

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

ΟΙΚΟΝΟΜΙΚΟ  
ΠΑΝΕΠΙΣΤΗΜΙΟ  
ΑΘΗΝΩΝ  
ΒΙΒΛΙΟΘΗΚΗ  
ειδ. 53702  
Αρ. 005.8  
ταξ. πολ

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**“Θέματα τυποποίησης και αυτοματοποιημένης διαχείρισης  
Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων”**

Ελένη Πολυδώρου

M3960017

Επιβλέπων Καθηγητής: Δημήτρης Γκρίτζαλης

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ  
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΘΗΝΑ, ΙΑΝΟΥΑΡΙΟΣ 1998



Διευκρινίζεται ότι οι απόψεις που διατυπώνονται στην παρούσα διατριβή ανήκουν στη συγγραφέα και όχι στους συνεισφέροντες κατ' οιονδήποτε τρόπο στη συγγραφή της εργασίας. Οι απόψεις άλλων ερευνητών διευκρινίζονται με την αναφορά της πηγής από την οποία αντλήθηκε το σχετικό πληροφοριακό υλικό.

© Ελένη Πολυδώρου και Οικονομικό Πανεπιστήμιο Αθηνών

---

ΑΘΗΝΑ, ΙΑΝΟΥΑΡΙΟΣ 1998

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ



*Κοιτάζω γύρω μου, κοιτάζω μέσα μου.  
Η αρετή τρελάθηκε, η γεωμετρία τρελάθηκε, η ύλη τρελάθηκε.  
Πρέπει νάρθει πάλι ο νους ο νομοθέτης,  
να βάλει καινούρια τάξη, καινούριους νόμους,  
πιο πλούσια αφμονία  
να γίνει ο κόσμος*

*N.KAZANTZAKIS  
("Αναφορά στον Γκρέκο")*



*Αφιερώνεται  
σε όλους εκείνους  
που υπήρξαν δάσκαλοι για μένα,  
καθοδηγώντας  
τη σκέψη  
και τις πράξεις μου.*



## ΠΕΡΙΛΗΨΗ ΕΡΓΑΣΙΑΣ

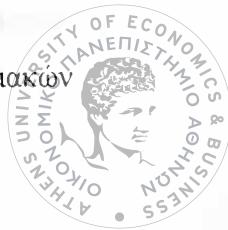
Η διπλωματική αυτή εργασία ανήκει και αναφέρεται σχεδόν στο σύνολό της στο γνωστικό πεδίο της Πληροφορικής. Εξάλλου, αναφορές σε επικουρικά επιστημονικά πεδία γίνονται όταν αυτό θεωρείται απαραίτητο για την πληρέστερη ανάπτυξη και κατανόηση των εννοιών. Η ειδικότερη επιστημονική περιοχή της Πληροφορικής όπου εντάσσεται η εργασία είναι αυτή της Ασφάλειας των Πληροφοριακών Συστημάτων και ειδικά των Πολιτικών Ασφάλειας των Πληροφοριακών Συστημάτων.

Έναυσμα για την παρούσα εργασία αποτέλεσε το ενδιαφέρον θέμα των Μεταπολιτικών Ασφάλειας των Πληροφοριακών Συστημάτων, που καλύπτουν θέματα όπως το είδος της πολιτικής, τα συστατικά της στοιχεία, το πεδίο εμβέλειάς της, τα όργανα που τη διαχειρίζονται, τις ενδεχόμενες σχέσεις μεταξύ των υπο-πολιτικών που τη συνθέτουν, κ.λπ. Μετά από συνοπτική μεν, προσεκτική δε μελέτη της σχετικής επιστημονικής κίνησης στο συγκεκριμένο πεδίο, παρατηρήθηκε ότι υφίσταται ενδιαφέρον για το θέμα της αυτοματοποίησης των Πολιτικών Ασφάλειας. Με τον όρο αυτό, και προσπαθώντας να αποδώσουμε το νόημα και όχι τον ορισμό του όρου, εννοούμε στη γενική περίπτωση τη διαδικασία μέσω της οποίας οι Πολιτικές Ασφάλειας ορίζονται, αναπτύσσονται και διαχειρίζονται με αυτοματοποιημένο ή τουλάχιστον ημιαυτοματοποιημένο τρόπο από Πληροφοριακά Συστήματα κατάλληλα γι' αυτό το σκοπό. Δεδομένης της άποψης αυτής, εκτιμήθηκε ότι το θέμα της τυποποίησης των Πολιτικών Ασφάλειας αποτελεί θεμέλιο λίθο τόσο για τις πολιτικές όσο και για τις Μεταπολιτικές Ασφάλειας. Η τυποποίηση έχει στην εργασία αυτή την έννοια της καθ' οιονδήποτε τρόπο, δηλαδή με χρήση ποικιλών μεθόδων, τυπικής απεικόνισης εννοιών της πραγματικότητας, τέτοιας ώστε το παραγόμενο αποτέλεσμα να έχει τα χαρακτηριστικά εκείνα που θα το θέτουν α) ελέγχιμο της συνέπειάς του με τις έννοιες που τυποποιεί και β) κατάλληλο και εύχρηστο για σχετικά άμεση χρήση σε σκοπούς αυτοματοποίησης διαστάσεων του χώρου προβληματισμού στον οποίο ανήκει.

Τα αρχικά αυτά συμπεράσματα σταδιακά οδήγησαν και σταθερά διαμόρφωσαν το θέμα αυτής της εργασίας. Το θέμα, και συνεπώς το κύριο συγγραφικό μέρος, περιστράφηκε γύρω από την τυποποίηση και αυτοματοποιημένη διαχείριση Πολιτικών Ασφάλειας. Σημαντικό μέρος της προσπάθειας κατά την προετοιμασία αποτέλεσε η αναζήτηση για τον εντοπισμό του αντίστοιχου, αν υπήρχε, επιστημονικού πεδίου. Προσπαθήσαμε δηλαδή να εντοπίσουμε στην επιστημονική δραστηριότητα που υπάρχει στο χώρο αν υφίσταται αντίστοιχο πεδίο ενδιαφέροντος και υπό ποιο τίτλο προσδιορίζεται. Εντοπίσαμε λοιπόν πολλές προσπάθειες που περιστρέφονταν θεματολογικά γύρω από το θέμα μας. πολλές από τις οποίες χρησιμοποιούν τον αγγλικό όρο "Information Systems Security Policy Engineering", ή συναφείς όρους, τον οποίο επιλέξαμε να μεταφράσουμε ως "Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων".

Επιπλέον, σημαντικά κρίνονται και μελετήθηκαν σε ανάλογο βαθμό τα ακόλουθα θέματα:

- Η ίδια η έννοια της Πολιτικής Ασφάλειας Πληροφοριακού Συστήματος.
  - Ο ρόλος και η σημασία της έννοιας αυτής για το χώρο των Πληροφοριακών Συστημάτων.



- Η σχέση των Πολιτικών Ασφάλειας και του οργανισμού.
  - Η έννοια της Μεταπολιτικής Ασφάλειας υπό το πρίσμα που διαμορφώνεται προηγούμενων των θεμάτων τυποποίησης και αυτοματοποίησης των Πολιτικών Ασφάλειας.
  - Θεωρητικά θέματα που θέτει η μελέτη των βασικών θεμάτων και ειδικότερα θέματα τυπικών μοντέλων, τυπικών περιγραφικών μεθόδων, ανάλυσης συστημάτων, δόμησης συστημάτων, κ.λ.π.

Το πρώτο κεφάλαιο της εργασίας συνοψίζει θέματα αντικειμένου, σκοπού και μεθοδολογίας της εργασίας. Επίσης διευκρινίζονται βασικά θέματα που πρέπει εξαρχής να έχει υπόψη του ο αναγνώστης, καθώς και σημεία που θα τον βοηθήσουν στην ευκολότερη και αρτιότερη ανάγνωση και κατανόηση του κειμένου. Συνεπώς, το κεφάλαιο αυτό είναι ιδιαίτερα σημαντικό και προαπαιτούμενο της ανάγνωσης του υπόλοιπου κειμένου.

Αναλυτικότερα επί του κυρίως μέρους της εργασίας, σε αρχική φάση ο αναγνώστης εισάγεται στην έννοια της Πολιτικής γενικώς. Ακολούθως, μελετάται διεξοδικά η έννοια της Πολιτικής Ασφάλειας Πληροφοριακού Συστήματος. Αναγνωρίζεται η ποικιλομορφία των απόψεων που υιοθετούνται περί του περιεχομένου του όρου. Η ποικιλομορφία αυτή είναι για εμάς αξιωματικά αποδεκτή, διότι αποτελεί πεποίθησή μας η άποψη ότι μία νέα σε ηλικία επιστημονική περιοχή συνιστά μία κατεξοχήν ερευνητική περιοχή και συνεπώς η μελέτη κάθε δυνατής, θεωρητικά ή εφαρμοσμένα εκφρασμένης, άποψης περί αυτής επιβάλλεται. Εντούτοις απαιτείται για μεθοδολογικούς λόγους να οριοθετήσουμε σχετικά την έννοια για τους σκοπούς αυτής της μελέτης. Τα σημεία αυτά μελετώνται στο δεύτερο κεφάλαιο. Στο κεφάλαιο αυτό τονίζεται η σημασία της Πολιτικής Ασφάλειας για τα σύγχρονα Πληροφοριακά Συστήματα. Στο πλαίσιο των αναγκών που οι σύγχρονες εξελίξεις θέτουν, πραγματοποιείται η εισαγωγή στην έννοια και στη σημασία της αυτοματοποίησης και τυποποίησης των πολιτικών ασφάλειας.

Το επόμενο κεφάλαιο εξετάζει σε αναλυτικό επίπεδο τις υπάρχουσες προσεγγίσεις προς την κατεύθυνση της τυποποίησης και αυτοματοποιημένης διαχείρισης Πολιτικών Ασφάλειας. Οι εξεταζόμενες προσεγγίσεις χρησιμοποιούν τις ακόλουθες μεθόδους προκειμένου να τυποποιήσουν-αυτοματοποιήσουν τις Πολιτικές Ασφάλειας:

- Βάσεις Κανόνων.
  - Χρήση της έννοιας των Λειτουργικών Απαιτήσεων των χρηστών σε συνδυασμό με Τυπικές Περιγραφικές Μεθόδους.
  - Μεθόδους που διέπονται από αρχές της Τεχνολογίας Λογισμικού.
  - Μελέτη χρήσιμων στοιχείων που προκύπτουν από την ανάλυση του Οργανισμού ως προς την Πολιτική Ασφάλειας.
  - Γλώσσες Αναπαράστασης Γνώσης.
  - Αρχές της Ανάλυσης Επικινδυνότητας και Πρότυπα Ασφάλειας Πληροφοριακών Συστημάτων.

Κάθε προσέγγιση μελετάται διεξοδικά από την άποψη της μεθοδολογίας που υιοθετεί. Η μεθοδολογία καλύπτει ένα ευρύ φάσμα θεμάτων και ανάλογα πλούσιο πληροφοριακό υλικό. Για κάθε πλαίσιο που εξετάζουμε καλύπτουμε τουλάχιστον, και ανάλογα με τα στοιχεία που συλλέξαμε, τα ακόλουθα θέματα:

- Αν και ποιά έννοια αποδίδει στην Πολιτική Ασφάλειας.

- Αν και ποιά έννοια αποδίδει στο Πληροφοριακό Σύστημα.
- Αν και πώς ορίζει το χώρο εφαρμογής της άποψης και λύσης την οποία παρουσιάζει.
- Ποιά εργαλεία και ποιές πρακτικές χρησιμοποιεί και με ποιό τρόπο προκειμένου να επιτύχει τους σκοπούς για τους οποίους αναλαμβάνει τη χρήση τους.

Το τέταρτο κεφάλαιο μελετά την έννοια της διαχείρισης περισσότερων Πολιτικών Ασφάλειας. Αυτή, άλλωστε, αποτελεί την εφαρμογή της έννοιας της Μεταπολιτικής και μία από τις σημαντικότερες, ίσως την πιο σημαντική, εφαρμογές της αυτοματοποιημένης διαχείρισης Πολιτικών Ασφάλειας. Οι προσεγγίσεις που αναλύουμε στο κεφάλαιο αυτό ολοκληρώνουν τις αντίστοιχες του προηγούμενου κεφαλαίου σχεδόν στο σύνολό τους, ενώ οι υπόλοιπες εισάγουν νέες απόψεις στη αυτοματοποιημένη διαχείριση πολιτικών ασφάλειας.

Σε πρώτη φάση, η δομημένη προσέγγιση με την οποία μελετήσαμε τα θέματα των δύο προηγούμενων κεφαλαίων δεν μας ήταν έκδηλη, πολύ δε περισσότερο τα δομικά της στοιχεία δεν γίνεται άμεσα προφανή στον αναγνώστη. Εντούτοις, το πληροφοριακό υλικό που τα κεφάλαια αυτά σύλλεξαν και οργάνωσαν, μας επέτρεψε ακολουθώντας τα τρία βήματα που περιγράφουμε να εστιάσουμε περαιτέρω τις μελέτες μας στα επόμενα σημεία:

### •BHMA ①: Χρήση εμπειρικών μεθόδων και προϋπάρχουσας γνώσης.

- 1.1: Χρησιμοποιώντας τις γνώσεις μας να διαχωρίσουμε σημεία ειδικού επιστημονικού ενδιαφέροντος και προβληματισμού στα θέματα που μελετήσαμε.

### •BHMA ②: Μελέτη θεωρητικών βάσεων.

- 2.1: Να μελετήσουμε τον τρόπο εφαρμογής γενικά αποδεκτών επιστημονικών τεχνικών μελέτης αδόμητων ή ημιδομημένων συστημάτων.
- 2.2: Να μελετήσουμε τις αρχές που διέπουν τα συστήματα αυτά.
- 2.3: Να μελετήσουμε τη χρησιμότητα και τον τρόπο με τον οποίο αναπτύσσονται ορισμένες τεχνικές και εργαλεία μελέτης των θεμάτων που μας απασχόλησαν.

### •BHMA ③: Δημιουργία ενός πλαισίου αναφοράς για μεθοδολογίες αυτοματοποιημένης διαχείρισης Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων.

- 3.1: Να εντοπίσουμε βασικά δομικά στοιχεία -κοινά σε όλες τις προσεγγίσεις- στη διαδικασία ανάπτυξης μεθοδολογιών διαχείρισης Πολιτικών Ασφάλειας για Πληροφοριακά Συστήματα, μέσα από τα στοιχεία που σύλλεξαμε.
- 3.2: Να οργανώσουμε τα δομικά αυτά στοιχεία σε ένα πλαίσιο που θα αντιπροσωπεύει τις προσεγγίσεις διαχείρισης Πολιτικών Ασφάλειας.
- 3.3: Να μελετήσουμε ενδεικτικούς τρόπους και τεχνικές αντιμετώπισης των σχετικών προβλημάτων, καταλήγοντας με τον τρόπο αυτό σε διατύπωση απαιτήσεων για σημαντικές διαστάσεις των σχετικών προσεγγίσεων.

Η ενασχόληση με τα σχετικά θέματα οδήγησαν στον καθορισμό ενός θέματος που παρουσίασε σοβαρό ενδιαφέρον. Η συγγραφή λοιπόν του πέμπτου κεφαλαίου υπήρξε αποτέλεσμα της μελέτης του θέματος της προσέγγισης των απαιτήσεων μίας μεθοδολογίας για *Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων*.

Καταλήγοντας, θα λέγαμε ότι παρόλο που η εργασία αυτή δεν ισχυρίζεται ότι εισάγει νέες διαστάσεις στον αντίστοιχο επιστημονικό χώρο, εντούτοις καλύπτει με συνέπεια και συστηματικότητα ένα ευρύ πεδίο σημαντικών θεμάτων, οργανώνοντας τα σημεία ενδιαφέροντος και παρέχοντας τελικά έναν τρόπο μεθοδολογικής μελέτης και ανάλυσης των υπαρχουσών προσεγγίσεων, ακριβώς όπως οριοθετείται από τους σκοπούς, το χαρακτήρα και το ύφος της.

## EXECUTIVE SUMMARY

# "INFORMATION SYSTEMS SECURITY POLICIES FORMALIZATION & AUTOMATED MANAGEMENT"

This MSc thesis belongs and refers, almost totally, to the scientific field of Informatics. Besides, references to other scientific fields are made when this is substantial for the sound description and comprehension of several concepts. The dissertation particularly belongs to the scientific field of Information Systems Security and especially to that of Information Systems Security Policies.

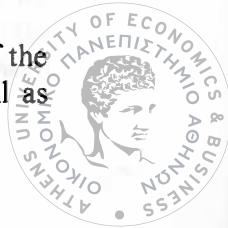
The ignition for the writing of this thesis was the scientifically interesting issue of *Information Systems Security Metapolicies*. After concise and careful study of the scientific activity at this specific field, we observed that there is interest for the issue of Information System Automated Management. With this term, and in an attempt to ascribe the meaning and not the definition of the term, we generally mean the procedure with which Security Policies are being defined, developed and managed automatically or at least semi-automatically by Information Systems adequate for that purpose. In light of this aspect we judged that the issue of *Information Systems Security Policies formalization* constitutes the cornerstone for both Security Policies and Security Metapolicies. The term formalization means for this dissertation the by all means -that is with the employment of several methods- formal description of concepts of the real world, so that the produced result has those characteristics that set it a) testable with reference to its consistency with the concepts it describes and b) appropriate and usable for relatively direct use in automation procedures.

Those initial conclusions gradually led to and steadily shaped the main subject of this thesis. The subject, and consequently the main part, revolves around the formalization and automated management of Security Policies. A major part of the author's effort during the preparation period was spent on the quest for the discovery of the respective scientific area in the field of Information Systems Security. Several scientific efforts and research were traced that related closely to our main point. Most of them use the term "Information Systems Security Policy Engineering", or contextual terms, to refer to it and this is the term we use as well.

Moreover, we apprise as important and, proportionally to this estimation, examine the following issues:

- The concept of Information Systems Security Policy itself.
- The role and importance of this concept for the Information Systems community.
- The relation between Security Policies and the Organization.
- The concept of Security Metapolicy in light of the issues of formalization and automated management of Security Policies.
- Theoretical issues set for discussion and especially issues covering formal models, formal specification techniques, systems analysis, systems structure, etc.

In the first chapter we summarize the subject, purpose and methodology of the dissertation. We also elucidate basic points the reader must bear in mind, as well as



points that will help him/her towards the easier and complete understanding of the text.

As far as the main part is concerned, the reader is initially introduced to the concept of Policy in general. Next to that, we in detail study the concept of Information System Security Policy. We discover and highlight the variety and diversity of the aspects Security Policies are studied under. This variety is respectable to us, as we believe that we have to evaluate every current view about Security Policies, before we stabilize any further opinion. For methodological reasons, of course, we have to determine some boundaries to the magnitude of current prospect on Security Policies. We consider these issues at the second chapter. In this chapter we underline the importance of Security Policies for the modern Information Systems. The introduction to the concepts of formalization and automated management of Security Policies is realized in the framework the development in Informatics sets.

The next chapter looks through the existent approaches to the direction of formalization and automated management of Security Policies. The approaches studied use the following methods in order to formalize-automate Security Policies:

- Rule Bases
- The concept of operational user requirements, combined with formal specification techniques.
- Methods influenced by Software Engineering concepts.
- Security study of the organizational environment of Security Policies.
- Knowledge representation languages.
- Concepts borrowed from Risk Analysis and Information Systems Security Standards.

Every approach is thoroughly studied from its *methodology* point of view. The methodology covers a wide spectrum of issues. For each approach we examine, or at least cover, the following issues:

- ☒ If and which meaning it attaches to the term Security Policy.
- ☒ If and which meaning it attaches to the term Information System.
- ☒ If and how it defines the application area of the proposed way of thinking about and of solving the related problems.
- ☒ Which tools and practices it uses and in which way, in order to achieve the purposes it employs them for.

The fourth chapter studies the concept of *Multiple Security Policies Management*. Besides, this concept represents the most apparent application of the term of Metapolicy and the most useful application of the automated Information Systems Security Policies management. Most of the approaches we present at this chapter integrate the ones of the previous chapter, while the rest introduce new aspects in automated Information Systems Security Policies management.

At first, the structured way we studied these issues was not apparent to us. Moreover, the respective structural elements are not being made apparent to the reader. In spite of that, the information those chapters collected and organized allowed us to focus on the following issues:



⌚ STEP ①: Use of empirical methods and existent knowledge.

- 1.1: By using our knowledge we were able to identify issues of special scientific interest and questioning.

⌚ STEP ②: Study of theoretical background.

- 2.1: Exploration of the application of widely acceptable scientific techniques at the study of unstructured or semi-structured problematic situations.
- 2.2: Study of the principles that rule these situations.
- 2.3: Study of the usefulness and the way certain techniques and tools, concerning the issues we are interested in, are developed by.

⌚ STEP ③: Development of a framework of reference for Information systems Security Policies Engineering.

- 3.1: Locationing of basic structuring elements -common to every approach- in the Information Systems Security Policies development procedures.
- 3.2: Organization of these elements in a framework which is capable of representing Security Policies management approaches.
- 3.3: Study of typical, as well as proper, ways and techniques for dealing with relevant problems, which led us to the formulation of requirements concerning important aspects of the approaches.

This way we concluded to a scientifically interesting issue. The fifth chapter resulted from the study of the *approachment of the requirements for an Information Systems Security Engineering Methodology*.

In conclusion, we could say that despite the fact that this dissertation does not allege to introduce new dimensions to the scientific area it belongs to, it accomplishes to cover consistently and systematically a wide spectrum of important issues, by organizing the points of interest and by proposing a way of methodological study and analysis of existing approaches, precisely the way dictated by its purpose, character and style.

## ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

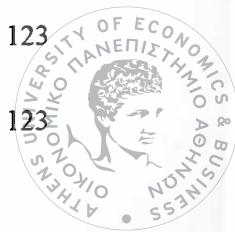
ΠΕΡΙΛΗΨΗ ΕΡΓΑΣΙΑΣ .....	i
EXECUTIVE SUMMARY .....	v
ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ .....	1
ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ .....	4
ΑΝΤΙ ΠΡΟΛΟΓΟΥ .....	6
<b>ΚΕΦΑΛΑΙΟ Ι: ΕΙΣΑΓΩΓΗ.....</b>	<b>7</b>
1.1 Εισαγωγικοί προβληματισμοί.....	8
1.2 Αντικείμενο, σκοπός και μεθοδολογία της εργασίας.....	9
1.3 Χρήσιμες παρατηρήσεις για τον αναγνώστη.....	11
1.4 Δομή της εργασίας .....	12
<b>ΚΕΦΑΛΑΙΟ ΙΙ: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΤΥΠΟΠΟΙΗΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ</b>	
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ .....	14
2.1 Περί "Πολιτικής" γενικότερα .....	15
2.2 Πολιτική Ασφάλειας Πληροφοριακού Συστήματος.....	16
2.3 Παραδειγματισμοί ανάπτυξης πολιτικών και τυποποίηση πολιτικών .....	18
2.4 Αυτοματοποιημένη διαχείριση των πολιτικών ασφάλειας Πληροφοριακών Συστημάτων.....	19
2.5 Χρησιμότητα της αυτοματοποιημένης διαχείρισης των πολιτικών ασφάλειας Πληροφοριακών Συστημάτων.....	21
<b>ΚΕΦΑΛΑΙΟ ΙΙΙ: ΤΥΠΟΠΟΙΗΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ .....</b>	<b>25</b>
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ .....	25
3.1 Εισαγωγή .....	26
3.2 Τυποποίηση πολιτικών ασφάλειας με χρήση Βάσεων Κανόνων.....	27
3.2.1 Εισαγωγή .....	27
3.2.2 Ένα πλαίσιο για τυποποίηση ασφαλούς συστήματος με χρήση κανόνων.....	28
3.2.2.1 Δομικά στοιχεία του πλαισίου .....	28
3.2.2.2 Συντακτικοί συμβολισμοί και σημασιολογία .....	29
3.2.2.3 Περιγραφή της διεπαφής .....	30
3.2.2.4 Κανόνες λειτουργίας της αφηρημένης μηχανής μετάθεσης καταστάσεων .....	31
3.2.2.5 Κανόνες προσπέλασης της βάσης κανόνων .....	31
3.2.3 Μία αυτοματοποιημένη μέθοδος παραγωγής βάσεων κανόνων για πολιτικές ασφάλειας .....	39
3.3 Τυποποίηση πολιτικών ασφάλειας με έμφαση στις λειτουργικές απαιτήσεις των χρηστών ..	41
3.3.1 Εισαγωγή .....	41
3.3.2 Παρουσίαση της προσέγγισης .....	42
3.3.2.1 Το Μοντέλο Δράσης .....	42
3.3.2.2 Ιδιότητες Ασφάλειας .....	44
3.3.2.3 Αντικειμενοστραφές μοντέλο ασφάλειας .....	44
3.3.2.4 Επηρεασμός και Παρατήρηση στο Αντικειμενοστραφές Μοντέλο .....	46
3.3.2.5 Απαιτήσεις ασφάλειας .....	46

3.3.2.6 Πολιτικές ασφάλειας.....	47
<b>3.4 Αυτοματοποιημένη διαχείριση πολιτικών ασφάλειας βασισμένη στις αρχές της Τεχνολογίας Λογισμικού.....</b>	<b>48</b>
3.4.1 Εισαγωγή .....	48
3.4.2 Συνθετικά στοιχεία του περιβάλλοντος αναφοράς .....	49
3.4.3 Συνθετικά στοιχεία της προσέγγισης.....	50
3.4.3.1 Βασικές αρχές .....	50
3.4.3.2 Σχεδιασμός πολιτικών ασφάλειας .....	51
3.4.3.3 Επικύρωση πολιτικών ασφάλειας .....	52
3.4.3.4 Υλοποίηση πολιτικών ασφάλειας .....	52
3.4.4 Παρουσίαση μίας ενδεικτικής εφαρμογής .....	53
3.4.4.1 Εισαγωγή .....	53
3.4.4.2 Η αρχιτεκτονική ασφάλειας BirliX .....	54
3.4.4.3 Το περιβάλλον διαχείρισης πολιτικών ασφάλειας SKIPPY .....	55
3.4.4.4 Η προσέγγιση της εφαρμογής ηλεκτρονικού εμπορίου CWASAR ως προς την ασφάλεια .....	60
<b>3.5 Τυποποίηση πολιτικών ασφάλειας βασισμένη σε γλώσσες αναπαράστασης γνώσης .....</b>	<b>63</b>
3.5.1 Το περιεχόμενο της έννοιας "πολιτική ασφάλειας" Πληροφοριακού Συστήματος... ..	63
3.5.2 Αναπαράσταση πολιτικών ασφάλειας μέσω της γλώσσας αναπαράστασης γνώσης "TELOS" .....	64
<b>3.6 Τυποποίηση των πολιτικών ασφάλειας για το πληροφοριακό σύστημα με έμφαση στην έννοια του οργανισμού .....</b>	<b>67</b>
3.6.1 Εισαγωγή .....	67
3.6.2 Βασικές αρχές της προσέγγισης .....	68
3.6.3 Παρουσίαση της προσέγγισης .....	68
<b>3.7 Μερικώς αυτοματοποιημένη ανάπτυξη πολιτικών ασφάλειας βασισμένη στο πλαίσιο IBAG και σε έννοιες της Ανάλυσης Επικινδυνότητας.....</b>	<b>72</b>
3.7.1 Εισαγωγή .....	72
3.7.2 Παρουσίαση της προσέγγισης .....	73
<b>ΚΕΦΑΛΑΙΟ IV: ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΣΟΤΕΡΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ .....</b>	<b>76</b>
4.1 Οι εξελίξεις που συνθέτουν το περιβάλλον της ασφαλούς επικοινωνίας και διαλειτουργικότητας Πληροφοριακών Συστημάτων .....	77
4.2 Ασφαλής διαλειτουργικότητα, σύνθεση και συμβατότητα πολιτικών ασφάλειας Πληροφοριακών Συστημάτων.....	78
4.3 Έννοια της "μεταπολιτικής" ασφάλειας σε Πληροφοριακά Συστήματα.....	82
4.4 Μέθοδοι διαχείρισης πολλαπλών πολιτικών ασφάλειας .....	85
4.4.1 Η μηχανή πολλαπλών πολιτικών ασφάλειας .....	85
4.4.2 Εφαρμογή της Θεωρίας Ασαφών Συνόλων στη διαχείριση πολλαπλών πολιτικών ασφάλειας .....	87
4.4.3 Υποστήριξη πολλαπλών πολιτικών ασφάλειας βασισμένη σε κονσταδούς.....	89
4.4.4 Υποστήριξη πολλαπλών πολιτικών ασφάλειας βασισμένη σε αναπαράσταση με γλώσσες γνώσης .....	93
<b>ΚΕΦΑΛΑΙΟ V: ΣΥΝΘΕΤΙΚΕΣ ΕΝΝΟΙΟΛΟΓΙΚΕΣ ΔΙΑΣΤΑΣΕΙΣ ΤΗΣ ΤΥΠΟΠΟΙΗΣΗΣ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ:.....</b>	<b>96</b>
<b>ΣΥΣΧΕΤΙΣΕΙΣ ΠΡΟΕΚΤΑΣΕΙΣ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ .....</b>	<b>96</b>
5.1 Εισαγωγή .....	97
5.2 Μοντέλα ασφάλειας Πληροφοριακών Συστημάτων .....	97
5.3 Η πολιτική ασφάλειας εντός του περιβάλλοντός της: Μοντελοποίηση του οργανισμού ως	

προς την πολιτική ασφάλειας.....	99
<b>5.4 Οι αντικειμενικές εκφραστικές δυνατότητες των τυπικών περιγραφικών μεθόδων.....</b>	<b>101</b>
5.4.1 Εισαγωγή .....	101
5.4.2 Είδη Τυπικών Περιγραφικών Μεθόδων .....	102
5.5.2.1 Μοντέλα Δεδομένων.....	102
5.4.2.2 Μοντέλα Διεπαφών.....	103
5.4.2.3 Μοντέλα Κατανεμημένων Συστημάτων.....	103
5.4.2.4 Μοντέλα Διαδικασιών.....	104
5.4.2.5 Μοντέλα Μετάθεσης Καταστάσεων.....	104
5.4.3 Απαιτήσεις για τις Τυπικές Περιγραφικές Μεθόδους .....	104
<b>5.5 Επίπεδα αφαίρεσης, αναταράστασης και δόμησης σε θέματα ανάλυσης συστημάτων.....</b>	<b>106</b>
5.5.1 Σχετικά με τη δόμηση συστημάτων προβλήματα.....	106
5.5.2 Ανάλυση των νοητικών διαδικασιών που μετέχουν στη διαδικασία δόμησης και τυποποίησης προβλημάτων που επιδέχονται αυτοματοποίηση .....	108
5.5.3 Ένα ενδεικτικό παράδειγμα.....	111
<b>5.6 Μία αφαιρετική προσέγγιση υψηλού επιπέδου για την ανάπτυξη ασφαλών Πληροφοριακών Συστημάτων.....</b>	<b>113</b>
5.6.1 Εννοιολογικά στοιχεία της προσέγγισης .....	113
5.6.2 Το τυπικό μοντέλο ανάπτυξης ασφαλών Πληροφοριακών Συστημάτων.....	114
<b>5.7 Προς την κατεύθυνση της διαμόρφωσης μιας μεθοδολογίας για Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων .....</b>	<b>116</b>
5.7.1 Εισαγωγή .....	116
5.7.2 Δομικά στοιχεία του πλαισίου αναφοράς .....	117
5.7.2.1 Συνοπτική περιγραφή της προσέγγισης .....	117
5.7.2.2 Ορισμός του αντικειμένου του προβληματισμού - Διαμόρφωση υποθέσεων .....	117
5.7.2.3 Προσδιορισμός δομικών στοιχείων του πλαισίου .....	119
5.7.2.4 Διαμόρφωση απαιτήσεων για τα δομικά στοιχεία .....	122
<b>ΣΥΜΠΕΡΑΣΜΑΤΑ .....</b>	<b>128</b>
<b>ΜΕΤΑΦΡΑΣΕΙΣ ΟΡΩΝ .....</b>	<b>136</b>
<b>ΕΥΡΕΤΗΡΙΟ ΟΡΩΝ .....</b>	<b>138</b>
<b>ΒΙΒΛΙΟΓΡΑΦΙΑ .....</b>	<b>141</b>

## ΠΙΝΑΚΑΣ ΣΧΗΜΑΤΩΝ

<b>ΣΧΗΜΑ 2.1.</b> Η διαδικασία αυτοματοποίησης της διαχείρισης των πολιτικών ασφάλειας ...	21
<b>ΣΧΗΜΑ 2.2.</b> Συσχέτιση των διαδικασιών τυποποίησης του συστήματος και της πολιτικής ...	22
<b>ΣΧΗΜΑ 3.1.</b> Το γενικευμένο Πλαίσιο για Έλεγχο Προσπέλασης.....	29
<b>ΣΧΗΜΑ 3.2.</b> Η διαδικασία παραγωγής των κανόνων.....	40
<b>ΣΧΗΜΑ 3.3.</b> Το περιβάλλον διαχείρισης πολιτικών ασφάλειας SKIPPY .....	56
<b>ΣΧΗΜΑ 3.4.</b> Το Δικτύωμα για τον έλεγχο προσπέλασης .....	58
<b>ΣΧΗΜΑ 3.5.</b> Η δομή ενός ορισμού στη γλώσσα περιγραφής απαιτήσεων.....	59
<b>ΣΧΗΜΑ 3.6.</b> Η αρχιτεκτονική του συστήματος CWASAR .....	63
<b>ΣΧΗΜΑ 3.7.</b> Τα συστατικά στοιχεία της πολιτικής ασφάλειας.....	65
<b>ΣΧΗΜΑ 3.8.</b> Το πλαίσιο IBAG σε αντιστοιχία με τα επίτεδα ανάπτυξης ασφαλούς πληροφοριακού συστήματος .....	75
<b>ΣΧΗΜΑ 3.9.</b> Το μοντέλο οντοτήτων-συσχετίσεων του εργαλείου SIDERO .....	76
<b>ΣΧΗΜΑ 4.1.</b> Προβλήματα ασφαλούς διαλειτουργικότητας.....	80
<b>ΣΧΗΜΑ 4.2.</b> Δομημένη περιγραφή μίας Πολιτικής Ασφάλειας .....	84
<b>ΣΧΗΜΑ 4.3.</b> Μεταπολιτική Οργάνωσης και Ελέγχου Πολιτικών Ασφάλειας .....	86
<b>ΣΧΗΜΑ 4.4.</b> Ορισμός του Επιπέδου Πολιτικής .....	92
<b>ΣΧΗΜΑ 4.5.</b> Ορισμός του επιπέδου Μοντέλων .....	92
<b>ΣΧΗΜΑ 4.6.</b> Ορισμός του επιπέδου Στιγμιοτύπων Πολιτικών Ασφάλειας .....	93
<b>ΣΧΗΜΑ 4.7.</b> Φάσεις της μεθοδολογίας ανάπτυξης μεταπολιτικών ασφάλειας.....	96
<b>ΣΧΗΜΑ 5.1.</b> Συνθετικές διαστάσεις της αντιμετώπισης του συστήματος αναφοράς.....	102
<b>ΣΧΗΜΑ 5.2.</b> Μοντέλο Διεπαφών .....	104
<b>ΣΧΗΜΑ 5.3.</b> Η διαδικασία αποσύνθεσης για τη μελέτη συστημάτων. ....	108
<b>ΣΧΗΜΑ 5.4.</b> Ένα μοντέλο σύνθεσης ενός πληροφοριακού συστήματος έτσι όπως το αντιλαμβάνεται στο εννοιολογικό επίπεδο για τις ανάγκες της ανάλυσης ο αναλυτής.....	113
<b>ΣΧΗΜΑ 5.5.</b> Οριζόντια και κάθετη ολοκλήρωση απαιτήσεων ασφάλειας .....	116
<b>ΣΧΗΜΑ 5.6.</b> Τα δομικά μέρη της προσέγγισης για τον προσδιορισμό των απαιτήσεων για τη μεθοδολογία Τεχνολογίας Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων.....	118
<b>ΣΧΗΜΑ 5.7.</b> Το πρώτο δομικό επίπεδο του πλαισίου αναφοράς .....	120
<b>ΣΧΗΜΑ 5.8.</b> Ανάλυση δομικού στοιχείου "ΟΡΙΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΜΕΛΕΤΗΣ" της μεθοδολογίας .....	122
<b>ΣΧΗΜΑ 5.9.</b> Ανάλυση δομικού στοιχείου "ΕΡΓΑΛΕΙΑ" της μεθοδολογίας .....	122
<b>ΣΧΗΜΑ 5.10.</b> Ανάλυση δομικού στοιχείου " ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ " της μεθοδολογίας .....	123
<b>ΣΧΗΜΑ 5.11.</b> Ανάλυση δομικού στοιχείου "ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ " της μεθοδολογίας .....	123



ΣΧΗΜΑ 5.12. Διαχωρισμός Αξιωματικών Υποθέσεων της προσέγγισης.....	124
ΣΧΗΜΑ 5.13. Απαιτήσεις του δομικού στοιχείου "ΕΡΓΑΛΕΙΑ".....	127

## ΑΝΤΙ ΠΡΟΛΟΓΟΥ

Η εργασία αυτή πραγματοποιήθηκε από τη φοιτήτρια του Μεταπτυχιακού Προγράμματος Εξειδίκευσης στα Πληροφοριακά Συστήματα του Οικονομικού Πανεπιστημίου Αθηνών Ελένη Πολυδώρου. Η εργασία συμπληρώνει τις απαιτήσεις ολοκλήρωσης σπουδών και εκπονήθηκε στα πλαίσια της Εκπόνησης Μεταπτυχιακής Διατριβής κατά τους μήνες Ιούλιο έως Δεκέμβριο του 1997. Επιβλέπων την εργασία ήταν ο κ. Δημήτρης Γκρίζαλης, Λέκτορας του Οικονομικού Πανεπιστημίου Αθηνών.

