	Start	End	Features
CM_Group		4	25	{kind=cryptography, majorT=Message Security, minorT=Delivery Checking, rule=Crypt}
CM_Group		49	56	{kind=firewalls, majorT=NetworkAccessControls, minorT=Firewalls, rule=firewalls}
CM_Group		133	140	{kind=firewalls, majorT=NetworkAccessControls, minorT=Firewalls, rule=firewalls}
CM_Group		214	223	{kind=passwords, majorT=Identification And Authentication, rule=passwords}
CM_Group		252	266	{kind=password_length, majorT=Identification And Authentication, minorT=Password}

Use for signatures.

Use to restrict the level of access between internal and external hosts.

Use to control which systems are permitted connections with the Internet.

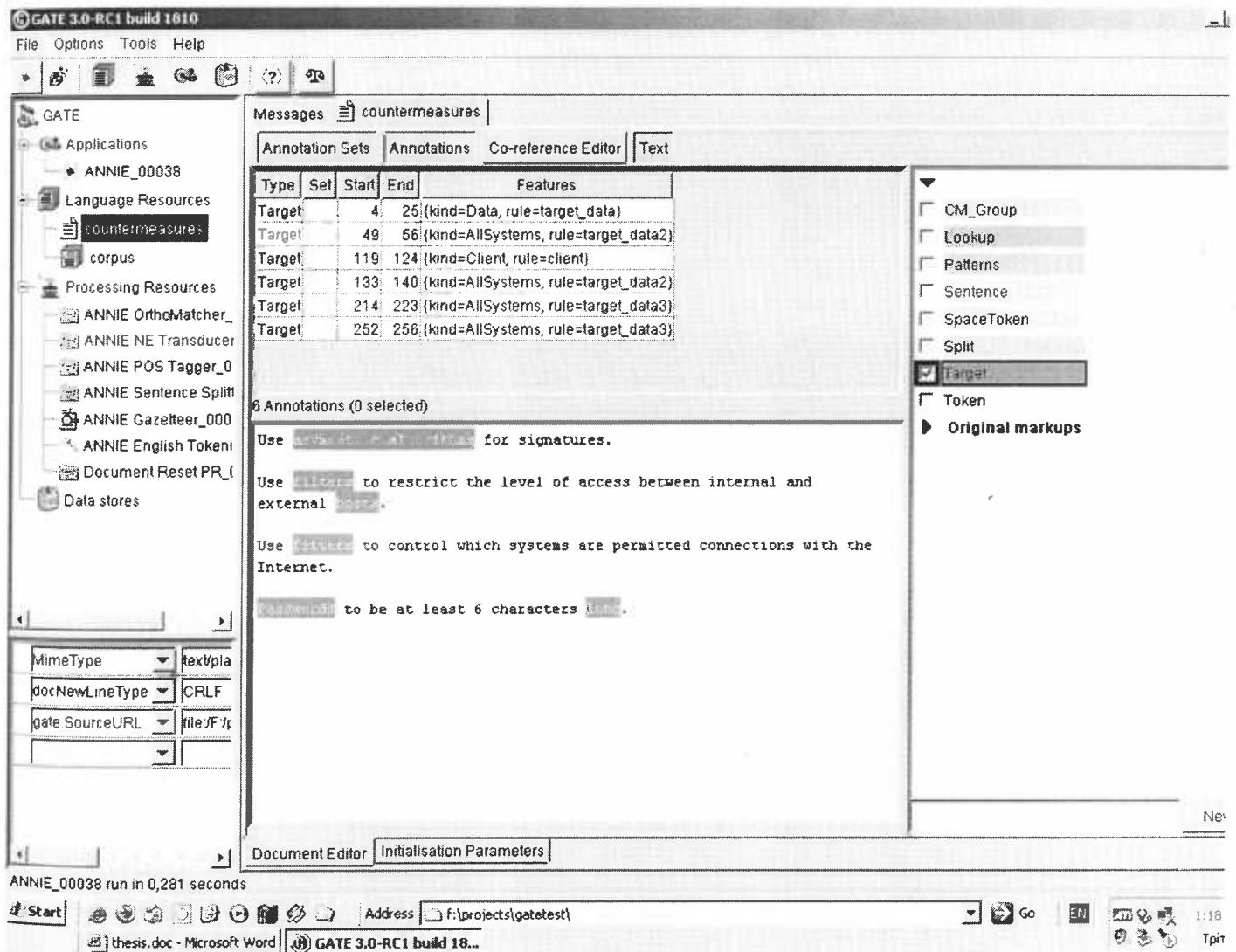
to be at least 6 characters

Εικόνα 23 : Εμφάνιση αποτελεσμάτων CM_Group

Στην παραπάνω εικόνα παρουσιάζονται οι λέξεις / φράσεις οι οποίες πιθανά να φανερώνουν την κατηγοριοποίηση του εκάστοτε αντιμέτρου. Το παράθυρο του GATE είναι χωρισμένο σε τρία μέρη. Στα δεξιά φαίνονται οι κατηγοριοποιήσεις των λέξεων και γενικώς ο οποιοσδήποτε υπομνηματισμός των φράσεων. Στο κάτω μέρος βρίσκεται το κείμενο, στο οποίο έχουν χωριστεί οι λέξεις / φράσεις ανάλογα με την επιλογή μας στο δεξιά μέρος και τέλος πάνω από το κείμενο βρίσκονται λεπτομέρειες και επιπλέον χαρακτηριστικά για την κάθε λέξη που απεικονίζεται χρωματιστά. Τα επιπλέον χαρακτηριστικά που ορίστηκαν είναι το Group στο οποίο ανήκει το αντίμετρο (majorT=NetworkAccessControl) καθώς και η υποκατηγορία αυτού, όπου αυτό έχει οριστεί (minorT=Firewalls). Παρατηρούμε λοιπόν ότι για την φράση asymmetric algorithms το σύστημα κατηγοριοποίησε την λέξη ως Message Security



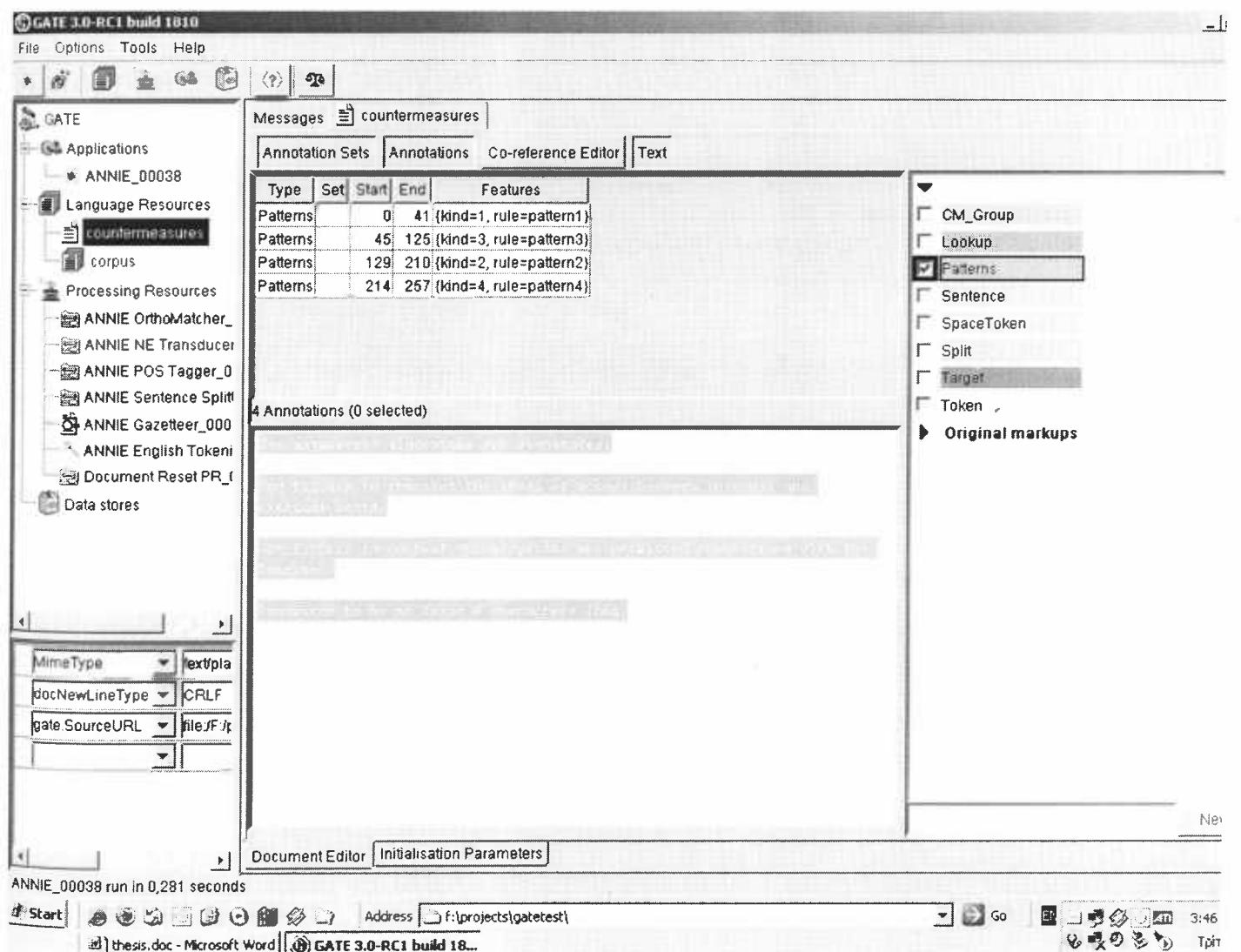
με υποκατηγορία Delivery Checking, την λέξη filters ως NetworkAccessControls με υποκατηγορία Firewalls και τέλος την λέξη Passwords ως Identification and Authentication και τέλος την λέξη long ως Identification and Authentication με υποκατηγορία Password Length (με έλεγχο του context στο οποίο βρέθηκε η λέξη). Οι παρατηρήσεις αυτές θα μας βοηθήσουν στην συνέχεια όπου βάσει αυτών θα είναι εφικτή η πλήρωση του πεδίου CM_Group (δομή αντίμετρου).



Εικόνα 24 : Εμφάνιση αποτελεσμάτων Target

Στην παραπάνω εικόνα παρουσιάζονται τα αποτελέσματα της αναζήτησης του αντικειμένου εφαρμογής του εκάστοτε αντίμετρου. Οι λέξεις από τις οποίες είναι εφικτή η εξαγωγή ενός συμπεράσματος αποκτούν ένα χαρακτηρισμό (annotation) Target. Επιπλέον χαρακτηριστικό του συγκεκριμένου υπομνηματισμού είναι το kind,

το οποίο φανερώνει το που τελικά θα εφαρμοστεί το αντίμετρο. Έτσι οι λέξεις που έχουν αναγνωριστεί ως πιθανά targets είναι οι asymmetric algorithms με kind=Data, η λέξη filters με kind>AllSystems²⁰, η λέξη Passwords με kind>AllSystems, η λέξη hosts με kind=Clients και τέλος η λέξη long με kind>AllSystems. Αξίζει να σημειωθεί ότι ενώ η λέξη passwords θεωρητικά παραπέμπει σε δεδομένα, εντούτοις αποτελεί μία ρύθμιση των μηχανημάτων τα οποία θέλουμε να προφυλάξουμε με στοιχειώδης μηχανισμούς πρόσβασης. Έτσι σε περίπτωση αναγνώρισης τέτοιου ειδών λέξεων / φράσεων το αντικείμενο εφαρμογής της οντολογίας θα είναι όλα τα μηχανήματα που συμμετέχουν στο δίκτυο και όχι τα δεδομένα.



Εικόνα 25 : Εμφάνιση αποτελεσμάτων Pattern

²⁰ Στην υλοποίηση της μεθόδου υποθέσαμε για απλότητα ότι η εφαρμογή τυχόν τειχών προστασίας (firewalls) μπορεί να γίνει σε οποιοδήποτε μηχάνημα και όχι αποκλειστικά σε δρομολογητές. Για τον λόγο αυτό σε πιθανή εύρεση λέξεων που να υποδηλώνουν ύπαρξη firewall υποθέτουμε ότι το αντίμετρο έχει εφαρμογή σε όλα τα συστήματα (kind>AllSystems)

Τέλος κατά την εκτέλεση της ANNIE ένα ακόμα στοιχείο το οποίο παρουσιάζεται είναι ο χαρακτηρισμός Pattern. Ανάλογα με το πώς είναι δομημένη η κάθε πρόταση, χαρακτηρίζεται και ανάλογα έτσι ώστε στην μετέπειτα επεξεργασία από τον κώδικα που αναπτύχθηκε να μπορέσουμε από κάθε πρόταση να εξάγουμε την κάθε απαραίτητη πληροφορία. Έτσι λοιπόν, όπως φανερώνεται και στην Εικόνα 25 κάτω από τον υπομνηματισμό (annotation) Pattern υπάρχει ένα επιπλέον πεδίο το kind το οποίο λαμβάνει αριθμητικές τιμές. Με μια μικρή αναλογία των αντιμέτρων με τους αριθμούς αυτούς μπορούμε εύκολα στην συνέχεια, εξετάζοντας το πεδίο αυτό να αποφανθούμε με ποιο pattern συμφωνεί η πρόταση αυτή. Στη συνέχεια ακολουθεί ένας πίνακας με τις αντιστοιχίσεις αυτές.

No	Αντιστοιχίσεις Αριθμών με Πρότυπα Γραφής Αντιμέτρων (Patterns)
1	<Verb> <Something> <Preposition (πρόθεση)> <Something>
2	<Verb> <Something> <to> <Something>
3	<Verb> <Something> <to> <Something> <Λίστα από προθέσεις> <Something>
4	<Noun> <to> <Verb> <Something>

Στην συνέχεια της παρουσίασης των αποτελεσμάτων παραθέτουμε τα αποτελέσματα όπως αυτά προέκυψαν από την εκτέλεση του κώδικα. Ο τελευταίος παρουσιάζεται καθολικά στο παράστημα.

Parousiasi domis antimetrou gia tin kathe protasi.

Sentence No 1

Subject: Administrators
 Group: GROUP: NetworkAccessControls SUBGROUP: Firewalls
 Target: AllSystems
 Action: Use filters

Constraints: No Constrain

Sentence No 2

Subject: Administrators
 Group: GROUP: Identification And Authentication SUBGROUP:
 Password Length
 Target: AllSystems
 Action: Passwords to be at least 6 characters long.
 Constraints: No Constrain

Sentence No 3

Subject: Administrators
 Group: GROUP: Message Security SUBGROUP: Delivery Checking
 Target: Data
 Action: Use asymmetric algorithms
 Constraints: No Constrain

Sentence No 4

Subject: Administrators
 Group: GROUP: NetworkAccessControls SUBGROUP: Firewalls
 Target: Client, AllSystems
 Action: Use filters
 Constraints: between internal and external hosts.

Στις πρώτες γραμμές εμφανίζονται μηνύματα που αφορούν στην εκκίνηση του GATE καθώς και στην αρχικοποίηση των διαδικασιών της ANNIE. Στη συνέχεια παρουσιάζονται τα αποτελέσματα εφαρμογής της μεθόδου στο αρχείο των αντιμέτρων. Για κάθε πρόταση εμφανίζονται τα πεδία της δομής του αντίμετρου όπως αυτή ορίστηκε σε προηγούμενες παραγράφους.

3.2. Αξιολόγηση Αποτελεσμάτων

Στις επόμενες παραγράφους ακολουθεί μία κριτική επισκόπηση των αποτελεσμάτων καθώς και μία σύγκριση αυτών με τα αποτελέσματα τα οποία θα εξαγόντουσαν με την βοήθεια ανθρώπινης δραστηριότητας.

3.2.1. Σύγκριση αποτελεσμάτων με τα επιθυμητά αποτελέσματα

Στο σημείο αυτό θα εξετάσουμε τα αποτελέσματα τα οποία προέκυψαν από την εφαρμογή της μεθόδου με τα αποτελέσματα τα οποία θα προέκυπταν από την ανθρώπινη επεξεργασία των δεδομένων. Όπως προαναφέρθηκε τα αντίμετρα τα οποία υπέστησαν επεξεργασία είναι τα ακόλουθα:

Use filters to control which systems are permitted connections with the Internet.

Passwords to be at least 6 characters long.

Use asymmetric algorithms for signatures.

Use filters to restrict the level of access between internal and external hosts.

Αναφορικά με το πρώτο αντίμετρο μπορούμε να παρατηρήσουμε τα εξής. Η ενέργεια που πρέπει να γίνει συμπίπτει με την εξαγομένη από το πρόγραμμα ενέργεια, Use filters. Επιπλέον το υποκείμενο το οποίο θα εφαρμόσει το αντίμετρο είναι οι διαχειριστές, όπως άλλωστε μπορεί να συμπεράνει και κάποιος διαβάζοντας το αντίμετρο. Τέλος η κατηγοριοποίηση του αντιμέτρου έχει γίνει εν μέρει με σωστό τρόπο μιας και το Group το οποίο ανήκει το αντίμετρο είναι όντως το Network Access Controls, όμως το subgroup έπρεπε να ήταν το Internet Firewalls και όχι Firewalls. Σχετικά με το αντικείμενο εφαρμογής του αντιμέτρου, AllSystems, θα μπορούσε να ισχυριστεί κάποιος ότι θα ήταν προτιμότερο να υλοποιηθούν οι έλεγχοι πρόσβασης στις συσκευές δικτύου και όχι σε κάθε τερματική συσκευή ζεχωριστά. Αν και η καλύτερη τεχνική είναι η τελευταία, αυτό δεν σημαίνει ότι η σύμβαση η οποία υιοθετήσαμε, δηλ. η εφαρμογή τέτοιων ελέγχων να γίνεται σε κάθε τερματική συσκευή, δεν είναι σωστή. Παρόλα αυτά, αν θελήσουμε να εκλεπτύνουμε το σημείο αυτό θα χρειαστεί περαιτέρω που αφορά στις συνδέσεις με το Internet (πχ

πραγματοποιούνται μέσω κεντρικού δρομολογητή; Είναι κλήση τηλεφωνική μέσω κάποιου φορέα; κ.α.).