Από το σημείο αυτό θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή και δάσκαλό μου κ. Δημήτρη Γκρίζαλη, επιβλέποντα την εργασία μου, για την καθοδήγηση που μου προσέφερε κατά την εκπόνηση της εργασίας αυτής, αλλά και για όλες τις πολύτιμες συμβουλές και κρίσεις του.

Επίσης θα ήθελα να ευχαριστήσω το συμφοιτητή μου Κώστα Μουλίνο για τις επικοδομητικές μας συζητήσεις επί του αντικειμένου και τη γενικότερη συνεργασία μας.

Ευχαριστώ για τη βοήθειά του τον υποψήφιο διδάκτορα του Οικονομικού Πανεπιστημίου Αθηνών Σπύρο Κοκολάκη.

Ευχαριστίες οφείλονται επίσης στους φίλους από το London School of Economics and Political Science και από το University of Manchester για τη βοήθειά τους στη συγκέντρωση του αρθρογραφικού υλικού που δεν ήταν δυνατό να εντοπίσω στην Ελλάδα.

Τέλος, ευχαριστίες για την ηθική και πρακτική τους συμπαράσταση οφείλονται στην οικογένειά μου και ειδικά σε εσάς Βάσω, Γεωργία και Γιώργο για περισσότερα από όσα μπορούν να εκφραστούν.

*Ελένη Πολυδώρου*

ΑΘΗΝΑ, Δεκέμβρης 1997



## 3. Κανονικός προβλεπόμενος:

Το διπλωματικό με αποτέλεσμα την Επίπροσθετή Επενδυτική σύμβαση με την πολιτική ασφάλειας αλλάζει την Εθνική Αρχή. Η νέα Αρχή με την ονομασία Εθνική Ασφάλειας θα επενδύει στην Επενδυτική Εποπτεία, δεδουλεύει σε πολιτική ασφάλειας, και είναι μεταπολεμική.

Η νέα Αρχή θα αποτελεί έναντι της κοινωνίας, μεταξύ της και της πολιτικής ασφάλειας, μεταξύ της και της πολιτικής δημόσιας υγείας, μεταξύ της και της πολιτικής δημόσιας ασφαλείας, μεταξύ της και της πολιτικής δημόσιας δικαιοσύνης, και μεταξύ της και της πολιτικής δημόσιας ασφαλείας.

Το διπλωματικό με αποτέλεσμα την Επίπροσθετή Επενδυτική σύμβαση με την πολιτική ασφάλειας αλλάζει την Εθνική Αρχή. Η νέα Αρχή με την ονομασία Εθνική Ασφάλειας θα επενδύει στην Επενδυτική Εποπτεία, δεδουλεύει σε πολιτική ασφάλειας, και είναι μεταπολεμική.

# ΚΕΦΑΛΑΙΟ Ι

## ΕΙΣΑΓΩΓΗ



## 1.1 Εισαγωγικοί προβληματισμοί

Το θέμα της προστασίας και ασφάλειας των Πληροφοριακών Συστημάτων αποτελεί πλέον ένα ενεργό επιστημονικό πεδίο της Πληροφορικής. Παράλληλα με τη διαδικασία πλήρους αποδοχής των Πληροφοριακών Συστημάτων βαδίζει η αναγνώριση της σημασίας ανάπτυξης ασφαλών συστημάτων.

Η παροχή ασφάλειας θεωρείται και είναι ζωτικής σημασίας αγαθό για τους σύγχρονους οργανισμούς, οι οποίοι τείνουν να αυξάνουν την εξάρτησή τους από τα Πληροφοριακά τους Συστήματα. Όπως διαπιστώθηκε από σχετικές έρευνες ([WAR-1995]), η αντίληψη που υπάρχει σε οργανισμούς που χρησιμοποιούν την Πληροφορική αναφορικά με την ασφάλεια, υφίσταται σε όρους **ζήτησης ή απαίτησης** (demand) χρόνου, χρημάτων και άλλων επιχειρηματικών πόρων.

Εντούτοις, οι σύγχρονοι οργανισμοί δεν καλύπτουν στο βαθμό που πρέπει - και κυρίως με τον ενδεδειγμένο τρόπο- τις απαιτήσεις ασφάλειας των συστημάτων τους. Η πλημμελής αυτή αντιμετώπιση ανάγει τις ρίζες της σε λανθασμένες αντιλήψεις σχετικά με το ρόλο και τη χρήση των Πληροφοριακών Συστημάτων και της ίδιας της ασφάλειας ως υπηρεσίας. Μπορούμε να παραθέσουμε ενδεικτικά ορισμένα τέτοια προβληματικά σημεία τα οποία δεν λαμβάνονται συνήθως υπόψη:

- Η αντίληψη που έχουμε αναφορικά με τη σχέση των επιχειρήσεων-οργανισμών και της τεχνολογίας της Πληροφορικής δεν είναι πλέον αυτονόητη, αλλά περίπλοκη και σε διαρκή μεταβολή. Το σημείο-κλειδί είναι να μελετήσουμε τον τρόπο με τον οποίο τα Πληροφοριακά Συστήματα ολοκληρώνονται στο επιχειρηματικό περιβάλλον.
- Η αντίληψη για την ασφάλεια των Πληροφοριακών Συστημάτων πρέπει να διέπεται από την αρχή της επανατροφοδότησης και της διαρκούς αμφισβήτησης. Το μη-αναμενόμενο στις σύγχρονες συνθήκες πρέπει να αναμένεται ούτως ή άλλως (!).
- Η ασφάλεια των Πληροφοριακών Συστημάτων δεν πολώνεται μεταξύ της τεχνολογικής ή της ανθρωποκεντρικής της διάστασης.

Η Πολιτική Ασφάλειας αποτελεί το πιο ασφαλές, πλήρες και συμφέρον μέσο για την προστασία και ασφάλεια των Πληροφοριακών Συστημάτων των οργανισμών: υποδεικνύει τους σωστούς και επαρκείς μηχανισμούς ασφάλειας σε συνάρτηση με την επικινδυνότητα που υπάρχει.

Η έννοιας της Πολιτικής Ασφάλειας παραπέμπει σε διαχειριστικές-διοικητικές (management-administrative) διαδικασίες λήψης αποφάσεων των οργανισμών. Η διάσταση αυτή είναι σημαντική διότι αφενός επιτρέπει την θεώρηση της ασφάλειας σε ανώτερα οργανωτικά επίπεδα, αφετέρου αποτελεί αντικειμενικό χαρακτηριστικό της έννοιας. Υπό μία τέτοια θεώρηση, η Πολιτική ασφάλειας έχει ένα ευρύ πεδίο ορισμού και εμβέλειας, ένα πλούσιο περιεχόμενο και μία γενικευμένη εννοιολογική υφή, στοιχείο που κάνει ενδιαφέρουσα τη μελέτη της. Ταυτόχρονα όμως το χαρακτηριστικό αυτό εισάγει προβλήματα στη διαμόρφωση συγκεκριμένων απόψεων και λύσεων σχετικά με σημεία προβληματισμού. Το στοιχείο αυτό θα φανεί και αργότερα στην ποικιλομορφία των ορισμών της Πολιτικής Ασφάλειας. Για τους λόγους αυτούς, απαιτείται να λαμβάνουμε υπόψη μας κάθε σοβαρή άποψη ορίζουσα τις Πολιτικές Ασφάλειας, εφόσον κάθε αντίληψη μπορεί να συνεισφέρει στη μελέτη

μιας τέτοιας έννοιας.

## 1.2 Αντικείμενο, σκοπός και μεθοδολογία της εργασίας

Η διατριβή αυτή εντάσσεται στο γνωστικό πεδίο της Πληροφορικής και ιδιαίτερα της Ασφάλειας των Πληροφοριακών Συστημάτων. Ειδικότερα δε ασχολείται με το θέμα της διαχείρισης Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων. Γενικά, οι **σκοποί** της εργασίας είναι οι ακόλουθοι:

- Να προσεγγιστεί η έννοια της Πολιτικής Ασφάλειας Πληροφοριακού Συστήματος και να αναδειχθεί μέσω ανάλυσης η σημασία της για το χώρο των Πληροφοριακών Συστημάτων.
- Να παρουσιαστεί ένα κατατοπιστικό εννοιολογικό θεματολόγιο σχετικό με τα ενδιαφέροντα σημεία στη μελέτη των Πολιτικών Ασφάλειας.
- Να προσεγγιστεί το θέμα της διαχείρισης Πολιτικών Ασφάλειας σε όρους τυποποίησης των Πολιτικών Ασφάλειας και αυτοματοποίησης της διαχείρισής τους.

Ειδικότερα, επιχειρήθηκε να επιτευχθούν τα ακόλουθα:

- Μελέτη της χρησιμότητας της διαχείρισης Πολιτικών Ασφάλειας και εντοπισμός των τάσεων στο ευρύτερο πεδίο της Πληροφορικής που θέτουν τα ενδιαφέροντα πεδία έρευνας. Τα πεδία αυτά προσδιορίστηκαν ως η "Τυποποίηση και Αυτοματοποιημένη Διαχείριση Πολιτικών Ασφάλειας".
- Αναζήτηση στη βιβλιογραφία και εντοπισμός του γνωστικού πεδίου υπό το οποίο μπορούν να μελετηθούν τα παραπάνω.
- Μελέτη των υπαρχουσών προσεγγίσεων<sup>1</sup> και προσπαθειών για τυποποίηση και αυτοματοποίηση Πολιτικών Ασφάλειας, καθώς και για διαχείριση περισσότερων Πολιτικών Ασφάλειας.
- Έρευνα και εντοπισμός ενός υποπεδίου έντονου προβληματισμού και ερευνητικού ενδιαφέροντος<sup>2</sup> το οποίο μπορεί να καλυφθεί επαρκώς και εστίαση της μελέτης στα συναφή με αυτό θέματα.

Τα θέματα αυτά καλύφθηκαν ως εξής: Εντοπίστηκε, συλλέχθηκε και διερευνήθηκε η σχετική βιβλιογραφία και εντοπίστηκε ότι υφίσταται γνωστική περιοχή στην Ασφάλεια Πληροφοριακών Συστημάτων, η οποία μελετά θέματα διαχείρισης Πολιτικών Ασφάλειας και ειδικότερα τυποποίησης και αυτοματοποίησης Πολιτικών Ασφάλειας. Το πεδίο αυτό ονομάζεται στην εργασία "Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων".

Στο σημείο αυτό οφείλουμε να επεξηγήσουμε τους όρους που μόλις χρησιμοποιήσαμε, οι οποίοι είναι βασικοί για την εργασία, τόσο ώστε να ανήκουν στον τίτλο της. Ο αναγνώστης πρέπει εξαρχής και καθόλη τη διάρκεια της εργασίας να λάβει υπόψη του ότι η γενικότερη προοπτική αυτής της εργασίας αντιμετωπίζει το

<sup>1</sup> Χρησιμοποιούμε τον όρο "προσέγγιση" προκειμένου να περιγράψουμε ορισμένες ερευνητικές προσπάθειες και τα αποτελέσματά τους, από την άποψη γενικά του τρόπου με τον οποίο αντιμετωπίζουν θέματα τυποποίησης και αυτοματοποίησης πολιτικών ασφάλειας.

<sup>2</sup> ...καθώς και προσωπικού ενδιαφέροντος...



Θέμα της αυτοματοποιημένης διαχείρισης Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων, το οποίο οι εξελίξεις επιβάλλουν, όπως άλλωστε θα αναλύσουμε διεξοδικότερα σε ακόλουθες παραγράφους. Εν όψει της προοπτικής αυτής, το θέμα της τυποποίησης πολιτικών ασφάλειας προκύπτει ως απαραίτητη προϋπόθεση. Η τυποποίηση έχει στην εργασία αυτή την έννοια της καθ' οιονδήποτε τρόπο, δηλαδή με χρήση ποικίλων μεθόδων, τυπικής απεικόνισης εννοιών της πραγματικότητας, τέτοιας ώστε το παραγόμενο αποτέλεσμα να έχει τα χαρακτηριστικά εκείνα που θα το θέτουν:

- ✓ Ελέγχιμο της συνέπειάς του με τις έννοιες που τυποποιεί και
- ✓ Κατάλληλο και εύχρηστο για σχετικά άμεση χρήση σε σκοπούς αυτοματοποίησης διαστάσεων του χώρου προβληματισμού στον οποίο ανήκει.

Εξάλλου, η αυτοματοποίηση νοείται με τη συνήθη έννοιά της στο χώρο των Πληροφοριακών Συστημάτων, δηλαδή ως η διαδικασία μέσω της οποίας οι Πολιτικές Ασφάλειας ορίζονται, αναπτύσσονται και διαχειρίζονται με αυτοματοποιημένο ή τυολάχιστον ημιαυτοματοποιημένο από Πληροφοριακά Συστήματα κατάλληλα για τους σκοπούς αυτούς. Θα προσπαθήσουμε, ωστόσο, να κατατοπίσουμε τον αναγνώστη σχετικά με τη χρησιμότητα της αυτοματοποιημένης διαχείρισης πολιτικών ασφάλειας, τόσο μέσω ανάλυσης σε θεωρητικό επίπεδο, όσο και μέσω παραδειγμάτων και εφαρμογών.

Η αρθρογραφία ταξινομήθηκε κατά θέματα στα ακόλουθα μέρη:

- Ανάπτυξη Πολιτικών Ασφάλειας (Security Policy Development)
- Διαχείριση Πολιτικών Ασφάλειας (Security Policy Management)
- Τυποποίηση Πολιτικών Ασφάλειας (Security Policy Formalization)
- Αυτοματοποίηση Πολιτικών Ασφάλειας (Security Policy Automated Management)
- Γενική επί της Ασφάλειας Πληροφοριακών Συστημάτων
- Γενική των επικουρικών γνωστικών πεδίων (τυπικές μέθοδοι, πληροφοριακά συστήματα, κ.λπ.)

Σφουγγάρισμα το αρθρογραφικό υλικό, εντοπίσαμε ενότητες οργάνωσης του πληροφοριακού υλικού της διατριβής και μελετήθηκαν αναλυτικά και συγγράφηκαν τα πρώτα τέσσερα κεφάλαια:

- ☒ Κεφάλαιο I: Γενική Εισαγωγή της Διατριβής
- ☒ Κεφάλαιο II: Εισαγωγή στην έννοια της Πολιτικής Ασφάλειας Πληροφοριακού Συστήματος
- ☒ Κεφάλαιο III: Μελέτη των προσεγγίσεων τυποποίησης και αυτοματοποίησης Πολιτικών Ασφάλειας
- ☒ Κεφάλαιο IV: Μελέτη των προσεγγίσεων διαχείρισης περισσότερων Πολιτικών Ασφάλειας

Η εντατική ενασχόληση με τα σχετικά θέματα κατά τη μελέτη της βιβλιογραφίας και τη συγγραφή οδήγησαν στον καθορισμό ενός θέματος που παρουσίασε σοβαρό ενδιαφέρον. Η συγγραφή λοιπόν του πέμπτου κεφαλαίου υπήρξε αποτέλεσμα της μελέτης του θέματος της προσέγγισης των απαιτήσεων μίας μεθοδολογίας για Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων.

Οι γνώσεις που απαιτούνται για την κατανόηση της εργασίας περιλαμβάνουν θέματα Ανάλυσης, Σχεδίασης και Ασφάλειας Πληροφοριακών Συστημάτων, καθώς και βασικές γνώσεις Διακριτών Μαθηματικών. Η εργασία απευθύνεται δε σε κάθε ενδιαφερόμενο για τη γνωστική αυτή περιοχή, ο οποίος έχει τις γνώσεις προκειμένου να κατανοήσει και αξιολογήσει τα συγγραφόμενα.

### 1.3 Χρήσιμες παρατηρήσεις για τον αναγνώστη

Οι παρατηρήσεις αυτής της παραγράφου αποτελούν ένα χρήσιμο βοήθημα για τον αναγνώστη προκειμένου για την ευκολότερη ανάγνωση όσο και κατανόηση του κειμένου.

#### ■ Η βιβλιογραφία της εργασίας

Η βιβλιογραφία που χρησιμοποιήθηκε παρατίθεται στο τέλος της μελέτης. Μπορεί να παρατηρηθεί ότι η βιβλιογραφία είναι στη συντριπτική της πλειοψηφία αγγλική και αποτελείται από μεμονωμένα άρθρα. Ο αναγνώστης που θα αναζητήσει την αρθρογραφία θα πρέπει να έχει υπόψη του ότι αυτή αναζητήθηκε τόσο σε ελληνικές βιβλιοθήκες όσο και σε παραρτήματα της Βιβλιοθήκης της Μ.Βρετανίας (British Library) και στο INTERNET.

#### ☒ Η γλώσσα του κειμένου

Η γλώσσα στην οποία γράφουμε είναι η ελληνική. Σημειώστε όμως ότι η βιβλιογραφία ήταν κατά το συντριπτικό ποσοστό της αγγλική. Έτσι, η μετάφραση των αγγλικών όρων προσπαθεί να αποδώσει όσο το δυνατόν πληρέστερα το νόημα που ο αγγλικός όρος εκφράζει. Δεδομένου του γεγονότος ότι εν γένει το αναγνωστικό κοινό έχει αναπτύξει οικείότητα με την αγγλική βιβλιογραφία, η επιλογή μας είναι να αναφέρουμε ως βασικό τον αγγλικό ή ελληνικό όρο, ανάλογα με την εκφραστικότητα του καθενός. Εξάλλου, τα αποσπάσματα που αναγράφονται αυτούσια από την πηγή τους επιλέγεται κατά κύριο λόγο να αποδίδονται στην αντίστοιχη γλώσσα.

#### ✍ Ορολογία

Το κείμενο είναι πλούσιο σε εξειδικευμένους όρους, οι οποίοι αναλύονται στο βαθμό που αυτό θεωρείται αναγκαίο, με κριτήρια το αναγνωστικό κοινό, τη συσχέτιση με το αντικείμενο που εκάστοτε αναλύεται, ανάλυση που έχει προηγηθεί ή αναφορές προηγούμενων ή επόμενων κεφαλαίων. Η έννοια των όρων προσδιορίζεται άμεσα από το περιεχόμενο της εκάστοτε παραγράφου. Αυτό σημαίνει ότι κάποιος όρος μπορεί να έχει ελαφρές διαφοροποιήσεις ανάλογα με τα συμφραζόμενα<sup>3</sup>. Όταν κρίνεται όμως ότι απαιτείται διευκρίνιση θα επεξηγείται ο όρος. Ο αναγνώστης που είναι ελαφρά εξοικειωμένος με σχετικά θέματα (όπως υποδεικνύεται στην παράγρ.1.2.) είναι σε θέση να κατανοεί και να ερμηνεύει τις διαφοροποιήσεις.

Πρέπει να τονίσουμε ότι η ορολογία που υιοθετείται σε ορισμένα σημεία αποδίδεται στη συγγραφέα και μόνον. Θεωρούμε σημαντικό να παραπέμψουμε

<sup>3</sup> Για παράδειγμα, ο όρος "μοντέλο" χρησιμοποιείται με διαφορετική έννοια στην ενότητα που αφορά μοντέλα πολιτικών ασφάλειας και με άλλη έννοια στην ενότητα των τυπικών περιγραφικών μεθόδων.



εξαρχής τον αναγνώστη στο τέλος του κειμένου όπου παρατίθονται οι μεταφράσεις των ξενικών όρων στους οποίους αναφερθήκαμε. Εξάλλου, η επιλογή για χρήση της αγγλικής ή ελληνικής απόδοσης των όρων γίνεται όπως προαναφέραμε.

### ■ **Χρήση εισαγωγικών σημειωμάτων και λέξεων-κλειδιών**

Επιλέξαμε αυτούς τους δύο τρόπους σαν βοηθήματα προκειμένου να βοηθήσουμε τον αναγνώστη να σχηματίσει μία άποψη για τα θέματα που μελετώνται. Έτσι, πριν από κάθε μεγάλη ή σημαντική ενότητα υπάρχει μία εισαγωγική παράγραφος καθώς και λέξεις-κλειδιά που χαρακτηρίζουν τη θεματολογία. Η χρήση συνοπτικών σημειωμάτων, μετά από την ανάλυση κάθε θέματος, είναι μάλλον περιορισμένη και αυτό διότι θεωρήσαμε ότι είναι προτιμότερο τα επιμέρους συμπεράσματα να βρίσκονται πλησίον της ανάλυσης που τα παρήγαγε και να αποτελούν μέρος της ανάλυσης αυτής. Το τελευταίο κεφάλαιο κάνει πιο ευρεία χρήση του εργαλείου αυτού.

### ■ **Χρήση παρενθετικού λόγου, υποσημειώσεων και παραπομπών**

Για τα σημεία τα οποία δεν κρίνεται ότι πρέπει να περιληφθούν άμεσα στο κείμενο, υπάρχει συνήθως υποσημείωση που παραπέμπει στη σχετική πηγή άντλησης περισσότερης πληροφόρησης. Επίσης αποφεύγονται οι παραπομπές εντός του κειμένου, ώστε να μειώνεται κατά το δυνατό η εξάρτηση της κατανόησης από διασταύρωση πληροφοριών.

### ■ **Χρήση εξειδικευμένης μαθηματικής γλώσσας, συμβολισμών και γλωσσών προγραμματισμού**

Σε ορισμένα σημεία είναι απαραίτητη η παρουσίαση μαθηματικοποιημένων θεωριών ή αποσπασμάτων λογισμικού, συνεπώς δεν μπορεί να αποφευχθεί η χρήση των αντίστοιχων συμβόλων και γλώσσας. Γίνεται ωστόσο προσπάθεια, τόσο να περιοριστεί η παράθεση τέτοιων αποσπασμάτων όσο και να μειωθεί η πολυπλοκότητα της παρουσίασης. Γενικά όμως όπως είπαμε, απαιτούνται βασικές προγραμματιστικές γνώσεις, όπως και γνώσεις τυπικών περιγραφικών μεθόδων.

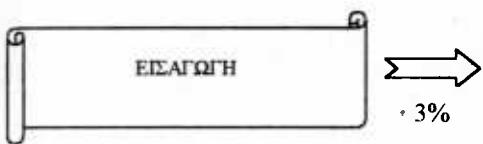
## 1.4 Δομή της εργασίας

Το πληροφοριακό μας υλικό οργανώνεται στα ακόλουθα μέρη:

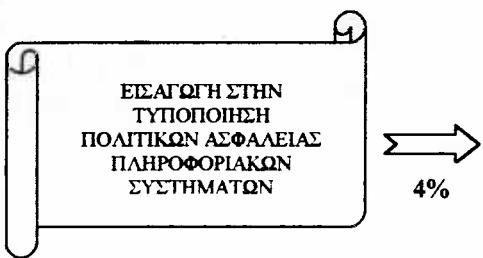
- Πρόλογο.
- Πέντε κεφάλαια, καθένα από τα οποία αντιπροσωπεύει μία συγκεκριμένη νοηματική ενότητα.
- Βιβλιογραφία.
- Ευρετήριο σημαντικών όρων.
- Μεταφράσεις όρων.
- Βιβλιογραφία.

Το περιεχόμενο κάθε κεφαλαίου αντιπροσωπεύει μία συγκεκριμένη νοηματική ενότητα. Στο ακόλουθο σχήμα παρουσιάζουμε την οργάνωση της ύλης των πέντε κεφαλαίων της εργασίας συνοπτικά και γραφικά.

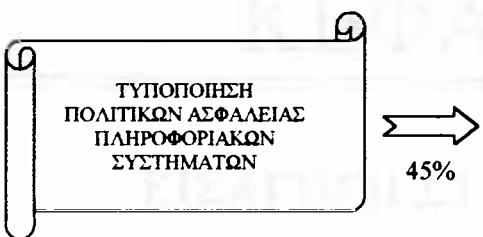




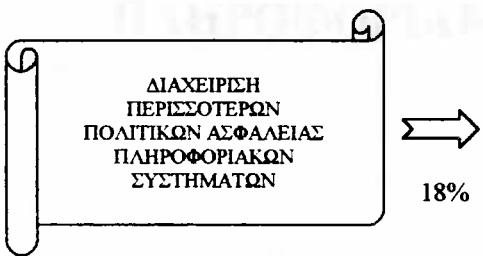
- ♦ Αντικείμενο, σκοπός και σημασία της μελέτης
- ♦ Χρήσιμες παρατηρήσεις για τον αναγνώστη



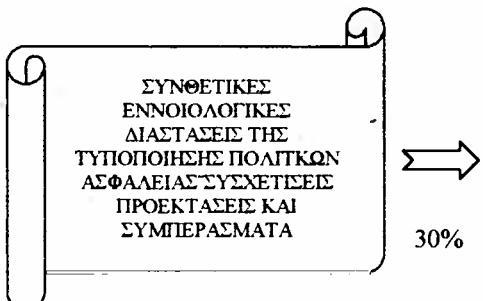
- ♦ Ανάλυση της έννοιας της πολιτικής
- ♦ Ορισμός και ανάλυση της έννοιας της Πολιτικής Ασφάλειας Πληροφοριακού Συστήματος
- ♦ Ανάλυση των εννοιών της τυποποίησης και αυτοματοποίησης Πολιτικής Ασφάλειας Πληροφοριακού Συστήματος



- ♦ Αναλυτική παρουσίαση μεθοδολογιών τυποποίησης Πολιτικών Ασφάλειας
- ♦ Αναλυτική παρουσίαση μεθόδων και πρακτικών τυποποίησης και αυτοματοποίησης Πολιτικών Ασφάλειας



- ♦ Έννοια της διαχείρισης περισσότερων Πολιτικών Ασφάλειας
- ♦ Παρουσίαση μεθοδολογιών διαχείρισης πολλών Πολιτικών Ασφάλειας



- ♦ Σύνοψη
- ♦ Διαμόρφωση αντικειμένου προβληματισμού και καθορισμός στόχου μελέτης
- ♦ Ανάλυση βασικών εννοιών που αφορούν θέματα τυποποίησης και αυτοματοποίησης Πολιτικών Ασφάλειας
- ♦ Παρουσίαση γνώσεων υποδομής προκειμένου για τη διαμόρφωση μιας μεθοδολογίας επί του αντικειμένου-στόχου
- ♦ Διερεύνηση του αντικειμένου-στόχου
- ♦ Κατευθύνσεις έρευνας

## 2.2 Τοποθετήσεις στην πλατφόρμα

Από την πλατφόρμα, δύο τύποι τοποθετήσεων διαθέσιμες:

• Η απλή τοποθετήση, όπου μεταβιβάζεται στην πλατφόρμα η πληροφορία για την επιλεγμένη πολιτική ασφαλείας, η οποία αποτελείται από την πληροφορία που έχει προστατευτεί από την πλατφόρμα. Η απλή τοποθετήση διαθέτει μεγάλη απλοποίηση, αλλά δεν είναι συναρπαγή, καθώς η πληροφορία που προστατεύεται από την πλατφόρμα δεν μπορεί να παραδοθεί σε άλλη πλατφόρμα.

• Η απλή τοποθετήση με προστατευόμενη πληροφορία (ΕΠΙΦΕΚ), η οποία αποτελείται από την πληροφορία που προστατεύεται από την πλατφόρμα, αλλά δεν μπορεί να παραδοθεί σε άλλη πλατφόρμα.

## ΚΕΦΑΛΑΙΟ ΙΙ

### ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΤΥΠΟΠΟΙΗΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

## 2.1 Περί "Πολιτικής" γενικότερα

Διαμόρφωση Πολιτικής, Δομή Πολιτικής, Ανθρώπινη Συμπεριφορά

Θα αποτελούσε κατά την κρίση μας μία πολύ ενδιαφέρουσα όσο και χρήσιμη εργασία η παρουσίαση της έννοιας της "πολιτικής" γενικότερα, προτού επιχειρηθεί μία αναλυτικότερη προσέγγιση στις πολιτικές ασφάλειας. Γιατί βέβαια η λέξη "πολιτική" βρίσκει εφαρμογή και σε ένα ευρύ πεδίο τομέων της πολιτικής, οικονομικής, κοινωνικής, κ.λπ. πρακτικής. Στους τομείς αυτούς η πολιτική εμφανίζεται με την έννοια της "στρατηγικής δράσης" σε διάφορα επίπεδα σημαντικότητας και λεπτομέρειας.

Όπως πολύ χαρακτηριστικά σημειώνεται στο [HER-1986], τα θέματα που αφορούν τη διαμόρφωση πολιτικών αποτελούν σύνθετα προβλήματα που απαιτούν έρευνα σε όλα τα επίπεδα, τη στιγμή που περίπου έναν και μισό αιώνα πριν (1868) διατυπωνόταν από τον Mill η παρακάτω άποψη<sup>4</sup>:

"... Μέσα σε μία κοινωνία, τα ανθρώπινα όντα δεν άλλες ιδιότητες παρά αυτές που συνεπάγονται και μπορούν να αποδοθούν και να καταλήξουν στους νόμους της φύσης για τα όντα αυτά".

Οι πολιτικές θεωρούνται κατά πολλούς σαν αντικείμενα που αποσκοπούν στον επηρεασμό της ανθρώπινης συμπεριφορά προς το επιθυμητό ("...guiding behavior in desired directions..."). Αυτό σημαίνει ότι οι βάσεις για τη διαμόρφωση των πολιτικών πρέπει να είναι επιθυμητά σενάρια αποτελεσμάτων. Επίσης διατυπώνεται η άποψη ότι οι πολιτικές συνδέονται στενά με οικονομικής φύσης σκοπούς τους οποίους προσπαθούν να προασπίσουν. Οι House και Tyndall [HER-1986] οριοθετούν τη διαμόρφωση πολιτικής σαν "πρόγραμμα σχεδιασμένο να επιτεύξει ορισμένους στόχους, επιλέγοντας μέσα από εναλλακτικές λύσεις και ισορροπώντας ανάμεσα σε επιλογές".

Ο Hertz επιλέγει να θεωρεί τις πολιτικές σαν

"... δηλώσεις στόχων, συνδυασμένες με σύνολα κανόνων, ή διαδικασιών που υποδεικνύουν κανόνες, οι οποίοι αποσκοπούν στην επίτευξη κατά το δυνατό όλων των παραπάνω στόχων..."

Η διαδικασία διαμόρφωσης της πολιτικής είναι ηθελημένη και επιθυμητή και η μορφή με την οποία παρουσιάζεται η πολιτική είναι συνήθως ο γραπτός λόγος. Η διαδικασία διαμόρφωσης πολιτικής περιλαμβάνει κατά τον Hertz τα ακόλουθα στάδια: α) Διατύπωση πολιτικής, β) Υλοποίηση πολιτικής και γ) Αξιολόγηση πολιτικής. Αναγνωρίζεται βέβαια ότι οι Πολιτικές δεν είναι στατικές αλλά υπόκεινται σε διαδικασία συνεχούς επαναδιατύπωσης ανάλογα με τις ανάγκες που προκύπτουν μετά την αξιολόγηση. Κατά τον ορισμό αυτό αναγνωρίζεται ο όρος της "δομής της πολιτικής" (policy structure, [HER-1986]) ως

"... the written (occasionally unwritten) recognition of a general problem or problem area, along with recommendations which specify, mandate, suggest or allow, ways of dealing with, or solving, some or all of the issues that may arise within that problem area..."

<sup>4</sup> Ελεύθερη μετάφραση από το [HER-1986].



Οι συστάσεις αυτές μπορεί να έχουν ιεραρχική/δενδρική δομή, από την άποψη ότι μπορεί να εξετάζουν εναλλακτικές περιπτώσεις (if ... then ... else ...) ή να προτείνουν διαφορετικές δράσεις (either ... or).

Εξάλλου, χρήσιμες είναι και οι απόψεις του Wilensky (1983) [HER-1986], ο οποίος ενέταξε τη διαμόρφωση πολιτικής στην "Θεωρία Προγραμματισμού" (Theory of Plans) την οποία πρότεινε. Η Θεωρία Προγραμματισμού αποτελείται από δύο υποθεωρίες: 1)τη Θεωρία Σχεδιασμού, μία διαδικασία με την οποία ένας φορέας (agent) καθορίζει και εκτελεί ένα σχέδιο δράσης και 2)τη Θεωρία Κατανόησης, με την οποία ένας φορέας κατανοεί μία κατάσταση και διαμορφώνει ένα σύνολο υποθετικών στόχων και σχεδίων. Η δεύτερη δραστηριότητα προηγείται της πρώτης.

Στις διάφορες εκφάνσεις της ζωής, όπου μπορούμε να δούμε την πολιτική να εμπλέκεται, αυτή αποτελεί δεδομένο ελέγχου εισόδου (control input variable) στα δεδομένα εισόδου (input data) τα οποία παράγονται από ένα περιβάλλον και τα οποία πρέπει να αναγνωριστούν, εξεταστούν και παράξουν συγκεκριμένες, επιλεγμένες από ένα σύνολο δηλαδή, δράσεις. Οι "υποχρεωτικές πολιτικές" συνεπάγονται την ενεργοποίηση συγκεκριμένων, υποχρεωτικών δράσεων. Οι δομές που αυτές απαιτούν είναι μάλλον απλές, ξεκάθαρες και καλά διατυπωμένες. Οι "ευέλικτες πολιτικές" αφήνουν περιθώριο για συμπεριληψη και περισσοτέρων περιπτώσεων (δεδομένων εισόδου). Στην περύπτωση που θέλουμε να περιγράψουμε τέτοιες πολιτικές η διαδικασία περιπλέκεται και απαιτεί τη συλλογή και επεξεργασία νέων δεδομένων, τα οποία ενίστε μπορεί να επηρεάσουν τους στόχους της πολιτικής.

## 2.2 Πολιτική Ασφάλειας Πληροφοριακού Συστήματος

Ασφάλεια Πληροφοριακών Συστημάτων, Πολιτική Ασφάλειας Πληροφοριακών Συστημάτων, Τεχνική Πολιτική Ασφάλειας, Πολιτική Ασφάλειας Οργανισμού, Κανόνες, Στόχοι, Απαιτήσεις

Θα έπρεπε να αποτελεί πρώτιστο έργο μας κατά τη συγγραφή αυτής της εργασίας ο ορισμός, ο περιορισμός κατά μία άλλη έννοια, ή τελικά η σαφής δήλωση της έννοιας με την οποία η έκφραση αυτή θα χρησιμοποιείται στην παρούσα εργασία. Πρέπει να παραδεχτούμε ότι η προσπάθεια αυτή αποτέλεσε μία από τις δυσκολότερες αυτής της μελέτης, όπως πολύ καλά θα γνωρίζουν όσοι έχουν ασχοληθεί με τη βιβλιογραφία επί του θέματος όσο και με την ασφάλεια γενικότερα, καθώς οι απόψεις και οι ορισμοί ποικίλουν σημαντικά. Το γεγονός αυτό της ποικιλομορφίας της θεωρητικής υποδομής στο πεδίο της ασφάλειας παρουσιάζεται γενικότερα όσον αφορά τη διευκρίνιση πολλών εννοιών, λόγω της σχετικά πρόσφατης διαμόρφωσής της ως διακριτού πεδίου μελέτης και έρευνας στο γνωστικό πεδίο της Πληροφορικής.

Έτσι, οι διάφορες λέξεις αφενός μπορεί να χρησιμοποιούνται ως έχουσες την ίδια περίπου σημασία και αφετέρου οι ίδιες λέξεις μπορεί νά αποκτούν διαφορετική σημασία ανάλογα με τη χρήση τους από διάφορα υποκείμενα για διαφορετικούς σκοπούς. Ιδιαίτερη σύγχυση από μέρους της ερευνητικής κοινότητας παρατηρείται εξάλλου στη χρήση των όρων "πληροφορία", "πληροφοριακό σύστημα", "τεχνολογία πληροφορίας", που μπορούν να συνοδεύουν τη λέξη "ασφάλεια". Στην παρούσα εργασία δεν θα ασχοληθούμε με τη διευκρίνιση αυτών ακριβώς των τελευταίων εννοιών και θα τις θεωρήσουμε ισοδύναμες χάριν απλούστευσης του υπόλοιπου διευκρινιστικού έργου μας.

Καταρχήν η λέξη "πολιτική" εμφανίζεται συνήθως με τις ακόλουθες ερμηνείες [OXF-1989]:

"plan of action / statement of ideals / written statement of the terms of a situation"

Στη βιβλιογραφία εξάλλου εμφανίζονται οι ακόλουθοι ορισμοί αναφορικά με την "πολιτική" και την "πολιτική ασφάλειας" στο χώρο της Πληροφορικής:

"policies are management instructions indicating how an organization is to be run"

"they are high level statements intended to provide guidance to those who must make present and future decisions"

"policies are generalised requirements"

To ITSEC [ITSEC-1991] ορίζει τις ακόλουθες έννοιες:

"A corporate security policy is the set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed with a user organization"

"A system security policy specifies the set of laws, rules and practices that regulate how sensitive information and other resources are managed protected abd distributed within a specific system"

"A technical security policy is the set of laws, rules and practices regulating the processing of sensitive information and the use of resources by the hardware and the software of an IT system or product"

Τέτοιου είδους ορισμοί και απόψεις υπάρχουν πολλοί περισσότεροι (για παράδειγμα στο [KOK-1997a] παρατίθονται διάφοροι τέτοιοι ορισμοί που έχουν υιοθετηθεί από ερευνητές). Τελικά όμως, στις πλείστες των περιπτώσεων (βλ. για παράδειγμα τα [CCTA-1996] και [UNI-1993]), η πολιτική ασφάλειας ταιριάζει περισσότερο με τα στοιχεία που διατυπώνει η παρακάτω απόψη:

"Information security policies include typically general statements of goals, objectives beliefs, ethics and responsibilities often accompanied by the general means for obtaining these things (such as procedures)"

Τα μόνιμα χαρακτηριστικά μιας πολιτικής ασφάλειας παρά ταύτα - πρέπει να είναι τα ακόλουθα:

- η πολιτική απαιτεί υποχρεωτική συμμόρφωση
- η πολιτική είναι συνήθως γενικευμένης σημασίας (για τον οργανισμό) ή αναφοράς ή προορισμένη να διαρκέσει για αρκετά χρόνια (και κατά συνέπεια). Η πολιτική, δηλαδή, δεν κάνει εξειδικευμένες αναφορές (για παράδειγμα σε τεχνολογικούς όρους, σε συγκεκριμένα άτομα -αλλά σε ρόλους-, κ.λπ.) και συνεπώς δεν αλλάζει συχνά, παρά μόνον όταν σημαντικές αλλαγές νοοτροπίας το επιβάλλουν
- η πολιτική εκφράζει γενικότερες απόψεις ή αρχές του οργανισμού ή αποτελεί ένα υψηλού επιπέδου εργαλείο

Τελικά η άποψη την οποία θα υιοθετήσουμε στην εργασία αυτή είναι ο δεύτερος κατά ITSEC ορισμός, ακριβώς επειδή αποτελεί τη μορφή με την οποία συνήθως αναπτύσσονται οι πολιτικές ασφάλειας. Πρέπει να παρατηρήσουμε ότι με την πρώτη εντύπωση ο ορισμός αυτός περιορίζει αρκετά την εν λόγω έννοια, απομακρύνοντάς την από τα μόνιμα χαρακτηριστικά τα οποία παραθέσαμε. Αυτό

γίνεται μάλλον για λόγους σαφήνειας και δεν αποκλείει αυτά τα χαρακτηριστικά. Εντούτοις πολλές φορές θα έρθουμε αντιμέτωποι σε μεθοδολογικό επίπεδο με έννοιες που σχετίζονται με τον πρώτο ορισμό και συνεπώς η διευκρίνησή μας στο σημείο αυτό δεν διέπεται από αυστηρότητα.

## 2.3 Παραδειγματισμοί ανάπτυξης πολιτικών και τυποποίηση πολιτικών

Αυτοματοποιημένη Διαχείριση Πολιτικών, Φυσικοί Νόμοι, Αξίες, Παραδείγματα  
Ανάπτυξης Πολιτικών Ασφάλειας Μετασύστημα

Θεωρούμε σημαντικό να ξεκινήσουμε την ανάλυσή μας από την διαδικασία ανάπτυξης των πολιτικών γενικότερα και κατ' αυτό τον τρόπο να αντλήσουμε αφορμές που θα μας οδηγήσουν στις απαιτήσεις της τυποποίησης των πολιτικών ασφάλειας. Στην παράγραφο αυτή θα κάνουμε την υπόθεση ότι επιθυμία μας είναι να μπορέσουμε να φτάσουμε σε ένα επίπεδο τυποποίησης της πολιτικής μας, το οποίο θα μας επιτρέπει να τη διαχειριστούμε αυτοματοποιημένα. Κάτι τέτοιο συνεπάγεται ίσως ότι "αν θέλουμε να επηρεάσουμε τη συμπεριφορά του υπολογιστή τότε θα πρέπει να ενσωματώσουμε μία συγκεκριμένη πολιτική στα προγράμματα που αυτός υλοποιεί!".

Ο Hertz, όπως είπαμε στην παράγρ.2.1, σημειώνει ότι οι πολιτικές εμφανίζονται συνήθως ως γραπτές δηλώσεις συνοδευόμενες από διαδικασίες που υποδεικνύουν τον τρόπο με τον οποίο μπορούν αυτές να υλοποιηθούν. Τις περισσότερες φορές μάλιστα οι οργανισμοί δεν διατυπώνουν αρκετά ξεκάθαρα τις ίδιες τις αρχές της πολιτικής τους, εντούτοις όμως προσδιορίζουν αρκετά καλά τις διαδικασίες με τις οποίες επιτυγχάνονται οι στόχοι της πολιτικής. Το επίπεδο λεπτομέρειας στη διατύπωση των δηλώσεων μπορεί να διαφέρει μέσα στα όρια που θα έθεταν κάποιοι ακριβείς κανόνες (precise rules) έως κάποιες αόριστες δηλώσεις προθέσεως (statements of intent).

Αν θέλουμε να διαχειριζόμαστε την πολιτική μας μέσω ενός αυτοματοποιημένου συστήματος, θα πρέπει το επίπεδο τυποποίησης αυτής να είναι όσο το δυνατό υψηλότερο. Αυτό συμβαίνει εφόσον τα υπολογιστικά προγράμματα μπορούν να επεξεργαστούν μόνον αυστηρά καθορισμένα στοιχεία τα οποία μάλιστα αναταρίστανται τυπικά (formally), με κάποια μέθοδο υψηλού βαθμού ακρίβειας. Προκειμένου να τυποποιήσουμε την πολιτική μας, **το σημείο αφετηρίας πρέπει να είναι το υψηλότερο σημείο αφαίρεσης στο οποίο μπορούμε να την περιγράψουμε**. Παρόλο που η δήλωση αυτή φαίνεται να συγκρούεται με την έννοια της τυποποίησης, η οποία μας οδηγεί σε ένα χαμηλό επίπεδο αφαίρεσης, εντούτοις θα διαπιστώσει κανείς ότι αγνοώντας το υψηλότερο επίπεδο ανάλυσης, χάνονται σημαντικότατες πληροφορίες οι οποίες ουσιαστικά υπογράφουν και αντιτροσωπεύουν την πολιτική. Μύλαμε εδώ για το ουσιαστικό περιβάλλον μιας πολιτικής (context), που δεν είναι άλλο από τους "**Φυσικούς Νόμους**" που τη διέπουν και από τους οποίους δεν μπορούμε να απαλλαγούμε, πόσο μάλλον να τους αγνοήσουμε. Είναι αυτοί οι οποίοι, λόγω της δύναμής τους αλλά και της δικής μας αδυναμίας να τους εντοπίσουμε με ακρίβεια, συνήθως οδηγούν στις περισσότερες αντιφάσεις και συγκρούσεις στην εφαρμογή ή στην μελέτη των πολιτικών.

Το σημείο αυτό, ο εντοπισμός δηλαδή και η αυστηρή περιγραφή των παραδειγμάτων και των υποθέσεων ανώτερου επιπέδου που διέπουν μία πολιτική, είναι το σημαντικότερο και δυσκολότερο κεφάλαιο σε μία συζήτηση περί τυποποίησης πολιτικών. Τα παραδείγματα αφορούν κατά κύριο λόγω, και σε τελική

ανάλυση, τις ουσιαστικές ιδέες που οδήγησαν την ανάπτυξη της πολιτικής. Οι ιδέες αυτές ανταποκρίνονται στο σύνολο αξιών των ατόμων που ενεπλάκησαν στη διαδικασία της ανάπτυξης (όπως λ.χ. το ορίζει η E.Mumford στο [MUM-1985]), καθώς και στις αξίες που υποδεικνύει το ίδιο το περιβάλλον ανάπτυξης και εφαρμογής της πολιτικής.

Στο σημείο αυτό να παρατηρήσουμε το εξής: Πολλές φορές, όσο συστηματική και δομημένη κι αν είναι η προσπάθεια να δημιουργήσουμε μοντέλα απόψεων του πραγματικού κόσμου τα οποία πρέπει να αλληλεπιδράσουν, παρατηρείται το γεγονός ότι η εφαρμογή τους σε πραγματικές συνθήκες σπάνια δίνει τα υπολογισμένα αποτελέσματα. Αυτό συμβαίνει διότι προσπαθούμε να εφαρμόσουμε τις νόρμες των μοντελοποιημένων εκδόσεων του πραγματικού συστήματος στο ίδιο το πραγματικό σύστημα. Το τελευταίο αυτό δεν ανταποκρίνεται επακριβώς στο μοντέλο που έχουμε δημιουργήσει. Κάθε μοντελοποίηση ενός πραγματικού συστήματος πρέπει να λαμβάνει υπόψη της ότι τα αποτελέσματα κάθε λειτουργίας δεν εφαρμόζονται τελικά μόνο στο μοντέλο του συστήματος έτσι όπως το αντιληφθήκαμε αλλά και στο αντίστοιχο μετασύστημα, το οποίο τελικά βρίσκεται εκτός του πεδίου μοντελοποίησης. Αυτό είναι που πρέπει να προσπαθήσουμε να λάβουμε υπόψη μας σε οποιαδήποτε εφαρμογή. Η δημιουργία του μοντέλου του αντίστοιχου μετασυστήματος αποτελεί τη λύση του προβλήματος.

Την έννοια του μετασυστήματος θα την αντιμετωπίσουμε πολλές φορές, με διάφορες μορφές. Ο αναγνώστης θα παρατηρήσει ότι ο ορισμός του μετασυστήματος περιλαμβάνει ποικιλία ορισμάτων (π.χ. το σύστημα των λέξεων-γλώσσας που χρησιμοποιείται, το σύστημα μοντέλων που περιγράφει κάποια στοιχεία του πραγματικού συστήματος, συμβολισμούς, κλ.π.), τα οποία αποτελούν πολλές φορές τα εργαλεία προκειμένου να ερμηνεύσουμε ή να κατανοήσουμε την πραγματικότητα.. Πάντως, θα γίνει κατανοητό ότι το μετασύστημα αντιπροσωπεύει κάθε φορά το "δύσκολο" μέρος σε κάθε προσπάθεια, αφού αποτελεί το **μεταφραστικό μέσο ανάμεσα στην στην ίδια την πραγματικότητα και στην ανθρώπινη αντίληψη για την πραγματικότητα αυτή**.

Αφού λοιπόν αναγνωρίσουμε τη σοβαρότητα του θέματος αυτού, χρειαζόμαστε να χρησιμοποιήσουμε τις υπάρχουσες μεθόδους επεξεργασίας παραδειγμάτων ή να επινοήσουμε νέες προκειμένου να αναλύσουμε, να κατανοήσουμε και, το σημαντικότερο, να επαληθεύσουμε τις πρωτογενείς και θεμελιώδεις υποθέσεις που διέπουν κάθε πολιτική. Στο θέμα αυτό, που αποτελεί μία ανεκτλήρωτη μέχρι τούδε απαίτηση στο χώρο της τυποποίησης των πολιτικών, θα επανέλθουμε πολλές φορές κατά τη διάρκεια αυτής της μελέτης εντοπίζοντας τους τρόπους που χρησιμοποιούνται για την επίλυσή του.

## 2.4 Αυτοματοποιημένη διαχείριση των πολιτικών ασφάλειας Πληροφοριακών Συστημάτων

Τυποποίηση Πολιτικών Ασφάλειας, Τυποποίηση Διαχείρισης Πολιτικών Ασφάλειας,  
Μοντελοποίηση, Τεχνολογία Πολιτικών Ασφάλειας, Παραδειγματισμοί Ασφάλειας

Προκειμένου να περιγράψουμε την έννοια της τυποποίησης αναφορικά με τις πολιτικές ασφάλειας, η οποία σε πολλά σημεία ισοδυναμεί με τα όσα ισχύουν για πολιτικές γενικότερα, ακολουθούμε την εξής τακτική: Θα θεωρήσουμε ότι θέτουμε κάποιο αρχικό στόχο τον οποίο πρέπει να επιτύχουμε και σταδιακά θα οδηγηθούμε

σε σημαντικά θέματα του αντικειμένου μας.

Θεωρούμε ότι στόχος μας είναι να δημιουργήσουμε μία μεθοδολογία και ένα ολοκληρωμένο περιβάλλον αυτοματοποιημένης διαχείρισης πολιτικών ασφάλειας (παρακάτω θα εξηγήσουμε τους λόγους για τους οποίους θα επιθυμούσαμε να είχαμε στη διάθεσή μας ένα τέτοιο εργαλείο). Η διαδικασία είναι η ίδια με αυτήν που ακολουθείται στη ανάπτυξη οποιουδήποτε αυτοματοποιημένου συστήματος που ξεκινάει από τη διαπίστωση προβληματικών σημείων μίας κατάστασης που χρειάζονται -και μπορούν να υποστούν- αυτοματοποίηση της διαχείρισής τους:

Καταρχήν απαιτείται να καθορίσουμε, να αναλύσουμε και να τεκμηριώσουμε τα δεδομένα μας (BHMA I). Απαιτείται να περιγράψουμε με ακριβή και συγκεκριμένο τρόπο τα στοιχεία που πρόκειται να αυτοματοποιηθούν και ακολούθως να τα δώσουμε ως είσοδο σε μία διαδικασία μετατροπής στα μηχανικά τους ανάλογα. Η ακρίβεια αναφέρεται στην αυστηρή περιγραφή του συστήματος και της αντίστοιχης πολιτικής, έτσι ώστε να εντοπιστούν όλες οι διαστάσεις που χρειάζονται προκειμένου τα αυτοματοποιημένα ανάλογα να ανταποκρίνονται στο πραγματικό σύστημα και την πολιτική, ενώ απαιτείται και ένας συγκεκριμένος τρόπος περιγραφής, προκειμένου το υπολογιστικό σύστημα να "κατανοήσει" τα δεδομένα που θα λάβει ως είσοδο.

Η διαδικασία περιγραφής του πραγματικού συστήματος και της πολιτικής αφορά την εργασία της τυποποίησης (BHMA II). Αυτή δε, περιλαμβάνει διάφορες μεθόδους, όπως μοντελοποίηση (modeling), περιγραφικές γλώσσες (description languages), χρήση μεθόδων ανάλυσης δεδομένων (data analysis), εξόρυξης δεδομένων (data mining), αναπαράστασης γνώσης (knowledge representation), βάσεων κανόνων γνώσης (knowledge rule bases), τεχνητής νοημοσύνης (artificial intelligence), εμπειριών συστημάτων (expert systems), κ.λπ.

Όμως, κάθε έργο αυτοματοποίησης ενός συστήματος σε υπολογιστικό περιβάλλον συνεπάγεται τη δημιουργία των τεχνολογικών αντίστοιχων (engineering) των στοιχείων (αντικειμένων και λειτουργιών) του συστήματος και της πολιτικής. Αυτό σημαίνει ότι πρέπει να δημιουργήσουμε τα μηχανικά ανάλογα των στοιχείων του φυσικού συστήματος (BHMA III) και της αντίστοιχης πολιτικής.

Τα παραπάνω τρία βήματα στην πορεία των σύλλογισμών μας με βάση την αρχική μας υπόθεση αρχικοποιούν τα τρία μεγάλα κεφάλαια της μελέτης αυτής, όπως φαίνεται στο παρακάτω σχήμα:

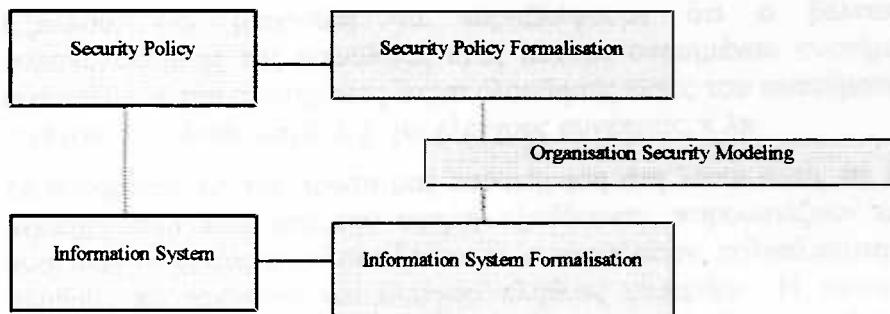


ΣΧΗΜΑ 2.1. Η διαδικασία αυτοματοποίησης της διαχείρισης των πολιτικών ασφάλειας.

Οι αρχές που έχουμε ήδη εντοπίσει μπορούν να επικουρηθούν από συμπληρωματικές έννοιες οι οποίες θα μας βοηθήσουν να ενώσουμε όλα τα κομμάτια του παζλ σε ένα σχήμα το οποίο θα καλύπτει, σε ένα σχετικά υψηλό

εννοιολογικά επίπεδο τη γνωστική που εξετάζουμε.

Θα θέλαμε στην ιδανική περίπτωση να επιτύχουμε πλήρη εφαρμογή της πολιτικής, ενσωματώντας την τήρησή της σε κάθε αντικείμενο του συστήματος. Χρησιμοποιώντας τα συμπεράσματα των προηγούμενων συλλογισμών μας, γνωρίζουμε ότι απαιτείται τυποποίηση των στοιχείων που εμπλέκονται, δηλαδή της πολιτικής και του συστήματος. Προκειμένου να αντιστοιχηθούν οι τυποποιημένες εκδόσεις αυτών πρέπει να αντιμετωπίσουμε την εργασία της τυποποίησης, όπως φαίνεται στο ακόλουθο σχήμα. Το σχήμα αυτό δείχνει την εμπλοκή της έννοιας της Ανάλυσης του Οργανισμού ως προς την Ασφάλεια (Organisation Security Modeling) και τη σημασία της διαδικασίας αυτής προκειμένου να λάβουμε υπόψη μας στοιχεία της Πολιτικής Ασφάλειας που καθορίζονται από το γενικότερο περιβάλλον του οργανισμού (βλ. για παράδειγμα παράγρ.3.6).



**ΣΧΗΜΑ 2.2. Συσχέτιση των διαδικασιών τυποποίησης του συστήματος και της πολιτικής.**

## 2.5 Χρησιμότητα της αυτοματοποιημένης διαχείρισης των πολιτικών ασφάλειας Πληροφοριακών Συστημάτων

Εξειδίκευση, Πολυπλοκότητα

Στην προηγούμενη παράγραφο ξεκινήσαμε με την υπόθεση ότι θεωρούμε ότι η αυτοματοποιημένη διαχείριση Πολιτικών Ασφάλειας είναι απαραίτητη, την οποία εντούτοις δεν τεκμηριώσαμε. Το θέμα αυτό θα μας απασχολήσει στην παρούσα παράγραφο.

Καταρχήν πρέπει να σημειώσουμε ότι το θέμα των πολιτικών ασφάλειας έκανε έντονη τη σημασία του από τη στιγμή που η ίδια η ασφάλεια άρχισε να αποτελεί ένα κεφαλαιώδες θέμα στο χώρο των Πληροφοριακών Συστημάτων. Η ανάπτυξη πολιτικής ασφάλειας είναι μία διαδικασία που δομεί, δικαιολογεί και εξασφαλίζει τις λειτουργίες ασφάλειας ενός οργανισμού. Η πολιτική ασφάλειας - πρέπει να- αποτελεί το σημείο αναφοράς και να συνδέει όλες τις σχετικές με ασφάλεια διαδικασίες ενός οργανισμού. Συνοπτικά μπορούμε να πούμε ότι η πολιτική ασφάλειας καλύπτει με γενικά αποδεκτό τρόπο όλες τις περιοχές όπου η λήψη αποφάσεων αντιμετωπίζει θέματα ασφάλειας για ένα σύστημα.

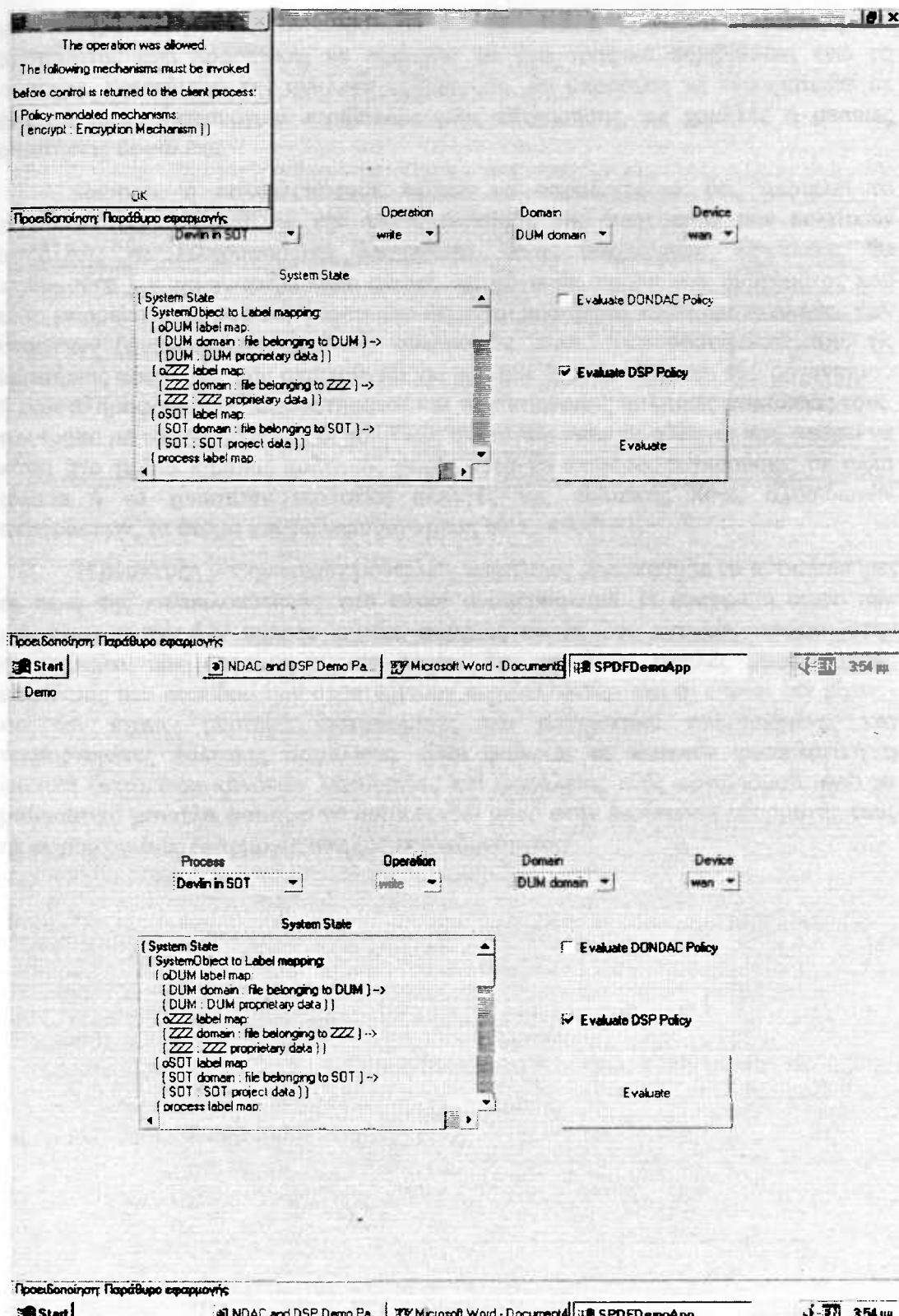
Η ανάγκη για αυτοματοποίηση των πολιτικών ασφάλειας συνδέεται με τις

ακόλουθες εξελίξεις στην περιοχή των Πληροφοριακών Συστημάτων:

1. Καταρχήν μπορούμε να τη δούμε μέσα στο ευρύτερο πλαίσιο που συνθέτει η τάση για αυτοματοποίηση διαδικασιών όλων των γνωστικών περιοχών οι οποίες χαρακτηρίζονται από υψηλή εξειδίκευση (παρόμοιες προσπάθειες έχουν εντοπιστεί στο χώρο του νομικού επαγγέλματος).
2. Οι πολιτικές ασφάλειας των οργανισμών για τα πληροφοριακά τους συστήματα δεν μπορούσαν να παραμείνουν εκτός της αυτοματοποίησης, από τη στιγμή που οι λειτουργίες των οργανισμών οι σχετικές με την πληροφορία -και όχι μόνο- συστηματικά ακολουθούσαν αυτό το δρόμο. Το τελευταίο αυτό γεγονός, σε συνδυασμό με την εκθετική αύξηση των κρουσμάτων προσβολών σε Πληροφοριακά Συστήματα, κάνει επιτακτική την ύπαρξη αυτοματοποιημένης μορφής ελέγχων, επιθεωρήσεων και συνεχών αξιολογήσεων των συστημάτων. Ο σωστός έλεγχος των χαρακτηριστικών ασφάλειας των συστημάτων αυξάνει την εμπιστοσύνη που έχουμε γι' αυτά.
3. Εξάλλου, δεν μπορούμε να παραβλέψουμε ότι ο βέλτιστος τρόπος παρακολούθησης της ασφάλειας ενός αυτοματοποιημένου συστήματος είναι η ενσωμάτωση του συστήματος παρακολούθησης εντός του συστήματος, έτσι ώστε να έχουμε τη δυνατότητα λ.χ. για ελέγχους συνέπειας, κ.λπ.
4. Σε συνάρτηση με την πρώτη μας παρατήρηση στη λίστα αυτή, θα λέγαμε ότι οι περιοχές που παρουσιάζουν υψηλή εξειδίκευση, παρουσιάζουν επίσης υψηλή δύσκολία σε όρους αλληλοεπιδράσεων, συγκρούσεων, πολυπλοκότητας, κάλυψης πλήθους περιπτώσεων και ελέγχου πλήθους στοιχείων. Η αυτοματοποιημένη επεξεργασία των θεμάτων αυτών θα απλοποιούσε το θέμα της διαχείρισής τους σημαντικά και θα βελτίωνε πολύ την ανθρώπινη παρακολούθηση.

Δεν πρέπει να αγνοήσουμε εξάλλου το γεγονός ότι τα περισσότερα (λειτουργικά) συστήματα προσφέρουν υπηρεσίες ή χαρακτηριστικά ασφάλειας, τα οποία όμως δεν είναι ευέλικτα ώστε να προσαρμόζονται<sup>5</sup> στις εκάστοτε ανάγκες. Έτσι, πολλά από αυτά προσφέρονται στην αγορά με τη μορφή έτοιμου προϊόντος, το οποίο δεν μπορεί εύκολα να αλλαχτεί από το χρήστη. Άπτεται επίσης μίας δύσκολης και ευαίσθητης περιοχής της Πληροφορικής, την οποία οι χρήστες συχνά δεν γνωρίζουν. Προκειμένου να λάβουμε μία εικόνα για μία πιθανή λύση, μπορούμε να δώσουμε το παράδειγμα ενός "πακέτου" που αξιολογεί ενέργειες χρηστών σε ένα ή περισσότερα αλληλεπιδρώντα συστήματα [www-1997]. Το ακόλουθο σχήμα δείχνει μία γραφική διεπαφή.

<sup>5</sup> Στην αγγλική απόδοση: "...they are not configurable ..."



**ΣΧΗΜΑ 2.3. Η διεπαφή ενός εργαλείου διαχείρισης πολιτικών ασφάλειας.**

Το σύστημα αυτό αποτελεί μέρος μία ευρύτερης προσπάθειας που ασχολείται

με αναπαράσταση πολιτικών ασφάλειας και υλοποιείται σε JAVA. Η διεπαφή του συστήματος έχει προοπτικές να εξελιχθεί σε ένα γραφικό περιβάλλον, ενώ το σύστημα, υφιστάμενο την ανάλογη αξιολόγηση, θα μπορούσε να ενσωματωθεί σε ένα σύγχρονο λειτουργικό περιβάλλον μίας επιχείρησης, με χαμηλές ή μεσαίες απαιτήσεις ασφάλειας.

Ωστόσο, η πολυπλοκότητα, πρέπει να παραδεχτούμε ότι, αποτελεί το σημαντικότερο κίνητρο για την αυτοματοποίηση της διαχείρισης των πολιτικών ασφάλειας σε Πληροφοριακά Συστήματα. Ένας διαχειριστής ασφάλειας θα επιθυμούσε λ.χ. να γνωρίζει κάθε στιγμή όχι μόνο τα σημεία του συστήματος που είναι επιρρεπή σε προσβολή ή αυτά που δέχονται προσβολή, αλλά και το πλήθος των στοιχείων (φυσικών αντικειμένων, εφαρμογών, κ.λπ.) του συστήματός του, τις απαιτήσεις ασφάλειας που απαιτούνται για το κάθε ένα, τα τμήματα του οργανισμού ή ενός πληροφοριακού υποσυστήματος και τις αντίστοιχες πολιτικές ασφάλειάς τους, τον τρόπο με τον οποίο αυτές οι πολιτικές συνεργάζονται, τις αλλαγές που μπορεί να κάνει στο τμήμα κάποιας πολιτικής χωρίς αυτό να επιφέρει συγκρούσεις σε άλλα σημεία ή να χρειστούν τεράστιες αλλαγές της πολιτικής λόγω αλυσιδωτών αντιδράσεων, τα άτομα και τις υπευθυνότητές τους, κ.λπ<sup>6</sup>.