Το επόμενο αντίμετρο αποτελεί ίσως και το ευκολότερο αναφορικά με την προσέγγιση που έχει παρουσιαστεί σε προηγούμενες παραγράφους. Η δομή του είναι σχετικά απλή και συνεπώς όλα τα πεδία τα οποία έχουν οριστεί στην δομή του αντιμέτρου μπορούν εύκολα να προκύψουν με την προσέγγιση που ακολουθείται. Έτσι όλα τα πεδία συμφωνούν με αυτά τα οποία αποτύπωνε κάποιος από την ανάλυση του αντίμετρου. Η μόνη ίσως διαφορά η οποία μπορεί να προέκυπτε είναι στο υποκείμενο που θα εφαρμόσει το αντίμετρο αυτό. Συγκεκριμένα, θα μπορούσε να παρατηρηθεί ότι το password του κάθε χρήστη είναι προσωπικό και κάτω από την ευθύνη του καθενός να πληρεί κάποιες προϋποθέσεις, όπως στο συγκεκριμένο παράδειγμα εκείνο το μήκους. Άρα θα μπορούσαμε να πούμε ότι το υποκείμενο είναι συνολικά οι χρήστες και όχι ειδικά οι διαχειριστές.

Συνεχίζοντας την ανάλυση των αντιμέτρων, παρατηρούμε τα εξής για το τρίτο κατά σειρά αντίμετρο. Η κατηγοριοποίηση του αντιμέτρου συμπίπτει με την κατηγοριοποίηση που προέκυψε, θεωρώντας βέβαια ότι και ο ειδικός στην ασφάλεια ο οποίος θα κατηγοριοποιήσει τα αντίμετρα θα χρησιμοποιήσει και αυτός τα groups και τα subgroups της CRAMM. Η ενέργεια που πρέπει να γίνει (TI), είναι η χρήση των ασύμμετρων αλγορίθμων για τις ηλεκτρονικές υπογραφές. Στα αποτελέσματα τις μεθόδου η ενέργεια συμπίπτει με την παραπάνω παρατήρηση. Επιπλέον το αντικείμενο εφαρμογής είναι τα δεδομένα όπως αυτό παρουσιάστηκε και στην προηγούμενη παράγραφο. Τέλος και ο τομέας των αντιμέτρων συμπίπτει με τα υπολογιστικά αποτελέσματα μιας και δεν προκύπτει από το αντίμετρο κάποιο είδος περιορισμού στην εφαρμογή του αντίμετρου. Αντιθέτως η ανθρώπινη επεξεργασία θα διέφερε με τα αποτελέσματα στο υποκείμενο το οποίο θα εφαρμόσει το αντίμετρο αυτό. Ενώ στα αποτελέσματα της μεθόδου παρουσιάστηκε υποκείμενο οι διαχειριστές, εύκολα μπορεί κανείς να συμπεράνει ότι το συγκεκριμένο αντίμετρο θα το εφαρμόσουν ακόμα και οι χρήστες στην ανταλλαγή μηνυμάτων αν φυσικά χρησιμοποιούν ηλεκτρονικές υπογραφές. Συνεπώς το υποκείμενο είναι οι χρήστες στο σύνολό τους και όχι μόνο οι διαχειριστές. Η εξαγωγή του πεδίου αυτού απαιτεί ιδιαίτερη τροφοδότηση του συστήματος με έμμεση γνώση. Συγκεκριμένα ο συλλογισμός που πραγματοποιήθηκε ήταν το γεγονός ότι οι ηλεκτρονικές υπογραφές χρησιμοποιούνται από όλους όσους έχουν δικαίωμα αποστολής και παραλαβής

μηνυμάτων και άρα και αυτοί πρέπει να ανήκουν στο υποκείμενα εφαρμογής του αντιμέτρου.

Εξετάζοντας το επόμενο αντίμετρο διαπιστώνουμε τα εξής. Αναφορικά με το υποκείμενο (subject), την ενέργεια (action) καθώς και την κατηγοριοποίηση του αντιμέτρου, η ανθρώπινη επεξεργασία θα παρήγαγε τα ίδια αποτελέσματα, δηλαδή τους διαχειριστές (administrators) για το υποκείμενο, την χρησιμοποίηση φίλτρων (Use filters) ως την ενέργεια, και το Network Access Controls και Firewalls ως το group και το subgroup, αντίστοιχα του αντίμετρου. Αναφορικά με το αντικείμενο εφαρμογής και τους περιορισμούς του αντιμέτρου, οι κανόνες που έχουμε θεσπίσει στην εφαρμογή παρουσίασαν δύο αντικείμενα, τα Client και AllSystems, και περιορισμό το between internal and external hosts. Το αντίμετρο αφορά σε εγκαθίδρυση συνδέσεων μεταξύ εσωτερικών και εξωτερικών υπολογιστών. Αυτό με την σειρά του συνεπάγεται ότι τα φίλτρα τα οποία θα εγκατασταθούν δεν είναι ανάγκη να υπάρχουν σε κάθε μηχάνημα το οποίο πραγματοποιεί μία τέτοια σύνδεση. Αντίθετα η εγκατάσταση τέτοιων φίλτρων πρέπει να γίνει σε συσκευές δικτύου όπως Firewalls, ή δρομολογητών μέσω των οποίων εγκαθίσταται μία τέτοια σύνοδος. Συνεπώς το αντίμετρο δεν εφαρμόζεται καθολικά αλλά μόνο σε συσκευές δικτύου. Κάτι τέτοιο, όπως και στην προηγούμενη περίπτωση, απαιτεί την εξαγωγή έμμεσης γνώσης ή την τροφοδότηση του συστήματος με αυτή, η οποία αφορά στο κομμάτι των συνδέσεων μεταξύ δύο υπολογιστών, του εσωτερικού του δικτύου καθώς και του εξωτερικού.

Στην συνέχεια ακολουθεί το αρχείο εξόδου όπως αυτό παρουσιάστηκε σε προηγούμενη παράγραφο με την μόνη διαφορά ότι παρουσιάζονται (μέσα σε παρενθέσεις και με πλάγια γραφή) και τα αποτελέσματα που θα προέκυπταν από ανθρώπινη επεξεργασία.

Parousiasi domis antimetrou gia tin kate protasi.

Sentence No 1

Subject: Administrators (*Administrators*)
 Group: GROUP: NetworkAccessControls SUBGROUP: Firewalls
 (*GROUP: NetworkAccessControls* *SUBGROUP: Internet*
 Firewalls)
 Target: AllSystems (*Routers*)
 Action: Use filters (*Use filters*)
 Constraints: No Constrain (*Only to those routers that establish connections with the Internet*)

Sentence No 2

Subject: Administrators (*Everyone*)
 Group: GROUP: Identification And Authentication SUBGROUP:
 Password Length (*GROUP: Identification And Authentication*
 SUBGROUP: Password Length)
 Target: AllSystems (*AllSystems*)
 Action: Passwords to be at least 6 characters long. (*Passwords to be at least 6 characters long.*)
 Constraints: No Constrain (*No constraint*)

Sentence No 3

Subject: Administrators (*Everyone*)
 Group: GROUP: Message Security SUBGROUP: Delivery Checking
 (*GROUP: Message Security* *SUBGROUP: Delivery Checking*)
 Target: Data (*Data*)
 Action: Use asymmetric algorithms (*Use asymmetric algorithms*)
 Constraints: No Constrain (*No constrain*)

Sentence No 4

Subject: Administrators (*Administrators*)
Group: GROUP: NetworkAccessControls SUBGROUP: Firewalls
(*GROUP: NetworkAccessControls SUBGROUP: Firewalls*)
Target: Client, AllSystems (*Routers*)
Action: Use filters (*Use filters*)
Constraints: between internal and external hosts. (*between internal and external hosts.*)

3.2.2. Κριτική επισκόπηση των αποτελεσμάτων της τυπικής αποτύπωσης

Στην παράγραφο αυτή παρουσιάζεται μία κριτική των αποτελεσμάτων, όπως αυτά παρουσιάστηκαν σε προηγούμενη ενότητα. Τα αποτελέσματα τα οποία προέκυψαν από την υλοποίηση της μεθόδου θα μπορούσαν να χαρακτηριστούν ικανοποιητικά όχι όμως καθολικά. Ένα από τα σημεία τα οποία δεν υλοποιήθηκαν είναι αυτό της σύνδεσης με την οντολογία. Δυστυχώς ο χρόνος που διήρκησε η εκπόνηση αυτής της διπλωματικής εργασίας δεν είναι αρκετός για την υλοποίηση ενός τέτοιου εγχειρήματος. Υπό φυσιολογικές συνθήκες κάτι τέτοιο θα απαιτούσε αρκετούς ανθρώπινους πόρους και ολοκληρωτική αφοσίωση των εμπλεκομένων στο θέμα αυτό.

Στον τομέα της εξαγωγής της γνώσης από τα αντίμετρα της πολιτικής ασφάλειας μπορούμε να παρατηρήσουμε τα εξής. Η προσέγγιση που ακολουθήθηκε με την υιοθέτηση της αναγνώρισης κάποιων προτύπων δεν αποτελεί πανάκια. Πιθανά να υπάρχουν και άλλες προσεγγίσεις οι οποίες να παρουσιάσουν καλύτερα αποτελέσματα. Αυτό μπορεί να γίνει κατανοητό μελετώντας τα αποτελέσματα που παρουσιάστηκαν. Ένα μεγάλο μειονέκτημα της μεθόδου αυτής είναι το γεγονός ότι σε πολλές περιπτώσεις απαιτείται ο συνδυασμός της γνώσης που προέκυψε με έμμεση γνώση (γνώση που προκύπτει από συλλογισμούς αντίστοιχους με τους ανθρώπινους). Η μέθοδος με τα πρότυπα πιθανά να συνδυάζεται δυσκολότερα με την έμμεση γνώση από ότι μια τελείως διαφορετική προσέγγιση. Μια τέτοια εκλέπτυνση όμως είναι αναγκαία για την ακριβέστερη αποτύπωση των απαιτήσεων ασφάλειας με τυπικό τρόπο. Συνεπώς μία μέθοδος η οποία θα λαμβάνει υπόψη της περισσότερο την υπονοούμενη γνώση μπορεί να παρουσιάσει ακριβέστερα αποτελέσματα.

Επιπλέον τα εργαλεία τα οποία χρησιμοποιήθηκαν για την εφαρμογή της μεθόδου (GATE και Protégé) δεν είναι αρκετά ώριμα για να υποστηρίξουν ένα τέτοιο εγχείρημα. Και τα δύο λογισμικά δημιουργήθηκαν από πανεπιστημιακές έρευνας και βρίσκονται συνεχώς υπό ανάπτυξη. Επίσης τα εγχειρίδια χρήσης που παρέχονται αφορούν στην συντριπτική τους πλειοψηφία την χρήση της γραφικής διεπαφής και όχι του παρεχόμενου API. Το γεγονός αυτό καθιστά ακόμα δυσκολότερη την δημιουργία μιας εφαρμογής που θα βασίζεται στο API και των δύο προγραμμάτων. Τέλος υπάρχουν αρκετά σημεία και στα δύο προγράμματα τα οποία δεν έχουν υλοποιηθεί και θα βοηθήσουν προς την κατεύθυνση της υλοποίησης της μεθόδου. Χαρακτηριστικά αναφέρουμε την διαχείριση οντολογιών μέσω του GATE. Τόσο

στην ιστοσελίδα όσο και στα εγχειρίδια χρήσης αναφερόταν η διαχείριση οντολογιών μέσα από το GATE και ταυτόχρονα η σύνδεσή της με το κείμενο και τους χαρακτηρισμούς των λέξεων (annotations) που έχουν προκύψει μετά την εκτέλεση της ANNIE. Μετά από αρκετές μέρες πειραματισμού διαπιστώθηκε ότι κάτι τέτοιο δεν είχε υλοποιηθεί απλά υπήρχαν οι συναρτήσεις χωρίς καμία λειτουργικότητα (κατά την κλήση τους αυτές δεν εκτελούσαν τίποτα). Σε ηλεκτρονική επικοινωνία που υπήρξε με τους προγραμματιστές του GATE μας επιβεβαίωσαν το γεγονός και μας προέτρεψαν να επεκτείνουμε τον κώδικα μόνοι μας. Είναι λοιπόν φανερό ότι η υλοποίηση μιας τέτοιας προσέγγισης με τέτοιες δυσκολίες και με δεδομένο τον περιορισμένο χρόνο, δεν μπορεί παρά να είναι εν μέρει σωστή και να απαιτεί περαιτέρω χρόνο αλλά και υποστήριξη από ωριμότερα προγράμματα.

Από την άλλη πλευρά μπορούμε να πούμε ότι η συγκεκριμένη μέθοδος αποτελεί ένα τελείως διαφορετικό βήμα από τις υπάρχουσες προσεγγίσεις προς την κατεύθυνση της τυπικής αποτύπωσης των απαιτήσεων ασφάλειας και ιδιωτικότητας των δικτύων. Στις υπόλοιπες προσεγγίσεις υπονοείται η ύπαρξη ενός ατόμου ειδικού στην ασφάλεια πληροφοριακών συστημάτων ο οποίος έχει ταυτόχρονη γνώση και της μεθόδου που υλοποιείται για να μπορεί να αποτυπώσει τυπικά τα αντίμετρα της πολιτικής ασφάλειας στην εκάστοτε μέθοδο. Το γεγονός ότι εστιάζουμε την πρόσοχή μας στην αυτοματοποίηση της μεθόδου με όσο το δυνατόν λιγότερη ανθρώπινη παρέμβαση, καθιστά την προσέγγιση που παρουσιάζεται στην διπλωματική εργασία ευέλικτη και εύκολα προσαρμόσιμη σε τυχόν αλλαγές του δικτύου, όπως άλλωστε συμβαίνει και με τα ad-hoc δίκτυα.

Ταυτόχρονα ένα ακόμη πλεονέκτημα της προσέγγισης αυτής είναι η χρήση των οντολογιών ως αποθηκευτικό μέσο της γνώσης περί των απαιτήσεων ασφάλειας. Οι περισσότερες από τις υπάρχουσες προσεγγίσεις εστιάζουν την προσοχή τους μόνο στο κομμάτι της τυπικής αποτύπωσης των απαιτήσεων ασφάλειας χωρίς να λαμβάνουν υπόψη τους αρκετές παραμέτρους όπως για παράδειγμα επαναχρησιμοποίηση της γνώσης, εύκολη ανάγνωση και διαχείριση από ανθρώπους που δεν γνωρίζουν την μέθοδο καθώς και την πολυπλοκότητα του συγκεκριμένου ερευνητικού τομέα. Αναφορικά με το τελευταίο, οι οντολογίες προσφέρουν αιτιολογικούς μηχανισμούς που αφορούν στην εξαγωγή συμπερασμάτων για τις κλάσης που συμμετέχουν στην οντολογία, όπως για παράδειγμα συνθήκες ικανού και αναγκαίου, σύνδεση τάξεων μεταξύ τους κάτω από ορισμένες συνθήκες κ.α.



Τέλος η μέθοδος που αναλύθηκε είναι αρθρωτή σε όλο το εύρος της. Το γεγονός αυτό την καθιστά εύκολη στην διαχείρισή της σε περιπτώσεις λαθών αλλά και, το σημαντικότερο, στην υλοποίηση και ανάπτυξή της. Το τμήμα της εξαγωγής της γνώσης είναι τελείως αυτόνομο σε σχέση με την τυπική αποτύπωση της γνώσης. Επιπλέον, και το τμήμα της εξαγωγής γνώσης από τα αντίμετρα αποτελείται από τέσσερα διακριτά τμήματα όπως αυτά παρουσιάζονται στην Εικόνα 16. Έτσι για παράδειγμα σε τυχόν αλλαγή της διαδικασίας εισαγωγής της διαχειριστικής πληροφορίας στην οντολογία δεν επηρεάζονται τα υπόλοιπα τμήματα της μεθόδου αλλά ούτε και η οντολογία ασφάλειας.

4. Συμπεράσματα και Μελλοντική Έρευνα

Η έννοια της ασφάλειας αποτελεί πλέον ένα από τα κυρίαρχα ζητήματα σε μεγάλα, αλλά και μικρά, υπολογιστικά συστήματα. Η πολυπλοκότητα των υπολογιστικών συστημάτων σε συνδυασμό με την αλληλεπίδρασή τους μέσω δικτύων και του Παγκόσμιου Ιστού, καθιστούν την ασφάλεια ένα κρίσιμο παράγοντα για τους σύγχρονους οργανισμούς. Τα τελευταία χρόνια έχει δοθεί ιδιαίτερο βάρος στη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων. Η τυπική αποτύπωση των απαιτήσεων ασφάλειας αποτελεί μείζον θέμα, ιδίως στην περίοδο της συνεχούς αυξανόμενης κλίμακας τόσο των ενδο-εταιρικών δικτύων όσο και του Παγκόσμιου Ιστού γενικότερα.