Η ανάπτυξη μαθηματικών μοντέλων ασφάλειας προσπάθησε να αντιμετωπίσει το θέμα της πολυπλοκότητας, στο οποίο αναφερθήκαμε. Η εφαρμογή όμως των μοντέλων αυτών δεν υπήρξε ευρεία, ακριβώς επειδή δεν ανταποκρίνονταν στην πλειονότητα των οργανισμών, οι οποίοι δεν απαιτούν υψηλές προδιαγραφές ασφάλειας του επιπέδου των στρατιωτικών περιβαλλόντων και οι οποίοι δεν είχαν - και δεν έχουν- αυστηρά διατυπωμένες και μαθηματικά τυποποιημένες και τεκμηριωμένες πολιτικές ασφάλειας. Ετσι φαίνεται σε κάποιον φυσιολογική η λεκτική διατύπωση κανόνων λειτουργίας και ασφάλειας ενός οργανισμού, ενώ τα μαθηματικά μοντέλα φαίνεται να απαιτούνται μόνο στην περίπτωση εφαρμογής τους σε συγκεκριμένες εφαρμογές υψηλής επικινδυνότητας.

<sup>6</sup>Η ορολογία δεν είναι αντηρή σε αυτό το σημείο.

## ΚΕΦΑΛΑΙΟ III

### ΤΥΠΟΠΟΙΗΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



### 3.1 Εισαγωγή

Αντικειμενοστράφεια, Δίκτυα Petri, Χάρτες Δραστηριοτήτων-Ρόλων, Διαγράμματα Ροής Δεδομένων

Στην εισαγωγική αυτή παράγραφο θα προσπαθήσουμε να αποδώσουμε μία ενδεικτική προσέγγιση στην τυποποίηση πολιτικών, η οποία θα φανεί χρήσιμη για πολλά από τα ακόλουθα κεφάλαια εφόσον παρουσιάζει έναν τρόπο σκέψης αναφορικά με την αναπαράσταση Πολιτικών Ασφάλειας. Η αναφορά μας δεν περιορίζεται από την έννοια της "Πολιτικής Ασφάλειας", αλλά προσδιορίζεται περισσότερο από την έννοια της πολιτικής γενικότερα. Αυτό που μας ενδιαφέρει πρωταρχικά είναι η κατανόηση των εννοιολογικών στοιχείων που αναγνωρίζονται ως δομικά στοιχεία μιας πολιτικής. Δευτερεύοντας μπορούμε να παρακολουθήσουμε έννοιες που επικουρούν την προσπάθεια τυποποίησης. Η προσέγγιση στηρίζεται στην αρχή της αντικειμενοστράφειας, η οποία όπως θα δούμε συμφωνεί σε πολλά σημεία με τις απαιτήσεις που θέτουν οι περισσότερες περιπτώσεις.

Στη γενική περίπτωση λοιπόν, μπορούμε να ξεκινήσουμε από την παρατήρηση ότι η συνήθης διατύπωση των πολιτικών είναι σε μορφή κανόνων ή στόχων. Ορίζουμε λοιπόν ένα Αντικείμενο (Object) ως μία τριάδα:

- Πολιτική (policy)
- Φορέας (agent)
- Δραστηριότητα (action)

Στην τριάδα αυτή, η "Πολιτική" είναι ένα αντικείμενο τύπου "Αντικείμενο Πολιτικής" (Policy Object). Οι ιδιότητες (properties) του αντικειμένου αυτού είναι κανόνες, νόμοι, διαδικασίες ή στόχοι και μπορεί να είναι παθητικό (passive), οπότε ελέγχεται από Αντικείμενα τύπου "Αντικείμενο Δραστηριότητας", ή ενεργητικό (active), οπότε ενεργοποιεί ή απενεργοποιεί αντικείμενα τύπου "Αντικείμενο Δραστηριότητας". Οι "πράξεις" του αντικειμένου είναι οι εξής: δημιουργία (creation), προσθήκη (addition), διαγραφή (deletion), και τροποποίηση (modification).

Το αντικείμενο "Φορέας" αντιπροσωπεύει άτομα που εμπλέκονται στην διαχείριση των αντικειμένων τύπου "Αντικείμενο Πολιτικής" ή που αποτελούν μέρος του συστήματος και (οι ιδιότητές τους) μπορεί να είναι:

- απλοί παρατηρητές
- εκτελεστές Δραστηριότητας
- ιδιοκτήτες Δραστηριότητας, έχοντες δικαιώματα επ' αυτής
- δημιουργοί Δραστηριότητας
- πελάτες, που μπορούν να αλλάξουν μία Δραστηριότητα

Τα αντικείμενα τύπου "Αντικείμενο Δραστηριότητας" περιλαμβάνουν ορισμένες δομές (π.χ. φορέας και πολιτική) και διαδικασίες και σηματοδοτούν την έναρξη μίας λειτουργίας με την αποστολή μηνυμάτων μεταξύ των διαφόρων στιγμιοτύπων των αντικειμένων. Οι λειτουργίες είναι περιορισμένες (constrained) από τα αντικείμενα τύπου "πολιτικής". Έτσι, μπορούμε να θεωρήσουμε ότι η λειτουργικότητα αυτού του σχήματος συνίσταται στις σχέσεις αλληλεπίδρασης αντικειμένων, οι οποίες ρυθμίζονται από αντικείμενα τύπου "πολιτικής".

Μετά από αυτή την αρχική αντικειμενοστραφή προσέγγιση στη σύλληψη των

πολιτικών, μπορούμε περαιτέρω να επεκταθούμε χρησιμοποιώντας γραφικές αναπαραστάσεις, προκειμένου να απεικονίσουμε μία πραγματική ροή γεγονότων. Οι τεχνικές που μπορούμε να χρησιμοποιήσουμε περιλαμβάνουν: Διαγράμματα Ροής Δεδομένων (ΔΡΔ, Data Flow Diagrams), Χάρτες Δραστηριοτήτων-Ρόλων (ΧΔΡ, Activity-Role Chart) ή Δίκτυα Petri (Petri Nets). Στην τελευταία περίπτωση, που υπερκαλύπτει τις δύο προηγούμενες, μπορούμε εύκολα να απεικονίσουμε τα στιγμιότυπα των αντικειμένων που θα προσδιορίσουμε ως κόμβους και τα μηνύματα μεταξύ αυτών ως τόξα και να παρακολουθήσουμε ένα πραγματικό σενάριο.

Ο καθορισμός όλων των αντικειμένων τύπου "Δράση" και "Φορέας" και η αναγνώριση των "ιδιοτήτων" και των "μεθόδων" τους είναι μάλλον εύκολη ή τουλάχιστον αρκετά προσιτή. Αν θέλουμε όμως να καλύψουμε όλες τις περιπτώσεις στιγμιότυπων τύπου "πολιτική", θα διαπιστώσουμε ότι χρειάζονται δοκιμές με άπειρα σενάρια έτσι ώστε να διαμορφώσουμε πολιτικές που θα ελέγχουν ομαλά το σύστημα. Η αναγνώριση φυσικά απλών δηλώσεων (του τύπου για παράδειγμα: το αντικείμενο x τύπου y εκτελείται μόνο από στιγμιότυπα αντικειμένων τύπου z), είναι εύκολη. Η αναγνώριση όμως -και κυρίως η προσαρμογή- δηλώσεων υψηλότερου επιπέδου αφαίρεσης σε χαμηλό επίπεδο εφαρμογής είναι μία δύσκολη εργασία η οποία προφανώς απαιτεί κάποιου είδους τεχνική απόδειξης της συνέπειας του σχήματος μετά την ένταξη νέων στοιχείων. Το γεγονός βέβαια ότι το αντικείμενο στραφές σχήμα επιτρέπει την κληρονομικότητα, επικουρεί αυτή την εργασία διότι επιτρέπει εύκολες τροποποιήσεις και προσθήκες στα αντικείμενα χωρίς να χρειάζεται να αλλάξει ριζικά το σχήμα. Η αλυσιδωτές συνέπειες που μπορεί να προκύψουν ελέγχονται εν μέρει από το ίδιο το σχήμα.

## 3.2 Τυποποίηση πολιτικών ασφάλειας με χρήση Βάσεων Κανόνων

Γενικευμένο Πλαίσιο για Έλεγχο Προσπέλασης, Έμπιστη Υπολογιστική Βάση, Έμπειρα Συστήματα, Βάσεις Κανόνων, Μηχανή Μετάθεσης Καταστάσεων

### 3.2.1 Εισαγωγή

Η προσέγγιση που υποστηρίζει την αυτοματοποιημένη διαχείριση των πολιτικών ασφάλειας μέσω της δημιουργίας και διαχείρισης βάσεων κανόνων, παρόμοιων με αυτούς που τα Έμπειρα Συστήματα προτείνουν, είναι μία άποψη που βρίσκει μεγάλη απήχηση, αν κρίνουμε από το πλήθος των προσπαθειών που εντοπίζονται σε αυτό το χώρο. Μάλιστα, ο τρόπος αυτός έχει επεκταθεί γενικότερα στο χώρο της ασφάλειας των Πληροφοριακών Συστημάτων, καλύπτοντας τον μεγάλο τομέα της Ανάλυσης Επικινδυνότητας, ο οποίος, κατά την άποψή μας, έχει να αποκομίσει πολλές ωφέλειες από τη χρήση αυτών των μεθόδων. Η ενότητα αυτή θα αντιμετωπίσει δυο προσπάθειες που χρησιμοποιούν κανόνες για την αυτοματοποίηση πολιτικών ασφάλειας, περιγράφοντας κατ' αντιστοιχία και σε δύο επίπεδα ανάλυσης, αρχικά λεπτομερέστερα και ακολούθως περιληπτικά, τις αρχές που διέπουν αυτές τις προσεγγίσεις.



### 3.2.2 Ένα πλαίσιο για τυποποίηση ασφαλούς συστήματος με χρήση κανόνων

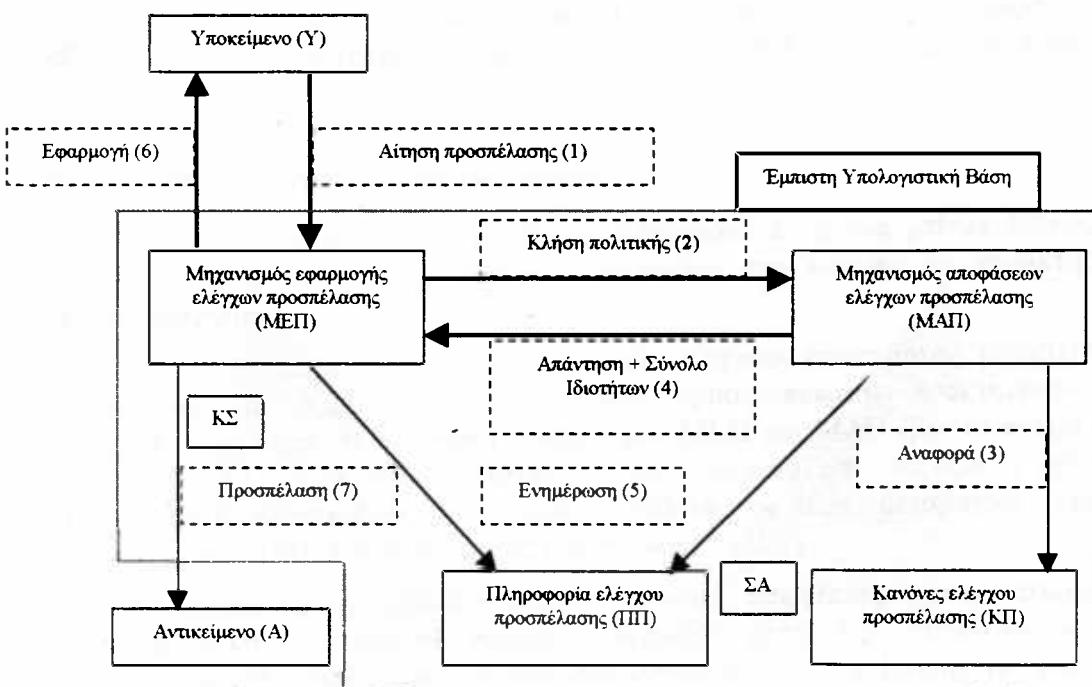
#### 3.2.2.1 Δομικά στοιχεία του πλαισίου

Το έργο με την ονομασία "Γενικευμένο Πλαίσιο για Έλεγχο Προσπέλασης" [LAP-1991] θέτει ως σκοπό του τη δημιουργία μιας τεχνολογίας η οποία θα επιτρέπει τη βέλτιστη αποδοτικότητα από τη χρήση ασφαλών συστημάτων, μέσω της ενσωμάτωσης και εφαρμογής πολλών πολιτικών ασφάλειας, και ιδιαίτερα Πολιτικών Περιορισμών Προσπέλασης (Access Control Restriction Policies), σε ένα και μόνο σύστημα.

Τα βασικά συνθετικά στοιχεία του πλαισίου αυτού είναι τα ακόλουθα:

- **Υποκείμενα (Subjects) – Αντικείμενα (Objects):** πρόκειται για τις οντότητες από τις οποίες αποτελείται το σύστημα.
- **Ιδιότητες (Properties):** περιγράφουν χαρακτηριστικά των υποκειμένων και αντικειμένων. Το σύστημα θα βασίσει τις αποφάσεις του για προσπέλαση σε αυτές τις ιδιότητες. Παραδείγματα ιδιοτήτων αποτελούν τα εξής: τύπος αντικειμένου, πεδίο διαδικασίας, ταυτότητα ιδιοκτήτη, επίπεδο ασφάλειας, κ.λπ.
- **Εξουσιοδότηση (Authority):** μία εξουσιοδοτημένη οντότητα ορίζει πολιτικές ασφάλειας.
- **Κανόνες (Rules):** ένα σύνολο τυποποιημένων εκφράσεων το οποίο καθορίζει τις αποφάσεις αναφορικά με τον έλεγχο προσπέλασης, αντανακλώντας τις πολιτικές ασφάλειας του συστήματος.

Τα βασικά συνθετικά στοιχεία του πλαισίου παρουσιάζονται δομικά από το ακόλουθο σχήμα:



ΣΧΗΜΑ 3.1. Το γενικευμένο Πλαίσιο για Έλεγχο Προσπέλασης.

ΠΗΓΗ: [LAP-1991]

Όπως παρατηρούμε, το σύστημα διαχωρίζεται σε δύο κύρια μέρη: α)Στο κυρίως σύστημα (ΚΣ), το οποίο θεωρείται ότι περιγράφει τη συμπεριφορά του συστήματος σε όρους κανόνων λειτουργίας, αντιπροσωπεύεται από τον "Μηχανισμό Εφαρμογής των Ελέγχων Προσπέλασης" (ΜΕΠ) και μοντελοποιείται σαν μία αφηρημένη μηχανή μεταβάσεων κάταστασης, όπου οι κανόνες λειτουργίας ορίζουν έγκυρες μεταθέσεις του συστήματος και β)Στο σύστημα ασφάλειας (ΣΑ) το οποίο θεωρείται ότι περιέχει τις πολιτικές ασφάλειας του συστήματος σε όρους κανόνων προσπέλασης, αντιπροσωπεύεται από το "Μηχανισμό Αποφάσεων Ελέγχων Προσπέλασης" (ΜΑΠ) και μοντελοποιείται σαν μία βάση κανόνων.

Τα δύο αυτά τμήματα, ΜΕΠ και ΜΑΠ, επικοινωνούν μεταξύ τους με μία διεπαφή η οποία πρέπει τυπικά να οριστεί. Για κάθε κανόνα λειτουργίας της μηχανής καταστάσεων, ο οποίος αντιστοιχεί σε μία κλήση συστήματος, καλείται μία συνάρτηση "Κανόνες\_Πρόσβασης" (στην οποία θα αναφερόμαστε ως *Access\_Rules*) η οποία είναι αυτή που προσπελαύνει το ΜΑΠ και ακολούθως τους Κανόνες της Βάσης. Συγκεκριμένα, η προσπέλαση γίνεται μέσω των παραμέτρων της συνάρτησης αυτής. Οι παράμετροι αυτές αποτελούν την "Πληροφορία Ελέγχου Προσπέλασης". Ο τυπικός ορισμός των "κανόνων πρόσβασης" και των έγκυρων παραμέτρων τους αποτελεί τον ορισμό της διεπαφής.

Ο όρος "πολιτική ασφάλειας" για το συγκεκριμένο πλαίσιο έχει την έννοια των δηλώσεων πολιτικής ασφάλειας είτε με τη μορφή τυπικών μοντέλων, είτε με τη μορφή αποσπασματικών δηλώσεων πολιτικών ασφάλειας, είτε με τη μορφή αποσπασματικών ημιτυπικών μοντελοποιήσεων πολιτικών ασφάλειας, όπως θα διαπιστώσουμε στα ακόλουθα.

Πρέπει να σημειώσουμε στο σημείο αυτό ότι το επίπεδο αφαίρεσης των οποίο επιλέγει το παρόν πλαίσιο είναι μάλλον χαμηλός και η άποψη αυτή θα τεκμηριωθεί περαιτέρω στην ανάλυση που ακολουθεί. Επί του παρόντος χρειάζεται να αναφέρουμε ότι η ακόλουθη περιγραφή αφορά ένα UNIX V λειτουργικό σύστημα (βλ. [LAP-1991]).

### 3.2.2.2 Συντακτικοί συμβολισμοί και σημασιολογία

Η γλώσσα που το πλαίσιο αυτό χρησιμοποιεί είναι ένα μείγμα διαφόρων τύπων συμβολισμών και σημασιολογίας, στοιχείων που κάποιος θα χαρακτηρίζει μάλλον **εμπειρικά**.

Πιο συγκεκριμένα, ένα σύνολο εντολών, κλήσεων συστήματος, μεταβλητών συστήματος και παραμέτρων του UNIX χρησιμοποιείται προκειμένου να μοντελοποιηθεί μέρος της διεπαφής μεταξύ των ΜΕΠ και ΜΑΠ (βλ. το σχήμα της παράγρ. 3.2.2.1). Ένα σύνολο αιτήσεων αποτελούμενο από παρόμοιες εντολές δημιουργείται προκειμένου να αναπαρασταθούν σε ένα μεταβατικό στάδιο αφαίρεσης οι κλήσεις του συστήματος (βλ. παράγρ.3.2.2.3).

Προκειμένου να μοντελοποιηθούν έννοιες ασφάλειας, χρησιμοποιούνται συμβολισμοί και σημασιολογία ευρέως διαδεδομένα (όπως λ.χ. επίπεδο ασφάλειας, κυριαρχία επιπέδου ασφάλειας επί επιπέδου ασφάλειας, κ.λπ.). Επίσης για τον ίδιο σκοπό ορίζονται νέα κατηγορήματα για τη συγκεκριμένη λογική (βλ. παράγρ. 3.2.2.4).



Τέλος, χρησιμοποιείται ένα είδος προγραμματιστικής γλώσσας υψηλού επιπέδου (ψευδοκώδικας) προκειμένου να εκφραστούν οι κανόνες.

Θεωρείται δε, ότι το επίπεδο το οποίο αυτή η λογική παρέχει βρίσκεται πολύ κοντά στην υλοποίηση, καθώς η άποψη των συγγραφέων [LAP-1991] υποστηρίζει ότι τα μοντέλα που ο αναλυτής χτίζει για τέτοιους είδους σκοπούς πρέπει να είναι τόσο αφαιρετικά, όσο δεν θα επιτρέπουν μεγάλο βαθμό επικινδυνότητας για αγνόηση από τον σχεδιαστή σημαντικών λεπτομερειών υλοποίησης.

### 3.2.2.3 Περιγραφή της διεπαφής

Η διεπαφή υλοποιεί, όπως είπαμε, την επικοινωνία μεταξύ ΜΕΠ και ΜΑΠ.

Η "Πληροφορία Ελέγχου Προσπέλασης" μπορεί να περιλαμβάνει τα ακόλουθα δεδομένα (δίδονται σε αφαιρετική μορφή και πρέπει να αντιστοιχηθούν σε δεδομένα συστήματος): File (Αρχείο), Directory (Κατάλογος), Interprocess Communication Data (icd, Δεδομένα αποθηκευτικών δομών του συστήματος για επικοινωνία διεργασιών, π.χ. σηματοφορείς), System Control Data (scd, Δεδομένα αποθηκευτικών μεταβλητών ελέγχου του συστήματος, π.χ. inode).

Οι αιτήσεις που συνθέτουν τη διεπαφή και "κουβαλούν" την παραπάνω πληροφορία είναι συνοπτικά<sup>7</sup> οι εξής:

ALIAS(process, file)	ALTER(process, icd)
CHANGE_OWNER(process, scd(file/directory))	CHANGE_ROLE(process, role attribute, role value)
CLONE(process1, process2)	CREATE(process, file/directory, scd, icd)
DELETE_DATA(process, file)	GET_PERMISSIONS_DATA(process, scd(file/directory))
GET_STATUS_DATA(process, scd(file/directory))	MODIFY_ACCESS_DATA(process, scd(file/directory))
MODIFY_ATTRIBUTE(process, user/process/object, attribute, value)	MODIFY_PERMISSIONS_DATA(process, scd(file/directory))
READ(process, directory)	READ_ATTRIBUTE(process, user/process/object, attribute)
READ&WRITE_OPEN(process, file/icd)	READ_OPEN(process, file)
SEARCH(process, directory)	SEND_SIGNAL(process1, process2)
TERMINATE(process)	TRACE(process1, process2)
WRITE(process, directory)	WRITE_OPEN(process, file)

ΠΗΓΗ: [LAP-1991]

<sup>7</sup> Ο αναγνώστης πρέπει να έχει σχετική εξοικείωση με θέματα Λειτουργικών Συστημάτων προκειμένου για την κατανόηση αυτών των εννοιών.

### 3.2.2.4 Κανόνες λειτουργίας της αφηρημένης μηχανής μετάθεσης καταστάσεων

Οι κανόνες λειτουργίας της αφηρημένης μηχανής μετάθεσης κατάστασης πρέπει να καλύπτουν το σύνολο των κλήσεων συστήματος και στην περίπτωσή μας είναι οι ακόλουθοι:

Open, Read, Fork, Create, Execute, Kill, Unlink

και αντιστοιχούν σε σχετικές κλήσεις συστήματος (βλ. [LAP-1991] και [KAB-1995]). Η επιλογή του είδους της αντιστοίχισης, αν δηλαδή θα είναι ένα-προς-ένα προς τις κλήσεις του συστήματος, οπότε επιλέγεται κάποιος υψηλός βαθμός λεπτομέρειας, ή πολλά-προς-ένα, οπότε αυξάνεται ο βαθμός κατανόησης του παραγόμενου μοντέλου, είναι μία σχεδιαστική επιλογή που αφορά το επίπεδο αφαίρεσης που θέλει να έχει ο αναλυτής.

### 3.2.2.5 Κανόνες προσπέλασης της βάσης κανόνων

Προκειμένου να οριστούν οι κανόνες, μία ακολουθία βημάτων πρέπει να ολοκληρωθεί ως εξής:

#### ⇒ BHMA 1: Επιλογή των πολιτικών ασφάλειας που θα υλοποιηθούν

Το πρώτο βήμα στον καθορισμό των κανόνων είναι η επιλογή των πολιτικών ασφάλειας που θέλουμε να ενσωματώσουμε στο σύστημά μας. Για τους σκοπούς αυτής της παρουσίασης επιλέγουμε τις ακόλουθες δύο πολιτικές ασφάλειας:

- Την παραδοσιακή 'MAC' (Mandatory Access Control Policy, Πολιτική Υποχρεωτικού Ελέγχου Προσπέλασης), η οποία έχει ως βάση της την απόδοση επιπέδων ασφάλειας για την παροχή εξουσιοδοτήσεων σε αντικείμενα τύπου <scd/icd/file/directory> και
- Μία άτυπη "Πολιτική Λειτουργικού Ελέγχου" (Functional Control Policy), η οποία υλοποιεί ένα είδος ελέγχου προσπέλασης βασισμένου σε ρόλους χρηστών. Υποστηρίζονται οι ρόλοι: διαχειριστής συστήματος, διαχειριστής ασφάλειας και χρήστης. Τα αντικείμενα του συστήματος έχουν τη διαβάθμιση: γενικού τόπου, τόπου συστήματος και τόπου ασφάλειας.

#### ⇒ BHMA 2: Καθορισμός Πληροφορίας Ελέγχου Προσπέλασης

Προκειμένου να περιγράψουμε τις παραπάνω πολιτικές χρειάζεται να καθορίσουμε τη διεπαφή με την οποία οι παραπάνω κανόνες λειτουργίας επικοινωνούν με το "Μηχανισμό Αποφάσεων Ελέγχων Προσπέλασης" και ειδικότερα τα είδη της "Πληροφορίας Ελέγχου Προσπέλασης" που οι αιτήσεις προσπέλασης πρέπει να μεταφέρουν:

Πληροφορία Ελέγχου Προσπέλασης για έναν χρήστη	Πληροφορία Ελέγχου Προσπέλασης για μία διαδικασία	Πληροφορία Ελέγχου Προσπέλασης για ένα αντικείμενο
Τεκμήρια προσπέλασης χρήστη (MAC)	Ιδιοκτήτης (δείκτης στο αναγνωριστικό διαδικασίας, επίπεδο ασφάλειας χρήστη, τύπο διαδικασίας)	Επίπεδο ασφάλειας (MAC)
Ρόλος χρήστη (FCP)		Κατηγορία αντικειμένου (FCP)  Τύπος αντικειμένου (MAC) ΠΗΓΗ: [LAP-1991]

### Θ ΒΗΜΑ 3: Αρχική διαμόρφωση κανόνων MAC σε μορφή μήτρας

Οι κανόνες που απαιτούνται για την εφαρμογή της MAC πολιτικής ασφάλειας σε αρχική μορφή είναι<sup>8</sup>:

ΑΝΤΙΚΕΙΜΕΝΑ ΤΥΠΟΥ *file*

ΑΙΤΗΣΗ	ΠΡΟΫΠΟΘΕΣΗ ΠΡΟΣΠΕΛΑΣΗΣ
CREATE	O set equal to P
DELETE	P=O
DELETE DATA	P=O
EXECUTE	P>=O
READ	-
READ OPEN	P>=O
READ&WRITE-OPEN	P=O
WRITE	-
WRITE-OPEN	P=O

ΠΗΓΗ: [LAP-1991]

ΑΝΤΙΚΕΙΜΕΝΑ ΤΥΠΟΥ *icd*

ΑΙΤΗΣΗ	ΠΡΟΫΠΟΘΕΣΗ ΠΡΟΣΠΕΛΑΣΗΣ
ALTER	P=O
CREATE	O set equal to P
DELETE	P=O
READ	-
WRITE	-
READ&WRITE OPEN	P=O

ΠΗΓΗ: [LAP-1991]

<sup>8</sup> Ο συμβολισμός “Ο” αντιπροσωπεύει το επίπεδο ασφάλειας του αντικειμένου, ενώ ο συμβολισμός “P/P1/P2” το επίπεδο ασφάλειας της διαδικασίας

**ΑΝΤΙΚΕΙΜΕΝΑ ΤΥΠΟΥ *directory***

ΑΙΤΗΣΗ	ΠΡΟΫΠΟΘΕΣΗ ΠΡΟΣΠΕΛΑΣΗΣ
CREATE	O set equal to P
DELETE	P=0
READ	P>=0
SEARCH	P>=0
WRITE	P=0

ΠΗΓΗ: [LAP-1991]

**ΑΝΤΙΚΕΙΜΕΝΑ ΤΥΠΟΥ *scd***

ΑΙΤΗΣΗ	ΠΡΟΫΠΟΘΕΣΗ ΠΡΟΣΠΕΛΑΣΗΣ
CHANGE OWNER	P=0
CREATE	O set equal to P
DELETE	P=0
GET PERMISSIONS DATA	P>=0
GET STATUS DATA	P>=0
GET PERMISSIONS DATA	P=0
MODIFY ACCESS DATA	P=0

ΠΗΓΗ: [LAP-1991]

**ΔΙΑΧΕΙΡΙΣΗ ΔΙΕΡΓΑΣΙΩΝ**

ΑΙΤΗΣΗ	ΠΡΟΫΠΟΘΕΣΗ ΠΡΟΣΠΕΛΑΣΗΣ
CLONE	P2 set equal to P1
SEND SIGNAL	P1=P2

ΠΗΓΗ: [LAP-1991]

Η συμβατότητα μεταξύ ρόλων χρηστών και διαβαθμίσεων των αντικειμένων του συστήματος ορίζεται ως εξής:

R=χρήστης	συμβατότητα με	C=γενικός τύπος
R=διαχειριστής συστήματος	συμβατότητα με	C=γενικός τύπος & C=τύπος συστήματος
R=διαχειριστής ασφάλειας	συμβατότητα με	C=γενικός τύπος & C=τύπος ασφάλειας

ΠΗΓΗ: [LAP-1991]

**Σ ΒΗΜΑ 5: Καθορισμός στοιχείων συντακτικού και σημασιολογίας**

Κάθε πολιτική υλοποιείται με έναν ή περισσότερους κανόνες. Κάθε κανόνας είναι μία έκφραση που έχει μία από τις ακόλουθες τιμές:

ΤΙΜΗ KANONA	ENNOIA ΤΙΜΗΣ KANONA
YES	Η αίτηση μπορεί να ικανοποιηθεί.
NO	Η αίτηση δεν μπορεί να ικανοποιηθεί.
DC	Η αίτηση ικανοποιείται χωρίς ο μηχανισμός εφαρμογής της πολιτικής να χρειάζεται να κάνει τους συνήθεις ελέγχους. Χρήσιμα δεδομένα επίσης παράγονται.
UNDEFINED	Η αίτηση δεν αναγνωρίστηκε και δεν ικανοποιείται. Χρήσιμα δεδομένα επίσης παράγονται.

ΠΗΓΗ: [LAP-1991]

Προκειμένου να ορίσουμε το αποτέλεσμα της συνάρτησης *Access\_Rules* χρειαζόμαστε τον τελεστή «+», οποίος ορίζεται ως εξής:

ΟΡΙΣΜΑ1	ΟΡΙΣΜΑ2	ΟΡΙΣΜΑ1+ΟΡΙΣΜΑ2
YES	YES	YES
YES	NO	NO
YES	DC	YES
YES	UNDEFINED	UNDEFINED
NO	YES	NO
NO	NO	NO
NO	DC	NO
NO	UNDEFINED	UNDEFINED
DC	YES	YES
DC	NO	NO
DC	DC	DC
DC	UNDEFINED	UNDEFINED
UNDEFINED	YES	UNDEFINED
UNDEFINED	NO	UNDEFINED
UNDEFINED	DC	UNDEFINED
UNDEFINED	UNDEFINED	UNDEFINED

ΠΗΓΗ: [LAP-1991]

Προκειμένου να ορίσουμε τους κανόνες για την πολιτική MAC χρειαζόμαστε τους ακόλουθους τελεστές:

(level1)Equals(level2)	TRUE αν το level1 ισούται με το level2 FALSE διαφορετικά
(level1)Dominates(level2)	TRUE αν το level1 κυριαρχεί του level2 FALSE διαφορετικά

ΠΗΓΗ: [LAP-1991]

## ⇒ BHMA 6: Ορισμός της συνάρτησης *Access\_Rules*

Η συνάρτηση *Access\_Rules* έχει την ακόλουθη μορφή:

**Access\_Rules(request(input argument), process/object(input argument), ..., process/object(input argument)):**  
**Function\_value=MAC+FCP:**  
**IF Function\_value is UNDEFINED**  
**THEN**  
System-error  
**ELSE**  
Return(Function\_value);

ΠΗΓΗ: [LAP-1991]

## ⇒ BHMA 7: Ορισμός γενικής μορφής κανόνα

Ένας Κανόνας Προστέλασης έχει την ακόλουθη γενική μορφή:

**POLICY <- (POLICY RULE)**

\* Ο συμβολισμός **POLICY <- (POLICY RULE)** σημαίνει ότι η μεταβλητή POLICY θα πάρει την τιμή της έκφρασης στην παρένθεση\*/

**POLICY RULE:**

**SELECT CASE request**

**CASE request, request, ..., request**

Statement block

**CASE request, request, ..., request**

Statement block

**END SELECT**

ΠΗΓΗ: [LAP-1991]

## ⇒ BHMA 8: Κανόνες για την πολιτική MAC

Οι κανόνες για την πολιτική ασφάλειας MAC είναι οι ακόλουθοι:

**MAC ← (MAC Rule 1)**

**MAC Rule 1:**

**SELECT CASE request**

**CASE alias**

return (DC);

**CASE alter**

**SELECT CASE object-type[object]**

**CASE ipc**

**IF**

Security-level[process] equals security-level[object]

**THEN**

return(YES);

**ELSE**

return(NO);

**CASE ELSE**

return(UNDEFINED);



CASE clone

    return(set-attribute(security-level[process2], security-level[process1]):YES);

CASE create

    return(set-attribute(security-level[object], security-level[process]):YES);

CASE execute

SELECT CASE object-type[object]

    CASE file

        IF

            Security-level[process] dominates security-level[object]

        THEN

            return(YES);

        ELSE

            return(NO);

CASE ELSE

    return(UNDEFINED);

CASE modify-attribute("arguments are process, qualifier, attribute, value")

SELECT CASE qualifier[input argument]

CASE user

    IF

        Security-level[process] equals access-approvals[user pointed to by qualifier]

    THEN

        SELECT CASE attribute[input argument]

        CASE access-approvals

    IF

        System-role[user pointed to by owner[process]] equals security-officer

    THEN

        return(YES);

    ELSE

        return(NO);

CASE ELSE

    return(YES);

ELSE

    return(NO);

CASE process

SELECT CASE attribute[input argument]

CASE security-level

    return(NO);

CASE ELSE

    IF

        Security-level[process] equals security-level[process pointed to by qualifier]

    THEN

        return(YES);

    ELSE

        return(NO);

CASE object

    IF

        Security-level[process] equals security-level[object pointed to by qualifier]

    THEN

        SELECT CASE attribute[input argument]

        CASE access-approvals

    IF

        System-role[user pointed to by owner[process]] equals security-officer

    THEN

```
return(YES);
ELSE
return(NO);
CASE ELSE
    return(YES);
ELSE
    return(NO);
CASE ELSE
    return(UNDEFINED);
CASE read
SELECT CASE object-type[object]
CASE directory
    IF
        Security-level[process] dominates security-level[object]
    THEN
        return(YES);
    ELSE
        return(NO);
CASE file,ipc
    return(DC);
CASE ELSE
    return(UNDEFINED);
CASE read-open
SELECT CASE object-type[object]
CASE file
    IF
        Security-level[process] dominates security-level[object]
    THEN
        return(YES);
    ELSE
        return(NO);
CASE ELSE
    return(UNDEFINED);
CASE read&write-open
SELECT CASE object-type[object]
CASE file, ipc
    IF
        Security-level[process] equals security-level[object]
    THEN
        return (YES);
    ELSE
        return(NO);
CASE ELSE
    return(UNDEFINED);
CASE write-open
SELECT CASE object-type[object]
CASE file
    IF
        security-level[object] equals security-level[process];
    THEN
        return(YES);
    ELSE
        return(NO);
```

**CASE ELSE**

return(UNDEFINED);

**CASE change-owner, change-role, delete, delete-data, get-permissions-data, get-status-data, modify-access-data, modify-permissions-data, read-attribute, search, send-signal, terminate, trace, write**

/\*Return is omitted as it should be specified differently in each CASE \*/

**CASE ELSE**

return(UNDEFINED);

**END SELECT**

ΠΗΓΗ: [LAP-1991]

**⇒ BHMA 9: Κανόνες για την πολιτική FCP**

Οι κανόνες για την πολιτική ασφάλειας FCP είναι οι ακόλουθοι:

**FC ← (FC Rule 1)**

**FC Rule 1:**

**SELECT CASE request**

**CASE alias, alter, change-owner, create, delete, delete-data, execute, get-permissions-data, get-status-data, modify-access-data, modify-permissions-data, read, read&write-open, red-open, search, write, write-open**

**IF**

(system-role[user pointed to by owner[process]] is user **AND** object-category[object] is general)

**OR**

(system-role[user pointed to by owner[process]] is administrator **AND** object-category[object] is system or general)

**OR**

(system-role[user pointed to by owner[process]] is security-officer **AND** object-category[object] is security or general)

**OR**

(system-role[user pointed to by owner[process]] is daemon AND object-category[object] is system or general)

**THEN**

return(YES);

**ELSE**

return(NO);

**CASE clone, read-attribute, send-signal, terminate, trace**

return(YES);

/\*nextCASEs omitted\*/

**CASE ELSE**

return(UNDEFINED);

**END SELECT**

ΠΗΓΗ: [LAP-1991]

Όπως μπορούμε να παρατηρήσουμε, απαιτείται κάποια εξοικείωση με τη σημασιολογία των πολιτικών που υλοποιούνται. Η παρούσα προσπάθεια ασχολείται μεν με την υποστήριξη της διαχείρισης πολλών πολιτικών ασφάλειας (στη σχετική αναφορά μπορούμε να παρακολουθήσουμε αντίστοιχες διαδικασίες για την πολιτική των Clark&Wilson, κλ.π.), αλλά δεν αντιμετωπίζει το θέμα της ταυτόχρονης υποστήριξης περισσότερων πολιτικών ασφάλειας.