Σκοπός της διατριβής αυτής είναι η παρουσίαση μίας καινοτομικής μεθόδου προς την κατεύθυνση της τυπικής αποτύπωσης των απαιτήσεων ασφάλειας. Συγκεκριμένα η μέθοδος αυτή χρησιμοποιεί έννοιες που αποτελούν την αιχμή του δόρατος τόσο στον τομέα της εξαγωγής γνώσης από φυσική γλώσσα (Natural Language Processing) όσο και στον τομέα της αποτύπωσης γνώσης με τυπικό τρόπο (οντολογίες). Αν και η θεωρητική θεμελίωση της προσέγγισης αυτής δομείται ικανοποιητικά, το πρακτικό μέρος υπολείπεται, εξαιτίας του περιορισμένου χρόνου για την υλοποίηση ενός τέτοιου εγχειρήματος καθώς και της χρήσης εργαλείων που βρίσκονται ακόμα σε ανάπτυξη και διαρκή αξιολόγηση.

Τα αποτελέσματα τα οποία παρουσιάστηκαν σε προηγούμενες ενότητες αποτελούν ένα πρώτο βήμα προς την υλοποίηση της αρχιτεκτονικής που παρουσιάστηκε στην παράγραφο 2.3. Η ταύτιση του θεωρητικού υποβάθρου με το πρακτικό αλλά και η βελτίωση της μεθόδου τυπικής αποτύπωσης των απαιτήσεων ασφάλειας στο σύνολό της απαιτεί περαιτέρω έρευνα και προσπάθεια. Τα κύρια σημεία αυτής παρουσιάζονται στην συνέχεια ξεκινώντας από βραχυπρόθεσμους στόχους που μπορούν να πραγματοποιηθούν άμεσα και καταλήγοντας σε σκέψεις και προτάσεις για συνολική ανάπτυξη της μεθόδου.

- Αρχικά ένα πρώτο στάδιο αποτελεί η άρση των περιορισμών που έχουν υιοθετηθεί στην παράγραφο 1.1.4.2. Έτσι κύριος στόχος είναι η επέκταση της μεθόδου έτσι ώστε να είναι ικανή να αναγνωρίσει τόσο το αντικείμενο



εφαρμογής ενός αντιμέτρου καθώς και το υποκείμενο που θα το εφαρμόσει με μεγαλύτερο βαθμό ακρίβειας.

- Επόμενο στάδιο είναι η επέκταση της σημασιολογικής ανάλυσης του κειμένου. Η υπάρχουσα μέθοδος που χρησιμοποιείται είναι σε θέση να αναγνωρίσει ένα πολύ μικρό ποσοστό των αντιμέτρων όσον αφορά στην κατηγοριοποίηση αυτού αλλά και στην αναγνώριση του προτύπου που ανήκει (βλέπε ενότητα 3). Για τον σκοπό αυτό πρέπει να μελετηθούν περισσότερα αντίμετρα και στην συνέχεια να προσπαθήσουμε να εξάγουμε κοινά πρότυπα (patterns) που αφορούν στην δομή της πρότασης.
- Η οντολογία ασφάλειας που παρουσιάστηκε στην παράγραφο 2.2.1 αποτελεί μερική αποτύπωση γνώσης περί την διαχείριση ασφάλεια των πληροφοριακών συστημάτων. Η επέκτασή της με καινούργιες έννοιες / κλάσεις με την βοήθεια των οποίων θα αποτυπώνεται επαρκέστερα και ακριβέστερα η γνώση περί την διαχείριση της ασφάλειας των Π.Σ. κρίνεται αναγκαία για την επέκταση της μεθόδου.
- Μία επιπλέον κατεύθυνση έρευνας αποτελεί η βελτίωση της μεθόδου στον τομέα της επεξεργασίας των διαδικαστικών αντιμέτρων (procedural countermeasures) ασφάλειας. Τα διαδικαστικά αντίμετρα αποτελούν ίσως την δυσκολότερη μορφή αντιμέτρων αναφορικά με την επεξεργασία φυσικής γλώσσας. Αιτία, και συνάμα μία ακόμη κατεύθυνση που πρέπει να εξερευνηθεί περαιτέρω, είναι το γεγονός ότι για την εξαγωγή γνώσης από τα περισσότερα αντίμετρα απαιτείται η τροφοδότηση του συστήματος με έμμεση γνώση σε μεγάλο βαθμό. Όπως παρατηρήθηκε και στην παράγραφο 3.1.3 σημαντικό ρόλο στην εικλέπτυνση των στοιχείων ενός αντιμέτρου διαδραματίζει η ανθρώπινη σκέψη η οποία επαγωγικά μπορεί να εξάγει κάποια συμπεράσματα σχετικά με την εφαρμογή του αντιμέτρου. Πρέπει λοιπόν το σύστημα να είναι σε θέση να αναζητήσει την γνώση που του λείπει στο σωστό σημείο (πχ Γνωσιακές βάσεις δεδομένων, άνθρωποι κ.α.)

5. Βιβλιογραφία

- [1] Cunningham H., 1999, *Information Extraction: a User Guide (revised version)*, Research Memorandum CS-99-07, Department of Computer Science, University of Sheffield.
- [2] Lassila O., Swick R.R., 1999, *Resource Description Framework (RDF) Model and Syntax Specification*, W3C Proposed Recommendation, <http://www.w3.org/TR/PR-rdf-syntax/>, Δεκέμβριος 2004.
- [3] Μπαμπινιώτης Γ., 1998, Λεξικό της Νέας Ελληνικής Γλώσσας, Κέντρο Λεξικολογίας, Αθήνα.
- [4] Crowther J., 1995, Oxford: Advanced Learner's Dictionary, Oxford University Press, USA.
- [5] Bray T., Paoli J., Sperberg-McQueen C. M., and Maler E., 2000, *Extensible Markup Language (XML) 1.0 (Second Edition)*, W3C Recommendation, Technical report, World Wide Web Consortium, <http://www.w3.org/TR/REC-xml>, Δεκέμβριος 2004.
- [6] Brickley D. and Guha R., 2000, *Resource Description Framework (RDF) Schema Specification 1.0.*, W3C Recommendation, <http://www.w3.org/TR/2000/CR-rdf-schema-20000327/>
- [7] Dean M., Connolly D., Harmelen F., Hendler J., Horrocks I., McGuinness D. L., Patel-Schneider P. F., 2002, *OWL Web Ontology Language 1.0 Reference*, [ON-LINE], <http://www.w3.org/TR/owl-ref/>, Δεκέμβριος 2004.
- [8] Fensel D., Horrocks I., Harmelen F., Decker S., Erdmann M., and Klein M., 2000, “OIL in a nutshell”, *In Proc. of the 12th Eur. Workshop on Knowledge Acquisition, Modelling, and Management (EKAW'00)*, 1937: 1–16.
- [9] Fensel D., Harmelen F., Horrocks I., McGuinness D. L., and Patel-Schneider P. F., 2001, “OIL: An ontology infrastructure for the semantic web”, *IEEE Intelligent Systems*, 16(2):38–45.
- [10] Hendler J. and McGuinness D. L., 2000, “The DARPA Agent Markup Language”, *IEEE Intelligent Systems*, 15(6):67–73.
- [11] Lassila O. and Swick R. R., 1999, *Resource Description Framework (RDF) Model and Syntax Specification*, W3C Recommendation, Technical report,



- World Wide Web Consortium, <http://www.w3.org/TR/1999/REC-rdf-syntax-19990222/>, Δεκέμβριος 2004.
- [12] Smith M., Welty C., McGuinness D., 2004, *OWL Web Ontology Language Guide*, W3C Recommendation, <http://www.w3.org/TR/owl-guide/>, Δεκέμβριος 2004.
- [13] Cunningham H., Maynard D., Bontcheva K., Tablan V., 2002, “GATE: A Framework and Graphical Development Environment for Robust NLP Tools and Applications”, *Proceedings of the 40th Anniversary Meeting of the Association for Computational Linguistics (ACL'02)*, pp. 168-175.
- [14] Cunningham H., Maynard D., Bontcheva K., Tablan V., Ursu C., Dimitrov M., Dowman M., Aswani N., *Developing Language Processing Components with GATE (a user Guide)*, July 2004, [ON-LINE], <http://gate.ac.uk/releases/gate-3.0-beta1-build1717--ALL/tao.pdf>, 2005
- [15] Cunningham H., 2002, “GATE, a General Architecture for Text Engineering”, *Computers and the Humanities*, 36:223–254.
- [16] Maynard D., Cunningham H., Bontcheva K., Catizone R., Demetriou G., Gaizauskas R., Hamza O., Hepple M., Herring P., Mitchell B., Oakes M., Peters W., Setzer A., Stevenson M., Tablan V., Ursu C. and Wilks Y., 2000, “A Survey of Uses of GATE”, Technical Report CS-00-06, Department of Computer Science, University of Sheffield.
- [17] Appelt D., 1999, “An Introduction to Information Extraction”, *Artificial Intelligence Communications*, 12(3):161–172.
- [18] Cunningham H., Maynard D., Bontcheva K., Tablan V., 2002, “GATE: A Framework and Graphical Development Environment for Robust NLP Tools and Applications”, *Proceedings of the 40th Anniversary Meeting of the Association for Computational Linguistics (ACL'02)*.
- [19] Hepple M., 2000, “Independence and commitment: Assumptions for rapid training and execution of rule-based POS taggers”, *In Proceedings of the 38th Annual Meeting of the Association for Computational Linguistics (ACL-2000)*.
- [20] D.E. Appelt. 1996. The Common Pattern Specification Language. Technical report, SRI International, Artificial Intelligence Center.
- [21] Cunningham H., Maynard D., Bontcheva K., Tablan V., Ursu C., Dimitrov M., Dowman M., Aswani N., *Developing Language Processing Components*

- with GATE (a user Guide), July 2004, [ON-LINE],
<http://gate.ac.uk/releases/gate-3.0-beta1-build1717--ALL/tao.pdf>, 2005*
- [22] Mahon H., Bernet Y, Herzog S, 1999, *Requirements for a Policy Management System*, [ON-LINE], <http://www.ietf.org/draft-ietf-policy-req-01.txt>, Δεκέμβριος 2004.
- [23] N. Damianou, A Policy Framework for Management of Distributed Systems, PhD Thesis, London, February 2002.
- [24] N. Damianou, N. Dulay, E. Lupu, M Sloman: Ponder: A Language for Specifying Security and Management Policies for Distributed Systems Imperial College Research Report DoC 2001, Oct. 2000
- [25] Damianou N., Dulay N., Lupu E., Sloman M, 2001, “The Ponder Specification Language”, *Workshop on Policies for Distributed Systems and Networks (Policy2001)*, HP Labs Bristol, pp. 18-38.
- [26] Lupu E., Sloman M., Dulay N., Damianou N., 2000, “Ponder: Realising Enterprise Viewpoint Concepts”, *4th International Enterprise Distributed Object Computing Conference (EDOC 2000)* pp: 66-75.
- [27] Moffett, J.D. and Sloman, M.S., 1991, “The Representation of Policies as System Objects”, *Conference on Organizational Computer Systems*, pp.171-184.
- [28] Moffett, J.D. and Sloman, M.S., 1993, “Policy Hierarchies for Distributed Systems Management”, *IEEE Journal on Selected Areas in Communications*, pp.1404-1414.
- [29] Michael J. B., 2001, “Natural-Language Processing Support for Developing Policy-Governed Software Systems”, *39th Int. Conf. on Technologies for Object-Oriented Languages and Systems*, IEEE Computer Society Press, pp.263-274.
- [30] Ortalo, R., 1998, “A Flexible Method for Information System Security Policy Specification”, *In Proceedings of 5th European Symposium on Research in Computer Security (ESORICS 98)*, pp. 67-84.
- [31] Miller J., 2001, *HELP! How to specify policies?*, [ON-LINE], <http://enterprise.shl.com/policy/help.pdf>, Δεκέμβριος 2004.
- [32] Hoagland J.A., Pandey R. and Levitt K.N. 1998, “Security Policy Specification Using a Graphical Approach”, Technical report CSE-98-3, UC Davis Computer Science Department.



- [33] Bandara A. K., Lupu E., Moffett J. D., Russo A., 2004, “A Goal-based Approach to Policy Refinement”, *5th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2004)*, pp: 229-239.
- [34] Darimont R. and Lamsweerde A., 1996, “Formal Refinement Patterns for Goal-Driven Requirements Elaboration”, *4th ACM Symposium on the Foundations of Software Engineering (FSE4)*, pp. 179-190.
- [35] Russo A., Miller R., Nuseibeh B. and Kramer J., 2002, “An Abductive Approach for Analysing Event-Based Requirements Specifications”, *18th Int. Conf. on Logic Programming (ICLP)*, pp. 22-37.
- [36] Lamsweerde A., 2000, “Requirements engineering in the year 00: a research perspective. International Conference on Software Engineering”, *Proceedings of the 22nd international conference on Software engineering*, pp. 5 -19.
- [37] Chlamtac I., Conti M. and Liu J. N., 2003, “Mobile ad hoc networking: imperatives and challenges”, *Ad Hoc Networks*, 1(1): 13-64.
- [38] Karygiannis T., Owens L., Wireless Network Security: 802.11, Bluetooth and Handheld Devices, NIST Special Publication no. 800-48, U.S. Dept. of Commerce, USA 2002.
- [39] Stajano F. and Anderson R. J., 1999, “The resurrecting duckling: Security issues for ad-hoc wireless networks”, *Security Protocols*, 7th International Workshop Proceedings, pp. 172-194.
- [40] *Nmap scanner*, [ON-LINE], 2003, <http://www.insecure.org/nmap>, Δεκέμβριος 2004.
- [41] *Netstumbler 802.11 network scanner*, [ON-LINE], 2002, <http://www.stumbler.net>, Δεκέμβριος 2004.
- [42] *GFiLANGuard*, [ON-LINE], 2002, <http://www.gfi.com/lannetscan/>, Δεκέμβριος 2004.
- [43] Noy N., McGuiness D., 2001, “*Ontology Development 101: A Guide to Creating Your First Ontology*”, Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880.
- [44] Holsapple C., Joshi K., 2002, “A collaborative Approach to Ontology Design”, *Commun. ACM*, 45(2):42-47.

- [45] Gruber T., 1993, "Toward principles for the design of ontologies used for knowledge sharing", *Int. J. Hum.-Comput. Stud.*, 43 (5-6): 907-928.
- [46] ISO/IEC (2000-12-01) "ISO/IEC 17799" In Information technology - Code of practice for information security management, Vol. 1st ed. ISO.
- [47] BSI (1999) "British Standard 7799 Part 2" In Information Technology - Specification for Information Security Management System BSI.
- [48] ISO/IEC (1999) "*ISO/IEC 15408*" In *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, Part 2: Security functional requirements, Part 3: Security assurance requirements*.
- [49] Standards, Australian and New Zealand (1999) "*Australian/New Zealand Standard for Risk Management 4360*" Australia and New Zealand.
- [50] BSI (2001) "*British Standard BS ISO/IEC 17799:2000*".
- [51] *CIM Tutorial*, [ON-LINE], 2003, DMTF, WBEM Solutions Inc, www.wbemsolutions.com/tutorials/CIM/, Δεκέμβριος 2004.
- [52] Γκρίτζαλης, Δ. τ. (2001) "Ασφάλεια στις Τεχνολογίες Πληροφοριών και Επικοινωνιών". In Εργαστήριο Π.Σ. και Β.Δ. Αθήνα.
- [53] Κάτσικας, Σ. (1995) "Διαχείριση Κινδύνων Π.Σ.". In Ασφάλεια Πληροφοριών ΕΠΥ, Αθήνα.
- [54] MG-3, 1996, *A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems*, [ON-LINE], http://www.cse-cst.gc.ca/en/documents/knowledge_centre/gov_publications/itsg/mg3.pdf, Δεκέμβριος 2004.
- [55] *Security risk tools and resources*, [ON-LINE], 2004, <http://www.knowledgeleader.com/iafreewebsite.nsf/content/SecurityResources!OpenDocument>, Δεκέμβριος 2004.

6. Παραρτήματα

6.1. GATE

Σε αυτή την ενότητα παρουσιάζονται τα αρχεία που δημιουργήθηκαν με σκοπό την παραμετροποίηση του GATE για την εξαγωγή γνώσης από τα αντίμετρα της πολιτικής ασφάλειας.

Gazetteer

Αρχείο so_passwords.lst:

```
passwords
password
Password
Passwords
```

Αρχείο so_routers.lst:

```
router
routers
```

Αρχείο so_servers.lst:

```
application server
application server
file server
file servers
ftp server
ftp servers
mail server
mail servers
proxy server
proxy servers
server
servers
web server
web servers
```

Αρχείο so_cryptography.lst:

```
asymmetric algorithm
asymmetric algorithms
```

cryptographic
cryptographic method
cryptographic methods
cryptography
cryptosystem
symmetric algorithm
symmetric algorithms

Αρχείο so_firewalls.lst:

filters
filter
filtering device
software firewall
hardware firewall

Αρχείο so_hosts.lst:

host
hosts
computer
computers
pc
pc's
terminal

Αρχείο so_password_length.lst:

length
long

Προσθήκη των ακόλουθων γραμμών στο αρχείο lists.lst για την γνωστοποίηση των παραπάνω αρχείων στον Gazetteer καθώς και για την κατηγοριοποίηση των λέξεων που βρίσκονται στο κάθε αρχείο:

so_cryptography.lst:MessageSecurity:DeliveryChecking
so_firewalls.lst:NetworkAccessControls:Firewalls
so_hosts.lst:NetworkEquipment:Client
so_passwords.lst:IdentificationAndAuthentication
so_password_length.lst:IdentificationAndAuthentication:PasswordLength
so_routers.lst:NetworkEquipment:Router
so_servers.lst:NetworkEquipment:Server

NE Transducer*Αρχείο so_patterns.jape:*

```
Phase: SO_PATTERNS
Options: control = appelt

Rule:pattern4
Priority: 10
(
  {{Token.category == NNP} | {Token.category == NNP}}
  {SpaceToken}
  {{Token}}
  {SpaceToken})+
  {Token}
  {Split}
):pattern4
-->
:pattern4.Patterns = {kind = "4", rule = "pattern4"}
```

```
Rule:pattern1
Priority: 20
(
  {Token.category == VB}
  {SpaceToken}
  {{Token}}
  {SpaceToken})+
  {Token.category == IN}
  {{SpaceToken}}
  {Token})+
  {Split}
):pattern1
-->
:pattern1.Patterns = {kind = "1", rule = "pattern1"}
```

```
Rule:pattern2
Priority: 30
(
  {Token.category == VB}
  {SpaceToken}
  {{Token}}
  {SpaceToken})+
  {Token.category == TO}
  {{SpaceToken}}
  {Token})+
  {Split}
):pattern2
-->
:pattern2.Patterns = {kind = "2", rule = "pattern2"}
```

```
Rule:pattern3
Priority: 40
```

```

(
  {Token.category == VB}
  {SpaceToken}
  ({Token}
  {SpaceToken})+
  {Token.category == TO}
  {SpaceToken}
  ({Token}
  {SpaceToken})+
  {Token.string == "between"}
  {SpaceToken}
  ({Token})+
  {Split}
):pattern3
-->
:pattern3.Patterns = {kind = "3", rule = "pattern3"}

```

Αρχείο so_rules.jape:

```

Phase: SO_RULES
Options: control = appelt

Rule:passwords
Priority: 10
(
  {Lookup.majorType == IdentificationAndAuthentication}

):password
-->
:password.CM_Group = {kind = "passwords", majorT = "Identification And Authentication", rule = "passwords"}


Rule:passwords_length
Priority: 20
(
  {Lookup.majorType == IdentificationAndAuthentication,
  Lookup.minorType == PasswordLength}

):password_length
-->
:password_length.CM_Group = {kind = "password_length", majorT = "Identification And Authentication", minorT = "Password Length", rule = "passwords_length"}


Rule:cryptography
Priority: 30
(
  {Lookup.majorType == MessageSecurity, Lookup.minorType ==
  DeliveryChecking}
):cryptography
-->

```

```
:cryptography.CM_Group = {kind = "cryptography", majorT = "Message Security", minorT = "Delivery Checking", rule = "Cryptography"}
```

```
Rule:firewalls
Priority: 40
(
  {Lookup.majorType == NetworkAccessControls, Lookup.minorType == Firewalls}
):firewalls
-->
:firewalls.CM_Group = {kind = "firewalls", majorT = "NetworkAccessControls", minorT = "Firewalls", rule = "firewalls"}
```

```
Rule:client
Priority:50
(
  {Lookup.majorType == NetworkEquipment, Lookup.minorType == Client}
):client
-->
:client.Target = {kind = "Client", rule = "client"}
```

```
Rule:server
Priority:60
(
  {Lookup.majorType == NetworkEquipment, Lookup.minorType == Server}
):server
-->
:server.Target = {kind = "Server", rule = "server"}
```

```
Rule:router
Priority:70
(
  {Lookup.majorType == NetworkEquipment, Lookup.minorType == Router}
):router
-->
:router.Target = {kind = "Router", rule = "router"}
```

Αρχείο so_target.jape:

```
Phase: SO_TARGET
Input: Token Lookup SpaceToken Client Server Router CM_Group
Options: control = appelt
```

```
Rule:target_data
Priority: 10
(
  {CM_Group.kind=="cryptography"}
):target_data
-->
```

```

:target_data.Target = {kind = "Data", rule = "target_data"}

Rule:target_data2
Priority: 20
{
  {CM_Group.kind=="firewalls"}
):target_data2
-->
:target_data2.Target = {kind = "AllSystems", rule = "target_data2"}


Rule:target_data3
Priority: 30
{
  {CM_Group.kind=="passwords"} |
  {CM_Group.kind=="password_length"}
):target_data3
-->
:target_data3.Target = {kind = "AllSystems", rule = "target_data3"}

```

Προσθήκη των ακόλουθων γραμμών στο αρχείο main.jape για την γνωστοποίηση των παραπάνω αρχείων στον NE Transducer και την επεξεργασία των παραπάνω κανόνων JAPE.

```

so_patterns
so_rules
so_target

```

6.2. Παράθεση πηγαίου κώδικα JAVA

Παρακάτω ακολουθεί ο πηγαίος κώδικας της μεθόδου που παρουσιάστηκε. Ο κώδικας είναι υλοποιημένος σε γλώσσα JAVA.

StandAloneAnnie.java

Created with JBuilder

```

/*
 *  StandAloneAnnie.java
 *
 *
 * Copyright (c) 2000-2001, The University of Sheffield.
 *
 * This file is part of GATE (see http://gate.ac.uk/), and is
free
 * software, licenced under the GNU Library General Public
License,
 * Version 2, June1991.
 *
 * A copy of this licence is included in the distribution in
the file
 * licence.html, and is also available at
http://gate.ac.uk/gate/licence.html.
 *
 * hamish, 29/1/2002
 *
 * $Id: StandAloneAnnie.java,v 1.2 2002/02/06 15:23:49 nasso
Exp $
 */

import java.util.*;
import java.io.*;
import java.net.*;
import java.lang.String;

import gate.*;
import gate.creole.*;
import gate.creole.ontology.*;
import gate.util.*;
import gate.gui.*;
import gate.corpora.RepositioningInfo;
import com.ontotext.gate.ontology.TaxonomyImpl;
import com.ontotext.gate.ontology.OntologyImpl;
import com.ontotext.gate.ontology.DAMLOntology;
import com.ontotext.gate.ontology.DAMLKnowledgeBaseImpl;

/**
 * For simplicity's sake, we don't do any exception handling.

```



```

*/
public class StandAloneAnnie {

    /** The Corpus Pipeline application to contain ANNIE */
    private SerialAnalyserController annieController;

    //Static variables for easier use of the array struct..
    private static int subject = 0;
    private static int cmgroup = 1;
    private static int target = 2;
    private static int action = 3;
    private static int constraints = 4;

    //The cm can afford 10 sentences.. Must be changed manually
    if more than
    //10 sentences will be annotated..
    private static String cm[][] = new String[10][5];
    private static int pattern;

    /**
     * Initialise the ANNIE system. This creates a "corpus
     pipeline"
     * application that can be used to run sets of documents
     through
     * the extraction system.
     */
    public void initAnnie() throws GateException {
        Out.prln("Initialising ANNIE...");

        // create a serial analyser controller to run ANNIE with
        annieController =
            (SerialAnalyserController) Factory.createResource(
                "gate.creole.SerialAnalyserController",
        Factory.newFeatureMap(),
            Factory.newFeatureMap(), "MyANNIE"
        );

        // load each PR as defined in ANNIEConstants
        for (int i = 0; i < ANNIEConstants.PR_NAMES.length; i++) {
            FeatureMap params = Factory.newFeatureMap(); // use
            default parameters
            ProcessingResource pr = (ProcessingResource)
                Factory.createResource(ANNIEConstants.PR_NAMES[i],
            params);

            Out.println(ANNIEConstants.PR_NAMES[i]);

            // add the PR to the pipeline controller
            annieController.add(pr);
        } // for each ANNIE PR

        Out.prln("...ANNIE loaded");
    } // initAnnie()
}

```



```

/** Tell ANNIE's controller about the corpus you want to run
on */
public void setCorpus(Corpus corpus) {
    annieController.setCorpus(corpus);
} // setCorpus

/** Run ANNIE */
public void execute() throws GateException {
    Out.prln("Running ANNIE...");
    annieController.execute();
    Out.prln("...ANNIE complete");
} // execute()

/**
 * Run from the command-line, with a path and the name of
the
 * countermeasures that you wish to be annotated..
 * This code will run with all the documents in memory - if
you
 * want to unload each from memory after use, add code to
store
 * the corpus in a DataStore.
*/
public static void main(String args[]) throws GateException,
IOException {
    // initialize neccessary constants...
    initConstants();

    // initialise the GATE library
    Out.prln("Initialising GATE...");
    Gate.init();
    Out.prln("...GATE initialised");

    // initialise ANNIE (this may take several minutes)
    StandAloneAnnie annie = new StandAloneAnnie();
    annie.initAnnie();

    // Initialise the corpus to be annotated...
    Corpus corpus = (Corpus) initCorpora(args[0]);

    // tell the pipeline about the corpus and run it
    annie.setCorpus(corpus);
    annie.execute();

    //Get the Document you want.. Name = args[1]
    Document docum;
    int docint;
    if ( (docint = getIntDocument(args[1], corpus)) != -1) {
        docum = (Document) corpus.get(docint);
    }
    else {
        Out.println("Den vrika Document me onoma" + args[1]);
        return;
    }
}

```

```

//Initialize subject with the attribute administrators
since there is
//no extra data for this field that can be extracted from
the cm..
//Rows must be changed manually if there is a change in
the number of
//sentences..
for (int i = 0; i <= 3; i++)
    cm[i][subject] = "Administrators";

//Initialize Contrains so that nothing appears as null..
for (int i = 0; i <= 3; i++)
    cm[i][constraints] = "No Constraint";

//Get the sentences from the desired doc..
Iterator sentenceIterator =
docum.getAnnotations().get("Sentence")
    .iterator();
int sentencenum = 1;
//Get the tokens..
AnnotationSet tokenannot =
docum.getAnnotations().get("Token");
while (sentenceIterator.hasNext()) {
    //Get the start and end offset of the sentence.
    //AnnotationSet currentannot =
docum.getAnnotations("Sentence");
    Annotation currSentenceAnn = (Annotation)
sentenceIterator.next();
    Long startoffset = new
Long(currSentenceAnn.getStartNode())
        .getOffset().intValue();
    Long endoffset = new Long(currSentenceAnn.getEndNode())
        .getOffset().intValue();
    //Out.println("Sentence no" + sentencenum);
    //Out.println(docum.getContent().toString().substring(
    //    startoffset.intValue(),
    //    endoffset.intValue()));

    //Get the target for the countermeasure
    AnnotationSet targetannot =
docum.getAnnotations().get("Target")
    .get(startoffset, endoffset);
    if (targetannot.size() == 1) {
        Annotation trg = (Annotation)
targetannot.iterator().next();
        cm[sentencenum - 1][target] =
trg.getFeatures().get("kind")
            .toString();
    }
    if (targetannot.size() == 0) {
        //Simvasi: Οtan den uparzei target upothehoume oti
einai Data..
        cm[sentencenum - 1][target] = "Data";
        Out.println(cm[sentencenum - 1][target]);
    }
    //Out.println(targetannot.size());
}

```

```

if (targetannot.size() > 1) {
    boolean firsttarget = true;
    Iterator targetiter = targetannot.iterator();
    while (targetiter.hasNext()) {
        Annotation trg = (Annotation) targetiter.next();
        if (firsttarget) {
            cm[sentencenum - 1][target] =
trg.getFeatures().get("kind")
                .toString();
            firsttarget = false;
            //Out.println(cm[sentencenum - 1][target]);
        }
        else {
            if (!cm[sentencenum -
1][target].matches(trg.getFeatures()
                .get("kind").toString()))
                cm[sentencenum - 1][target] = cm[sentencenum -
1][target] +
                    ", " +
trg.getFeatures().get("kind").toString();
            }
        //complete the string..
        //cm[sentencenum -1][target] = cm[sentencenum-
1][target] + " || ";
    }
    if (targetannot.size() > 2) {
        //too many targets recognized.. Assuming that is for
Data..
        cm[sentencenum - 1][target] = "Data";
    }

    //Get the cmgroup..
    AnnotationSet cmgroupannot =
docum.getAnnotations().get("CM_Group")
    .get(startoffset, endoffset);
    Iterator cmgiter = cmgroupannot.iterator(); //it may be
more than one..
    String group = "";
    String subgroup = "";
    boolean firstgroup = true;
    if (cmgroupannot.size() <= 2) {
        while (cmgiter.hasNext()) {
            Annotation cmg = (Annotation) cmgiter.next();
            group = cmg.getFeatures().get("majorT").toString();
            if (firstgroup) {
                group =
cmg.getFeatures().get("majorT").toString();
                if (cmg.getFeatures().containsKey("minorT"))
                    subgroup =
cmg.getFeatures().get("minorT").toString();
                firstgroup = false;
            }
            else {
                if
(!group.matches(cmg.getFeatures().get("majorT").toString())) {

```

```

        group = group + ", " +
cmg.getFeatures().get("majorT")
        .toString();
    }
    if (cmg.getFeatures().containsKey("minorT")) {
        if
(!subgroup.matches(cmg.getFeatures().get("minorT"))
        .toString())) {
            subgroup = subgroup + ", " +
cmg.getFeatures().get("minorT")
        .toString();
    }
}
}
}
}

cm[sentencenum - 1][cmgroup] = "GROUP: " + group + "
SUBGROUP: " +
subgroup;

//Get the pattern that was recognized..
AnnotationSet patternannot =
docum.getAnnotations().get("Patterns")
        .get(startoffset, endoffset);
Annotation pt = (Annotation)
patternannot.iterator().next();
pattern =
Integer.parseInt(pt.getFeatures().get("kind").toString());

//Get the annotation set "Token" for this sentence..
AnnotationSet posNNRange = tokenannot.get(startoffset,
endoffset);

/**The Array List is used for sorting purposes.. You can
also
 * use the SortedAnnotationList in StandAloneAnnie..
 */
ArrayList posNNRangeList = new ArrayList(posNNRange);
Collections.sort(posNNRangeList, new
gate.util.OffsetComparator());
Iterator tokeniter = posNNRangeList.iterator();
Long startact = new Long(0);
Long endact = new Long(0);
boolean firsttime = true;
Long startconst = new Long(0);
Long endconst = new Long(0);
switch (pattern) {
    case 1:

        //Use assymetric algorithms for signatures.
        while (tokeniter.hasNext()) {
            Annotation NNannot = (Annotation)
tokeniter.next();
            /**One way of getting the text along with the
annotation type..

```

```

        *
        * int start =
NNannot.getStartNode().getOffset().intValue();
        * int end =
NNannot.getEndNode().getOffset().intValue();
        * String annotText =
docum.getContent().toString().
        * substring(start, end);
        * Out.println(annotText + " , " +
fmap.get("category"));
        */
//And the other..
FeatureMap fmap = NNannot.getFeatures();
String name =

fmap.get(ANNIEConstants.TOKEN_STRING_FEATURE_NAME).toString();
String cat = fmap.

get(ANNIEConstants.TOKEN_CATEGORY_FEATURE_NAME).toString();
if (firsttime) {
    startact = NNannot.getStartNode().getOffset();
    firsttime = false;
}
if (cat.matches("IN")) {
    endact = NNannot.getEndNode().getOffset();
}
} // Token Iterator

//Out.println(startact + " " + endact);
cm[sentencenum - 1][action] =
docum.getContent().toString()
.substring(startact.intValue(),
(endact.intValue() - 1));
break;
case 2:

    /**Use filters to control which systems are
permitted connections
    * with the Internet.
    */
while (tokeniter.hasNext()) {
    Annotation NNannot = (Annotation)
tokeniter.next();
    /**One way of getting the text along with the
annotation type..
    *
    * int start =
NNannot.getStartNode().getOffset().intValue();
    * int end =
NNannot.getEndNode().getOffset().intValue();
    * String annotText =
docum.getContent().toString().
    * substring(start, end);
    * Out.println(annotText + " , " +
fmap.get("category"));
    */
}

```



```

//And the other..
FeatureMap fmap = NNannot.getFeatures();
String name = 

fmap.get(ANNIEConstants.TOKEN_STRING_FEATURE_NAME).toString();
String cat = fmap.

get(ANNIEConstants.TOKEN_CATEGORY_FEATURE_NAME).toString();
if (firsttime) {
    startact = NNannot.getStartNode().getOffset();
    firsttime = false;
}
if (cat.matches("TO")) {
    endact = NNannot.getStartNode().getOffset();
}
} // Token Iterator

//Out.println(startact + " " + endact);
cm[sentencenum - 1][action] =
docum.getContent().toString()
.substring(startact.intValue(),
(endact.intValue() - 1));
break;

case 3:

    /**Use filters to restrict the level of access
between
     *internal and external hosts.
     */
    while (tokeniter.hasNext()) {
        Annotation NNannot = (Annotation)
tokeniter.next();
        /**One way of getting the text along with the
annotation type..
        *
        * int start =
NNannot.getStartNode().getOffset().intValue();
        * int end =
NNannot.getEndNode().getOffset().intValue();
        * String annotText =
docum.getContent().toString().
        * substring(start, end);
        * Out.println(annotText + " , " +
fmap.get("category"));
        */
        //And the other..
        FeatureMap fmap = NNannot.getFeatures();
        String name = 

fmap.get(ANNIEConstants.TOKEN_STRING_FEATURE_NAME).toString();
String cat = fmap.

get(ANNIEConstants.TOKEN_CATEGORY_FEATURE_NAME).toString();
//Out.println(cat);
if (firsttime) {