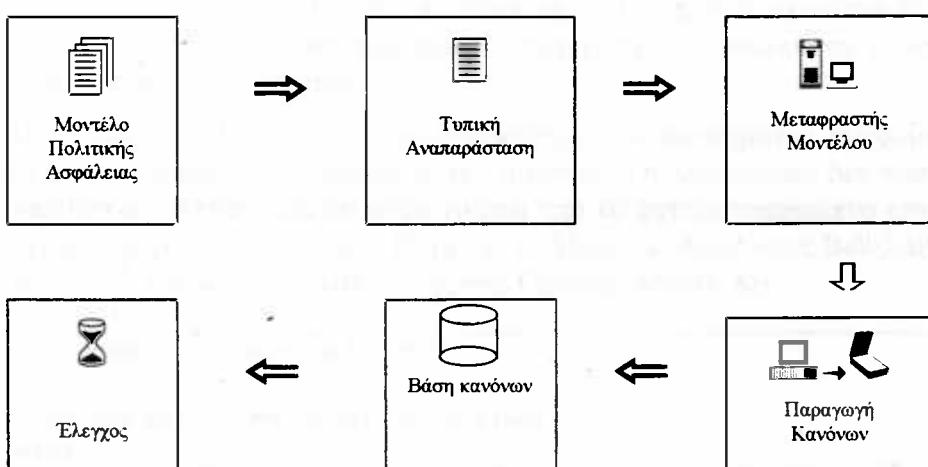


### 3.2.3 Μία αυτοματοποιημένη μέθοδος παραγωγής βάσεων κανόνων για πολιτικές ασφάλειας

Στην παράγραφο αυτή θα παρουσιάσουμε τις προδιαγραφές και την λειτουργικότητα ενός αυτοματοποιημένου περιβάλλοντος για διαχείριση πολιτικών ασφάλειας με χρήση βάσεων κανόνων. Η προσπάθεια αποτέλεσε μέρος μίας ευρύτερης η οποία αποσκοπούσε στη δημιουργία Έμπιστων Υπολογιστικών Βάσεων (Trusted Computing Bases, TCBs), βασισμένων σε κανόνες, έτσι ώστε να είναι δυνατή η ύπαρξη διαφόρων εναλασσόμενων πολιτικών ασφάλειας, αντιπροσωπευόμενων από αντίστοιχες βάσεις κανόνων.

Η δημιουργία των κανόνων είναι αυτοματοποιημένη σε κάποιο βαθμό μέσω του "Περιβάλλοντος Ανάπτυξης Μοντέλων Ασφάλειας SMDE" (Security Model Development Environment) [PAG-1989]. Οι απαιτούμενες διαδικασίες, που προηγούνται της παραγωγής της βάσης των κανόνων από το αυτοματοποιημένο περιβάλλον, περιλαμβάνουν καταρχήν την επιλογή του μοντέλου -πολιτικής- ασφάλειας. Η συγκεκριμένη μέθοδος απαιτεί την επιλογή μοντέλων που στηρίζονται στην αναπαράσταση του ασφαλούς συστήματος, ή μπορούν να μεταβληθούν ώστε να αναπαρίστανται κατ' αυτό τον τρόπο, ως μίας μηχανής πεπερασμένων καταστάσεων, όπου υπάρχουν ασφαλείς καταστάσεις και μεταβάσεις καταστάσεων από ασφαλή στάδια. Η μέθοδος απαιτεί επίσης όπως το μοντέλο δεν είναι υψηλής αφαιρετικότητας, ακριβώς επειδή αποδίδει μεγάλη σημασία σε απόψεις λειτουργικότητας. Έτσι προϋποτίθεται ότι το υπάρχον μοντέλο πρέπει να τροποποιηθεί κατά τρόπο που είναι δυνατή η αναπαράστασή του σε μορφή συμβατή με τις παραπάνω απαιτήσεις. Χρειάζεται βέβαια η απαραίτητη εξοικείωση με το αυτοματοποιημένο περιβάλλον προκειμένου να είμαστε σε θέση να προδιαγράψουμε επακριβώς τις απαραίτητες προϋποθέσεις.

Τα στάδια της διαδικασίας παραγωγής των κανόνων παρουσιάζονται γραφικά στο παρακάτω σχήμα:



ΣΧΗΜΑ 3.2. Η διαδικασία παραγωγής των κανόνων.

'Όπως μπορούμε να παρατηρήσουμε, το Μοντέλο της Πολιτικής Ασφάλειας πρέπει πρώτα να εκφραστεί σε μία κοινή γλώσσα. Η γλώσσα αυτή περιλαμβάνει γενικά τρεις δομές αναπαράστασης: τις Δομές Δεδομένων, τους Περιορισμούς και τις Λειτουργίες. Μπορούμε να φανταστούμε τις Δομές Δεδομένων παρόμοιες με αυτές πολλών προγραμματιστικών γλωσσών (κλασικά σε όρους τύπων και μεταβλητών). Για παράδειγμα η Μήτρα Προσπέλασης του Μοντέλου Ασφάλειας Bell-LaPadula σε Δομή Δεδομένων του παρόντος πλαισίου έχει ως εξής:

```
/*types definitions*/  
type Accesses is (read, write, append, execute);  
type Access_Set is set of Accesses;  
type Access_Matrices is  
Array from Subjects, Objects to Access_Set;  
/*variable declaration*/  
Current_access: Access_Matrices;
```

ΠΗΓΗ: [PAG-1989]

Οι Περιορισμοί αντιπροσωπεύουν τις ιδιότητες ασφάλειας του μοντέλου. Διαχωρίζονται δε σε στατικούς και δυναμικούς. Οι στατικοί είναι πάντοτε αληθείς, όπως για παράδειγμα η Απλή Ιδιότητα Ασφάλειας του Μοντέλου Bell-LaPadula:

```
static constraint Simple_Security_Property is  
begin  
/*for every subject and object it must hold that*/  
for all sub:Subjects; ob:Objects  
/*if there holds access between them*/  
(read in Current_Access (sub,ob) or  
write in Current_Access (sub,ob)) →  
/*then it is implied that the security level of the subject dominates that of the object*/  
Current_Security_Label (sub) >= Security_Label (ob);  
end Simple_Security_Property;
```

ΠΗΓΗ: [PAG-1989]

Οι δυναμικοί περιορισμοί αφορούν τις μεταβάσεις καταστάσεων και πρέπει να ικανοποιούνται προκειμένου να διατηρείται η ασφάλεια του συστήματος. Έτσι, μπορούμε να καταλάβουμε ότι συνήθως αυτοί οι περιορισμοί συγκρίνουν τις τιμές μεταβλητών και εξετάζουν το αποτέλεσμα της σύγκρισης με αναφορά σε γνώση που αφορά τη συγκεκριμένη μετάβαση.

Οι Λειτουργίες αφορούν τη λειτουργικότητα του συστήματος αναφοράς και ουσιαστικά περιγράφουν τις μεταβάσεις της μηχανής. Οι λειτουργίες δεν περιέχουν έλεγχο υποθέσεων. Υποτίθεται ότι αυτό γίνεται από το αυτοματοποιημένο εργαλείο. Ας περιγράψουμε τη λειτουργία Get\_Read για το Μοντέλο Ασφάλειας Bell-LaPadula, ως πρόσθεση του δικαιώματος ανάγνωσης στο Current\_Access\_Set:

```
operation Get_Read (user:Subjects; ob:Objects);  
begin  
Current_Access(user,ob):=Current_Access(user,ob) + read;  
end Get_Read;
```

ΠΗΓΗ: [PAG-1989]

Αφού λοιπόν περιγράψουμε σωστά το μοντέλο μας, το εισάγουμε στο Μεταφραστή ο οποίος αποθηκεύει την αναπαράσταση σε δέντρο. Το επόμενο βήμα



αφορά την παραγωγή των κανόνων για κάθε Λειτουργία και διεξάγεται από αυτοματοποιημένο εργαλείο επίσης. Ο τρόπος με τον οποίο παράγεται κάποιος κανόνας είναι βασικά ο ακόλουθος: οι άλλαγές που η εκτέλεση κάθε λειτουργίας συνεπάγεται ελέγχονται σε αντιπαράθεση με τους περιορισμούς, ώστε να καθοριστούν οι συνθήκες που πρέπει να ικανοποιούνται, προκειμένου το σύστημα να μην μεταπέσει σε μη-ασφαλή κατάσταση. Για το παράδειγμα της λειτουργίας Get\_Read που δώσαμε προηγουμένως, ο κάνονας θα ήταν ο εξής:

```
function GET_READ_RULE (user:Subjects;ob:Objects) return boolean is
/*the following means that user may attain read access to ob if his security level dominates that of the
ob and he has the necessary discretionary access rights*/
begin
/*this is from the Simple_Security_Property constraint*/
Dominates (Current_Security_Level(user), Security_Level(ob))
and
/*this is from the Discretionary_Security_Property constraint*/
Member_of(read, access_permission(user,ob));
end GET_READ_RULE;
```

ΠΗΓΗ: [PAG-1989]

Η βάση των κανόνων μετά από αυτή τη διαδικασία έχει ολοκληρωθεί. Η βάση αυτή πρέπει να ολοκληρωθεί με μία ειδικά σχεδιασμένη TCB, έναν πυρήνα δηλαδή. Προκειμένου να εξεταστεί η συνέπεια του σχήματος που έχει προκύψει, υπάρχει ένα αυτοματοποιημένο εργαλείο προσομείωσης το οποίο επιτρέπει τον έλεγχο της βάσης με εκτέλεση σεναρίων. Ένα σενάριο περιγράφει στην κοινή γλώσσα μία αρχική διάρθρωση συστήματος και ακολουθώς παρουσιάζει ορισμένες αιτήσεις που σε μία πραγματική κατάσταση θα έδινε ένας χρήστης. Ο σκοπός είναι να παρουσιαστεί ο τρόπος με τον οποίο οι αιτήσεις αυτές, που μεταφράζονται σε κλήσεις του συστήματος, προκαλούν καλέσματα του πυρήνα που δημιουργήθηκε και των κανόνων που αυτός περιέχει.

Πρέπει να σημειώσουμε ότι απαιτούνται διαδοχικές δοκιμές και προσαρμογές του εκάστοτε μοντέλου προκειμένου να επιτευχθεί πλήρης συμβατότητα των απαιτήσεων που το πλαίσιο θέτει και της λειτουργικότητας που το μοντέλο υποστηρίζει.

### 3.3 Τυποποίηση πολιτικών ασφάλειας με έμφαση στις λειτουργικές απαιτήσεις των χρηστών

Απαιτήσεις Ασφάλειας, Μοντέλο Δράσης, Αντικειμενοστράφεια, Τυπικές Μέθοδοι Ορισμού Απαιτήσεων, Ροή Πληροφορίας

#### 3.3.1 Εισαγωγή

Είναι γενικά αποδεκτό ότι η ανάπτυξη ασφαλών συστημάτων βασίζεται σε κάποια μία μεθοδολογία η οποία λαμβάνει υπόψη της τον καθορισμό των απαιτήσεων ασφάλειας για το συγκεκριμένο περιβάλλον από τους εκάστοτε χρήστες αυτού. Εντούτοις, οι υπάρχοντες τρόποι με τους οποίους η ασφάλεια εντάσσεται σε ένα σύστημα ακολουθούν μάλλον την εξής προσέγγιση: τα υπάρχοντα μοντέλα πολιτικών ασφάλειας Πληροφοριακών Συστημάτων εντάσσονται στο υπολογιστικό



σύστημα χωρίς να αποδίδεται προσοχή στην ασφάλεια του πληροφοριακού συστήματος.

Σύμφωνα με κάποια άλλη προσέγγιση, η ένταξη ασφάλειας σε ένα πληροφοριακό σύστημα αντιμετωπίζεται σε διαδοχικά στάδια αφαίρεσης, τα οποία σταδιακά αφορούν εξειδικεύσεις (refinements) στις αναπαραστάσεις του συστήματος και των ιδιοτήτων ασφάλειας αυτού (security properties).

Το πλαίσιο που θα παρουσιάσουμε σε αυτή την ενότητα ανήκει στην C.Eckert (για περισσότερες λεπτομέρειες ο αναγνώστης παραπέμπεται στην αναφορά [ECK-1995]). Το πλαίσιο αυτό προβλέπει μία "από-πάνω-προς-τα-κάτω" προσέγγιση στην ένταξη ασφάλειας σε Πληροφοριακά Συστήματα και λαμβάνει υπόψη του περιορισμούς εμπιστευτικότητας (confidentiality) και ακεραιότητας (integrity), σε όρους περιορισμών πρόσβασης (access control) και διακίνησης της πληροφορίας (information flow).

Οι εξής μέθοδοι χρησιμοποιούνται για τους σκοπούς της ανάπτυξης του πλαισίου:

- Η συμπεριφορά του συστήματος τυποποιείται χρησιμοποιώντας ένα "Μοντέλο Δράσης" (Action Model). Το μοντέλο αυτό παρέχει την απαραίτητη βασική τυποποίηση (Basic Formalism), δηλαδή το συντακτικό και τη σημασιολογία, προκειμένου να ορίσουμε ιδιότητες ασφάλειας επί του συστήματος.
- Οι ιδιότητες ασφάλειας τυποποιούνται με χρήση μιας συγκεκριμένης "λογικής απαιτήσεων ασφάλειας", η οποία παρουσιάζεται.
- Τέλος, το πληροφοριακό σύστημα μοντελοποιείται με αντικειμενοστραφή προσέγγιση, κατάλληλη να ενσωματώσει ορισμένες ιδιότητες ασφάλειας καθώς και πολιτικές ασφάλειας που αφορούν τις ιδιότητες περιορισμών πρόσβασης και διακίνησης της πληροφορίας.

Στα ακόλουθα θα αναφερθούμε στα παραπάνω σημεία αναλυτικότερα. Ο βαθμός λεπτομέρειας εξαρτάται από το ενδιαφέρον που παρουσιάζει κάθε σημείο και την αναγκαιότητα της ανάπτυξης του για την ανάλυση επόμενων σημείων. Παρουσιάζουμε σχετικά αναλυτικά αυτό το πλαίσιο διότι ενδιαφέρει τους σκοπούς επίδειξης της χρήσης τυπικών μεθόδων και δίνει μία άποψη ανάπτυξης μοντέλων ασφαλών πληροφοριακών συστημάτων. Παρόλα αυτά έχουν γίνει απλουστεύσεις στους συμβολισμούς του συντακτικού και της σημασιολογίας.

### 3.3.2 Παρουσίαση της προσέγγισης

#### 3.3.2.1 To Μοντέλο Δράσης

Το πληροφοριακό σύστημα μοντελοποιείται σαν μία αφηρημένη μηχανή (abstract machine), όπως προβλέπεται από τον ακόλουθο ορισμό:

#### ΟΡΙΣΜΟΣ I

Ένα σύστημα μοντελοποιείται από μία πεντάδα  $\mathbf{AM} = (V, \Sigma, A, \Gamma, S_0)$ , όπου:

1.  $V$  είναι το σύνολο των αντικειμένων, με  $\text{Range}(v)$  το σύνολο τιμών για το αντικείμενο  $v$ .
2.  $\Sigma = \times \text{Range}(v)$  είναι το σύνολο των καταστάσεων του συστήματος και,

- για  $v \in V \Rightarrow s[v] \in Range(v)$  είναι η τιμή του αντικειμένου  $v$  στην κατάσταση  $s$ .
3.  $A$  είναι το σύνολο των "ατομικών πράξεων" (atomic actions). Ισχύει ότι για κάθε  $a \in A$ , το  $EN_a$  εκφράζει τη συνθήκη ενεργοποίησης του  $a$  και μία ακολουθία πράξεων δηλώνεται ως  $\langle A \rangle$ .
  4.  $\Gamma$  είναι η σχέση μετάβασης κατάστασης και ισχύει:  $\Gamma \subseteq \Sigma \times A \times \Sigma$ .
  5. Μία πράξη  $a$  καλείται "ενεργή" στην κατάσταση  $s$  αν και μόνον αν η  $EN_a$  είναι αληθής στην κατάσταση  $s \in \Sigma$ .
  6. Η αντιστοίχιση  $\epsilon\eta: \Sigma \rightarrow P(A)$  εκφράζει το σύνολο των συνθηκών ενεργοποίησης στην κατάσταση  $s \in \Sigma$ .
  7.  $S_0 \subseteq S$  είναι ένα σύνολο αρχικών καταστάσεων του συστήματος.

Σύμφωνα με τον παραπάνω ορισμό, ισχύουν τα ακόλουθα:

- i.  $V$  είναι το σύνολο των αντικειμένων
- ii.  $A$  είναι το σύνολο των υπολογιστικών βημάτων της μηχανής
- iii.  $\Sigma$  είναι το σύνολο που ορίζεται από τις τιμές των αντικειμένων
- iv.  $\Gamma$  είναι η σχέση που εκφράζει τις μεταβάσεις κατάστασης της μηχανής
- v.  $S_0$  είναι το αρχικό σύνολο καταστάσεων της μηχανής
- vi. Η εκτέλεση μίας πράξης  $a$  προκαλεί μία μετάβαση κατάστασης. Προτού εκτελεστεί μία πράξη πρέπει να γίνεται αληθής μία υπόθεση, η  $EN_a$ . Εξάλλου στην εκτέλεση μιας πράξης συμμετέχουν δύο σύνολα αντικειμένων: το *Πεδίο Ορισμού (Domain Set)*  $D_a$  περιλαμβάνει τα αντικείμενα που μπορούν να διαβαστούν κατά την εκτέλεση της πράξης, ενώ το *Σύνολο Τιμών (Range Set)*  $R_a$  τα αντικείμενα που μπορούν να τροποποιηθούν. Το σύστημα που περιγράψαμε ξεκινάει με μία αρχική κατάσταση  $s_0 \in S_0$  και εκτελώντας ατομικές πράξεις, μέσα από τη σχέση μετάβασης κατάστασης επιλέγει την επόμενη κατάστασή του.
- vii. Μία ακολουθία πράξεων  $\langle A \rangle$  είναι αποδεκτή στο  $AM$  αν η πρώτη πράξη της ακολουθίας είναι εκτελέσιμη (ενεργή) μετά από μία αρχική κατάσταση. Επιπλέον, κάθε πράξη της ακολουθίας πρέπει να είναι εκτελέσιμη στην κατάσταση που προκύπτει από την εκτέλεση της προηγούμενή της στην ακολουθία.
- viii. Η ακολουθία καταστάσεων που σχετίζονται με μία αποδεκτή ακολουθία πράξεων  $\langle A \rangle$  ονομάζεται υπολογισμός  $\sigma_A$ .
- ix. Το σύνολο  $A^*$  περιλαμβάνει τις αποδεκτές ακολουθίες  $\langle A \rangle$ .
- x. Το σύνολο  $\Sigma^*$  περιλαμβάνει τους υπολογισμούς  $\sigma_A$ .

Η προσέγγιση δεν ορίζει τι ακριβώς υπονοείται με την έκφραση "πράξη" και αφήνει στο επιλεχθέν επίπεδο αφαιρεσης να καθορίσει κάτι τέτοιο. Αντ' αυτού, ορίζει το αποτέλεσμα μιας πράξης ως εξής:

## Ο ΟΡΙΣΜΟΣ II

Δοσμένου ενός συστήματος  $AM$ , το αποτέλεσμα μιας πράξης  $b \in A$  σε έναν υπολογισμό  $\sigma_A$  ορίζεται από τη συνάρτηση  $ef_a$ :

$$ef_a : \Sigma^* \times A \rightarrow P(\Sigma \times V \times \cup Range(v)) \cup \{nil\}$$

Σύμφωνα με τον παραπάνω ορισμό, ισχύουν τα ακόλουθα:

- i. Το αποτέλεσμα μιας πράξης  $b$  που εκτελείται σε έναν υπολογισμό  $\sigma_A$  είτε αποτελείται από μία τριάδα  $\langle \text{του} \text{ τροποποιημένου} \text{ αντικειμένου} \text{ } v, \text{ της} \rangle$

προκύπτουσας κατάστασης  $s'$ , της νέας τιμής  $s'[v]$  του αντικειμένου  $v$  όταν  $b \in \langle A \rangle$ , είτε είναι κενό ( $\{nil\}$ ) αν δεν ισχύει  $b \in \langle A \rangle$ .

### 3.3.2.2 Ιδιότητες Ασφάλειας

Οι ιδιότητες ασφάλειας ορίζονται και περιγράφονται ως σχέσεις μεταξύ των πράξεων, και ειδικότερα ως ικανότητα μίας πράξης να καθορίσει τα αποτελέσματα άλλης πράξης, σε όρους **επηρεασμού των αποτελεσμάτων** και **παρατήρησης των αποτελεσμάτων** άλλων πράξεων.

#### • ΟΡΙΣΜΟΣ III

Μία πράξη  $a$  **επηρεάζει** (influences) τα αποτελέσματα μίας άλλης πράξης  $b$  στην ακόλουθια  $\sigma_A = s_0, \dots, s_k$  μέσω του αντικειμένου  $v$  αν και μόνον αν το κατηγόρημα  $inf_a(l, a, b, v)$  είναι αληθές στην κατάσταση  $s_k$ .

Το κατηγόρημα  $inf_a(l, a, b, v)$  είναι αληθές στην κατάσταση  $s_k$  αν και μόνον αν αληθεύει μία από τις ακόλουθες συνθήκες:

1. Η συνθήκη ενεργοποίησης της πράξης  $b$  εξαρτάται από την εκτέλεση της πράξης  $a$  ή
2. Η τιμή του αντικειμένου  $x \in Range(b)$  εξαρτάται από την εκτέλεση της πράξης  $a$ .

#### • ΟΡΙΣΜΟΣ IV

Μία πράξη  $a$  **παρατηρεί** (observes) τα αποτελέσματα μίας άλλης πράξης  $b$  στην ακόλουθια  $\sigma_A = s_0, \dots, s_k$  μέσω του αντικειμένου  $x$  αν και μόνον αν το κατηγόρημα  $obs_a(l, a, b, x)$  είναι αληθές στην κατάσταση  $s_k$ .

Το κατηγόρημα  $obs_a(l, a, b, x)$  είναι αληθές στην κατάσταση  $s_k$  αν και μόνον αν αληθεύει η ακόλουθη συνθήκη:

1. Ένα αντικείμενο  $v \in Domain(b)$  εκτελεί την πράξη  $a$  και συμβαίνει ροή πληροφορίας από την  $a$  στην  $b$ , μέσω του  $v$  στο  $x \in Range(b)$ .

### 3.3.2.3 Αντικειμενοστραφές μοντέλο ασφάλειας

Το μοντέλο δράσης, το οποίο περιγράφηκε στην παράγρ.3.3.2.1, είναι αρκετά λεπτομερές. Προκειμένου να εισάγουμε έννοιες ασφάλειας, δημιουργούμε ένα αντικειμενοστραφές μοντέλο του συστήματος.

#### • ΟΡΙΣΜΟΣ V

Η εξάδα  $MS = (AM, (K, O, B, u\_rep), R, RL, \Pi_b, \Pi_k)$  μοντελοποιεί ένα αντικειμενοστραφές μοντέλο ασφαλούς συστήματος, όπου:

1.  $AM$  είναι το μοντέλο δράσης του συστήματος
2.  $(K, O, B, u\_rep)$  είναι το αντικειμενοστραφές μοντέλο του συστήματος, όπου:
  - 2.1.  $K$  είναι ένα σύνολο αντικειμένων
  - 2.2.  $K \subseteq K'$  είναι το σύνολο των αντιπροσώπων των χρηστών
  - 2.3.  $\forall k \in K, E(k)$  είναι το σύνολο των μεθόδων του αντικειμένου  $k$
  - 2.4.  $O$  είναι το σύνολο των λειτουργιών, όπου ισχύει:

$\forall op \in O, in(op)$  και  $out(op)$  είναι οι παράμετροι εισόδου και εξόδου αντίστοιχα για τη λειτουργία  $op$

- 2.5. για κάθε κάλεσμα  $inst(op)$  της λειτουργίας  $op$ , ισχύει ότι η  $εξειδίκευση$

(refinement) των πράξεων της δίνεται από τον τύπο:  $\rho(inst(op) = \langle a_1, \dots, a_m \rangle, a_i \in A)$ . Με άλλα λόγια ο τύπος αυτός ορίζει την ακολουθία των πράξεων, δηλαδή τα υπολογιστικά βήματα της λειτουργίας  $op$ .

2.6. Το σύνολο των αντικειμένων  $V$  περιέχει ορισμένα αντικείμενα που ονομάζονται λίστες ελέγχου προσπέλασης,  $acl$ , και ορίζονται ως εξής:

2.7.  $\forall k \in K \Rightarrow$

$\exists acl_k \in V : \forall s \in \Sigma : s[acl_k] = \{(k', OP) | k' \in B \cup R \cup K \cup O \wedge OP \subseteq E(k)\}$   
όπου  $B$  είναι το σύνολο των χρηστών.

2.8. Η αντιστοίχιση  $u\_rep : B \rightarrow P(K')$  αντιστοιχίζει σε κάθε χρήστη του συστήματος ένα σύνολο αντιπροσώπων, όπου ισχύει:

$\forall b, b' \in B : b \neq b' \Rightarrow u\_rep(b) \cap u\_rep(b') = \emptyset$

2.9. Η αντιστοίχιση  $ass\_u(u\eta) : K' \rightarrow B$ , αντιστοιχίζει έναν αντιπρόσωπο σε έναν χρήστη, όπου ισχύει:

$ass\_u(u\eta) = b \Leftrightarrow u\eta \in u\_rep(b)$

3.  $R$  είναι το σύνολο των δικαιωμάτων προσπέλασης και ισχύει  $O \in R$ .

4.  $RL = \{R_1, \dots, R_m\}$  είναι το σύνολο των ρόλων.

5. Η αντιστοίχιση

$\Pi_k : K' \rightarrow RL$ , με  $\Pi_k(ur) = R_j \Leftrightarrow \exists b \in B : R_j \in \Pi_b(b) \wedge b = ass\_u(ur)$   
αντιστοιχίζει σε κάθε αντιπρόσωπο  $ur$  έναν ρόλο  $R_j$ .

6. Ισχύει ότι  $\forall b \in B : \forall ur, ur' \in u\_rep(b) : ur \neq ur' \Leftrightarrow \Pi_k(ur) \neq \Pi_k(ur')$ . Αυτό σημαίνει ότι αν υπάρχουν δύο διαφορετικοί αντιπρόσωποι για έναν χρήστη, οι αντιπρόσωποι αυτοί θα πρέπει να έχουν διαφορετικούς ρόλους.

Σύμφωνα με τους παραπάνω ορισμούς:

- Ένα σύστημα μοντελοποιείται από ένα σύνολο αντικειμένων  $K$ . Για κάθε στοιχείο  $k \in K$  ορίζεται ένα σύνολο μεθόδων και λειτουργιών αυτού, οι οποίες καλούνται από άλλα αντικείμενα. Κάθε αντικείμενο μπορεί να είναι ενεργό ή παθητικό.
- Το σύνολο των χρηστών είναι το  $B$ , ενώ κάθε χρήστης αντιπροσωπεύεται από ένα σύνολο (ενεργών) αντικειμένων (αντιπροσώπων)  $u\_rep(b)$  τα οποία εκτελούν λειτουργίες γι' αυτόν. Κάθε κάλεσμα λειτουργίας δημιουργεί ένα στιγμιότυπο αυτής, που λαμβάνει τις παραμέτρους εισόδου και δημιουργεί μία ακολουθία βημάτων που ονομάζεται εξειδίκευση των πράξεων της λειτουργίας. Η τελευταία πράξη της ακολουθίας δημιουργεί τις παραμέτρους εξόδου και διαγράφει τη λειτουργία.
- Κάθε αντικείμενο είναι προστατευμένο και οι μέθοδοι του ορίζουν το σύνολο των δικαιωμάτων προσπέλασής  $R$  που έχουν οι χρήστες του. Για κάθε αντικείμενο  $k$ , ορίζεται ένα αντικείμενο που ονομάζεται λίστα προσπέλασης, το οποίο προστατεύει το αντικείμενο από μη επιτρεπόμενη προσπέλαση. Η τιμή αυτής της λίστας σε μία δεδομένη κατάσταση  $s$  του συστήματος για το αντικείμενο  $k$  είναι  $s/acl_k/$  και μπορεί να αλλάζει δυναμικά.
- Επειδή κάθε στιγμή ένας χρήστης μπορεί να εκτελεί διαφορετικές λειτουργίες με διαφορετικά δικαιώματα προσπέλασης σε ένα σύστημα, εισάγεται η έννοια του ρόλου. Το σύνολο των ρόλων είναι το  $RL$ , και κάθε ρόλος συνδέεται με ένα χρήστη μέσω της  $rl_b$  ενώ επειδή κάθε χρήστης αντιπροσωπεύεται στο σύστημα η παραπάνω αντιστοίχιση είναι ουσιαστικά η  $rl_k$ .

### 3.3.2.4 Επηρεασμός και Παρατήρηση στο Αντικειμενοστραφές Μοντέλο

Ο επηρεασμός μεταξύ δύο χρηστών ορίζεται ως εξής:

#### ⌚ ΟΡΙΣΜΟΣ VI

Δοσμένων των ακόλουθων υποθέσεων (I):

1. ενός συστήματος  $MS$
2. μίας αποδεκτής ακολουθίας πράξεων  $\langle A \rangle = s_0, \dots, s_r$
3. του αντίστοιχου υπολογισμού  $\sigma_A$
4. δύο αντιπροσώπων χρηστών  $ur_1, ur_2 \in K$
5. δύο λειτουργιών  $op_1, op_2 \in O$
6. ενός αντικειμένου  $v \in V$
7. και μίας κατάστασης  $s_i \in \sigma_A$

Ο χρήστης  $ur_1$  επηρεάζει τον χρήστη  $ur_2$  στην ακολουθία  $\langle A \rangle$ , μέσω του αντικειμένου  $v$  και των λειτουργιών  $op_1$  και  $op_2$ , αν και μόνο αν το κατηγόρημα  $inf_k$  είναι αληθές στην κατάσταση  $s_r$ . Αυτό προϋποθέτει ότι η εξειδίκευση πράξεων ενός καλέσματος  $inst\_op_1$  της λειτουργίας  $op_1$  από τον χρήστη  $ur_1$  περιέχει μία πράξη που επηρεάζει μία άλλη πράξη η οποία (δεύτερη) περιέχεται στην εκλέπτυνση πράξεων ενός καλέσματος  $inst\_op_2$  της λειτουργίας  $op_2$  από τον χρήστη  $ur_2$ .

Με τον τρόπο αυτό δημιουργείται *ροή πληροφορίας* (information flow) μεταξύ των δύο χρηστών.

#### ⌚ ΟΡΙΣΜΟΣ VII

Δοσμένων των υποθέσεων (I) του προηγούμενου ορισμού

Ο χρήστης  $ur_1$  παρατηρεί τον χρήστη  $ur_2$  στην ακολουθία  $\langle A \rangle$ , μέσω του αντικειμένου  $v$  και των λειτουργιών  $op_1$  και  $op_2$ , αν και μόνο αν το κατηγόρημα  $obs_k$  είναι αληθές στην κατάσταση  $s_r$ . Αυτό προϋποθέτει ότι η τιμή της παραμέτρου εξόδου μίας τουλάχιστον λειτουργίας που εκτελέστηκε από τον χρήστη  $ur_2$  εξαρτάται από το αποτέλεσμα της εκτέλεσης μίας τουλάχιστον λειτουργίας που εκτελέστηκε από τον χρήστη  $ur_2$ .