```

```

        startact = NNannot.getStartNode().getOffset();
        firsttime = false;
    }
    if (cat.matches("TO")) {
        endact = NNannot.getStartNode().getOffset();
        //Out.println("mpika sto endact");
    }
    if (name.matches("between")) {
        startconst = NNannot.getStartNode().getOffset();
        endconst = endoffset;
    }
}
} // Token Iterator

cm[sentencenum - 1][action] =
docum.getContent().toString()
    .substring(startact.intValue(),
(endact.intValue() - 1));

cm[sentencenum - 1][constraints] =
docum.getContent().toString().
    substring(startconst.intValue(),
endconst.intValue());

break;

case 4:

//..Passwords to be at least 6 characters long..
//Parse the sentence based on the pattern..
/**In this case the whole sentence is the action and
nothing else
 * can be extracted from the sentence..
 */
cm[sentencenum - 1][action] =
docum.getContent().toString().substring(
    startoffset.intValue(), endoffset.intValue());
break;
}

while (tokeniter.hasNext()) {
    Annotation NNannot = (Annotation) tokeniter.next();
    /**One way of getting the text along with the
annotation type..
 *
 * int start =
NNannot.getStartNode().getOffset().intValue();
 * int end =
NNannot.getEndNode().getOffset().intValue();
 * String annotText = docum.getContent().toString().
 * substring(start, end);
 * Out.println(annotText + " , " +
fmap.get("category"));
 */
//And the other..
FeatureMap fmap = NNannot.getFeatures();
String name =

```

```

fmap.get(ANNIEConstants.TOKEN_STRING_FEATURE_NAME).toString();
    String cat =
fmap.get(ANNIEConstants.TOKEN_CATEGORY_FEATURE_NAME).toString();
);
    //Out.println(name + " , " + cat);
} // Token Iterator

int result = posNNRange.size();
//Out.println("Result = " + result);

//Go to the next Sentence
sentencenum++;
} // sentence Iterator

//Print the results..
showResults(cm, sentencenum);

//End of process
} // mail

public static void showResults(String cms[][], int
sentences) {
    Out.println("\n-----");
    Out.println("Parousiasi domis antimetrou gia tin kathe
protasi.");
    //Out.print("SUBJECT || GROUP: SUBGROUP: || TARGET ||
ACTION");
    //Out.print(" || CONSTRAINTS\n");
    Out.println("-----\n");
    for (int i = 0; i <= sentences - 2; i++) {
        Out.println("Sentence No " + (i + 1));
        Out.println("-----");
        for (int j = 0; j <= 4; j++) {
            switch (j) {
                case 0:
                    Out.println(" Subject:\t" + cms[i][j]);
                    break;
                case 1:
                    Out.println(" Group:\t" + cms[i][j]);
                    break;
                case 2:
                    Out.println(" Target:\t" + cms[i][j]);
                    break;
                case 3:
                    Out.println(" Action:\t" + cms[i][j]);
                    break;
                case 4:
                    Out.println(" Constraints:\t" + cms[i][j]);
                    break;
            }
        }
        Out.println();
    }
}

```

```

    }
    Out.println("");
    Out.println("-----");
    ----");
}

public static Corpus initCorpora(String pathToDirectory)
throws
    java.io.IOException, ResourceInstantiationException {
    Corpus corpus = (Corpus)
Factory.createResource("gate.corpora.CorporusImpl");
    File directory = new File(pathToDirectory);
    File files[] = directory.listFiles();
    //gate.util.ExtensionFileFilter txtfilter = new gate.util
    //ExtensionFileFilter();
    //txtfilter.addExtension("txt");
    //URL url = directory.toURL();
    //corpus.populate(url,txtfilter,"UTF-8",false);
    for (int i = 0; i < files.length; i++) {
        URL u = files[i].toURL();
        //If the file is not a txt (for example a directory)
then do nothing
        if (u.toString().endsWith("txt")) {
            FeatureMap params = Factory.newFeatureMap();
            params.put("name", files[i].getName());
            params.put("sourceUrl", u);
            params.put("preserveOriginalContent", new
Boolean(true));
            params.put("collectRepositioningInfo", new
Boolean(true));
            Out.prln("Creating doc for " + u);
            Document doc = (Document)

Factory.createResource("gate.corpora.DocumentImpl", params);
            corpus.add(doc);
        }
    } // for each of args*/
    corpus.setName("MyCorpus_" + Gate.genSym());
    return corpus;
}

public static void initConstants() {
    System.setProperty("gate.home", "C:\\Program Files\\GATE
3.0 RC1\\");
    System.setProperty("KNOWN_PLUGIN_PATH_KEY",
                      "C:\\Program Files\\GATE 3.0
RC1\\plugins\\");
}

public static int getIntDocument(String doc, Corpus cor) {
    Iterator corporusiter = cor.iterator();
    int tempint = 0;
    int where = -1;
    while (corpusiter.hasNext()) {
        Document tempdoc = (Document) corporusiter.next();
        if (tempdoc.getName().equals(doc))

```

```

        where = tempint;
        tempint++;
    }

    return where;
}

public static class SortedAnnotationList
    extends Vector {
    public SortedAnnotationList() {
        super();
    } // SortedAnnotationList

    public boolean addSortedExclusive(Annotation annot) {
        Annotation currAnot = null;

        // overlapping check
        for (int i = 0; i < size(); ++i) {
            currAnot = (Annotation) get(i);
            if (annot.overlaps(currAnot)) {
                return false;
            } // if
        } // for

        long annotStart =
annot.getStartNode().getOffset().longValue();
        long currStart;
        // insert
        for (int i = 0; i < size(); ++i) {
            currAnot = (Annotation) get(i);
            currStart =
currAnot.getStartNode().getOffset().longValue();
            if (annotStart < currStart) {
                insertElementAt(annot, i);
                // Out.println("Current start: "+currStart);
                return true;
            } // if
        } // for

        int size = size();
        insertElementAt(annot, size);
        // Out.println("Insert start: "+annotStart+ " at size
position: "+size);
        return true;
    } // addSorted
} // SortedAnnotationList
} // class StandAloneAnnie

```

StandAloneAnnie.java

Created with JBuilder



6.3. Protégé – Οντολογία Ασφάλειας

Παρακάτω ακολουθεί ο κώδικας OWL της οντολογίας ασφάλειας.

```
<?xml version="1.0"?>
<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:owl="http://www.w3.org/2002/07/owl#"
  xmlns="http://www.owl-ontologies.com/unnamed.owl#"
  xml:base="http://www.owl-ontologies.com/unnamed.owl">
<owl:Ontology rdf:about="" />
<owl:Class rdf:ID="TelnetServer">
  <owl:disjointWith>
    <owl:Class rdf:ID="FTPServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="ApplicationServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="FileServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="MailServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="ProxyServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="WebServer"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:ID="Server"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:ID="GroupwareServer"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="UserManual">
  <rdfs:subClassOf>
    <owl:Class rdf:ID="Information"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:ID="ContinuityPlans"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Database"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="InformationBackup"/>
  </owl:disjointWith>
```

```

</owl:Class>
<owl:Class rdf:ID="Network">
  <owl:disjointWith>
    <owl:Class rdf:ID="Personnel"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Services"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:ID="Asset"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:ID="LogRecord"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Data"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Documents"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Information"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Firmware"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Hardware"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Software"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="CommunicationsEquipment"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:ID="CIMNetwork"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Transparent">
  <owl:disjointWith>
    <owl:Class rdf:ID="Remsh"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Local"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Interactive"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:ID="Gateway"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:ID="Interlock"/>
  </owl:disjointWith>
  <owl:disjointWith>

```

```

<owl:Class rdf:ID="Proxy"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:ID="Raptor"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="DevelopmentToolsAndUtilities">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Software"/>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:ID="ApplicationSoftware"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="SystemSoftware"/>
    </owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="Integrity">
    <owl:disjointWith>
        <owl:Class rdf:ID="RiskEvaluationCriterion"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Controls"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="AssetValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Consequence"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="RiskValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Threat"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="ValueDefinition"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Countermeasure"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Impact"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Frequency"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="UnwantedIncident"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Stakeholder"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:ID="Vulnerability"/>
    </owl:disjointWith>

```

```

</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="Attack"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="Authenticity"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Class rdf:ID="SecurityRequirement"/>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:ID="SecurityPolicy"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="Availability"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="Risk"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="Compliance"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:ID="NonRepudiation"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="FaxMachine">
  <owl:disjointWith>
    <owl:Class rdf:ID="PABXs"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Router"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:ID="AnsweringMachines"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Compliance">

```

```

<owl:disjointWith>
  <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Frequency"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith>
  <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Threat"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Class rdf:ID="RiskAssessment"/>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Countermeasure"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#ValueDefinition"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Authenticity"/>
</owl:disjointWith>
<owl:disjointWith>

```



```

<owl:Class rdf:about="#NonRepudiation"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Attack"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetValue"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#SecurityPolicy"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Threat">
    <owl:disjointWith rdf:resource="#Compliance"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Impact"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#ValueDefinition"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Risk"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
                >1</owl:cardinality>
            <owl:onProperty>
                <owl:DatatypeProperty rdf:ID="ThreatType"/>
            </owl:onProperty>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#SecurityPolicy"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#ThreatAgent"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Frequency"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Restriction>

```

```

<owl:onProperty>
  <owl:ObjectProperty rdf:ID="Causes"/>
</owl:onProperty>
<owl:someValuesFrom>
  <owl:Class rdf:about="#UnwantedIncident"/>
</owl:someValuesFrom>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<rdfs:subClassOf>
<owl:Restriction>
  <owl:onProperty>
    <owl:ObjectProperty rdf:about="#Causes"/>
  </owl:onProperty>
  <owl:someValuesFrom>
    <owl:Class>
      <owl:unionOf rdf:parseType="Collection">
        <owl:Class rdf:about="#Risk"/>
        <owl:Class rdf:about="#UnwantedIncident"/>
      </owl:unionOf>
    </owl:Class>
  </owl:someValuesFrom>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Authenticity"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Class rdf:about="#RiskAssessment"/>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<rdfs:subClassOf>
<owl:Restriction>
  <owl:onProperty>
    <owl:ObjectProperty rdf:ID="Targets"/>
  </owl:onProperty>
  <owl:someValuesFrom>
    <owl:Class rdf:about="#Asset"/>
  </owl:someValuesFrom>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Asset"/>

```

```

</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="ThreatID"/>
        </owl:onProperty>
        <owl:cardinality>
            >1</owl:cardinality>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Confidentiality"/>
    </owl:disjointWith>
    <owl:equivalentClass>
        <owl:Class>
            <owl:intersectionOf rdf:parseType="Collection">
                <owl:Restriction>
                    <owl:allValuesFrom>
                        <owl:Class rdf:about="#Vulnerability"/>
                    </owl:allValuesFrom>
                    <owl:onProperty>
                        <owl:ObjectProperty rdf:ID="Exploits"/>
                    </owl:onProperty>
                </owl:Restriction>
                <owl:Restriction>
                    <owl:onProperty>
                        <owl:ObjectProperty rdf:ID="HasFrequency"/>
                    </owl:onProperty>
                    <owl:allValuesFrom>
                        <owl:Class rdf:about="#Frequency"/>
                    </owl:allValuesFrom>
                </owl:Restriction>
                <owl:Restriction>
                    <owl:minCardinality>
                        >1</owl:minCardinality>
                    <owl:onProperty>
                        <owl:DatatypeProperty rdf:ID="Severity"/>
                    </owl:onProperty>
                </owl:Restriction>
            </owl:intersectionOf>
        </owl:Class>
    </owl:equivalentClass>
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:minCardinality>
                >1</owl:minCardinality>
            <owl:onProperty>
                <owl:DatatypeProperty rdf:ID="Posibility"/>
            </owl:onProperty>
        </owl:Restriction>
    </rdfs:subClassOf>

```



```

</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#NonRepudiation"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Attack"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Countermeasure"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:someValuesFrom>
            <owl:Class rdf:about="#Risk"/>
        </owl:someValuesFrom>
        <owl:onProperty>
            <owl:ObjectProperty rdf:about="#Causes"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
            >1</owl:minCardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="ThreatName"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Authenticity">
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskEvaluation"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Impact"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Consequence"/>
    </owl:disjointWith>

```

```

</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Countermeasure"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetValue"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<rdfs:subClassOf>
  <owl:Class rdf:about="#SecurityRequirement"/>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith>
  <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#NonRepudiation"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#SecurityPolicy"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Frequency"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#ValueDefinition"/>
</owl:disjointWith>
<owl:disjointWith>

```

```

<owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Attack"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="AuthorizationPolicy">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#SecurityPolicy"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#ValueDefinition">
    <owl:disjointWith rdf:resource="#Compliance"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Confidentiality"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#SecurityPolicy"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Authenticity"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Attack"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskEvaluationCriterion"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Availability"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Countermeasure"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#NonRepudiation"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#SensitivityLevel"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#RiskAssessment"/>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#UnwantedIncident"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Threat"/>
    <owl:disjointWith rdf:resource="#Integrity"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Asset"/>
    </owl:disjointWith>
    <owl:disjointWith>

```

```

<owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Frequency"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="SSLProtocol">
    <owl:disjointWith>
        <owl:Class rdf:ID="TLSProtocol"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:ID="TransportLayerProtocol"/>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:ID="SSHProtocol"/>
    </owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="CIMUserEntity">
    <rdfs:subClassOf>
        <owl:Class rdf:ID="CIMManagedElement"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="EnvironmentalThreat">
    <owl:disjointWith>
        <owl:Class rdf:ID="NaturalDisaster"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:ID="Environmental"/>
    </rdfs:subClassOf>

```

```

</owl:Class>
<owl:Class rdf:ID="Deliberate">
  <owl:disjointWith>
    <owl:Class rdf:ID="Accidental"/>
  </owl:disjointWith>
  <rdfs:subClassOf rdf:resource="#Threat"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Environmental"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="PublicNetwork">
  <owl:disjointWith>
    <owl:Class rdf:ID="NetworkEquipment"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="PrivateNetwork"/>
  </owl:disjointWith>
  <rdfs:subClassOf rdf:resource="#Network"/>
</owl:Class>
<owl:Class rdf:ID="Virus">
  <rdfs:subClassOf>
    <owl:Class rdf:ID="MaliciousCode"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Interactive">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Gateway"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#Raptor"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Proxy"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Local"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Remsh"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Transparent"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Interlock"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="HTMLEditor">
  <owl:disjointWith>
    <owl:Class rdf:ID="SetupUtilities"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="DatabaseTools"/>
  </owl:disjointWith>
  <rdfs:subClassOf
rdf:resource="#DevelopmentToolsAndUtilities"/>
  <owl:disjointWith>
    <owl:Class rdf:ID="ScriptingTools"/>

```

```

</owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="TextEditor">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#ApplicationSoftware"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#WebServer">
  <owl:disjointWith>
    <owl:Class rdf:about="#FTPServer"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#TelnetServer"/>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#ApplicationSoftware"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#ApplicationServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#ProxyServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#GroupwareServer"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Server"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#FileServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#MailServer"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Environmental">
  <rdfs:subClassOf rdf:resource="#Threat"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Accidental"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Deliberate"/>
</owl:Class>
<owl:Class rdf:ID="Email">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#ApplicationSoftware"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#SecurityPolicy">
  <owl:disjointWith>
    <owl:Class rdf:about="#AssetValue"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Threat"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
  
```

```

</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Class rdf:about="#RiskAssessment"/>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Class rdf:ID="CIMPolicy"/>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:someValuesFrom>
      <owl:Class rdf:about="#Controls"/>
    </owl:someValuesFrom>
    <owl:onProperty>
      <owl:ObjectProperty rdf:ID="Includes"/>
    </owl:onProperty>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Attack"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#NonRepudiation"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Countermeasure"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith>
  <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskValue"/>

```

```

</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Asset"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="Priority"/>
    </owl:onProperty>
    <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:cardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:minCardinality>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="UpdateTime"/>
    </owl:onProperty>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith>
  <owl:Class rdf:about="#Frequency"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Documents">
  <owl:disjointWith>
    <owl:Class rdf:about="#Firmware"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#LogRecord"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Services"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Personnel"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Software"/>
  </owl:disjointWith>

```



```

<owl:disjointWith>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Network"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Hardware"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Information"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Data"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Class rdf:about="#Asset"/>
</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="DigitalSignature">
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:someValuesFrom>
                <owl:Class rdf:ID="EncryptionAlgorithm"/>
            </owl:someValuesFrom>
            <owl:onProperty>
                <owl:ObjectProperty rdf:ID="Arises"/>
            </owl:onProperty>
        </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#NonRepudiation"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#PrivateNetwork">
    <rdfs:subClassOf rdf:resource="#Network"/>
    <owl:disjointWith rdf:resource="#PublicNetwork"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#NetworkEquipment"/>
    </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Countermeasure">
    <owl:disjointWith rdf:resource="#Compliance"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetValue"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:cardinality>
                <owl:datatype="http://www.w3.org/2001/XMLSchema#int"
                    >1</owl:cardinality>
            <owl:onProperty>
                <owl:DatatypeProperty rdf:ID="CountermeasureType"/>
            </owl:onProperty>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Consequence"/>
    </owl:disjointWith>
</owl:Class>

```

```

</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="Versatility"/>
    </owl:onProperty>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:minCardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="Subject"/>
    </owl:onProperty>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:minCardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="Effectiveness"/>
    </owl:onProperty>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:minCardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Class rdf:about="#RiskAssessment"/>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Frequency"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#NonRepudiation"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="Constraint"/>
    </owl:onProperty>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:minCardinality>
  </owl:Restriction>
</rdfs:subClassOf>

```

```

>1</owl:minCardinality>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#Attack"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:onProperty>
            <owl:ObjectProperty rdf:ID="Reduces"/>
        </owl:onProperty>
        <owl:someValuesFrom>
            <owl:Class rdf:about="#Vulnerability"/>
        </owl:someValuesFrom>
    </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:someValuesFrom rdf:resource="#Threat"/>
        <owl:onProperty rdf:resource="#Targets"/>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:equivalentClass>
    <owl:Restriction>
        <owl:onProperty>
            <owl:ObjectProperty rdf:ID="Protects"/>
        </owl:onProperty>
        <owl:allValuesFrom>
            <owl:Class rdf:about="#Asset"/>
        </owl:allValuesFrom>
    </owl:Restriction>
</owl:equivalentClass>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith>
    <owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Authenticity"/>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int">1</owl:minCardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="LevelOfAssurance"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>

```

```

</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="OperationalCost"/>
    </owl:onProperty>
    <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:cardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="AcquisitionCost"/>
    </owl:onProperty>
    <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:cardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:cardinality>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="CountermeasureID"/>
    </owl:onProperty>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Threat"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:someValuesFrom>
      <owl:Class rdf:about="#Impact"/>
    </owl:someValuesFrom>
    <owl:onProperty rdf:resource="#Reduces"/>
  </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:minCardinality>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="InstallationCost"/>

```

```

        </owl:onProperty>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Confidentiality"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Controls"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Asset"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetInventory"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#SecurityPolicy"/>
</owl:Class>
<owl:Class rdf:ID="AccessControl">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#RiskAssessment"/>
    </rdfs:subClassOf>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Controls"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#NonRepudiation">
    <owl:disjointWith>
        <owl:Class rdf:about="#Frequency"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#ThreatAgent"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#SecurityPolicy"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Consequence"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Stakeholder"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Integrity"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskEvaluation"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Threat"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Confidentiality"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Risk"/>
    </owl:disjointWith>

```



```

<owl:disjointWith>
  <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith>
  <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Class rdf:about="#SecurityRequirement"/>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Attack"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
</owl:Class>
<owl:Class rdf:ID="PrivateKey">
  <rdfs:subClassOf>
    <owl:Class rdf:ID="CryptographicKey"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#RiskAssessment">
  <rdfs:subClassOf>
    <owl:Class rdf:ID="SecurityManagedElement"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Hub">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#NetworkEquipment"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Masquerade">
  <rdfs:subClassOf rdf:resource="#Deliberate"/>
</owl:Class>

```



```

<owl:Class rdf:ID="CIMCertificateAuthority">
  <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:about="#FTPServer">
  <owl:disjointWith rdf:resource="#WebServer"/>
  <owl:disjointWith rdf:resource="#TelnetServer"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#MailServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#FileServer"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Server"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#ApplicationServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#ProxyServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#GroupwareServer"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#MailServer">
  <owl:disjointWith rdf:resource="#FTPServer"/>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Server"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#ApplicationServer"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#GroupwareServer"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#WebServer"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#FileServer"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#TelnetServer"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#ProxyServer"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#CIMNetwork">
  <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:about="#Database">
  <owl:disjointWith>
    <owl:Class rdf:about="#ContinuityPlans"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#UserManual"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#InformationBackup"/>
  </owl:disjointWith>
</owl:Class>

```

```

<rdfs:subClassOf>
  <owl:Class rdf:about="#Information"/>
</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Asset">
  <owl:disjointWith rdf:resource="#SecurityPolicy"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="AssetID"/>
    </owl:onProperty>
    <owl:cardinality
      rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:cardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:someValuesFrom rdf:resource="#Compliance"/>
    <owl:onProperty>
      <owl:ObjectProperty rdf:ID="HasCompliance"/>
    </owl:onProperty>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:someValuesFrom rdf:resource="#NonRepudiation"/>
    <owl:onProperty>
      <owl:ObjectProperty rdf:ID="HasNonRepudiation"/>
    </owl:onProperty>
  </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:ObjectProperty rdf:ID="HasIntegrity"/>
    </owl:onProperty>
    <owl:someValuesFrom rdf:resource="#Integrity"/>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>

```

```

<owl:DatatypeProperty rdf:ID="AssetType"/>
</owl:onProperty>
<owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
<owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith>
<owl:Class rdf:about="#Attack"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith>
<owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<rdfs:subClassOf>
<owl:Restriction>
<owl:onProperty>
<owl:ObjectProperty rdf:ID="HasConfidentiality"/>
</owl:onProperty>
<owl:someValuesFrom>
<owl:Class rdf:about="#Confidentiality"/>
</owl:someValuesFrom>
</owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
<owl:Restriction>
<owl:onProperty>
<owl:ObjectProperty rdf:ID="HasAvailability"/>
</owl:onProperty>
<owl:someValuesFrom>
<owl:Class rdf:about="#Availability"/>
</owl:someValuesFrom>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
<owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
<owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith>
<owl:Class rdf:about="#Frequency"/>
</owl:disjointWith>
<owl:disjointWith>
<owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<owl:equivalentClass>
<owl:Class>
<owl:intersectionOf rdf:parseType="Collection">
<owl:Restriction>
<owl:onProperty>
<owl:ObjectProperty rdf:ID="HasAssetValue"/>
</owl:onProperty>

```

```

<owl:allValuesFrom>
    <owl:Class rdf:about="#AssetValue"/>
</owl:allValuesFrom>
</owl:Restriction>
<owl:Class rdf:about="#RiskAssessment"/>
<owl:Restriction>
    <owl:allValuesFrom>
        <owl:Class rdf:about="#SensitivityLevel"/>
    </owl:allValuesFrom>
    <owl:onProperty>
        <owl:ObjectProperty
rdf:ID="HasSensitivityLevel"/>
    </owl:onProperty>
</owl:Restriction>
</owl:intersectionOf>
</owl:Class>
</owl:equivalentClass>
<owl:disjointWith>
    <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:onProperty>
            <owl:ObjectProperty rdf:ID="HasAuthenticity"/>
        </owl:onProperty>
        <owl:someValuesFrom rdf:resource="#Authenticity"/>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetValue"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="Password">
    <rdfs:subClassOf>
        <owl:Class rdf:ID="CIMCredential"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Sensor">
    <rdfs:subClassOf>
        <owl:Class rdf:ID="CIMLogicalDevice"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="ComputerEquipment">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Hardware"/>
    </rdfs:subClassOf>
</owl:Class>

```



```

</owl:Class>
<owl:Class rdf:ID="OperatingSystemAccessControl">
  <rdfs:subClassOf rdf:resource="#AccessControl"/>
</owl:Class>
<owl:Class rdf:ID="Antivirus">
  <owl:disjointWith>
    <owl:Class rdf:ID="Firewall"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="NetworkCountermeasure"/>
  </owl:disjointWith>
  <rdfs:subClassOf rdf:resource="#Countermeasure"/>
</owl:Class>
<owl:Class rdf:about="#Personnel">
  <owl:disjointWith>
    <owl:Class rdf:about="#LogRecord"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Hardware"/>
  </owl:disjointWith>
  <rdfs:subClassOf rdf:resource="#Asset"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Software"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Data"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Firmware"/>
  </owl:disjointWith>
  <rdfs:subClassOf rdf:resource="#CIMUserEntity"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Information"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Services"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Network"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Documents"/>
</owl:Class>
<owl:Class rdf:about="#InformationBackup">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Information"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#ContinuityPlans"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Database"/>
  <owl:disjointWith rdf:resource="#UserManual"/>
</owl:Class>
<owl:Class rdf:about="#NetworkEquipment">
  <rdfs:subClassOf rdf:resource="#Network"/>
  <owl:disjointWith rdf:resource="#PublicNetwork"/>

```

```

<owl:disjointWith rdf:resource="#PrivateNetwork"/>
<rdfs:subClassOf>
    <owl:Class rdf:ID="CIMProduct"/>
</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Accidental">
    <owl:disjointWith rdf:resource="#Environmental"/>
    <rdfs:subClassOf rdf:resource="#Threat"/>
    <owl:disjointWith rdf:resource="#Deliberate"/>
</owl:Class>
<owl:Class rdf:about="#Attack">
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetInventory"/>
    </owl:disjointWith>
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Impact"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Confidentiality"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Compliance"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Vulnerability"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
                >1</owl:cardinality>
            <owl:onProperty>
                <owl:DatatypeProperty rdf:ID="AttackID"/>
            </owl:onProperty>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Consequence"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Frequency"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskEvaluation"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#SensitivityLevel"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Stakeholder"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Countermeasure"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskValue"/>
    </owl:disjointWith>

```

```

</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:someValuesFrom rdf:resource="#Threat"/>
    <owl:onProperty rdf:resource="#Arises"/>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Asset"/>
<owl:disjointWith>
  <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="AttackType"/>
    </owl:onProperty>
    <owl:cardinality>
      >1</owl:cardinality>
    </owl:Restriction>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#SecurityPolicy"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Authenticity"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="AttackName"/>
    </owl:onProperty>
    <owl:minCardinality>
      >1</owl:minCardinality>
    </owl:Restriction>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="Redundancy">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Availability"/>

```



```

</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#TransportLayerProtocol">
  <owl:disjointWith>
    <owl:Class rdf:ID="InternetLayerSecurityProtocol"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="ApplicationLayerProtocol"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:ID="Protocol"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:ID="Layer2ForwardingProtocol"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:ID="Layer2TunnelingProtocol"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Raptor">
  <owl:disjointWith rdf:resource="#Interactive"/>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Gateway"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#Proxy"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Local"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Interlock"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Remsh"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Transparent"/>
</owl:Class>
<owl:Class rdf:ID="User">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Stakeholder"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="CIMPublicKey">
  <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:about="#AssetValue">
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskValue"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#NonRepudiation"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Frequency"/>
  </owl:disjointWith>
  <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
  <owl:disjointWith>

```

```

<owl:Class rdf:about="#SensitivityLevel"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Asset"/>
<owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Threat"/>
</owl:Class>
<owl:Class rdf:ID="AccessPoint">
    <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
</owl:Class>
<owl:Class rdf:about="#Services">
    <owl:disjointWith>

```

```

<owl:Class rdf:about="#Information"/>
</owl:disjointWith>
<rdfs:subClassOf rdf:resource="#Asset"/>
<owl:disjointWith rdf:resource="#Documents"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Data"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Network"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Firmware"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Personnel"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Hardware"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#LogRecord"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Software"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#ApplicationServer">
    <owl:disjointWith>
        <owl:Class rdf:about="#FileServer"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#TelnetServer"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#GroupwareServer"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#WebServer"/>
    <owl:disjointWith rdf:resource="#FTPServer"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#ProxyServer"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Server"/>
    </rdfs:subClassOf>
    <owl:disjointWith rdf:resource="#MailServer"/>
</owl:Class>
<owl:Class rdf:about="#SecurityRequirement">
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:ID="PolicyOwner">
    <rdfs:subClassOf rdf:resource="#CIMUserEntity"/>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Stakeholder"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="InternetKeySecurityProtocol">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#InternetLayerSecurityProtocol"/>
    </rdfs:subClassOf>

```



```

<owl:disjointWith>
    <owl:Class rdf:ID="IPSecurityProtocol"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="CIMGroup">
    <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:ID="Checksum">
    <rdfs:subClassOf rdf:resource="#Integrity"/>
</owl:Class>
<owl:Class rdf:ID="PacketFilter">
    <owl:disjointWith>
        <owl:Class rdf:ID="StatefulPacketInspection"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Firewall"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="HashingAlgorithm">
    <rdfs:subClassOf rdf:resource="#Integrity"/>
</owl:Class>
<owl:Class rdf:about="#ApplicationLayerProtocol">
    <owl:disjointWith>
        <owl:Class rdf:about="#InternetLayerSecurityProtocol"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Protocol"/>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Layer2TunnelingProtocol"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Layer2ForwardingProtocol"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#TransportLayerProtocol"/>
</owl:Class>
<owl:Class rdf:about="#SensitivityLevel">
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
                >1</owl:cardinality>
            <owl:onProperty>
                <owl:DatatypeProperty rdf:ID="Proprietary"/>
            </owl:onProperty>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith rdf:resource="#Authenticity"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Availability"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Countermeasure"/>
    <owl:disjointWith>

```

```

<owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Attack"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
    >1</owl:cardinality>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="TopSecret"/>
    </owl:onProperty>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith>
  <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
  <owl:Class rdf:about="#Frequency"/>
</owl:disjointWith>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith rdf:resource="#Asset"/>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith>
  <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith>
  <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="HighlyConfidential"/>
    </owl:onProperty>
    <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
      >1</owl:cardinality>
  </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
  <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>

```

```

<owl:Class rdf:about="#Vulnerability"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Impact"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Threat"/>
</owl:Class>
<owl:Class rdf:ID="Client">
    <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
</owl:Class>
<owl:Class rdf:ID="WordProcessor">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#ApplicationSoftware"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#CIMPolicy">
    <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:ID="CIMPrivilege">
    <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:about="#Vulnerability">
    <owl:disjointWith>
        <owl:Class rdf:about="#Impact"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#NonRepudiation"/>
    <owl:disjointWith rdf:resource="#Asset"/>
    <owl:disjointWith rdf:resource="#Attack"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskValue"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#AssetValue"/>
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:onProperty>
                <owl:ObjectProperty rdf:ID="Enables"/>
            </owl:onProperty>
            <owl:someValuesFrom>
                <owl:Class rdf:about="#Risk"/>
            </owl:someValuesFrom>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Frequency"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Consequence"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#UnwantedIncident"/>
    </owl:disjointWith>

```



```

</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Threat"/>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:someValuesFrom rdf:resource="#Asset"/>
        <owl:onProperty>
            <owl:ObjectProperty rdf:ID="Exposes"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Authenticity"/>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int">1</owl:cardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="VulnerabilityID"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith rdf:resource="#Integrity"/>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:someValuesFrom>
            <owl:Class rdf:about="#UnwantedIncident"/>

```

```

        </owl:someValuesFrom>
        <owl:onProperty rdf:resource="#Enables"/>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
</owl:Class>
<owl:Class rdf:ID="Processor">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#CIMLogicalDevice"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Server">
    <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
</owl:Class>
<owl:Class rdf:ID="Modem">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#CIMLogicalDevice"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Flood">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#NaturalDisaster"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Impact">
    <owl:disjointWith rdf:resource="#Compliance"/>
    <owl:disjointWith rdf:resource="#Attack"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskValue"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskEvaluation"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Controls"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Availability"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Stakeholder"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Asset"/>
    <owl:disjointWith rdf:resource="#Vulnerability"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Frequency"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#AssetValue"/>
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Confidentiality"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Restriction>

```

```

<owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
<owl:onProperty>
    <owl:DatatypeProperty rdf:ID="AssetCostDecrease"/>
</owl:onProperty>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="ImpactID"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
</owl:Class>
<owl:Class rdf:about="#Frequency">
    <owl:disjointWith rdf:resource="#NonRepudiation"/>
    <owl:disjointWith rdf:resource="#Countermeasure"/>
    <owl:disjointWith rdf:resource="#Impact"/>
    <owl:disjointWith rdf:resource="#SensitivityLevel"/>
    <owl:disjointWith rdf:resource="#Asset"/>
    <owl:disjointWith rdf:resource="#SecurityPolicy"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Risk"/>
    </owl:disjointWith>
    <owl:disjointWith>

```



```

<owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Controls"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith rdf:resource="#Vulnerability"/>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Consequence"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#ProxyServer">
    <owl:disjointWith rdf:resource="#TelnetServer"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#FileServer"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#MailServer"/>
    <rdfs:subClassOf rdf:resource="#Server"/>
    <owl:disjointWith rdf:resource="#WebServer"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#GroupwareServer"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#FTPServer"/>
    <owl:disjointWith rdf:resource="#ApplicationServer"/>
</owl:Class>

```



```

<owl:Class rdf:about="#Information">
  <owl:disjointWith>
    <owl:Class rdf:about="#Firmware"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Documents"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Software"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Data"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Personnel"/>
  <rdfs:subClassOf rdf:resource="#Asset"/>
  <owl:disjointWith rdf:resource="#Services"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#LogRecord"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Network"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Hardware"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Layer2TunnelingProtocol">
  <owl:disjointWith rdf:resource="#TransportLayerProtocol"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#InternetLayerSecurityProtocol"/>
  </owl:disjointWith>
  <owl:disjointWith
rdf:resource="#ApplicationLayerProtocol"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Layer2ForwardingProtocol"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Protocol"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Consequence">
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Asset"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Stakeholder"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Integrity"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Controls"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
  </owl:disjointWith>

```



```

</owl:disjointWith>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<owl:disjointWith rdf:resource="#Vulnerability"/>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Frequency"/>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:ID="Rule">
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:ID="Wiring">
    <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
</owl:Class>
<owl:Class rdf:ID="Keyboard">
    <rdfs:subClassOf>
        <owl:Class rdf:ID="UserDevice"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#NaturalDisaster">
    <rdfs:subClassOf rdf:resource="#Environmental"/>
    <owl:disjointWith rdf:resource="#EnvironmentalThreat"/>
</owl:Class>
<owl:Class rdf:ID="SymmetricKeyCryptography">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Confidentiality"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Layer2ForwardingProtocol">
    <owl:disjointWith>

```

```

<owl:Class rdf:about="#InternetLayerSecurityProtocol"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Class rdf:about="#Protocol"/>
</rdfs:subClassOf>
<owl:disjointWith
rdf:resource="#Layer2TunnelingProtocol"/>
    <owl:disjointWith rdf:resource="#TransportLayerProtocol"/>
    <owl:disjointWith
rdf:resource="#ApplicationLayerProtocol"/>
</owl:Class>
<owl:Class rdf:about="#Router">
    <owl:disjointWith>
        <owl:Class rdf:about="#PABXs"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#AnsweringMachines"/>
    </owl:disjointWith>
    <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
    <owl:disjointWith rdf:resource="#FaxMachine"/>
</owl:Class>
<owl:Class rdf:about="#Controls">
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskEvaluation"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Countermeasure"/>
    <owl:disjointWith rdf:resource="#SensitivityLevel"/>
    <owl:disjointWith rdf:resource="#ValueDefinition"/>
    <owl:disjointWith rdf:resource="#Authenticity"/>
    <owl:disjointWith rdf:resource="#Threat"/>
    <owl:disjointWith rdf:resource="#Compliance"/>
    <owl:disjointWith rdf:resource="#Frequency"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskValue"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Integrity"/>
    <owl:disjointWith rdf:resource="#Vulnerability"/>
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
    <owl:disjointWith rdf:resource="#SecurityPolicy"/>
    <owl:disjointWith rdf:resource="#Consequence"/>
    <owl:disjointWith rdf:resource="#Asset"/>
    <owl:disjointWith rdf:resource="#Attack"/>
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:onProperty rdf:resource="#Includes"/>
            <owl:someValuesFrom rdf:resource="#Countermeasure"/>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetInventory"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#ThreatAgent"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#AssetValue"/>
    <owl:disjointWith>