### 3.3.2.5 Απαιτήσεις ασφάλειας

Η θεωρητική η οποία επιλέγεται προκειμένου να οριστούν απαιτήσεις ασφάλειας, ονομαζόμενη "ἰογική απαιτήσεων ασφάλειας", είναι η ακόλουθη:

#### ⌚ ΟΡΙΣΜΟΣ VIII

Δοσμένων των ακόλουθων:

1. ενός συστήματος  $MS$
2. ενός συνόλου αντικειμένων  $V$  αυτού
3. ενός συνόλου όλων των συμβολισμών και κατηγορημάτων που αποτελούν το συντακτικό που χρησιμοποιείται
4. του συνόλου όλων των έγκυρων τύπων του συντακτικού, συμβολιζόμενου ως  $TFO$
5. μίας συνθήκης  $Cond \in TFO$



ορίζεται η σημασιολογία<sup>9</sup> των ακόλουθων κατηγορημάτων:

1. Το υπό συνθήκη κατηγόρημα μη-επηρεασμού, *cninf*, προβλέπει ότι ικανοποιηθείσης μιας συνθήκης *Cond*, δεν υπάρχει επηρεασμός μεταξύ δύο αντιπροσώπων, *u\_rep(ur<sub>1</sub>)* και *u\_rep(ur<sub>2</sub>)*, των χρηστών *ur<sub>1</sub>*, και *ur<sub>2</sub>*, αναφορικά με την εκτέλεση των λειτουργιών *op<sub>1</sub>*, και *op<sub>2</sub>*.
2. Το υπό συνθήκη κατηγόρημα μη-παρατήρησης, *cnobs*, προβλέπει ότι ικανοποιηθείσης μιας συνθήκης *Cond*, δεν υπάρχει παρατήρηση μεταξύ δύο αντιπροσώπων, *u\_rep(ur<sub>1</sub>)* και *u\_rep(ur<sub>2</sub>)*, των χρηστών *ur<sub>1</sub>*, και *ur<sub>2</sub>*, αναφορικά με την εκτέλεση των λειτουργιών *op<sub>1</sub>*, και *op<sub>2</sub>*.
3. Το υπό συνθήκη κατηγόρημα περιορισμού προσπέλασης *acc*, προβλέπει ότι ο αντιπρόσωπος *u\_rep(ur)* ενός χρήστη *ur*, δεν μπορεί να εκτελέσει μέσω του αντικειμένου *v* τη λειτουργία *op* αν δεν ικανοποιείται η συνθήκη *Cond*.

### 3.3.2.6 Πολιτικές ασφάλειας

Χρησιμοποιώντας την παραπάνω λογική μπορούμε να ορίσουμε πολιτικές ασφάλειας για το σύστημά μας:

## Ο ΟΡΙΣΜΟΣ ΙΧ

Δοσμένου ενός συστήματος *MS*, μία πολιτική ασφάλειας *P*, είναι ένας τύπος της λογικής απαιτήσεων ασφάλειας (που περιγράφηκε στην προηγούμενη παράγραφο), που ορίζεται από έναν αρχικό τύπο που αφορά τις επιτρεπόμενες και μη-επιτρεπόμενες προσπελάσεις στην αρχική κατάσταση, έναν τύπο μη-επηρεασμού, έναν τύπο μη-παρατήρησης και έναν τύπο περιορισμού προσπέλασης.

Ο τρόπος με τον οποίο μοντελοποιήθηκε το σύστημα είναι λειτουργικός διότι επιτρέπει να ορίσουμε με τον τρόπο που επιθυμούμε τις απαιτήσεις ασφάλειας και να τις ενσωματώσουμε φορμαλιστικά στην πολιτική και στο σύστημά μας. Ο τρόπος με τον οποίο ορίζονται τα κατηγορήματα επιτρέπει ευελιξία στον ορισμό απαιτήσεων ασφάλειας μέσω της συνθήκης *Cond*. Μπορούμε λ.χ. να ορίσουμε διαφορετικές συνθήκες ανάλογα με τις απαιτήσεις της εφαρμογής που έχουμε ή να χρησιμοποιήσουμε τους ρόλους εφαρμόζοντας περιορισμούς για την τιμή της λίστας προσπέλασης στη συνθήκη *Cond*. Εξάλλου στη σχετική αναφορά γίνεται επίδειξη του τρόπου με τον οποίο γνωστά μοντέλα πολιτικών ασφάλειας αναπαρίστανται μέσω αυτού του μοντέλου.

Επίσης, το πλαίσιο αυτό επιτυγχάνει έναν ομαλό και ενιαίο τρόπο με τον οποίο πραγματοποιούνται διαδικασίες σχετικές με ενσωμάτωση απαιτήσεων ασφάλειας λειτουργίες αλλά και λειτουργίες ελέγχου της εφαρμογής των απαιτήσεων από το σύστημα. Αυτό επιτυγχάνεται λόγω του ότι κάθε σχετική με ασφάλεια τυποποίηση βασίστηκε και ορίστηκε στο "Μοντέλο Δράσης" του συστήματος. Πρέπει ωστόσο να σημειώσουμε ότι το μοντέλο αυτό δίνει έμφαση σε περιορισμούς ακεραιότητας (σε όρους ροών πληροφορίας).

<sup>9</sup> Για τον ακριβή ορισμό του συντακτικού και της σημασιολογίας βλ. την αναφορά [ECK-1995] σελ. 249.



### 3.4 Αυτοματοποιημένη διαχείριση πολιτικών ασφάλειας βασισμένη στις αρχές της Τεχνολογίας Λογισμικού

Τεχνολογία Λογισμικού, Αντικειμενοστράφεια, Κατανεμημένα Συστήματα, Κουστωδοί, Ροή Πληροφορίας, Έλεγχος Προσπέλασης, Τυπικές Μέθοδοι Ορισμού Απαιτήσεων Λογισμικού

#### 3.4.1 Εισαγωγή

Η ενότητα αυτή θα παρουσιάσει στοιχεία θεωρίας και υλοποίησης για μία συγκεκριμένη περίττωση αυτοματοποιημένης διαχείρισης πολιτικών ασφάλειας<sup>10</sup>. Αντίστοιχη ευρεία ερευνητική προσπάθεια πραγματοποιείται στη Γερμανία από ερευνητική ομάδα με επικεφαλείς τους W.Khuenhouser και C.Bryce. Θα αναφερόμαστε στο συγκεκριμένο πλαίσιο και στο συγκεκριμένο κεφάλαιο, με τον όρο "Τυποποίηση και αυτοματοποίηση πολιτικών ασφάλειας βασισμένη στις αρχές της τεχνολογίας λογισμικού". Οι αντίστοιχες αναφορές χρησιμοποιούν συχνά τον όρο "*Information Security Engineering*".

Ο αρχικός στόχος του θεωρητικού και εφαρμοσμένου πλαισίου είναι διπτός:

- Ακριβής καθορισμός των στόχων ασφάλειας ενός συστήματος.
- Ακριβής καθορισμός των τεχνικών που θα εξασφαλίσουν την επίτευξη των στόχων.

Η έννοια της *Πολιτικής Ασφάλειας* είναι βασική στο πλαίσιο εννοιών που θα περιγράψουμε, εφόσον αποτελεί το επεξεργαζόμενο με τις τεχνικές στοιχείο με σκοπό την τυποποίηση και αυτοματοποίησή του. Μετέπειτα του καθορισμού τους, η επεξεργασία των πολιτικών ασφάλειας συνίσταται στις εξής ενέργειες:

- Σχεδιασμό (Design)
- Υλοποίηση (Implementation)
- Έλεγχο (Verification)

Οι δε κατευθύνσεις έρευνας και εργασίας αναφέρονται στα εξής δύο πεδία:

- Δημιουργία μεθόδων και εργαλείων υποστήριξης της διαδικασίας Τυποποίησης και Αυτοματοποίησης Πολιτικών Ασφάλειας.
- Δημιουργία μεθόδων και εργαλείων υποστήριξης της διαδικασίας ενσωμάτωσης και ολοκλήρωσης των πολιτικών ασφάλειας σε συγκεκριμένες πλατφόρμες υπολογιστικών συστημάτων.

Αναλυτικότερα, προκειμένου να ικανοποιηθούν κριτήρια ποιότητας στην ανάπτυξη και διαχείριση πολιτικών ασφάλειας, οι μέθοδοι και τα εργαλεία που αναπτύσσονται και χρησιμοποιούνται βασίζονται σε *τυπικές τεχνικές ορισμού απαιτήσεων* (*formal specification techniques*). Οι μέθοδοι και τα εργαλεία υποστηρίζουν τις φάσεις του ορισμού της σημασιολογίας της πολιτικής ασφάλειας (*security policy semantics*), της ανάλυσης των προδιαγραμμένων απαιτήσεων

<sup>10</sup> Τα σημεία τα οποία θίγουμε αποτελούν το αντικείμενο έργων που βρίσκονται σε εξέλιξη. Για περισσότερες πληροφορίες ο αναγνώστης παραπέμπεται στις σχετικές αναφορές που υπάρχουν στο κείμενο.

(specification analysis), του ελέγχου της υλοποίησης (implementation verification) και της πιστοποίησης των αποτελεσμάτων του λειτουργικού αποτελέσματος (certification of working result). Από την άλλη πλευρά και σύμφωνα με το παρόν πλαίσιο, πρέπει να σημειωθεί ότι η υλοποίηση ενός ασφαλούς συστήματος δεν αφορά μόνο την ανάπτυξη μιας πολιτικής ασφάλειας για το σύστημα αυτό, αλλά επίσης τον καθορισμό των στοιχείων της αρχιτεκτονικής του συστήματος βάσης (που χρησιμοποιείται ως υποδομή) και την επεξεργασία τους κατά τρόπο που η ενσωμάτωση της πολιτικής ασφάλειας θα επιτεύξει τη μέγιστη δυνατή λειτουργικότητα και ασφάλεια.

Ο τρόπος που επιλέχθηκε για την επεξεργασία των Πολιτικών Ασφάλειας ικανοποιεί όχι μόνο απαιτήσεις ποιότητας σε σχέση με τομείς που περιγράψαμε, αλλά επίσης διευκολύνει την επίτευξη των ακόλουθων στόχων:

- Ανάπτυξη μιας βιβλιοθήκης πολιτικών ασφάλειας που
  - θα διευκολύνει την επιλογή και εφαρμογή μέτρων ασφάλειας για κάθε τύπο εφαρμογής και
  - θα εξασφαλίζει την εύκολη ανάπτυξη νέων πολιτικών ασφάλειας με την επαναχρησιμοποίηση ήδη υπαρχόντων τμημάτων (modules).
- Ολοκλήρωση αυτής της βιβλιοθήκης σε ένα εύχρηστο περιβάλλον λογισμικού, κατάλληλο για ποικιλία εμπορικών περιβάλλοντων.
- Ενσωμάτωση στο παραπάνω σύστημα στοιχείων που θα επιτυγχάνουν τη διαχείριση περισσότερων πολιτικών ασφάλειας καλύπτοντας την περίπτωση επικοινωνούντων Πληροφοριακών Συστημάτων.
- Διερεύνηση του τρόπου με τον οποίο αρχές των εμπειρών συστημάτων μπορούν να υποστηρίξουν και να διευκολύνουν την ανάπτυξη και διαχείριση πολιτικών ασφάλειας.

Παρακάτω, θα περιγράψουμε το συγκεκριμένο πλαίσιο, αρχίζοντας με μία παρουσίαση του περιβάλλοντος αναφοράς. Ο αναγνώστης παραπέμπεται στο κεφ. 3.4.4., το οποίο περιγράφει μία εφαρμογή, προκειμένου να αντλήσει συγκεκριμένα στοιχεία θέματα στα οποία αναφερθήκαμε και θέματα που θα αναλύσουμε ευθύς αμέσως.

### 3.4.2 Συνθετικά στοιχεία του περιβάλλοντος αναφοράς

Το περιβάλλον<sup>11</sup> στο οποίο το πλαίσιο εφαρμόζεται, αποτελείται από διάφορους ανεξάρτητους, συνδεδεμένους και αμοιβαία υποπτευόμενους κόμβους. Στους κόμβους αυτούς υπάρχουν και λειτουργούν κάποιες εφαρμογές κάθε μία από τις οποίες χαρακτηρίζεται από κάποιες απαιτήσεις ασφάλειας, οι οποίες συνθέτουν την πολιτική ασφάλειας γι' αυτήν. Η πολιτική ασφάλειας θεωρείται ότι ελέγχει την εφαρμογή (βλ. αναλυτικότερα παράγρ.3.4.3.1).

Βασικά, η προσέγγιση επιλέγει να υλοποιήσει τους στόχους της μέσω μίας βιβλιοθήκης πολιτικών ασφάλειας για τις εφαρμογές. Η βιβλιοθήκη αυτή αποτελεί η ίδια μία εφαρμογή λογισμικού που αποτελείται από το τμήμα που περιέχει τους ορισμούς των τύπων πολιτικών ασφάλειας και από το τμήμα που περιέχει την

<sup>11</sup> Βλ. επίσης και παράγρ. 3.4.4.2.

υλοποίηση (τον κώδικα δηλαδή) για τους τύπους αυτούς. Στην ιδανική περίπτωση ένα τέτοιο σύστημα θα έπρεπε να ενσωματώνει διάφορα μοντέλα πολιτικών ασφάλειας, τα οποία θα έπρεπε να καλύπτουν ένα ευρύ πεδίο εφαρμοσμένων περιπτώσεων. Κατ' αυτό τον τρόπο, για ένα τυχαίο σύνολο απαιτήσεων ασφάλειας θα εντοπίζαμε τους αντίστοιχους τύπους που το υλοποιούν στο πλαίσιο αυτό. Εξάλλου το σύστημα πρέπει να υποστηρίζεται από μία διεπαφή, υπεύθυνη για την μετατροπή των ορισμένων από το χρήστη τύπων πολιτικών ασφάλειας σε τμήματα κώδικα. Η περιγραφή της σύνθεσης και λειτουργικότητας των τμημάτων της βιβλιοθήκης, στα οποία αναφερθήκαμε, καθώς και του συνολικού συστήματος, θα αποτελέσουν τα σημεία ανάλυσης της επόμενης παραγράφου.

### 3.4.3 Συνθετικά στοιχεία της προσέγγισης

#### 3.4.3.1 Βασικές αρχές

Πριν από την παρουσίαση του πλαισίου πρέπει να αναφερθούμε σε δύο **αρχές** οι οποίες στηρίζουν και στηρίζονται από το πλαίσιο αυτό, με τη δεύτερη να είναι εν μέρει συνέπεια της πρώτης. Η πρώτη αρχή διατείνεται ότι η προσφορά στοιχείων-ιδιοτήτων ασφάλειας στο χρήστη πρέπει να έχει τη μορφή του "πακεταρισμένου" προϊόντος (package). Το βασικό χαρακτηριστικό ενός τέτοιου προϊόντος είναι ότι έχει τις απαραίτητες ιδιότητες που κάνουν εύκολη την ενσωμάτωσή του (plugging in) στην υπάρχουσα εφαρμογή του χρήστη. Η δεύτερη αρχή υποστηρίζει ότι ένα από τα σημαντικότερα χαρακτηριστικά των προϊόντων της τεχνολογίας λογισμικού είναι η δυνατότητα "επαναχρησιμοποίησής" τους, έτσι ώστε να είναι εύχρηστα κατά τη διαδικασία συντήρησης (η οποία περιλαμβάνει αναβαθμίσεις, προσαρμογές σε νέες πλατφόρμες, αλλαγές μικρής ή μεγαλύτερης κλίμακας ή σε χαμηλό ή υψηλό επίπεδο αφαίρεσης στον κώδικα, συνεργασία μίας πολιτικής με μία νέα, κ.λπ.).

Πρέπει να παρατηρήσουμε σε αυτό το σημείο ότι οι δύο αυτές αρχές αποτελούν αντιπροσωπευτικές εκδηλώσεις δύο σύγχρονων τάσεων τις οποίες έχουμε αναλύσει σε προηγούμενη εργασία μας [POL-1997]. Η πρώτη αφορά την σχετική με την ασφάλεια Πληροφοριακών Συστημάτων αγορά, αλλά και την αγορά πληροφορικής γενικότερα, για απαίτηση πακεταρισμένων λύσεων (COTS, cut-of-the-self software) που ολοκληρώνουν τις βασικές απαιτήσεις ενός χώρου εφαρμογής και εύκολα εισάγονται στο αντίστοιχο περιβάλλον. Η δεύτερη σχετίζεται με μία επίσης γενική τάση του χώρου για χρησιμοποίηση του αντικειμενοστραφούς παραδείγματος στην αντίληψη των απαιτήσεων, στη σχεδίαση των προδιαγραφών και στην υλοποίηση αυτοματοποιημένων συστημάτων. Τα χαρακτηριστικά του αντικειμενοστραφούς παραδείγματος, ως γνωστόν, αποτελούν τις πιο σαφείς εφαρμογές της αρχής της επαναχρησιμοποίησης λογισμικού, καθώς και άλλων σχετικών ή παράγωγων ιδιοτήτων, τις οποίες θα έχουμε την ευκαιρία να δούμε στα επόμενα.

Εξαρχής, πρέπει επίσης να αναφέρουμε ότι οι βασικές δομικές μονάδες υλοποίησης των πολιτικών ασφάλειας στο πλαίσιο αυτό είναι ο κουστωδός (custodian) και μία βιβλιοθήκη που περιλαμβάνει, όπως είπαμε, τις πολιτικές ασφάλειας. Ο κουστωδός είναι μία μονάδα λογισμικού, ένα τμήμα κώδικα με άλλα λόγια, το οποίο αντιπροσωπεύει την πολιτική ασφάλειας. Ο κουστωδός αποτελεί ένα είδος "επόπτη" (reference monitor), ενώ διακρίνεται από δύο εκ των βασικών

χαρακτηριστικών αυτού, ονομαστικά εκ των: απροσβλητότητα (tamperproofness) μέσω σύνδεσης με την "έμπιστη υπολογιστική βάση" (Trusted Computing Base) και καθολική μεσολάβηση (total mediation) μεταξύ όλων των επικοινωνιών της εφαρμογής στην οποία αντιστοιχεί και την οποία "προστατεύει", με τις υπόλοιπες εφαρμογές.

Στα ακόλουθα, θα αναφερθούμε στη διαδικασία αυτοματοποιήσης των πολιτικών ασφάλειας στο πλαίσιο αυτό. Όπως έχουμε σημειώσει, σε ακόλουθη παράγραφο θα παρουσιαστεί ενδεικτικά ένα παράδειγμα εφαρμογής των αντιλήψεων που αναλύουμε.

### 3.4.3.2 Σχεδιασμός πολιτικών ασφάλειας

Δεδομένου του ότι οι υλοποιημένες εκδόσεις των πολιτικών ασφάλειας στο πλαίσιο αυτό είναι οι κουστώδοι, το στάδιο του σχεδιασμού αφορά κυρίως προγραμματισμό. Εντούτοις, το στάδιο του προγραμματισμού πρέπει να υποστηρίζεται από μία διαδικασία σχεδιασμού απαιτήσεων και προδιαγραφών η οποία προηγείται ή τουλάχιστον εμπλουτίζεται στην πορεία με την άντληση εμπειρίας μέσω της υλοποίησης και εφαρμογής. Γενικά, οι προδιαγραφές προβλέπουν ότι ο καθορισμός των στοιχείων του αυτοματοποιημένου αντίστοιχου της πολιτικής ασφάλειας γίνεται σε προγραμματιστική γλώσσα υψηλού επιπέδου που υποστηρίζει τις αρχές της αντικειμενοστράφειας και είναι συμβατή με υπολογιστική πλατφόρμα ευρείας αποδοχής<sup>12</sup>. Ακολούθως, προσδιορίζονται ομοιογενούς περιεχομένου τμήματα της πολιτικής (policy units) τα οποία θα αντιστοιχηθούν σε ανάλογα τμήματα της βιβλιοθήκης. Τα τμήματα αυτά περιλαμβάνουν τον ορισμό των βασικών τύπων κλάσεων που αντιστοιχούν στα τμήματα της πολιτικής. Η ανάπτυξη της πολιτικής ασφάλειας δεν ξεκινά με τη συγγραφή του κώδικα του κουστώδου αλλά ακολουθεί την εξής -συνοπτική- διαδικασία:

- αρχική σύλληψη της πολιτικής ασφάλειας
- επιλογή από τις υπάρχουσες βασικές κλάσεις, αυτών που αναλογούν στη συγκεκριμένη πολιτική
- δημιουργία εξειδικευμένων κλάσεων για τη συγκεκριμένη πολιτική υποβοηθούμενη από την κληρονομικότητα
- συγγραφή του κουστώδου

Με τη σειρά της η συγγραφή του κώδικα είναι επίσης σε ένα βαθμό τυποποιημένη, εφόσον υπάρχουν έτοιμα τμήματα κώδικα, που υλοποιούν βασικά τμήματα του λογισμικού μίας πολιτικής ασφάλειας. Αυτά τα τμήματα κώδικα βρίσκονται αποθηκευμένα σε μία βάση δεδομένων και μπορούν να αντιγραφούν από

<sup>12</sup> Οι αντίστοιχες πηγές που έχουμε στη διάθεσή μας για την ενότητα αυτή κάνουν αναφορές σε συγκεκριμένη υλοποίηση ενός τέτοιου πλαισίου. Η υλοποίηση αυτή δεν θα μας απασχολήσει ιδιαίτερα. Για λόγους πληρότητας και κατανόησης του κειμένου όμως πρέπει να σημειώσουμε ότι η υλοποίηση αυτή:

1) καλύπτει μεγάλο εύρος εφαρμοσμένων περιπτώσεων,  
2) αφορά την πλατφόρμα λειτουργικών συστημάτων UNIX και την γλώσσα προγραμματισμού C++ και  
3) επεξεργάζεται πολιτικές ασφάλειας που ανταποκρίνονται σε ένα διευρυμένο "Μοντέλο του Δικτυώματος" (Lattice Model)



αυτήν. Για παράδειγμα, η υλοποίηση των απαιτήσεων περιορισμού προσπέλασης με τη μέθοδο της μήτρας προσπέλασης, που αποτελεί μία κλασική προσέγγιση στον τομέα του ελέγχου πρόσβασης, υπάρχει έτοιμη και μπορεί να προσαρμοστεί στην εκάστοτε περίπτωση.

### 3.4.3.3 Επικύρωση πολιτικών ασφάλειας

Εφόσον ένα σημαντικό μέρος της διαδικασίας σχεδιασμού και υλοποίησης περιλαμβάνει προγραμματισμό, ένα επίσης μεγάλο τμήμα του ελέγχου συνίσταται σε τυπικούς ελέγχους κώδικα, καθώς και έλεγχο ικανοποίησης των απαιτήσεων από τον κώδικα μέσω αναδρομών-επιθεωρήσεων. Η ιδιότητα της επαναχρησιμοποίησης υπαρχόντων τμημάτων και η κληρονομικότητα διευκολύνουν σημαντικά τη διαδικασία του ελέγχου. Επίσης η χρήση μίας γλώσσας ορισμού τύπων σε υψηλό επίπεδο (high-level type definition language), που επιτρέπει τον ορισμό τύπων οι οποίοι μπορούν να εισαχθούν σε έναν μεταγλωττιστή που παράγει κλάσεις στη συγκεκριμένη προγραμματιστική γλώσσα, είναι σημαντική γιατί θέτει τον ορισμό απαιτήσεων ανεξάρτητο του περιβάλλοντος υλοποίησης.

Εκτός όμως αυτών των κλασικών ελέγχων, η διαδικασία ελέγχου έχει ως κύριο αντικείμενο τη χρησιμοποίηση των θεωριών που αποδεικνύουν την ασφάλεια ενός συστήματος (security proof theory) στη διαδικασία ανάπτυξης και εφαρμογής πολιτικών ασφάλειας. Αυτό σημαίνει ότι οι προδιαγραφές του πλαισίου πρέπει να ενσωματώνουν στοιχεία που θα επιτρέπουν την εύκολη χρήση αυτών των μεθόδων για επιβεβαίωση της ορθότητας των πολιτικών που δημιουργούνται. Η βασική πρόκληση στο σημείο αυτό είναι η χρήση τυπικών μοντέλων ασφάλειας, τα οποία διαθέτουν μεθόδους επιβεβαίωσης ιδιοτήτων ασφάλειας που η εκάστοτε πολιτική περιλαμβάνει, μεθόδους που το πλαίσιο πρέπει να υποστηρίζει. Η υποστήριξη των μεθόδων αυτών θα πρέπει να μπορεί να είναι αυτοματοποιημένη σε έναν αρκετά υψηλό βαθμό. Στην περίπτωση αυτή βέβαια, ο έλεγχος του συνόλου των απαιτήσεων ασφάλειας, που συνθέτουν την πολιτική, πρέπει να εξασφαλίζεται μέσω των μεθόδων που η προηγούμενη παράγραφος παρουσιάζει (έλεγχοι λογισμικού και συμβατότητας με απαιτήσεις), ή μέσω της συγγραφής κώδικα και του καθορισμού κανόνων που θα διενεργούν, αυτοματοποιημένα ή χειρονακτικά, τον ολοκληρωμένο έλεγχο.

Είναι επίσης σημαντική η διευκρίνιση ότι ένα τμήμα των διαδικασιών ελέγχου του εν λόγω πλαισίου καταλαμβάνει η τεκμηρίωση κάθε δομικού του μέρους. Η τεκμηρίωση δρα ως στοιχείο αναφοράς το οποίο θέτει τους κανόνες και τις προϋποθέσεις υπό τις οποίες το πλαίσιο είναι εφαρμόσιμο και μπορεί να καλύψει τις απαιτήσεις της εκάστοτε περίπτωσης.

### 3.4.3.4 Υλοποίηση πολιτικών ασφάλειας

Το βασικό αντικείμενο αυτής της διαδικασίας είναι η επινόηση μεθόδων για τη σύνδεση ενός κουστωδού με την αντίστοιχη εφαρμογή, καθώς και με το σύστημα, έτσι ώστε να ικανοποιεί τις απαιτήσεις της απροσβλητότητας και μεσολάβησης. Ο γενικός τρόπος με τον οποίο επιτυγχάνεται αυτή η απαίτηση περιλαμβάνει την ανάπτυξη εφαρμογών, τμημάτων κώδικα δηλαδή, που υλοποιούν την επικοινωνία με την εφαρμογή και το σύστημα.



Αναλυτικότερα, η εφαρμογή η οποία εποπτεύεται αρχικοποιείται σαν μία συνηθισμένη εφαρμογή στο σύστημα στην οποία διατίθεται ένας συγκεκριμένος χώρος διευθύνσεων. Ο κουστωδός της εφαρμογής είναι μία εφαρμογή η οποία αρχικοποιείται εκ παραλλήλου με δικαιώματα υπερχρήστη και στην οποία διατίθεται ένας χώρος απροσπέλαστων διευθύνσεων.

Στη γενική περίπτωση ενός περιβάλλοντος με χαρακτηριστικά που περιγράφηκαν στην παράγρ.3.4.2., όταν μία εφαρμογή "εξάγεται" στο σύστημα, υπάρχει ένας εξυπηρετητής που καταγράφει την ταυτότητά της καταγράφοντας την υποδοχή (socket) την οποία η εφαρμογή χρησιμοποιεί για να διαβάσει αιτήσεις άλλων εφαρμογών. Παρόμοια, όταν μία εφαρμογή θέλει να διαβάσει κάποια άλλη, πρέπει να ανακτήσει από αυτόν τον εξυπηρετητή την ταυτότητα της συγκεκριμένης εφαρμογής, δηλαδή την υποδοχή της, και να την ανοίξει, οπότε όλες οι αιτήσεις της θα καταγράφονται στην υποδοχή μέσω του εξυπηρετητή.

Όταν χρησιμοποιούνται κουστωδοί το σενάριο αυτό δεν μεταβάλλεται σημαντικά. Απλά ο εξυπηρετητής δεν δίνει στην αιτούσα διαδικασία την υποδοχή της αιτούμενης, αλλά την υποδοχή της εφαρμογής που υλοποιεί τον αντίστοιχο κουστωδό. Επίσης, σε ένα τέτοιο περιβάλλον υπάρχουν επιπρόσθετες διαδικασίες ασφάλειας των κουστωδών από τις διαδικασίες του συστήματος στις οποίες οι χρήστες δεν έχουν πρόσβαση. Αυτές οι διαδικασίες αποτελούν τμήματα του λογισμικού των κουστωδών.

### 3.4.4 Παρουσίαση μίας ενδεικτικής εφαρμογής

#### 3.4.4.1 Εισαγωγή

Προκειμένου να παρουσιάσουμε ένα εφαρμοσμένο παράδειγμα, είναι αναπόφευκτες οι αναφορές σε συγκεκριμένες υλοποιήσεις. Η προσπάθειά μας θα είναι να περιορίσουμε τις προσφυγές σε συγκεκριμένα στοιχεία κατά το δυνατό περισσότερο. Ας παρουσιάσουμε όμως τα στοιχεία που καταρχήν μας χρειάζονται.

Πρέπει καταρχήν να αναφέρουμε ότι οι πηγές εκ των οποίων αντλούμε τα παρόντα στοιχεία αφορούν μία συντονισμένη προσπάθεια υλοποίησης ενός πλαισίου για αυτοματοποιημένη ανάπτυξη και διαχείριση πολιτικών ασφάλειας. Τα ήδη υλοποιημένα τμήματα αυτού του πλαισίου περιλαμβάνουν ([BRY-1996], [BRY-1997a], [BRY-1997c]):

- ένα περιβάλλον για αυτοματοποιημένη σχεδίαση, ανάπτυξη και διαχείριση πολιτικών ασφάλειας (SKIPPY) οι οποίες στηρίζονται στις αρχές του Μοντέλου του Δικτύουματος και υλοποιούνται μέσω κουστωδών
- μία αρχιτεκτονική η οποία μπορεί να χρησιμοποιηθεί επιτυχώς ως υποδομή για τις απαιτήσεις της προσέγγισης (BirliX)
- μία εφαρμογή για υλοποίηση ενός περιβάλλοντος ηλεκτρονικού εμπορίου στην οποία χρησιμοποιούνται στοιχεία των προηγούμενων προσεγγίσεων.

Στα ακόλουθα θα προσπαθήσουμε να αποδώσουμε τις βασικές σχεδιαστικές αρχές και προδιαγραφές υλοποίησης που διέπουν αυτές τις προσπάθειες, στο βαθμό που αυτή η μελέτη το απαιτεί.

### 3.4.4.2 Η αρχιτεκτονική ασφάλειας BirliX

Ένα από τα δυσκολότερα έργα σε διάφορες επιστημονικές περιοχές είναι ο σαφής ορισμός όρων ή εκφράσεων τις οποίες έμφυτα ή ενστικτικώς χρησιμοποιούμε και κατανοούμε ως περιεχόμενο. Σαφώς, ο ορισμός της "αρχιτεκτονικής ασφάλειας" είναι κρίσιμος, είναι όμως γεγονός ότι συγκεκριμένα στο πεδίο της ασφάλειας των Πληροφοριακών Συστημάτων, πολλές είναι οι έννοιες οι οποίες είτε μένουν τυπικά αόριστες είτε αντιμετωπίζονται με ελαφρές διαφοροποιήσεις στο περιεχόμενο. Στο εννοιολογικό πλαίσιο που εξετάζουμε, η έννοια της αρχιτεκτονικής ασφάλειας ορίζεται ως εξής: **η αρχιτεκτονική ασφάλειας συνιστά μία πλήρη υποδομή (θεωρητική και εφαρμογής) η οποία επιτρέπει την εφαρμογή πολιτικών ασφάλειας που ανταποκρίνονται στις ανάγκες ποικίλων εφαρμογών, μέσω της εφαρμογής μηχανισμών ασφάλειας με έναν ορισμένο τρόπο.**

Επιχειρηματολογείται ότι η αρχιτεκτονική λειτουργικών συστημάτων BirliX είναι η κατάλληλη προκειμένου για την ανάπτυξη του παραπάνω πλαισίου. Πρόκειται για μία αντικειμενοστραφή αρχιτεκτονική η οποία ανταποκρίνεται κατά κύριο λόγο σε κατανεμημένα συστήματα. Εφόσον η εστίαση αυτής της μελέτης δεν είναι αυτά καθεαυτά τα κατανεμημένα συστήματα η επιλογή μας είναι να περιφριστούμε στην παρουσίαση εκείνων των στοιχείων που θα μας εξοικειώσουν με τη φιλοσοφία της αρχιτεκτονικής σχεδίασης, και όχι αυτών που αναφέρονται στις απαιτήσεις σχετικά με τα κατανεμημένα συστήματα.

Οι λόγοι για τους οποίους η συγκεκριμένη (αντικειμενοστραφής) προσέγγιση θεωρείται κατάλληλη για ανάπτυξη ασφαλών περιβαλλόντων είναι οι ακόλουθοι:

- Τα αντικείμενα-οντότητες επικοινωνούν με έναν συγκεκριμένο τρόπο, δηλαδή με την επίκληση μεθόδων. Ο τρόπος αυτός προσφέρει πεδίο εφαρμογής ολοκληρωμένων προσεγγίσεων (integration), τόσο στην επινόηση όσο και στην εφαρμογή λύσεων. Περαιτέρω, η ολοκλήρωση έχει θετικές επιπτώσεις και στα κόστη ανάπτυξης και εφαρμογής μηχανισμών.
- Οι διεπαφές των αντικειμένων περιλαμβάνουν ποικιλία σχέσεων. Το γεγονός αυτό υπονοεί ύπαρξη πεδίου ανάπτυξης ποικίλων σημασιολογικών σχέσεων.

Πολλοί από τους όρους που χρησιμοποιούνται διατηρούνται από το αντικειμενοστραφές παράδειγμα προγραμματισμού. Τα συστατικά στοιχεία του μοντέλου είναι τα ακόλουθα:

- Ένα αντικειμενοστραφές μοντέλο, που υλοποιείται από μία μηχανή μετάθεσης καταστάσεων, όπου οι εφαρμογές θεωρούνται ως αλληλεπιδρώντα αντικείμενα.
- Ένα σύνολο μηχανισμών ασφάλειας οι οποίοι ελέγχουν την επικοινωνία των αντικειμένων.
- Ένα σύνολο πολιτικών ασφάλειας (στόχων, κανόνων, συνθηκών), των οποίων η εφαρμογή εξαρτάται από τη λειτουργία της μηχανής και την εφαρμογή των μηχανισμών ασφάλειας.

Τα αντικείμενα του μοντέλου ολοκληρώνται σε μία αρχιτεκτονική δομή, η οποία ονομάζεται "υποδομή ασφάλειας" (security infrastructure). Για κάθε εμφάνιση ενός αντικειμένου του συστήματος (instance), ορίζεται ένας τύπος αντικειμένου που ανήκει σε αυτή τη δομή. Επιπλέον ορίζονται βασικές δομές (μέθοδοι και ιδιότητες) κοινές για όλους τους τύπους αντικειμένων. Η κληρονομικότητα, τα σπιγμούτυπα και η

επικοινωνία είναι οι μηχανισμοί μέσω των οποίων γίνεται εφικτή η ολοκλήρωση.