```



```

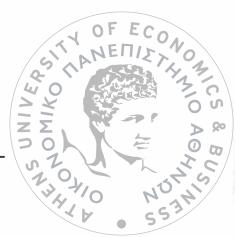
<owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Stakeholder"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#ScriptingTools">
    <rdfs:subClassOf
rdf:resource="#DevelopmentToolsAndUtilities"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#SetupUtilities"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#HTMLEditor"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#DatabaseTools"/>
    </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Local">
    <owl:disjointWith rdf:resource="#Transparent"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Proxy"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:about="#Gateway"/>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Interlock"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Interactive"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Remsh"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Raptor"/>
</owl:Class>
<owl:Class rdf:about="#SecurityManagedElement">
    <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:about="#FileServer">
    <owl:disjointWith rdf:resource="#MailServer"/>
    <owl:disjointWith rdf:resource="#FTPServer"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#GroupwareServer"/>

```

```

</owl:disjointWith>
<owl:disjointWith rdf:resource="#WebServer"/>
<rdfs:subClassOf rdf:resource="#Server"/>
<owl:disjointWith rdf:resource="#TelnetServer"/>
<owl:disjointWith rdf:resource="#ProxyServer"/>
<owl:disjointWith rdf:resource="#ApplicationServer"/>
</owl:Class>
<owl:Class rdf:about="#ApplicationSoftware">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Software"/>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#SystemSoftware"/>
  </owl:disjointWith>
  <owl:disjointWith
rdf:resource="#DevelopmentToolsAndUtilities"/>
</owl:Class>
<owl:Class rdf:about="#PABXs">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
  </rdfs:subClassOf>
  <owl:disjointWith rdf:resource="#FaxMachine"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#AnsweringMachines"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Router"/>
</owl:Class>
<owl:Class rdf:about="#NetworkCountermeasure">
  <owl:disjointWith>
    <owl:Class rdf:about="#Firewall"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Antivirus"/>
  <rdfs:subClassOf rdf:resource="#Countermeasure"/>
</owl:Class>
<owl:Class rdf:about="#MaliciousCode">
  <rdfs:subClassOf rdf:resource="#Deliberate"/>
</owl:Class>
<owl:Class rdf:about="#Stakeholder">
  <owl:disjointWith rdf:resource="#Compliance"/>
  <owl:disjointWith rdf:resource="#NonRepudiation"/>
  <owl:disjointWith rdf:resource="#Asset"/>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty>
        <owl:ObjectProperty rdf:ID="Owns"/>
      </owl:onProperty>
      <owl:someValuesFrom rdf:resource="#Asset"/>
    </owl:Restriction>
  </rdfs:subClassOf>
  <owl:disjointWith rdf:resource="#Vulnerability"/>
  <owl:disjointWith rdf:resource="#Controls"/>
  <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty rdf:resource="#Owns"/>
      <owl:someValuesFrom rdf:resource="#SecurityPolicy"/>

```



```

        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Confidentiality"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#AssetValue"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#ThreatAgent"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#SecurityPolicy"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#AssetInventory"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Threat"/>
    <owl:disjointWith rdf:resource="#Countermeasure"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#RiskEvaluationCriterion"/>
    </owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
        >1</owl:cardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="StakeholderID"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:someValuesFrom rdf:resource="#Rule"/>
        <owl:onProperty>
            <owl:ObjectProperty rdf:ID="Obeys"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith rdf:resource="#Frequency"/>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskValue"/>
</owl:disjointWith>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Authenticity"/>
<rdfs:subClassOf>
    <owl:Restriction>

```

```

<owl:onProperty>
  <owl:ObjectProperty rdf:ID="Has"/>
</owl:onProperty>
<owl:someValuesFrom>
  <owl:Class rdf:ID="Right"/>
</owl:someValuesFrom>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith>
  <owl:Class rdf:about="#RiskEvaluation"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Consequence"/>
<owl:disjointWith rdf:resource="#Integrity"/>
</owl:Class>
<owl:Class rdf:ID="Door">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CIMLogicalDevice"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#RiskValue">
  <owl:disjointWith rdf:resource="#ValueDefinition"/>
  <owl:disjointWith rdf:resource="#SensitivityLevel"/>
  <owl:disjointWith rdf:resource="#Countermeasure"/>
  <owl:disjointWith rdf:resource="#AssetValue"/>
  <owl:disjointWith rdf:resource="#Integrity"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Impact"/>
  <owl:disjointWith rdf:resource="#Compliance"/>
  <owl:disjointWith rdf:resource="#Consequence"/>
  <owl:disjointWith rdf:resource="#Vulnerability"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Authenticity"/>
  <owl:disjointWith rdf:resource="#Frequency"/>
  <owl:disjointWith rdf:resource="#Attack"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#SecurityPolicy"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Threat"/>
  <owl:disjointWith rdf:resource="#NonRepudiation"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
  </owl:disjointWith>

```



```

<owl:disjointWith rdf:resource="#Controls"/>
<owl:disjointWith rdf:resource="#Stakeholder"/>
<owl:disjointWith rdf:resource="#Asset"/>
<owl:disjointWith>
    <owl:Class rdf:about="#UnwantedIncident"/>
</owl:disjointWith>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:about="#Right">
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:about="#Software">
    <owl:disjointWith rdf:resource="#Information"/>
    <rdfs:subClassOf rdf:resource="#Asset"/>
    <owl:disjointWith rdf:resource="#Services"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Firmware"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Documents"/>
    <rdfs:subClassOf>
        <owl:Restriction>
            <owl:onProperty>
                <owl:ObjectProperty rdf:ID="Uses"/>
            </owl:onProperty>
            <owl:someValuesFrom>
                <owl:Class rdf:about="#LogRecord"/>
            </owl:someValuesFrom>
        </owl:Restriction>
    </rdfs:subClassOf>
    <owl:disjointWith>
        <owl:Class rdf:about="#Data"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#Hardware"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Network"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#CommunicationsEquipment"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Personnel"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#LogRecord"/>
    </owl:disjointWith>
    <rdfs:subClassOf>
        <owl:Class rdf:ID="CIMSoftwareElement"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Display">
    <rdfs:subClassOf>
        <owl:Class rdf:about="#UserDevice"/>
    </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#EncryptionAlgorithm">
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
    <rdfs:subClassOf>
        <owl:Restriction>

```



```

<owl:someValuesFrom>
  <owl:Class rdf:about="#CryptographicKey"/>
</owl:someValuesFrom>
<owl:onProperty>
  <owl:ObjectProperty rdf:ID="Creates"/>
</owl:onProperty>
</owl:Restriction>
</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="AccessControlPolicy">
  <rdfs:subClassOf rdf:resource="#CIMPolicy"/>
</owl:Class>
<owl:Class rdf:about="#Interlock">
  <owl:disjointWith rdf:resource="#Transparent"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Remsh"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Proxy"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Interactive"/>
  <owl:disjointWith rdf:resource="#Local"/>
  <owl:disjointWith rdf:resource="#Raptor"/>
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Gateway"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#UnwantedIncident">
  <owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:allValuesFrom rdf:resource="#Impact"/>
      <owl:onProperty rdf:resource="#Has"/>
    </owl:Restriction>
  </rdfs:subClassOf>
  <owl:disjointWith rdf:resource="#Asset"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#Availability"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Integrity"/>
  <owl:disjointWith rdf:resource="#Compliance"/>
  <owl:disjointWith rdf:resource="#Threat"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
  </owl:disjointWith>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:ID="ImportanceLevel"/>
      </owl:onProperty>
    </owl:Restriction>
  </rdfs:subClassOf>
</owl:Class>

```



```

<owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith rdf:resource="#Stakeholder"/>
<owl:disjointWith rdf:resource="#RiskValue"/>
<owl:disjointWith rdf:resource="#Consequence"/>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:onProperty>
            <owl:DatatypeProperty
rdf:ID="UnwantedIncidentCost"/>
        </owl:onProperty>
        <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Authenticity"/>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith rdf:resource="#Vulnerability"/>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#Controls"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="UnwantedIncidentID"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:onProperty rdf:resource="#Targets"/>
        <owl:someValuesFrom rdf:resource="#Asset"/>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
</owl:disjointWith>
```



```

<owl:disjointWith rdf:resource="#Frequency"/>
</owl:Class>
<owl:Class rdf:about="#Availability">
  <owl:disjointWith rdf:resource="#Authenticity"/>
  <owl:disjointWith rdf:resource="#SensitivityLevel"/>
  <owl:disjointWith rdf:resource="#Threat"/>
  <owl:disjointWith rdf:resource="#SecurityPolicy"/>
  <owl:disjointWith rdf:resource="#ValueDefinition"/>
  <owl:disjointWith rdf:resource="#Controls"/>
  <owl:disjointWith rdf:resource="#Impact"/>
  <owl:disjointWith rdf:resource="#AssetValue"/>
  <owl:disjointWith rdf:resource="#Integrity"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#UnwantedIncident"/>
  <rdfs:subClassOf rdf:resource="#SecurityRequirement"/>
  <owl:disjointWith rdf:resource="#NonRepudiation"/>
  <owl:disjointWith rdf:resource="#RiskValue"/>
  <owl:disjointWith rdf:resource="#Vulnerability"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluation"/>
  </owl:disjointWith>
  <owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Countermeasure"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Frequency"/>
  <owl:disjointWith rdf:resource="#Compliance"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Consequence"/>
  <owl:disjointWith rdf:resource="#Stakeholder"/>
  <owl:disjointWith rdf:resource="#Attack"/>
</owl:Class>
<owl:Class rdf:about="#RiskEvaluation">
  <owl:disjointWith rdf:resource="#RiskValue"/>
  <owl:disjointWith rdf:resource="#Vulnerability"/>
  <owl:disjointWith rdf:resource="#Asset"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Attack"/>
  <owl:disjointWith rdf:resource="#Threat"/>
  <owl:disjointWith rdf:resource="#Availability"/>
  <owl:disjointWith rdf:resource="#Countermeasure"/>
  <owl:disjointWith rdf:resource="#SensitivityLevel"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Risk"/>
  
```



```

</owl:disjointWith>
<owl:disjointWith rdf:resource="#Consequence"/>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith rdf:resource="#Frequency"/>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith rdf:resource="#Stakeholder"/>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith rdf:resource="#UnwantedIncident"/>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith rdf:resource="#Controls"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
</owl:Class>
<owl:Class rdf:about="#Gateway">
    <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
</owl:Class>
<owl:Class rdf:about="#Data">
    <owl:disjointWith rdf:resource="#Services"/>
    <owl:disjointWith rdf:resource="#Software"/>
    <owl:disjointWith rdf:resource="#Information"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#LogRecord"/>
    </owl:disjointWith>
    <owl:disjointWith>
        <owl:Class rdf:about="#CommunicationsEquipment"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Documents"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Hardware"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Personnel"/>
    <owl:disjointWith rdf:resource="#Network"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#Firmware"/>
    </owl:disjointWith>
    <rdfs:subClassOf rdf:resource="#Asset"/>
</owl:Class>
<owl:Class rdf:ID="WebBrowser">
    <rdfs:subClassOf rdf:resource="#ApplicationSoftware"/>
</owl:Class>
<owl:Class rdf:ID="DecryptionAlgorithm">
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:ID="ApplicationAccessControl">

```

```

<rdfs:subClassOf rdf:resource="#AccessControl"/>
</owl:Class>
<owl:Class rdf:ID="Scanner">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CIMLogicalDevice"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#LogRecord">
  <owl:disjointWith rdf:resource="#Network"/>
  <owl:disjointWith rdf:resource="#Services"/>
  <owl:disjointWith rdf:resource="#Software"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Firmware"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Information"/>
  <rdfs:subClassOf rdf:resource="#Asset"/>
  <owl:disjointWith rdf:resource="#Personnel"/>
  <owl:disjointWith rdf:resource="#Documents"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Data"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Hardware"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:ID="NetworkInterfaceCard">
  <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
</owl:Class>
<owl:Class rdf:ID="PowerSupply">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CIMLogicalDevice"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#UserDevice">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CIMLogicalDevice"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Decryption">
  <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty rdf:resource="#Uses"/>
      <owl:someValuesFrom
rdf:resource="#DecryptionAlgorithm"/>
    </owl:Restriction>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="LogicalPort">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CIMLogicalDevice"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="DoS">
  <rdfs:subClassOf rdf:resource="#Deliberate"/>

```



```

</owl:Class>
<owl:Class rdf:about="#Protocol">
  <rdfs:subClassOf rdf:resource="#NetworkCountermeasure"/>
</owl:Class>
<owl:Class rdf:about="#Proxy">
  <owl:disjointWith rdf:resource="#Transparent"/>
  <owl:disjointWith rdf:resource="#Local"/>
  <rdfs:subClassOf rdf:resource="#Gateway"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Remsh"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Raptor"/>
  <owl:disjointWith rdf:resource="#Interlock"/>
  <owl:disjointWith rdf:resource="#Interactive"/>
</owl:Class>
<owl:Class rdf:about="#StatefulPacketInspection">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#Firewall"/>
  </rdfs:subClassOf>
  <owl:disjointWith rdf:resource="#PacketFilter"/>
</owl:Class>
<owl:Class rdf:about="#Risk">
  <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Integrity"/>
  <owl:disjointWith rdf:resource="#Availability"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#ThreatAgent"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#RiskValue"/>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:someValuesFrom rdf:resource="#Asset"/>
      <owl:onProperty rdf:resource="#Targets"/>
    </owl:Restriction>
  </rdfs:subClassOf>
  <owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#UnwantedIncident"/>
  <owl:disjointWith rdf:resource="#NonRepudiation"/>
  <owl:disjointWith rdf:resource="#Stakeholder"/>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int">1</owl:cardinality>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:ID="RiskID"/>
      </owl:onProperty>
    </owl:Restriction>
  </rdfs:subClassOf>
  <owl:disjointWith rdf:resource="#ValueDefinition"/>
  <owl:disjointWith rdf:resource="#RiskEvaluation"/>

```

```

<owl:disjointWith rdf:resource="#Asset"/>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Frequency"/>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith rdf:resource="#Controls"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<owl:equivalentClass>
    <owl:Class>
        <owl:intersectionOf rdf:parseType="Collection">
            <owl:Restriction>
                <owl:onProperty>
                    <owl:ObjectProperty rdf:ID="HasRiskValue"/>
                </owl:onProperty>
                <owl:allValuesFrom rdf:resource="#RiskValue"/>
            </owl:Restriction>
            <owl:Restriction>
                <owl:onProperty rdf:resource="#HasFrequency"/>
                <owl:allValuesFrom rdf:resource="#Frequency"/>
            </owl:Restriction>
        </owl:intersectionOf>
    </owl:Class>
</owl:equivalentClass>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith rdf:resource="#Consequence"/>
<owl:disjointWith rdf:resource="#Vulnerability"/>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
            >1</owl:minCardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="Likelihood"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Encryption">
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:someValuesFrom
rdf:resource="#EncryptionAlgorithm"/>
        <owl:onProperty rdf:resource="#Uses"/>
    </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:about="#CIMLogicalDevice">
<rdfs:subClassOf>

```



```

<owl:Restriction>
  <owl:onProperty>
    <owl:DatatypeProperty rdf:ID="DeviceID"/>
  </owl:onProperty>
  <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
</owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf rdf:resource="#ComputerEquipment"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="CreationClassName"/>
    </owl:onProperty>
  </owl:Restriction>
</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#TLSProtocol">
  <rdfs:subClassOf rdf:resource="#TransportLayerProtocol"/>
  <owl:disjointWith rdf:resource="#SSLProtocol"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#SSHProtocol"/>
  </owl:disjointWith>
</owl:Class>
<owl:Class rdf:about="#Firewall">
  <owl:disjointWith rdf:resource="#Antivirus"/>
  <owl:disjointWith rdf:resource="#NetworkCountermeasure"/>
  <rdfs:subClassOf rdf:resource="#Countermeasure"/>
</owl:Class>
<owl:Class rdf:ID="Fire">
  <rdfs:subClassOf rdf:resource="#NaturalDisaster"/>
</owl:Class>
<owl:Class rdf:about="#ContinuityPlans">
  <owl:disjointWith rdf:resource="#Database"/>
  <owl:disjointWith rdf:resource="#InformationBackup"/>
  <rdfs:subClassOf rdf:resource="#Information"/>
  <owl:disjointWith rdf:resource="#UserManual"/>
</owl:Class>
<owl:Class rdf:ID="InformationSecurityPolicyDoc">
  <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:about="#CIMCredential">
  <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:about="#SSHProtocol">
  <owl:disjointWith rdf:resource="#TLSProtocol"/>
  <owl:disjointWith rdf:resource="#SSLProtocol"/>
  <rdfs:subClassOf rdf:resource="#TransportLayerProtocol"/>
</owl:Class>
<owl:Class rdf:about="#ThreatAgent">
  <rdfs:subClassOf>
    <owl:Restriction>

```

```

<owl:onProperty>
  <owl:DatatypeProperty rdf:ID="ThreatAgentName"/>
</owl:onProperty>
<owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
  >1</owl:cardinality>
</owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="Capability"/>
    </owl:onProperty>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
  >1</owl:minCardinality>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith rdf:resource="#UnwantedIncident"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="ThreatAgentCategory"/>
    </owl:onProperty>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
  >1</owl:minCardinality>
</owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Consequence"/>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith rdf:resource="#Vulnerability"/>
<owl:disjointWith>
  <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith rdf:resource="#Risk"/>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#Stakeholder"/>
<owl:disjointWith rdf:resource="#Controls"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
<owl:disjointWith rdf:resource="#Attack"/>
<rdfs:subClassOf>
  <owl:Restriction>
    <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
  >1</owl:minCardinality>
    <owl:onProperty>
      <owl:DatatypeProperty rdf:ID="Motivation"/>
    </owl:onProperty>
  </owl:Restriction>

```



```

</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
        >1</owl:minCardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="Opportunity"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
        >1</owl:cardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:about="#ThreatID"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Frequency"/>
<owl:equivalentClass>
    <owl:Restriction>
        <owl:onProperty>
            <owl:ObjectProperty rdf:ID="Initiates"/>
        </owl:onProperty>
        <owl:allValuesFrom rdf:resource="#Threat"/>
    </owl:Restriction>
</owl:equivalentClass>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith rdf:resource="#Asset"/>
<owl:disjointWith rdf:resource="#RiskValue"/>
<owl:disjointWith>
    <owl:Class rdf:about="#RiskEvaluationCriterion"/>
</owl:disjointWith>
<rdfs:subClassOf>
    <owl:Restriction>
        <owl:minCardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
        >1</owl:minCardinality>
        <owl:onProperty>
            <owl:DatatypeProperty rdf:ID="LevelOfEffort"/>
        </owl:onProperty>
    </owl:Restriction>
</rdfs:subClassOf>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Availability"/>
<owl:disjointWith rdf:resource="#RiskEvaluation"/>
</owl:Class>
<owl:Class rdf:ID="NetworkAccessControl">
    <rdfs:subClassOf rdf:resource="#AccessControl"/>

```



```

</owl:Class>
<owl:Class rdf:about="#CIMSoftwareElement">
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:ID="Version"/>
      </owl:onProperty>
    </owl:Restriction>
  </rdfs:subClassOf>
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:ID="Name"/>
      </owl:onProperty>
    </owl:Restriction>
  </rdfs:subClassOf>
  <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
</owl:Class>
<owl:Class rdf:about="#Firmware">
  <rdfs:subClassOf rdf:resource="#Asset"/>
  <owl:disjointWith rdf:resource="#Data"/>
  <owl:disjointWith rdf:resource="#LogRecord"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#Hardware"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Network"/>
  <owl:disjointWith rdf:resource="#Documents"/>
  <owl:disjointWith rdf:resource="#Software"/>
  <owl:disjointWith rdf:resource="#Information"/>
  <owl:disjointWith rdf:resource="#Personnel"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#CommunicationsEquipment"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Services"/>
</owl:Class>
<owl:Class rdf:ID="Cable">
  <rdfs:subClassOf rdf:resource="#NetworkEquipment"/>
</owl:Class>
<owl:Class rdf:ID="SecretKey">
  <rdfs:subClassOf>
    <owl:Class rdf:about="#CryptographicKey"/>
  </rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:ID="Eavesdropping">
  <rdfs:subClassOf rdf:resource="#Deliberate"/>
</owl:Class>
<owl:Class rdf:about="#RiskEvaluationCriterion">
  <owl:disjointWith rdf:resource="#Authenticity"/>
  <owl:disjointWith rdf:resource="#RiskEvaluation"/>
  <owl:disjointWith rdf:resource="#Stakeholder"/>

```

```

<owl:disjointWith rdf:resource="#Vulnerability"/>
<owl:disjointWith rdf:resource="#Frequency"/>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#Consequence"/>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith rdf:resource="#ThreatAgent"/>
<owl:disjointWith rdf:resource="#Controls"/>
<owl:disjointWith>
    <owl:Class rdf:about="#Confidentiality"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Compliance"/>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith rdf:resource="#UnwantedIncident"/>
<owl:disjointWith rdf:resource="#RiskValue"/>
<owl:disjointWith rdf:resource="#Asset"/>
<owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
</owl:disjointWith>
<owl:disjointWith rdf:resource="#Availability"/>
<owl:disjointWith rdf:resource="#Risk"/>
<owl:disjointWith rdf:resource="#AssetValue"/>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
</owl:Class>
<owl:Class rdf:ID="ObligationPolicy">
    <rdfs:subClassOf rdf:resource="#SecurityPolicy"/>
</owl:Class>
<owl:Class rdf:about="#DatabaseTools">
    <owl:disjointWith rdf:resource="#HTMLEditor"/>
    <owl:disjointWith>
        <owl:Class rdf:about="#SetupUtilities"/>
    </owl:disjointWith>
    <rdfs:subClassOf
rdf:resource="#DevelopmentToolsAndUtilities"/>
    <owl:disjointWith rdf:resource="#ScriptingTools"/>
</owl:Class>
<owl:Class rdf:about="#CryptographicKey">
    <rdfs:subClassOf rdf:resource="#RiskAssessment"/>
</owl:Class>
<owl:Class rdf:ID="FaultTolerance">
    <rdfs:subClassOf rdf:resource="#Availability"/>
</owl:Class>
<owl:Class rdf:about="#InternetLayerSecurityProtocol">
    <owl:disjointWith
rdf:resource="#ApplicationLayerProtocol"/>
    <owl:disjointWith rdf:resource="#TransportLayerProtocol"/>
    <owl:disjointWith
rdf:resource="#Layer2ForwardingProtocol"/>
    <owl:disjointWith
rdf:resource="#Layer2TunnelingProtocol"/>
    <rdfs:subClassOf rdf:resource="#Protocol"/>

```



```

</owl:Class>
<owl:Class rdf:about="#Confidentiality">
  <owl:disjointWith rdf:resource="#Controls"/>
  <owl:disjointWith rdf:resource="#ThreatAgent"/>
  <owl:disjointWith rdf:resource="#ValueDefinition"/>
  <owl:disjointWith rdf:resource="#Risk"/>
  <owl:disjointWith rdf:resource="#Consequence"/>
  <owl:disjointWith rdf:resource="#UnwantedIncident"/>
  <owl:disjointWith rdf:resource="#Authenticity"/>
  <owl:disjointWith rdf:resource="#SensitivityLevel"/>
  <owl:disjointWith rdf:resource="#Stakeholder"/>
  <owl:disjointWith rdf:resource="#Attack"/>
  <owl:disjointWith rdf:resource="#RiskEvaluation"/>
  <owl:disjointWith rdf:resource="#SecurityPolicy"/>
  <owl:disjointWith rdf:resource="#Countermeasure"/>
  <owl:disjointWith rdf:resource="#Impact"/>
  <owl:disjointWith rdf:resource="#NonRepudiation"/>
  <owl:disjointWith>
    <owl:Class rdf:about="#AssetInventory"/>
  </owl:disjointWith>
  <owl:disjointWith rdf:resource="#Availability"/>
  <owl:disjointWith rdf:resource="#Vulnerability"/>
  <owl:disjointWith rdf:resource="#RiskValue"/>
  <rdfs:subClassOf rdf:resource="#SecurityRequirement"/>
  <owl:disjointWith rdf:resource="#Compliance"/>
  <owl:disjointWith rdf:resource="#Frequency"/>
  <owl:disjointWith rdf:resource="#Threat"/>
  <owl:disjointWith rdf:resource="#AssetValue"/>
  <owl:disjointWith rdf:resource="#Integrity"/>
  <owl:disjointWith
rdf:resource="#RiskEvaluationCriterion"/>
</owl:Class>
<owl:Class rdf:about="#CIMProduct">
  <rdfs:subClassOf>
    <owl:Restriction>
      <owl:onProperty>
        <owl:DatatypeProperty rdf:about="#Name"/>
      </owl:onProperty>
      <owl:cardinality>
        <owl:datatype="http://www.w3.org/2001/XMLSchema#int"
          >1</owl:cardinality>
      </owl:Restriction>
    </rdfs:subClassOf>
    <rdfs:subClassOf rdf:resource="#CIMManagedElement"/>
    <rdfs:subClassOf>
      <owl:Restriction>
        <owl:onProperty>
          <owl:DatatypeProperty rdf:ID="Vendor"/>
        </owl:onProperty>
        <owl:cardinality>
          <owl:datatype="http://www.w3.org/2001/XMLSchema#int"
            >1</owl:cardinality>
        </owl:Restriction>
      </rdfs:subClassOf>
      <rdfs:subClassOf>
        <owl:Restriction>

```

```

<owl:cardinality
rdf:datatype="http://www.w3.org/2001/XMLSchema#int"
>1</owl:cardinality>
<owl:onProperty>
    <owl:DatatypeProperty rdf:ID="IdentifyingNumber"/>
</owl:onProperty>
</owl:Restriction>
</rdfs:subClassOf>
</owl:Class>
<owl:Class rdf:about="#Hardware">
    <owl:disjointWith>
        <owl:Class rdf:about="#CommunicationsEquipment"/>
    </owl:disjointWith>
    <owl:disjointWith rdf:resource="#Personnel"/>
    <owl:disjointWith rdf:resource="#Network"/>
    <owl:disjointWith rdf:resource="#Services"/>
    <owl:disjointWith rdf:resource="#Information"/>
    <owl:disjointWith rdf:resource="#Software"/>
    <rdfs:subClassOf rdf:resource="#Asset"/>
    <owl:disjointWith rdf:resource="#Data"/>
    <owl:disjointWith rdf:resource="#Firmware"/>
    <owl:disjointWith rdf:resource="#Documents"/>
    <owl:disjointWith rdf:resource="#LogRecord"/>
</owl:Class>
<owl:Class rdf:about="#CommunicationsEquipment">
    <owl:disjointWith rdf:resource="#Firmware"/>
    <owl:disjointWith rdf:resource="#Documents"/>
    <owl:disjointWith rdf:resource="#LogRecord"/>
    <owl:disjointWith rdf:resource="#Personnel"/>
    <owl:disjointWith rdf:resource="#Hardware"/>
    <owl:disjointWith rdf:resource="#Network"/>
    <rdfs:subClassOf rdf:resource="#Asset"/>
    <owl:disjointWith rdf:resource="#Software"/>
    <owl:disjointWith rdf:resource="#Data"/>
    <owl:disjointWith rdf:resource="#Information"/>
    <owl:disjointWith rdf:resource="#Services"/>
</owl:Class>
<owl:Class rdf:about="#IPSecurityProtocol">
    <rdfs:subClassOf
rdf:resource="#InternetLayerSecurityProtocol"/>
    <owl:disjointWith
rdf:resource="#InternetKeySecurityProtocol"/>
</owl:Class>
<owl:Class rdf:about="#GroupwareServer">
    <owl:disjointWith rdf:resource="#ApplicationServer"/>
    <rdfs:subClassOf rdf:resource="#Server"/>
    <owl:disjointWith rdf:resource="#WebServer"/>
    <owl:disjointWith rdf:resource="#FTPServer"/>
    <owl:disjointWith rdf:resource="#FileServer"/>
    <owl:disjointWith rdf:resource="#TelnetServer"/>
    <owl:disjointWith rdf:resource="#ProxyServer"/>
    <owl:disjointWith rdf:resource="#MailServer"/>
</owl:Class>
<owl:Class rdf:about="#AssetInventory">
    <owl:disjointWith rdf:resource="#Controls"/>
    <owl:disjointWith rdf:resource="#Asset"/>

```



```

<owl:disjointWith rdf:resource="#Risk"/>
<owl:disjointWith rdf:resource="#Stakeholder"/>
<owl:disjointWith rdf:resource="#ValueDefinition"/>
<owl:disjointWith rdf:resource="#ThreatAgent"/>
<owl:disjointWith rdf:resource="#Frequency"/>
<owl:disjointWith rdf:resource="#RiskValue"/>
<owl:disjointWith rdf:resource="#Consequence"/>
<owl:disjointWith rdf:resource="#RiskEvaluation"/>
<owl:disjointWith rdf:resource="#AssetValue"/>
<rdfs:subClassOf rdf:resource="#RiskAssessment"/>
<owl:disjointWith rdf:resource="#Authenticity"/>
<owl:disjointWith rdf:resource="#NonRepudiation"/>
<owl:disjointWith rdf:resource="#Impact"/>
<owl:disjointWith
rdf:resource="#RiskEvaluationCriterion"/>
<owl:disjointWith rdf:resource="#Confidentiality"/>
<owl:disjointWith rdf:resource="#UnwantedIncident"/>
<owl:disjointWith rdf:resource="#SensitivityLevel"/>
<owl:disjointWith rdf:resource="#Threat"/>
<owl:disjointWith rdf:resource="#Availability"/>
<owl:disjointWith rdf:resource="#Integrity"/>
<owl:disjointWith rdf:resource="#Compliance"/>
<owl:disjointWith rdf:resource="#Vulnerability"/>
<owl:disjointWith rdf:resource="#Countermeasure"/>
<owl:disjointWith rdf:resource="#Attack"/>
<owl:disjointWith rdf:resource="#SecurityPolicy"/>
</owl:Class>
<owl:Class rdf:about="#SystemSoftware">
  <owl:disjointWith rdf:resource="#ApplicationSoftware"/>
  <rdfs:subClassOf rdf:resource="#Software"/>
  <owl:disjointWith
rdf:resource="#DevelopmentToolsAndUtilities"/>
</owl:Class>
<owl:Class rdf:about="#AnsweringMachines">
  <owl:disjointWith rdf:resource="#PABXs"/>
  <rdfs:subClassOf rdf:resource="#CommunicationsEquipment"/>
  <owl:disjointWith rdf:resource="#FaxMachine"/>
  <owl:disjointWith rdf:resource="#Router"/>
</owl:Class>
<owl:Class rdf:ID="PublicKeyCryptography">
  <rdfs:subClassOf rdf:resource="#Confidentiality"/>
</owl:Class>
<owl:Class rdf:about="#SetupUtilities">
  <rdfs:subClassOf
rdf:resource="#DevelopmentToolsAndUtilities"/>
  <owl:disjointWith rdf:resource="#DatabaseTools"/>
  <owl:disjointWith rdf:resource="#ScriptingTools"/>
  <owl:disjointWith rdf:resource="#HTMLEditor"/>
</owl:Class>
<owl:Class rdf:about="#Remsh">
  <owl:disjointWith rdf:resource="#Interlock"/>
  <owl:disjointWith rdf:resource="#Raptor"/>
  <owl:disjointWith rdf:resource="#Transparent"/>
  <owl:disjointWith rdf:resource="#Interactive"/>
  <rdfs:subClassOf rdf:resource="#Gateway"/>
  <owl:disjointWith rdf:resource="#Proxy"/>

```

```

<owl:disjointWith rdf:resource="#Local"/>
</owl:Class>
<owl:Class rdf:ID="NetworkAdapter">
  <rdfs:subClassOf rdf:resource="#CIMLogicalDevice"/>
</owl:Class>
<owl:ObjectProperty rdf:about="#Causes">
  <rdf:type
rdf:resource="http://www.w3.org/2002/07/owl#TransitiveProperty
"/>
</owl:ObjectProperty>
<owl:ObjectProperty rdf:ID="Encrypt"/>
<owl:ObjectProperty rdf:ID="Decrypt"/>
<owl:DatatypeProperty rdf:about="#HighlyConfidential">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="SecurityControl">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#InstallationCost">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#float"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Opportunity">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#AttackType">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="ReplacementCost">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#float"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="Strength">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#AssetID">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#ImpactID">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Proprietary">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#AttackID">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>

```

```

<owl:DatatypeProperty rdf:about="#AcquisitionCost">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#float"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Vendor">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="AccessControlRight">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#ThreatAgentCategory">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#AssetType">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#LevelOfAssurance">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#LevelOfEffort">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="AccessControlRule">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#UpdateTime">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Effectiveness">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="HasCryptographicKey">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Priority">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Likelihood">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="ControlID">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
```



```

<owl:DatatypeProperty rdf:about="#ThreatID">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#AttackName">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="ExternalRisk">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#boolean"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#UnwantedIncidentCost">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#float"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Motivation">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Possibility">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Constraint">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#ThreatName">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#OperationalCost">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#float"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="BS7799ControlID">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#ThreatAgentName">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="InternalRisk">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#boolean"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Severity">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#CountermeasureType">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>

```



```

<owl:DatatypeProperty rdf:ID="Correctness">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#TopSecret">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Version">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#DeviceID">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Versatility">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Subject">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
    <rdfs:domain rdf:resource="#Asset"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="IntrinsicValue">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#float"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#ThreatType">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#UnwantedIncidentID">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="CompromiseImpact">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#StakeholderID">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:ID="Criticality">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#AssetCostDecrease">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#float"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#IdentifyingNumber">
  <rdfs:range
    rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>

```

```
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#RiskID">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Capability">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#Name">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#CreationClassName">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#CountermeasureID">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#ImportanceLevel">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#string"/>
</owl:DatatypeProperty>
<owl:DatatypeProperty rdf:about="#VulnerabilityID">
  <rdfs:range
rdf:resource="http://www.w3.org/2001/XMLSchema#int"/>
</owl:DatatypeProperty>
</rdf:RDF>

<!-- Created with Protege (with OWL Plugin 2.0 beta, Build
227)  http://protege.stanford.edu -->
```



Δωρεά