Οι μηχανισμοί ασφάλειας που προσφέρει η αρχιτεκτονική αντιστοιχούν σε δύο όψεις του αντικειμενοστραφούς σχήματος, την άποψη του αντικειμένου και την άποψη του υποκειμένου, και είναι κατ' αναλογία οι εξής:

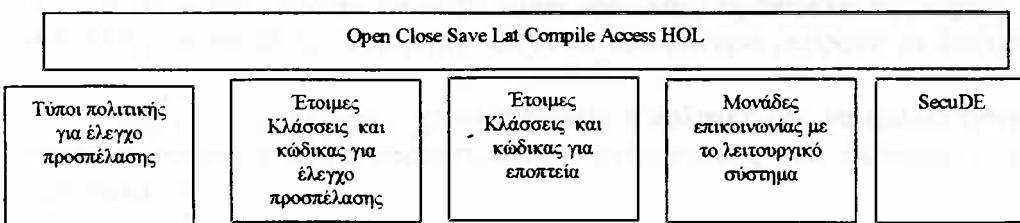
- Για κάθε αντικείμενο ορίζονται τα υποκείμενα που μπορούν να το προσπελαύνουν μέσω συγκεκριμένων μεθόδων του. Πρόκειται για το γνωστό μηχανισμό των "Λιστών Ελέγχου Προσπέλασης" (Access Control Lists), που υποστηρίζεται από διάφορα συστήματα. Στη συγκεκριμένη αρχιτεκτονική, η λειτουργικότητα αυτής της μεθόδου (σε όρους υποστήριξης ρόλων, τύπων οντοτήτων, ιεραρχιών οντοτήτων) επεκτείνεται προκειμένου να αυξηθεί η ευελιξία της. Υπάρχει η δυνατότητα εισαγωγής στη λίστα στοιχείων όπως σπιγμιότυπα, τύποι και κονσταδοί. Βέβαια, η επιπλέον λειτουργικότητα συνεπάγεται σαφώς επιπλέον κόστος διαχείρισης.
- Για κάθε υποκείμενο ορίζονται τα αντικείμενα στα οποία αυτό μπορεί να έχει προσπέλαση. Ο γνωστός όρος εδώ είναι οι "Λίστες Δυνατοτήτων" (Capability Lists, c-lists) και μέσω αυτών επιτυγχάνεται ο έλεγχος των κλήσεων που εξέρχονται από το υποκείμενο.

Μέσω των μηχανισμών αυτών και με βάση ορισμένες απαιτήσεις, όσον αφορά την ασφάλεια σε κατανεμημένα συστήματα, ορίζονται "Πεδία Εμπιστοσύνης" (confidence domains) [HÄR-1993].

#### 3.4.4.3 Το περιβάλλον διαχείρισης πολιτικών ασφάλειας SKIPPY

Το σχήμα 3.3. δείχνει τα υλοποιημένα βασικά μέρη του εν λόγω περιβάλλοντος, καθώς και μερικές από τις επιλογές του μενού της διεπαφής του. Η διεπαφή που χρησιμοποιείται είναι η Motif. Να σημειώσουμε ότι το SecuDE είναι ένα εμπορικό πακέτο-εργαλειοθήκη παρόμοιο με αυτό που αυτή η προσπάθεια προσπαθεί να υλοποιήσει και το οποίο περιλαμβάνει ευρέως διαδεδομένες συναρτήσεις κρυπτογράφησης. Επίσης το HOL είναι ένα πακέτο που παρέχει εύκολες διαδικασίες απόδειξης θεωρημάτων.

Όπως παρατηρούμε οι επιλογές του μενού περιλαμβάνουν τυπικές διαδικασίες επεξεργασίας αρχείων (χώρων επεξεργασίας) για μία πολιτική (Open, Save, Close), διαδικασίες πρόσβασης σε βάσεις με έτοιμα τμήματα κώδικα προγραμμάτων ή ορισμών κοινών δομών (access, κ.λπ).



ΣΧΗΜΑ 3.3. Το περιβάλλον διαχείρισης πολιτικών ασφάλειας SKIPPY.

ΠΗΓΗ: [BRY-1997c]

Επίσης, σημαντικά στοιχεία αποτελούν τα ακόλουθα:



- Η "γλώσσα ορισμού τύπων πολιτικών ασφάλειας" (type definition language), η οποία δανείζεται πολλά στοιχεία από τη γλώσσα Z (Z notation) [SPI-1992] αλλά είναι προσαρμοσμένη στις ανάγκες της εφαρμογής.
- Ο γεννήτορας κώδικα σε C++ από ορισμούς στη συγκεκριμένη γλώσσα ορισμού απαιτήσεων.
- Ο αλγόριθμος μετατροπής ορισμών τύπων πολιτικών ασφάλειας στο "Μοντέλο του Δικτυώματος" (Lat, βλ. παρακάτω).
- Μία άλγεβρα τυπικής αναπαράστασης πράξεων σε περισσότερες πολιτικές ασφάλειας.

Όπως είπαμε οι πολιτικές που υλοποιούνται πρέπει να στηρίζονται στο "Μοντέλο του Δικτυώματος". Αναγνωρίζεται η άποψη ότι το επιθυμητό περιβάλλον πρέπει να υποστηρίζει την ανάπτυξη πολλών πολιτικών ασφάλειας. Με άλλα λόγια θα ήταν σκόπιμο να επινοηθεί ένας συγκεκριμένος τύπος ορισμού πολιτικής που να καλύπτει πολλές περιπτώσεις ("...uniformly addressing of security policies...", [BRY-1997c]). Η συγκεκριμένη επιλογή οφείλεται τόσο στο γεγονός ότι αποτελεί ένα σημείο εκκίνησης, όσο και στην πεποίθηση ότι το συγκεκριμένο μοντέλο μπορεί να ενσωματώσει επιτυχώς διάφορα είδη πολιτικών ασφάλειας<sup>13</sup>. Δεν μπορούμε σαφώς να μην παρατηρήσουμε ότι η προσσέγιση είναι επηρεασμένη από τις αρχές του περιορισμού της προσπέλασης και της ροής της πληροφορίας. Ταυτόχρονα βέβαια σημειώνουμε ότι οι δύο αντές απόψεις επικρατούν στο χώρο της ασφάλειας των Πληροφοριακών Συστημάτων τόσο όσον αφορά τις θεωρητικές αναζητήσεις όσο και τις πρακτικές εφαρμογές.

Στην παρουσίαση του παραδείγματος ανάπτυξης μιας πολιτικής ασφάλειας στο περιβάλλον SKIPPY θα ακολουθήσουμε τη σειρά που προτάθηκε στην παράγρ.3.4.3.

Για τις ανάγκες της παρουσίασης, ας υποθέσουμε ότι η εφαρμογή για την οποία πρέπει να υλοποιήσουμε ένα πλαίσιο ασφάλειας συνίσταται σε μία εφαρμογή ηλεκτρονικού ταχυδρομείου. Επίσης υποθέτουμε ότι υπάρχει ένας αριθμός χρηστών με ισάριθμο πλήθος ταχυδρομικών κουτιών. Οι απαιτήσεις -πολιτική- ασφάλειας που αρχικά διατυπώνουμε είναι:

1. A1: Οι επικοινωνίες ηλεκτρονικού ταχυδρομείου πρέπει να εποπτεύονται μέσω της καταγραφής τους σε αρχείο (log file) χωρίς όμως να καταγράφονται τα περιεχόμενα των ανταλασσόμενων μηνυμάτων.
2. A2: Μόνο ο υπεύθυνος ασφάλειας έχει προσπέλαση στο περιεχόμενο των ηλεκτρονικών μηνυμάτων.
3. A3: Τα μηνύματα μπορούν να διαβαστούν μόνο κατά τη διάρκεια της νύχτας.
4. A4: Μόνο οι αποδέκτες που ρητά ορίζονται στο μήνυμα μπορούν να διαβάσουν το μήνυμα.
5. A5: Ενδέχεται σε μελλοντικό χρονικό σημείο η πολιτική μας να εμπλουτιστεί με στοιχεία ρόλων ή άλλα χαρακτηριστικά αναγνώρισης για σκοπούς ελέγχου προσπέλασης.

Τα βήματα της διαδικασίας έχουν ως εξής: 1) Σχεδιασμός πολιτικής ασφάλειας, 2) Έλεγχος πολιτικής ασφάλειας, 3) Υλοποίηση πολιτικής ασφάλειας.

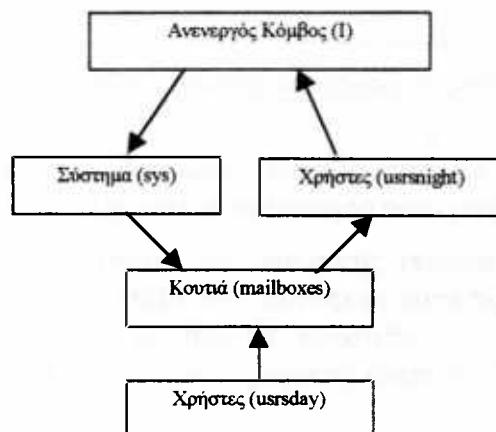
<sup>13</sup> Η αναλυτική επεξήγηση μπορεί να αναζητηθεί στο [BRY-1997b]



Θα αναφερθούμε αναλυτικά στο πρώτο μέρος, θα καλύψουμε συνοπτικότερα το επόμενο, ενώ θα περιγράψουμε απλά το τελευταίο εφόσον εξαρτάται από συγκεκριμένη υλοποίηση.

Προκειμένου να σχεδιάσουμε τον τρόπο με τον οποίο θα υλοποιήσουμε αυτή την πολιτική, η πρώτη μας κίνηση πρέπει να είναι ο έλεγχος των ήδη υπαρχουσών κλάσεων προκειμένου να διαπιστώσουμε αν μπορούμε να τις χρησιμοποιήσουμε.

Οι ήδη υπάρχουσες κλάσεις για εποπτεία είναι αρκετές<sup>14</sup> για να καλύψουν ως ένα βαθμό τις απαιτήσεις που τέθηκαν. Όσον αφορά τον έλεγχο προσπέλασης, χρησιμοποιήθηκαν έτοιμα τμήματα κλάσεων από το "Μοντέλο του Δικτυώματος". Ο αλγόριθμος μετατροπής των προδιαγραφών ελέγχου προσπέλασης σε ένα "Μοντέλο Δικτυώματος" δίνει τον παρακάτω γράφο:



ΣΧΗΜΑ 3.4. Το Δικτύωμα για τον έλεγχο προσπέλασης.

ΠΗΓΗ: [BRY-1997b]

Εκτός των περιορισμών προσπέλασης που μοντελοποιήθηκαν με βάση αυτό το σχήμα, αντιστοιχίζουμε στις υπόλοιπες προδιαγραφές, στις οποίες δεν αναλογεί κάποιο τυπικό μοντέλο πολιτικής ασφάλειας, τις ακόλουθες λειτουργίες:

- send\_mail και read\_mail που αντιστοιχούν στη συγκεκριμένη εφαρμογή
- day\_time και night\_time που αντιστοιχούν στη συγκεκριμένη πολιτική

Για την υλοποίηση της Α4, σε κάθε χρήστη δίδεται δικαιώματα ιδιοκτησίας για ένα ταχυδρομικό κουτί και ο έλεγχος της συνθήκης γίνεται προϋπόθεση για την εκτέλεση της διαδικασία read\_mail. Όλοι οι χρήστες έχουν δικαιώματα να στέλνουν μηνύματα σε άλλα κουτιά (δηλαδή σε άλλους χρήστες). Η αρχική κατάσταση της πολιτικής ασφάλειας περιλαμβάνει τις οντότητες και τα δικαιώματα προσπέλασης που υπάρχουν.

Στο ακόλουθο απόσπασμα χρησιμοποιείται η γλώσσα προσδιορισμού απαιτήσεων λογισμικού, για τη δήλωση αυτής της πολιτικής. Η δομή ενός ορισμού είναι η ακόλουθη:

<sup>14</sup> Δεν θα αναλύσουμε τις ήδη υπάρχουσες κλάσεις εδώ.

•Κατάσταση της πολιτικής (state)

- Σχήμα διαβάθμισης (classification schema) το οποίο (χρησιμοποιώντας το Δικτύωμα) εκφράζει τους διαχωρισμούς των οντοτήτων
- Μήτρα προσπέλασης της μορφής:  $m(e_1, e_2)$ , η οποία εκφράζει τα δικαιώματα προσπέλασης της οντότητας  $e_1$  στην  $e_2$

•Λειτουργίες που ενημερώνουν αυτή την κατάσταση (policy specific operations)

•Λειτουργίες της εφαρμογής την οποία η πολιτική θα ελέγχει (application specific operations)

**ΣΧΗΜΑ 3.5. Η δομή ενός ορισμού στη γλώσσα περιγραφής απαιτήσεων.**

Επίσης, δίνονται οι ακόλουθες διευκρινίσεις ως προς τις δεσμευμένες εκφράσεις ή σύμβολα προς πληρέστερη κατανόηση του ορισμού:

- **State:** δήλωση της κατάστασης της πολιτικής (περιλαμβάνει τον ορισμό της αρχικής κατάστασης και αμετάβλητων συνθηκών κατά τις αλλαγές)
- **Policy-Sets:** δήλωση των μεταβλητών της πολιτικής.
- **Classification:** δήλωση των σχέσεων μερικής διάταξης (partial relations) μεταξύ των οντοτήτων της πολιτικής.
- **Rights:** δήλωση των στοιχείων της μήτρας προσπέλασης  $m$  επιπλέον των υπαρχόντων.
- **Oper:** δήλωση των λειτουργιών που ενημερώνουν η ελέγχονται από την πολιτική.
- **where:** δήλωση σημασιολογίας.
- **pre:** δήλωση προϋποθέσεων για την εκτέλεση της λειτουργίας.
- **op:** δήλωση της σημασιολογίας του τελεστή σύγκρισης ( $\leq$ ) για τη διαβάθμιση της συγκεκριμένης πολιτικής.
- **Inv:** δήλωση σταθερών έγκυρων συνθηκών.

**Policy mailer=**

**Policy-Sets:**

/\*αντιπροσωπεύουν σύνολα οντοτήτων\*/  
role={usrday, usrsnight, sys, mailboxes, l};

**Classification:**

/\*αντιπροσωπεύει τις επιπρεπές ροές πληροφορίας για το "Μοντέλο του Δικτυώματος"\*/

role:{usrday ⊑ mailboxes, mailboxes ⊑ sys, mailboxes ⊑ usrsnight, sys ⊑ l, usr2 ⊑ l};

**Rights:**

/\*αντιπροσωπεύει τη μήτρα δικαιωμάτων προσπέλασης στην οποία απλά προστίθεται ένα νέο δικαίωμα\*/

{own};

**Oper:**

/\*ο χρήστης s διαβάζει μήνυμα από το κουτί o\*/  
read\_mail(s,o);

/\*μία οντότητα δεν μπορεί να διαβάσει άλλη οντότητα μεγαλύτερης διαβάθμισης\*/



**op:**  $s \leq_r o = cl(o) \leq_l cl(s)$ ;

/\*μόνο ο ιδιοκτήτης ή ο διαχειριστής έχουν αυτό το δικαίωμα\*/

**pre:**  $(s \leq_r o) \wedge ((own \in m(s,o)) \vee s = e_0)$ ;

**send\_mail(s,o):**

/\*ο χρήστης  $s$  στέλνει μήνυμα σε οποιοδήποτε κουτί  $o$  για το οποίο έχει δικαίωμα αποστολής\*/

**op:**  $s \leq_s o = cl(s) \leq_l cl(o)$ ;

**pre:**  $(s \leq_s o) \wedge ((send\_mail \in m(s,o))$ ;

**night\_time(s, o):**

/\*ο διαχειριστής του συστήματος αλλάζει το Δικτυωτό Μοντέλο έτσι ώστε να ισχύει τις νυχτερινές ώρες\*/

/\*μόνο ο διαχειριστής μπορεί να κάνει κάπι τέτοιο\*/

**op:**  $s \leq_n o = cl(s) = sys$ ;

/\*ορισμός σημασιολογίας: αλλαγή στην κατάσταση της πολιτικής\*/

**where**  $cl' = cl \oplus (s \rightarrow usrsnight)$ ;

**pre:**  $(s \leq_n o)$ ;

**day\_time(s,o):**

/\*ο διαχειριστής του συστήματος αλλάζει το Δικτυωτό Μοντέλο έτσι ώστε να ισχύει τις ώρες της μέρας\*/

/\*μόνο ο διαχειριστής μπορεί να κάνει κάπι τέτοιο\*/

**op:**  $s \leq_d o = cl(s) = sys$ ;

/\*ορισμός σημασιολογίας: αλλαγή στην κατάσταση της πολιτικής\*/

**where**  $cl' = cl \oplus (s \rightarrow usrsday)$ ;

**pre:**  $(s \leq_d o)$ ;

**Inv:** true;

/\*ορισμός έγκυρων καταστάσεων\*/

**State:**

/\*οι οντότητες του συστήματος\*/

**entities'** = { $i: N \mid 0 \leq i \leq 20 \bullet e_i$ };

/\* θο είναι ο διαχειριστής, θ1, έως θ10 είναι οι χρήστες, θ11, έως θ20 τα κουτιά τους, ενώ αρχικά βρισκόμαστε σε νυχτερινές ώρες\*/

$cl' = \{e_0 \rightarrow sys\} \cup \{i: N \mid 1 \leq i \leq 10 \bullet e_i \rightarrow usrsnight\} \cup \{i: N \mid 11 \leq i \leq 20 \bullet e_i \rightarrow mailboxes\}$ ;

/\*αρχικοποίηση μήτρας διακαιωμάτων με προσθήκη σε αυτή των δικαιωμάτων αποστολής μηνύματος και ιδικησίας κουπού/

$m' = \{i, j: N, N \mid (1 \leq i \leq 10), (11 \leq j \leq 20) \bullet (e_i, e_j) \rightarrow \{send\_mail\}\}$

⊕

$\{i: N \mid 1 \leq i \leq 10 \bullet (e_i, e_{i+10}) \rightarrow \{own\}\}$ ;

**End mailer.**

ΠΗΓΗ: [BRY-1997c]

Ο έλεγχος της πολιτικής που σχεδιάσαμε περιλαμβάνει έλεγχο των δεδομένων που διαμορφώνονται μετά τις αλλαγές ή προσθήκες στον κώδικα ή στις κλάσεις. Αναλυτικότερα, για την απαίτηση A1 δεν απαιτείται έλεγχος του κώδικα των κλάσεων εφόσον χρησιμοποιούνται μόνο οι υπάρχουσες οι οποίες είναι ήδη ελεγμένες. Η A2 απαιτεί όπως μόνο ο διαχειριστής έχει πρόσβαση στο περιεχόμενο των μηνυμάτων, δηλαδή:

$= ((cl(s)=sys) \wedge (cl(o)=mailboxes)) \Rightarrow pre \text{ read\_mail}(s,o)$

Αποδεικνύουμε τέτοιουν είδους προτάσεις χρησιμοποιώντας την άλγεβρα Z και υπάρχοντα δεδομένα από προηγούμενες αληθείς συνθήκες (π.χ. από τη δήλωση

του δικτυωτού μοντέλου), ή από την *κατάσταση* της πολιτικής (state). Επίσης το πακέτο HOL αποτελεί σημαντική βοήθεια στο σημείο αυτό. Στο πακέτο αυτό μπορούμε να ορίσουμε ορισμένα δεδομένα γενικά για πολιτικές, όπως για παράδειγμα τη διαβάθμιση (classification, cl) και τη μήτρα προσπέλασης (access matrix, m), και να προσαρμόσουμε τα στοιχεία εισόδου για την απόδειξη της εκάστοτε πολιτικής.

Η υλοποίηση απαιτεί όπως οι κλάσεις που συνθέτουν την πολιτική (δηλαδή τα τμήματα κώδικα για έλεγχο προσπέλασης, εποπτεία, καθώς και η κλάση η οποία αντιστοιχίζει τα αναγνωριστικά της πολιτικής e, σε αντικείμενα του συστήματος, process Ids και Object Ids) ενοποιηθούν και αρχικοποιηθούν. Η ασφάλεια που υποτίθεται ότι έχει το σύστημα ακολούθως είναι η ασφάλεια που παρέχει το λειτουργικό σύστημα-βάση, η ασφάλεια που παρέχει ο κώδικας του εξυπηρετητή ηλεκτρονικού ταχυδρομείου και η ορθότητα των μονάδων λογισμικού της πολιτικής που συγγράψαμε.

#### 3.4.4.4 Η προσέγγιση της εφαρμογής ηλεκτρονικού εμπορίου CWASAR ως προς την ασφάλεια

Το έργο CWASAR μελετά τη δημιουργία μιας υποδομής κατάλληλης για την ανάπτυξη εφαρμογών ηλεκτρονικού εμπορίου σε ευρωπαϊκό επίπεδο [BRY-1997a]. Η λειτουργικότητα της υποδομής αυτής δίνεται από το "Μοντέλο υπηρεσιών" (Service model). Εμείς ενδιαφερόμαστε για τα χαρακτηριστικά ασφάλειας (security features) του μοντέλου αυτού, τα οποία καταδεικνύουν πώς η ασφάλεια ενσωματώνεται στο πλαίσιο αυτό. Πρωταρχικά δεν ενδιαφερόμαστε για τις απαιτήσεις ασφάλειας (security requirements) σε ένα τέτοιο περιβάλλον. Για το λόγο αυτό, θα αναφέρουμε ονομαστικά τις απαιτήσεις αυτές:

- Ακεραιότητα
- Αυθεντικότητα
- Εποπτεία
- Εξουσιοδότηση
- Ασφάλεια επικοινωνιών

Η ασφάλεια ορίζεται επί των δεδομένων και των συναρτήσεων χειρισμού αυτών των δεδομένων. Εξάλλου ορίζεται και μία οντότητα χειρισμού της ασφάλειας η οποία ονομάζεται "Διαχειριστής Ασφάλειας" (Security Administrator) και αντιστοιχεί σε φυσικό πρόσωπο (ή μικρή ομάδα προσώπων) πλαισιωμένο από εργαλεία που υποβοηθούν το έργο του. Πιο συγκεκριμένα, ορίζεται μία μονάδα δεδομένων *Document*, με την οποία αντιμετωπίζονται όλα τα δεδομένα<sup>15</sup> από το σύστημα. Η μονάδα αυτή αντιστοιχεί σε μία κλάση του συστήματος. Για κάθε τέτοια μονάδα υπάρχει μία πολιτική ασφάλειας. Η πολιτική αυτή ορίζεται από μία κλάση κονσταντό. Το κατάλληλο στιγμιότυπο μιας τέτοιας κλάσης δημιουργείται κάθε φορά που ένα νέο δεδομένο τύπου *Document*, εισάγεται στο σύστημα. Τα δεδομένα επεξεργάζονται από αντίστοιχες συναρτήσεις (data handling functions). Η ασφάλεια υλοποιείται από μετα-συναρτήσεις ασφάλειας οι οποίες καλούνται στη θέση των

<sup>15</sup> Το "δεδομένο" έχει την έννοια της ελάχιστης δυνατής μονάδας πληροφορίας με νόημα για τη συγκεκριμένη εφαρμογή.



κανονικών συναρτήσεων. Οι συναρτήσεις αυτές υλοποιούν τις λειτουργίες των κανονικών συναρτήσεων αφού πρώτα "συμβουλευτούν" τον αντίστοιχο κουστωδό. Αποτελούν με άλλα λόγια τη διεπαφή με τον κουστωδό.

Ένα παράδειγμα θα διευκρινίσει τη θεωρία: Η συνάρτηση "get" επιστρέφει ένα αντικείμενο τύπου Document από τη Βάση Δεδομένων και υποθέτουμε ότι έχει οριστεί σε κάποιο σημείο, το οποίο δηλώνουμε ως SMWHR. Η συνάρτηση που ακολουθεί είναι η μετα-συνάρτηση για την get:

```
sf_get(Ident1:DocID; Ident2:CallerID)
begin
return ident1.custodian!get(Ident1, Ident2); /*πρόσβαση στο αντικείμενο μέσω του κουστωδού του.*/
end;
```

ΠΗΓΗ: [BRY-1997c]

Το γενικό μορφότυπο ενός κουστωδού, όπου ορίζεται η συνάρτηση του παραδείγματός μας και παραλείπονται οι υπόλοιπες, είναι το ακόλουθο:

```
class Custodian
state
procedure get(ident1:DocID; Ident2:CallerID)
/*επιστρέφει το αντικείμενο μετά από κάποια επεξεργασία*/
D:=SMWHR.get(Ident1);
return D;
end;

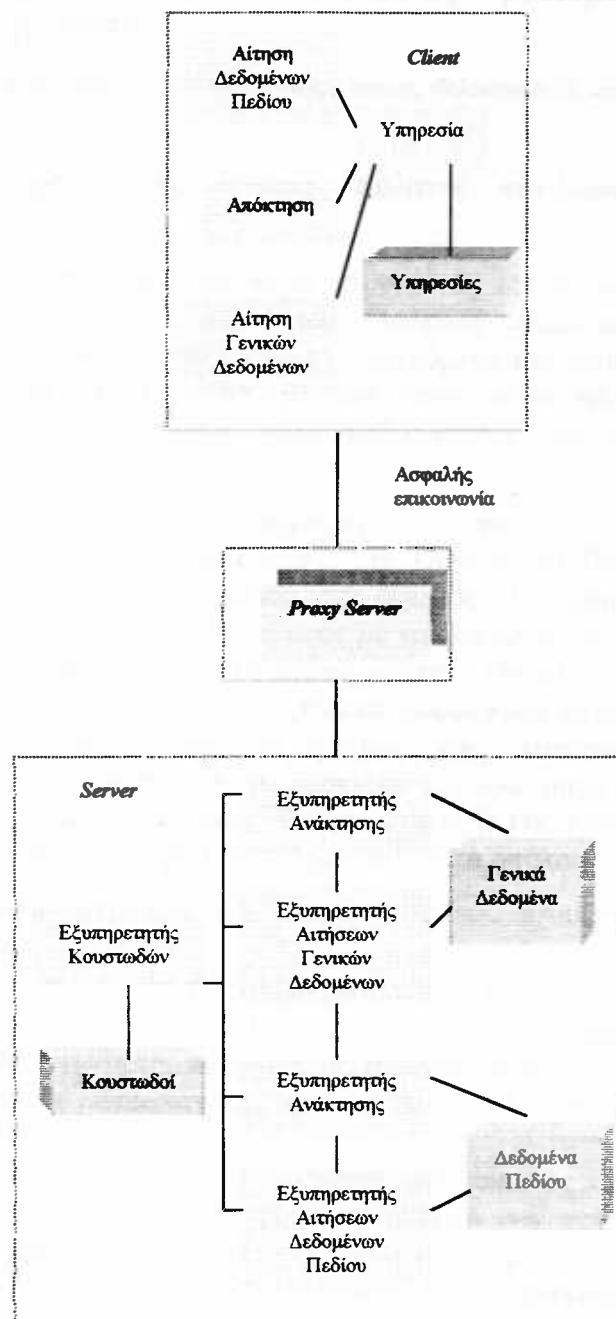
procedure put(Item:Document; Ident1:CallerID; Idebt2:DocID);
/*κάποια επεξεργασία*/
end;

end Custodian.
```

ΠΗΓΗ: [BRY-1997c]

Η αρχιτεκτονική του συστήματος παρουσιάζεται στο σχήμα 3.6. Παρατηρούμε ότι η ασφάλεια υλοποιείται με τον τρόπο που περιγράψαμε, ενώ υπάρχει ένας εξυπηρετητής-εκπρόσωπος (proxy server) για να χειρίζεται και να μεταβιβάζει τις αιτήσεις και τις αποκρίσεις, ενισχύοντας την ασφάλεια του συστήματος. Μπορούμε να φανταστούμε τα περιεχόμενα του εξυπηρετητή αυτού να ανταποκρίνονται στα ανάλογα του CWASAR εξυπηρετητή<sup>16</sup>.

<sup>16</sup> Τα χαρακτηριστικά ασφάλειας της αρχιτεκτονικής είναι ενδιαφέροντα άλλα δεν ανήκουν στο αντικείμενο της συζήτησης.



ΣΧΗΜΑ 3.6. Η αρχιτεκτονική του συστήματος CWASAR.

ΠΗΓΗ: [BRY-1997c]

### 3.5 Τυποποίηση πολιτικών ασφάλειας βασισμένη σε γλώσσες αναπαράστασης γνώσης

Γλώσσα Αναπαράστασης Γνώσης, Βάσεις Γνώσης, Φιλοσοφία Πολιτικής Ασφάλειας

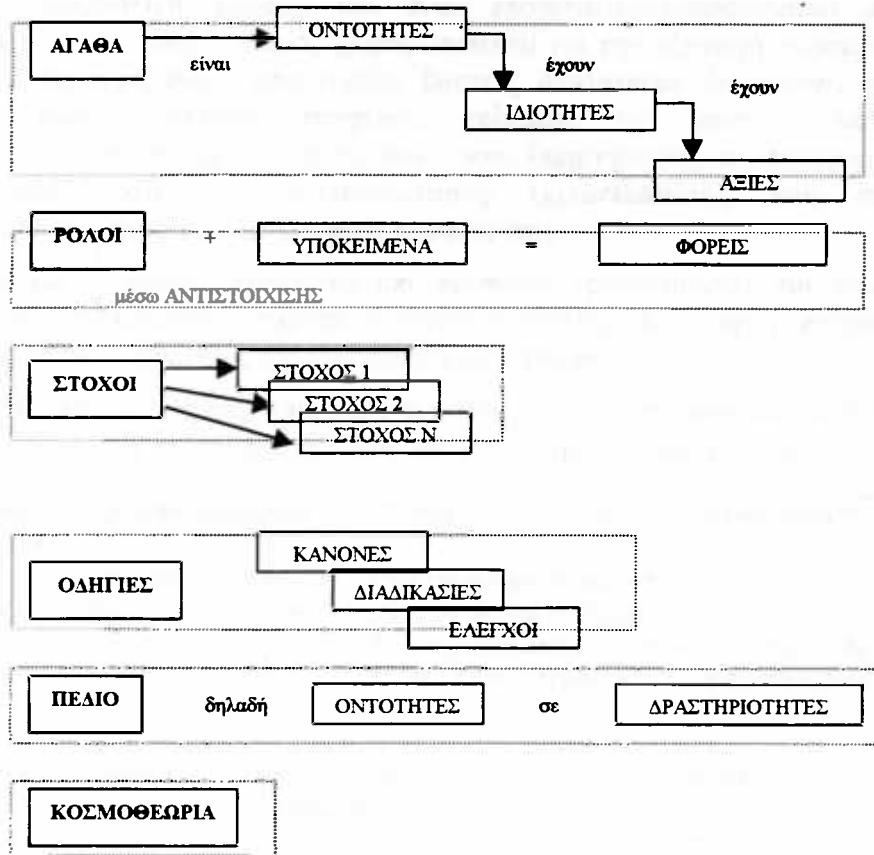
#### 3.5.1 Το περιεχόμενο της έννοιας "πολιτική ασφάλειας" Πληροφοριακού Συστήματος

Έχουμε παρατηρήσει ότι παρά το γεγονός ότι γενικά δεν υπάρχει ένας καθολικά αποδεκτός ορισμός της έννοιας "πολιτική ασφάλειας", κάθε προσέγγιση οριοθετεί με έναν συγκεκριμένο τρόπο το περιεχόμενο του όρου. Μάλιστα αργότερα θα παρατηρήσουμε ότι ο τρόπος με τον οποίο κάθε προσέγγιση προσεγγίζει εννοιολογικά την έννοια αυτή, είναι καθοριστικός και χαρακτηριστικός της μεθοδολογίας αντιμετώπισης του θέματος.

Μία αντιμετώπιση, που παρουσιάζεται από τους Ε.Κιουντούζη και Σ.Κοκολάκη που εργάζονται ερευνητικά στο Οικονομικό Πανεπιστήμιο Αθηνών, προτείνει έναν νέο τρόπο αντιμετώπισης του θέματος. Η εν λόγω προσέγγιση [ΚΟΚ-1997a] παραδέχεται ότι ο συνήθης τρόπος με τον οποίο οι οργανισμοί συγγράφουν τις πολιτικές ασφαλείας τους έχει τη μορφή γραπτού λόγου. Εντούτοις παρατηρείται ότι είναι ανάγκη να υπάρχει κάποιο τυπικό μορφότυπο ακόμη και σε αυτή την περίπτωση, εφόσον κάθε προσπάθεια ανάλυσης και τυποποίησης έχει ανάγκη από κάποια ομοιογένεια προκειμένου να θέσει τα αποτελέσματά της εφαρμόσιμα σε περισσότερες της μιας περιπτώσεις. Ορίζει λοιπόν [ΚΟΚ-1997a] ότι μια πολιτική ασφάλειας πρέπει να συντίθεται κατ' ελάχιστον από τα ακόλουθα στοιχεία:

- Αγαθά, δηλαδή οντότητες του συστήματος που έχουν αξία και πρέπει να προστατευθούν.
- Ρόλους, οι οποίοι ανατίθονται στις οντότητες του συστήματος.
- Στόχο, πρόκειται για το στόχο (ή τους στόχους) ασφάλειας που καθορίζει συνοπτικά την εστίαση της πολιτικής και θέτει περιορισμούς.
- Οδηγίες, με άλλα λόγια κανόνες που αποτελούν το βασικό συστατικό στοιχείο της πολιτικής.
- Πεδίο Ασφάλειας, με την έννοια του χώρου εμβέλειας της πολιτικής.
- Κοσμοθεωρία, η οποία περιλαμβάνει το σύνολο των πεποιθήσεων, αξιών και υποθέσεων που συνθέτουν την κουλτούρα του οργανισμού και του περιβάλλοντος αυτού και ανατροφοδοτούν τους μηχανισμούς του μέσω μιας διαδικασίας συνεχούς εκμάθησης.

Τα παραπάνω συστατικά στοιχεία αναλύονται σε γνωστές έννοιες και αναπαρίστανται γραφικά στο ακόλουθο σχήμα:



ΣΧΗΜΑ 3.7. Τα συστατικά στοιχεία της πολιτικής ασφάλειας.

ΠΗΓΗ: [ΚΟΚ-1997a]

### 3.5.2 Αναπαράσταση πολιτικών ασφάλειας μέσω της γλώσσας αναπαράστασης γνώσης "TELOS"

Θα ήταν ιδιαίτερα χρήσιμο να εισάγουμε τον αναγνώστη στη φιλοσοφία της χρησιμοποίησης γλωσσών αναπαράστασης γνώσης για την τυποποίηση πολιτικών ασφάλειας. Καταρχήν πρέπει να σημειώσουμε ότι αυτού του είδους οι προβληματισμοί δεν ξεκινούν μόνον ούτε αφορούν μόνον το πεδίο της ασφάλειας Πληροφοριακών Συστημάτων, αλλά αποτελούν επιστημονικές αναζητήσεις διαφόρων χώρων.

Η προσπάθεια βασίζεται στην παρατήρηση ότι **οι πολιτικές ασφάλειας διακρίνονται τόσο από άμεσα όσο και έμμεσα εκφραζόμενα χαρακτηριστικά και συστατικά στοιχεία** [ΚΟΚ-1997a & ΚΟΚ-1997b]. Επίσης ο τρόπος με τον οποίο βασικά θέματα αποφάσεων και επιλογών που πρέπει να αντιμετωπιστούν από το σύστημα και εμπίπτουν στο πεδίο ελέγχου της πολιτικής δεν καθορίζεται λεπτομερώς από αυτήν. Οι συγγραφείς διατείνονται ότι αυτή **η αναμφισβήτητη ύπαρξη δυσκαθοριζόμενων στοιχείων στις πολιτικές ασφάλειας υποστηρίζει τη χρήση γλωσσών αναπαράστασης γλώσσης για την έκφραση πολιτικών ασφάλειας**.

Η συγκεκριμένη γλώσσα αναπαράστασης που χρησιμοποιείται από την προσέγγιση είναι η γλώσσα *TELOS*. Η γλώσσα αυτή, γεγονός που διακρίνει όλες τις γλώσσες αναπαράστασης γνώσης, παρέχει μία *τυπική γλώσσα συμβολισμών* (notation), μία *βάση γνώσης* (knowledge base) που περιέχει δηλώσεις (statements) σε αυτή τη συμβολική γλώσσα και έναν *επαγωγικό συμπερασματικό μηχανισμό* (deductive mechanism) ο οποίος χρησιμοποιείται για την εξαγωγή συμπερασμάτων. Εξάλλου, το περιβάλλον υποστηρίζει βασικές διαδικασίες διαχείρισης της βάσης γνώσης, όπως ανάκτηση στοιχείων, επέκταση της βάσης, κ.λπ. Επίσης χρησιμοποιούνται οι μηχανισμοί της *συνένωσης* (aggregation), της *κατηγοριοποίησης* (classification) και της *γενικευσμότητας* (generalisation), που αποτελούν χαρακτηριστικά αντικειμενοστραφούς προσέγγισης.

Η βάση γνώσης αποτελείται από *προτάσεις* (propositions), που διακρίνονται σε *ατομικές* (individuals) αντιπροσωπεύουσες οντότητες και *ιδιότητες* (attributes), που αντιπροσωπεύουν δυαδικές σχέσεις μεταξύ οντότητων.

Ακολούθως, θα περιγράψουμε συνοπτικά τον τρόπο ορισμού των στοιχείων που συνθέτουν μία πολιτική ασφάλειας κατά την παρούσα προσέγγιση.

```
TELL CLASS PolicyElementMetaClass /*Ορισμός τύπου "PolicyElementMetaClass"*/
WITH
    Attributes: proposition; /*για τον ορισμό στοιχείων*/
    Relations: proposition; /*για τον ορισμό σχέσεων*/
    Constraints: proposition /*για την ακεραιότητα της πολιτικής. υπάρχει δε συγκεκριμένη άλγεβρα για την έκφραση αυτών*/
END

TELL CLASS PolicyElement /*Ορισμός στιγμιούπου μιας πολιτικής ασφάλειας
                           PolicyElement*/
WITH
    Attributes
        Title:string;
        Type:PolicyTypes; /*εξαρτάται από την εφαρμογή*/
        Owner:authority;
        Author:Person;
        Distribution:DistributionLevel; /*για παράδειγμα "περιορισμένο" "μη περιορισμένο" ή ελεγχόμενο*/
        Assurance:AssuranceClass; /*π.χ. επιθεωρήσεις, επίπεδο κρισμότητας, κ.λπ.*/
        Domain:Domain;
    Relations
        RelatedPolicies:PolicyElementMetaClass
END

/*οι ακόλουθοι ορισμοί περιγράφουν τα στοιχεία που συνθέτουν την πολιτική έτσι όπως την έχουμε περιγράψει*/
TELL CLASS PolicyContext IN policyElementMetaClass ISA PolicyElement
WITH
    Attributes
        Worldview:Views;
        Goal:Goals;
        Domain:DomainClass
END

TELL CLASS PolicyGuideline IN PolicyElementMetaClass ISA PolicyElement
```



WITH

Attributes

ID:Code;  
Description:Proposition;  
Trigger:Event

Relations

Contributing:PolicyGuideline;  
Prerequisite:PolicyGuideline;  
PrerequisiteFor:PolicyGuideline

END

TELL CLASS Role IN PolicyElementMetaClass ISA PolicyElement

WITH

Attributes

Description:Proposition;  
BindingSubjects:Subject;  
Activity:ActivityClass;  
Obligation:Proposition;  
Rights:Proposition;

Relations

RelatedRole  
RoleRelation:TypesOfRelations;  
Role:Role

END

TELL CLASS Asset IN EntityClass ISA PolicyElement

WITH

Attributes

AssetAttribute  
Description:Proposition;  
Value:Measurement

Relations

RelatedEntity  
Relationship:RelationshipType;  
Entity:EntityClass

Constraints

AssetConstraint:Proposition

END

TELL CLASS EntityClass IN PolicyElementMetaClass ISA PolicyElement

WITH

Attributes

Description:Proposition;

END

TELL CLASS Subject IN EntityClass ISA PolicyElement

WITH

Attributes

Type:Subjecttype;

END

TELL CLASS Agent IN PolicyElementMetaClass ISA Role,Subject

WITH

Attributes

GeneralDescription:Proposition;

Role:Role;  
Subject:Subject  
Relations  
Relationship:RelationshipType;  
RelatedAgent:Agent  
END

TELL CLASS Rule IN PolicyGuideline ISA PolicyElement

TELL CLASS Procedure IN PolicyGuideline ISA PolicyElement

TELL CLASS Control IN PolicyGuideline ISA PolicyElement

TELL CLASS Domain IN PolicyElementMetaClass

WITH

Attributes

Entity:EntityClass;  
Activity:ActivityClass;

Relations

Includes:Domain;  
Included:Domain;  
Overlaps:Domain;  
InteractsWith:Domain

END

TELL CLASS Activity IN PolicyElementMetaClass ISA PolicyElement

WITH

Attributes

Description:Proposition;  
Agent:Agent;  
Resource:Entity

END

ΠΗΓΗ: [ΚΟΚ-1997α]

Με τον τρόπο αυτό μπορούμε να ορίσουμε και τα υπόλοιπα στοιχεία της πολιτικής ασφάλειας, να εκλεπτύνουμε τους ορισμούς έτσι ώστε να περιλαμβάνουν πραγματικές περιπτώσεις και να συμπεριλάβουμε νέα στοιχεία. Μορούμε για παράδειγμα να ορίσουμε "Ετικέτες Ευαισθησίας" (Sensitivity Labels) και να τις θεωρήσουμε ως *Ιδιότητες* των Αγαθών. Τα χαρακτηριστικά της γλώσσας μας επιτρέπουν ευελιξία στην επεκτασιμότητα.

### 3.6 Τυποποίηση των πολιτικών ασφάλειας για το πληροφοριακό σύστημα με έμφαση στην έννοια του οργανισμού

Οργανισμός, Υπευθυνότητα, Υπηρεσίες, Μη-λειτουργικές απαστήσεις, Επικοινωνία, Θεωρία Έλλογων Δράσεων, Σημασιολογία

#### 3.6.1 Εισαγωγή

Η επόμενη προσέγγιση προέρχεται από ερευνητική εργασία που πραγματοποιείται στο University of Newcastle upon Tine και αφορά τη δημιουργία ενός πλαισίου αναφορικά με τη δημιουργία ασφαλών συστημάτων σε οργανισμούς. Η άποψη υπό την οποία θεωρείται η ανάπτυξη αυτού του πλαισίου στηρίζεται σε

αρχές αποδεκτές και βάσιμες. Θα παρατηρήσουμε ωστόσο ότι ορισμένες νεωτεριστικές απόψεις, που παρουσιάζονται από τον M. Martin, εισάγουν σκέψεις που απαιτούν περαιτέρω ερευνητική προσπάθεια.

### 3.6.2 Βασικές αρχές της προσέγγισης

Οι αρχές στις οποίες στηρίζεται η αντιμετώπιση που θα περιγράψουμε είναι οι ακόλουθες:

- Το σύστημα αναφοράς το οποίο χρειάζεται να αναλυθεί αναφορικά με τις απαιτήσεις ασφαλείας του, θεωρείται ότι αποτελείται από τα στοιχεία του συστήματος που συνθέτουν έναν σύγχρονο οργανισμό.
- Δίνεται έμφαση στον οργανισμό, δηλαδή το σύστημα αναφοράς ή το σύστημα στόχο. Όλες οι δομές που συνιστούν τον οργανισμό αυτό ως οντότητα πρέπει να αναγνωριστούν και να ληφθούν υπόψη σε οποιαδήποτε απόπειρα ανάλυσης του οργανισμού.
- Οι απαιτήσεις ασφάλειας ενός τέτοιου συστήματος θεωρούνται καταρχήν σαν μη-λειτουργικές απόψεις αυτού. Αναγνωρίζεται ότι αυτές οι μη-λειτουργικές απόψεις πρέπει τελικά να μεταφραστούν σε ορισμούς λειτουργικών απαιτήσεων για το σύστημα, που θα περιγράψουν είτε ύπαρξη είτε έλλειψη συγκεκριμένου βαθμού λειτουργικότητας.
- Οι μεθόδοι λογίας "μετάφρασης" απαιτήσεων από μη-λειτουργικές σε λειτουργικές δεν είναι τελειοποιημένες.
- Θεωρείται ότι ο πιο ενδεδειγμένος τρόπος προκειμένου να επιτευχθεί κάτι τέτοιο είναι η εις βάθονς ανάλυση των απαιτήσεων ασφάλειας με επίκεντρο τον ίδιο τον οργανισμό, τέτοια ώστε να κατανοηθεί πλήρως το "νόημά" τους, έτσι ώστε τα συμπεράσματα που θα προκύψουν να είναι σε θέση να δώσουν τα βασικά στοιχεία μίας γλώσσας ορισμού απαιτήσεων ασφάλειας σε λειτουργικό επίπεδο. Με αυτό τον τρόπο ο βαθμός στον οποίο οι απαιτήσεις που διαμορφώνουμε τυπικά, αναφορικά με την ασφάλεια του δεδομένου συστήματος συμπίπτουν με τις πεποιθήσεις που έχουμε σχετικά με την ασφάλεια του συστήματος σε άτυπο επίπεδο. Η προσέγγιση η οποία υιοθετείται για την ανάλυση ακολουθεί τον "από πάνω προς τα κάτω" (top-down) τρόπο εννοιολογικής αφαίρεσης.

### 3.6.3 Παρουσίαση της προσέγγισης

Δύο είναι τα μεγάλα κεφάλαια που περιλαμβάνει η προσέγγιση αυτή [MAR-1991]. Το πρώτο, αφορά τη μοντελοποίηση του οργανισμού και το δεύτερο την τυποποίηση της πολιτικής ασφάλειας του οργανισμού.

Η μέθοδος που χρησιμοποιείται προκειμένου για το πρώτο μέρος έχει ως στόχο να δώσει ένα **πλαίσιο διαδοχικών τυπικών περιγραφών ενός οργανισμού, συνεχώς μειούμενον βαθμού αφαίρεσης**. Θεωρείται εξάλλου ότι ο τρόπος με τον οποίο αυτό επιτυγχάνεται μπορεί να χρησιμοποιηθεί προκειμένου να βοηθήσει ανίδεους σε επίπεδο επιστημονικής (επί τυπικών μεθόδων ανάλυσης, πολιτικών ασφάλειας, κ.λπ.) κατάρτισης χρήστες, που όμως γνωρίζουν τον πρακτικό ορισμό του προβλήματος και του πεδίου αυτού, να εκφράσουν τις απαιτήσεις τους αναφορικά με τις απαιτήσεις που χρειάζονται για ενός ορισμένου σκοπού ανάλυσης. Η δε μοντελοποίηση αυτή γίνεται σε όρους:

- Υπευθυνοτήτων που ανατίθενται στα πλαίσια του οργανισμού και σχέσεων που δημιουργούνται εντός αυτού, αλλά και μεταξύ αυτού και του περιβάλλοντός του.
- Δραστηριοτήτων που εκτελούνται εντός αυτού.
- Πόρων που δημιουργούνται, αγοράζονται ή καταναλώνται κατά την εκτέλεση των παραπάνω δραστηριοτήτων.

Επίσης, θεωρείται ότι η μέθοδος αυτή είναι τέτοια που επιτρέπει στα αποτελέσματα της μοντελοποίησης να χρησιμοποιηθούν για σκοπούς διαδικασιών αυτοματοποίησης (engineering processes).

Το/τα μοντέλα που προκύπτουν με την εφαρμογή της μεθόδου πρέπει να περιλαμβάνουν:

1. Ορισμό οντοτήτων (agents) σε όρους υπευθυνοτήτων που κάθε οντότητα έχει προς τις υπόλοιπες.
2. Καθορισμός των σχέσεων μεταξύ των οντοτήτων σε όρους πόρων που η οντότητα χρησιμοποιεί στα πλαίσια που ορίζουν οι υπευθυνότητές της.
3. Ορισμό των πόρων σε όρους πρόσβασης που οι οντότητες έχουν σε αυτούς (όπως π.χ. δημιουργία, διαγραφή, ανάγνωση, γένεση, κ.λπ.).
4. Ορισμό ενός σχήματος που περιγράφει τις σχέσεις μεταξύ των πόρων πληροφορίας και των λοιπών πόρων, καθώς και τη συνέπεια αυτών των σχέσεων.
5. Ορισμό των συσχετίσεων μεταξύ των μοντέλων.

Ο τρόπος με τον οποίο εφαρμόζεται η έννοια της αφαίρεσης στη μέθοδο αυτή επιτρέπει να αναπτύσσονται διαδοχικά μοντέλα τα οποία στα υψηλά επίπεδα επιτρέπουν να ορίζονται εννοιολογικά σχήματα, ενώ καθώς η αφαίρεση βαίνει μειούμενη επιτυγχάνουν να ορίζουν πιο λογικά, του εννοιολογικού, σχήματα και να εντάσσουν σε αυτά στοιχεία πολιτικών ασφάλειας, διατηρώντας πάντα τη συνέπεια με το εννοιολογικό σχήμα.

Ο τρόπος επίσης με τον οποίο γίνεται η ανάλυση είναι ο ακόλουθος:

Καταρχάς, πρέπει να αναφερθεί ότι ο αριθμός των μοντέλων που θα παραχθούν εξαρτάται από τις εκτιμήσεις των αναλυτών και μπορούμε να τον εκτιμήσουμε αναφορικά με το εύρος του περιβάλλοντος που συνθέτει το ευρύτερο πεδίο μελέτης για τον οργανισμό μας. Μία κλασική προσέγγιση θα ανέπτυσε τρία μοντέλα: αυτό του κλάδου επιχειρήσεων στον οποίο ανήκει ο οργανισμός μας προκειμένου να περιγραφούν οι σχέσεις και οι αλληλεπιδράσεις με το περιβάλλον του, ένα γενικευμένο του τύπου του οργανισμού μας που θα δίνει τα βασικά στοιχεία που διαφοροποιούν τον οργανισμό από άλλες επιχειρήσεις και τέλος αυτό του συγκεκριμένου οργανισμού υπό μελέτη. Ακολούθως ταυτοποιούνται τα παραπάνω πέντε στοιχεία στους όρους ακριβώς που αναφέρθηκαν. Η ανάλυση αυτή είναι λεπτομερής στο βαθμό που ορίζεται από το επίπεδο αφαίρεσης, περιλαμβάνει όμως όλα τα απαραίτητα στοιχεία που θα απαιτούσε μία ανάλυση δραστηριοτήτων, ρόλων, πόρων, υπευθυνοτήτων στο περιβάλλον ενός οργανισμού. Η έννοια της υπευθυνότητας έχει κυρίαρχη ισχύ στο πλαίσιο αυτό. Τέλος πρέπει να σημειώσουμε ότι η ανάλυση δίνει έμφαση στο θέμα των περιορισμών στην πρόσβαση στους πόρους πληροφορίας, καθώς και στις αλληλεπιδράσεις μεταξύ των οντοτήτων.

Στην παραπάνω ανάλυση δεν εισάγουμε έννοιες που υποδεικνύουν οποιαδήποτε συγκεκριμένη υλοποίηση ή οποιαδήποτε συγκεκριμένη πολιτική ασφάλειας.

Η έννοια της **πολιτικής ασφάλειας** στην προσέγγιση αυτή είναι η ακόλουθη: ο σκοπός μιας πολιτικής ασφάλειας είναι να καθορίσει τα είδη της πρόσβασης σε πληροφοριακούς πόρους που είναι αποδεκτά και νόμιμα και να τα διαχωρίσει από αυτά που συνιστούν παραβίαση, με δεδομένο ότι έχουν εκτελεστεί συγκεκριμένες άλλες πράξεις. Το τελευταίο αυτό χαρακτηριστικό είναι πολύ σημαντικό και διαχωρίζει το μοντέλο που προτείνεται από άλλα μοντέλα ασφάλειας στο εξής: δίνεται έμφαση στο "ιστορικό" μίας συγκεκριμένης περίπτωσης (σε προηγούμενες δραστηριότητες, σε όλες τις οντότητες που λαμβάνουν μέρος, στη δομή των ρόλων και στις συσχετίσεις αυτών), όπου χρειάζεται να κληθεί η πολιτική ασφάλειας, τη στιγμή που άλλα μοντέλα λαμβάνουν υπόψη τους μόνο την ακολουθία των πράξεων που εμφανίζονται τη δεδομένη στιγμή.

Αναλυτικότερα, η αντιμετώπιση αυτή υιοθετείται ή πρέπει να υιοθετηθεί ήδη από την αρχή της κατασκευής ενός ασφαλούς συστήματος. Το εργαλείο το οποίο ενδείκνυται γι' αυτό το σκοπό είναι η "**Θεωρία των Έλλογων Δράσεων**"<sup>17</sup>, η οποία μελετά τον τρόπο με τον οποίο οντότητες εκτελούν καθήκοντα μέσα από την οργάνωση και ανάληψη κοινωνικών δραστηριοτήτων. Το γεγονός, με άλλα λόγια, ότι εκτελούνται συγκεκριμένες πράξεις δεν ενδιαφέρει από την άποψη της ανακάλυψης της ακολουθίας των λόγων που τις ενεργοποιούν, αλλά από την άποψη του καθορισμού των υποκείμενων δράσεων που προκύπτουν ως αποτέλεσμα των ρόλων και των καθηκόντων των οντοτήτων.

Η ανάλυση των συσχετίσεων κάθε είδους, και ιδιαίτερα των επικοινωνιών μεταξύ των οντοτήτων στο πλαίσιο μιας δράσης είναι καταλυτική γι' αυτή την προσέγγιση. Ετσι μπορούμε να πούμε ότι η προσέγγιση αυτή δίνει μία **βασισμένη στην επικοινωνία οντοτήτων υπόσταση στα μοντέλα ασφάλειας που εκφράζουν πολιτικές ασφάλειας**. Για παράδειγμα η πρόσβαση στους πόρους δεν θεωρείται ότι εξαρτάται από τους ρόλους των οντοτήτων που εμπλέκονται, αλλά από τις επικοινωνίες που προηγήθηκαν. Σημαντικές αρχές αυτής της θεωρίας είναι οι ακόλουθες:

- Αυστηρός καθορισμός του σκοπού κάθε επικοινωνίας. Το αποτέλεσμα δύο ακολουθιών επικοινωνιών μπορεί να είναι ταυτόσημο (π.χ. η απόκτηση ενός κωδικού πρόσβασης), εντούτοις η διαφοροποίηση στην προηγηθείσα επικοινωνία είναι εκείνη που καθορίζει το σκοπό.
- Περιγραφή (κατά το δυνατό) των προϋποθέσεων προκειμένου να διεξαχθεί η επικοινωνία. Οι πιο σημαντικές προϋποθέσεις αφορούν την εφικτότητα ή όχι μίας επικοινωνίας.
- Εμφαση στην περιγραφή της κατανοητότητας, συνοχής και πληρότητας μιας επικοινωνίας. Υπάρχει μία ολόκληρη θεωρία η οποία περιλαμβάνει τον ορισμό κριτηρίων για την περιγραφή μιας επικοινωνίας, η οποία μάλιστα είναι αρκετά τυπική (ορίζονται λ.χ. τύποι επικοινωνιών, όροι σύνδεσης της επικοινωνίας με τα συμφραζόμενα, δομή διαλόγου, περιορισμοί σε αυτήν, κ.λπ.), ώστε να επιτρέπει την εισαγωγή των αποτελεσμάτων της ανάλυσης σε μία βάση δεδομένων.
- Ανάλυση της επικοινωνίας στο ευρύτερο πλαίσιο που συγκροτούν τα δεδομένα καθήκοντα που ορίζονται εντός κάποιου οργανισμού.

<sup>17</sup> Ελεύθερη μετάφραση από το [MAR-1991].

- Ο πρωταρχικός λόγος για την ανάλυση των στοιχείων μίας επικοινωνίας είναι ότι μέσα από αυτήν γίνονται εμφανείς οι υπευθυνότητες (obligations, responsibilities). Περαιτέρω, οι υπευθυνότητες αυτές είναι εκείνες που συγκροτούν δηλώσεις μίας πολιτικής ασφάλειας (policy statements).

Προκειμένου να τεκμηριωθεί η βασισμένη σε επικοινωνίες υπόσταση των μοντέλων πολιτικών ασφάλειας, στην οποία αναφερθήκαμε, διενεργείται μία ανάλυση της λογικής των μοντέλων αυτών. Οι ειδικότερες ενέργειες μίας τέτοιας ανάλυσης περιλαμβάνουν:

### ■ **Ανάλυση της λογικής σύνταξης της γλώσσας**

Σκοπός αυτής της ενέργειας είναι η ανακάλυψη των δομών των απλών ή πολύπλοκων προτάσεων (στοιχείων επικοινωνίας). Όμως προκειμένου να είναι το παραγόμενο αποτέλεσμα κατάλληλο για τους σκοπούς που επιθυμούμε, πρέπει η ανάλυση να παράγει δομές κατάλληλες να αποδώσουν τη δημιουργία, κατανομή και αφαίρεση υπευθυνοτήτων στο περιβάλλον που συνθέτουν ένας οργανισμός και τα πληροφοριακά του συστήματα. Δεδομένης της πολυπλοκότητας μίας τέτοιας ανάλυσης πρέπει να γίνει η σύμβαση ότι τα μέλη του οργανισμού θα ορίσουν ένα πεπερασμένο σύνολο στοιχείων επικοινωνίας το οποίο θα υποστεί ανάλυση.

### ■ **Ορισμός λογικών υποθέσεων**

Οι υποθέσεις αυτές διασφαλίζουν τη συνέπεια των αποτελεσμάτων των αναλύσεών μας, και δει:

- Το γεγονός ότι είναι δυνατή η ανάλυση της λογικής σύνταξης της γλώσσας σε όρους λεκτικών δράσεων (του τύπου π.χ. δέξου, απέρριψε, κ.λπ.).
- Η λογική σύνταξης της γλώσσας μπορεί να παρασταθεί τυπικά.
- Είναι δυνατό να δημιουργηθεί μία τυπική σημασιολογία που θα ανταποκρίνεται στο τυπικό συντακτικό, έτσι ώστε να αντιστοιχίζει το συντακτικό αυτό σε ένα πεδίο στοιχείων (όπου τα στοιχεία αποτελούν υπευθυνότητες).
- Με δεδομένες τις παραπάνω υποθέσεις, συνδυασμένες με επιπλέον υποθέσεις εκ μέρους του οργανισμού (problem owner), διαμορφώνεται μία ακολουθία ενεργειών οι οποίες θεωρείται ότι μπορούν να αυτοματοποιηθούν.

### ■ **Ταντοποίηση των λογικών αρχών που διέπουν ένα μοντέλο πολιτικής ασφάλειας**

Οι ακόλουθες αρχές πρέπει να διέπουν ένα μοντέλο πολιτικής ασφάλειας προκειμένου αυτό να είναι συμβατό με τις αρχές της θεωρίας την οποία περιγράψαμε:

- Πρέπει να βασίζεται στη λογική ότι αυτό που ενδιαφέρει την ασφάλεια είναι ο συνεχής έλεγχος της συμπεριφοράς του συστήματος, με στόχο όχι αυτή καθεαυτή τη συμπεριφορά, αλλά το σκοπό του συστήματος, ο οποίος είναι η παροχή συγκεκριμένων υπηρεσιών στους χρήστες.
- Οι λογικές οντότητες του συστήματος πρέπει να αντιπροσωπεύουν είτε οντότητες που συμμετέχουν σε μία επικοινωνία, είτε πληροφοριακούς πόρους, και όχι υποκείμενα και αντικείμενα. Η διατήρηση αυτής της αρχής επιδρά και επί του βαθμού της αφαίρεσης που υιοθετείται.

- Οι δηλώσεις της πολιτικής ασφάλειας προκύπτουν από επικοινωνίες και οι περιορισμοί που υφίστανται για μία δεδομένη (αρχική) επικοινωνία πρέπει να διατηρούνται στην ακολουθία των επικοινωνιών που ενδεχόμενα ακολουθούν.
- Παρά το γεγονός ότι οποιαδήποτε προσπάθεια τυποποίησης πρέπει να είναι τόσο γενική ώστε, αφενός να διασφαλίζεται η συνέπειά της με την πραγματικότητα, αφετέρου δε να προεξοφλείται (κατά τὸ δυνατό) η εφαρμοσιμότητά της σε περισσότερες της μίας περιπτώσεις, πρέπει να λαμβάνεται υπόψη ότι σε ένα δεδομένο στάδιο της όλης προσπάθειας θα απαιτηθεί ερμηνεία κάθε αποτελέσματος των μελετών σε ένα συγκεκριμένο πεδίο-στόχο (target system). Αυτό σημαίνει ότι η προσπάθεια ανακάλυψης των λογικών δομών πρέπει αναπόφευκτα να αφορά κάποιο συγκεκριμένο είδος στοιχείων επικοινωνίας (instances) και όχι γενικευμένους τύπους επικοινωνίας (types).

Η εργασία που η παραπάνω θεωρία απαιτεί πρέπει να επικεντρωθεί κατά τις εκτιμήσεις μας στη δημιουργία, κατά πρώτο λόγο, ενός συστήματος ορισμού ασφάλειας στα πλαίσια που διαμορφώνονται από την παραπάνω θεωρία. Το σύστημα αυτό πρέπει να ορίσει εννοιολογικά τα δομικά στοιχεία που συνθέτουν το σύστημα αναφοράς, το βαθμό αφαίρεσης που απαιτείται, μία γλώσσα τυπικής περιγραφής των δομικών στοιχείων και μία σημασιολογία για τις τυπικές περιγραφές, που θα τις αντιστοιχίζουν στα εννοιολογικά τους αντίστοιχα. Ακολούθως απαιτείται η δημιουργία ενός αντίστοιχου συστήματος για τη δομή των επικοινωνιών. Το σύστημα αυτό θα ορίζει τις δομές των επικοινωνιών στα πλαίσια που διαμορφώνονται από την παραπάνω θεωρία, σε όρους τύπων επικοινωνίας, τύπων στοιχείων επικοινωνίας, κ.λπ. Ταυτοχρόνως απαιτείται ένα σύστημα ελέγχου της ανταπόκρισης μεταξύ των δύο προηγούμενων συστημάτων. Τέλος, χρειάζεται ένα σύστημα ορισμού του "νοήματος της πληροφορίας". Η ανάγκη αυτή προκύπτει από το γεγονός ότι μέσα στα πλαίσια που έθεσαν οι απαιτήσεις αυτής της θεωρίας, πρέπει να αποδωθεί ιδιαίτερη σημασία σε στοιχεία σημασιολογίας. Για παράδειγμα υπονοείται από την έμφαση στην επικοινωνία ότι ενδιαφέρει η μετάδοση όχι μόνο δεδομένων αλλά και νοημάτων (Οι όροι της βιβλιογραφίας που μπορεί να ενδιαφέρουν στο σημείο αυτό είναι οι ακόλουθοι: transmission of data, transmission of meaning, information flow, meaning flow).

### 3.7 Μερικώς αυτοματοποιημένη ανάπτυξη πολιτικών ασφάλειας βασισμένη στο πλαίσιο IBAG και σε έννοιες της Ανάλυσης Επικινδυνότητας

Ανάλυση Επικινδυνότητας IBAG, Αρχές, Οδηγίες, Αντίμετρα, Υποδομή Ασφάλειας, SIDERO

#### 3.7.1 Εισαγωγή

Η προσέγγιση την οποία θα αναπτύξουμε στην παράγραφο αυτή εντάσσεται στα πλαίσια ενός ευρωπαϊκού κοινοτικού προγράμματος το οποίο ασχολήθηκε με θέματα ασφάλειας στον τομέα των Πληροφοριακών Συστημάτων Υγείας [FLI-1997]. Οι στόχοι του έργου αυτού συνοψίζονται στην παραγωγή γενικών οδηγιών ασφάλειας για εγκαταστάσεις νοσοκομείων, καθώς και πρακτική εφαρμογή αντίμετρων μετά από διενέργεια Ανάλυσης Επικινδυνότητας. Όπως θα περιγραφεί

στα ακόλουθα, επιχειρήθηκε η κατά ιεραρχικά επίπεδα, ανάλογα με την ιεραρχική δόμηση υπευθυνοτήτων των οργανισμών, αντιμετώπιση των Πληροφοριακών Συστημάτων. Γενικά, η αναφορά σε στοιχεία που ανήκουν στο σύστημα που αποτελεί ο εκάστοτε οργανισμός Υγείας θεωρείται μεγάλης σημασίας για την ανάπτυξη και διαχείριση των πολιτικών ασφάλειας.

Στα πλαίσια αυτού του έργου έκπονήθηκε η ανάπτυξη ενός αυτοματοποιημένου εργαλείου υποστήριξης της διαχείρισης των πολιτικών ασφάλειας Πληροφοριακών Συστημάτων Υγείας.

Πρέπει να σημειώσουμε ότι η παρούσα προσέγγιση αφορά ένα συγκεκριμένο χώρο εφαρμογής πολιτικών ασφάλειας. Ωστόσο η επικέντρωση αυτή δεν επηρεάζει το ενδιαφέρον που παρουσιάζει η μεθοδολογία, η οποία πρωταρχικά ενδιαφέρει αυτή τη μελέτη. Θα εστιάσουμε λοιπόν στα σημεία που επιδεικνύουν μεθοδολογικά θέματα.

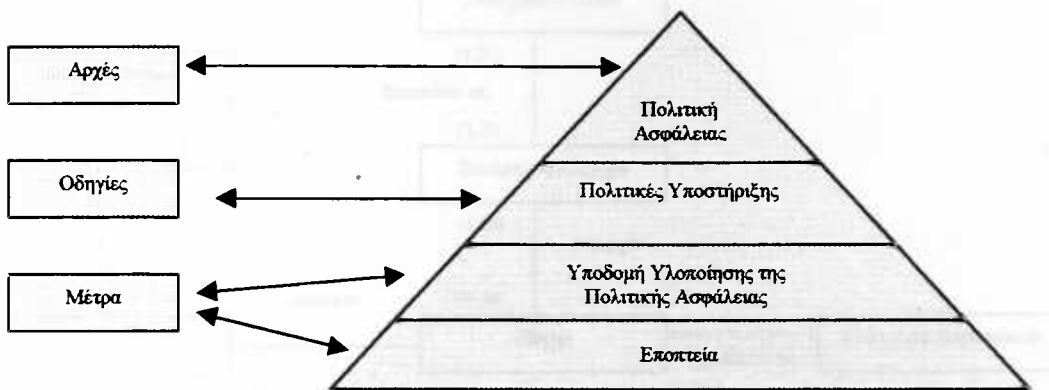
### 3.7.2 Παρουσίαση της προσέγγισης

Το πρώτο πρόβλημα το οποίο αναγνωρίστηκε αφορά την ανυπαρξία μίας κοινής και συνεπούς υποδομής αναφοράς (infrastructure), όσον αφορά τα σημαντικά συστατικά στοιχεία του περιβάλλοντος εφαρμογής<sup>18</sup>. Η ανάγκη για τον προσδιορισμό μίας υπάρχουσας δομής στην οποία θα στηριχτεί η νέα δομή, την οποία συνιστά η πολιτική ασφάλειας, αποτελεί σημαντικότατη διάσταση του θέματος της ανάπτυξης ενός πλαισίου που θα καλύπτει τη γενικότητα των περιπτώσεων.

Προκειμένου να αντιμετωπιστεί το θέμα αυτό, δημιουργήθηκε σε υψηλό επίπεδο αφαίρεσης ένα γενικευμένο μοντέλο του συστήματος εφαρμογής ως προς την ασφάλειά του. Το μοντέλο αυτό υιοθετεί μία ιεραρχική αφαιρετική άποψη για την ανάπτυξη, εφαρμογή και διαχείριση των πολιτικών ασφάλειας, όπου η αφαίρεση ορίζει επίπεδα Γενικών Αρχών, Οδηγιών και Μέτρων. Οι τρεις αυτές έννοιες αποτελούν κλειδιά για την παρούσα προσέγγιση. Η Ανάλυση Επικινδυνότητας, που αντιπροσωπεύεται από τον όρο "αντίμετρο", θεωρείται ένα από τα σημεία εκκίνησης.

Το πλαίσιο IBAG [IBAG-1993] επίσης, παρέχει μία πλήρη βάση αναφοράς για την ανάπτυξη και λειτουργία μίας πολιτικής ασφάλειας. Το πλαίσιο προϋποθέτει και προτείνει ένα τέτοιο σημείο εκκίνησης, ορίζοντας περιοχές τις οποίες ελέγχει μέσω συναρτήσεων ελέγχου. Αναγνωρίζονται επίπεδα στην ανάπτυξη και εφαρμογή των πολιτικών ασφάλειας. Η επιλογή του πλαισίου δικαιολογείται επίσης από το γεγονός ότι οι ανάγκες που θέτει το περιβάλλον εφαρμογής είναι συμβατές με τις απαιτήσεις του πλαισίου:

<sup>18</sup> Ο όρος "σύστημα/περιβάλλον εφαρμογής ή αναφοράς" δηλώνει το Πληροφοριακό Σύστημα Υγείας.



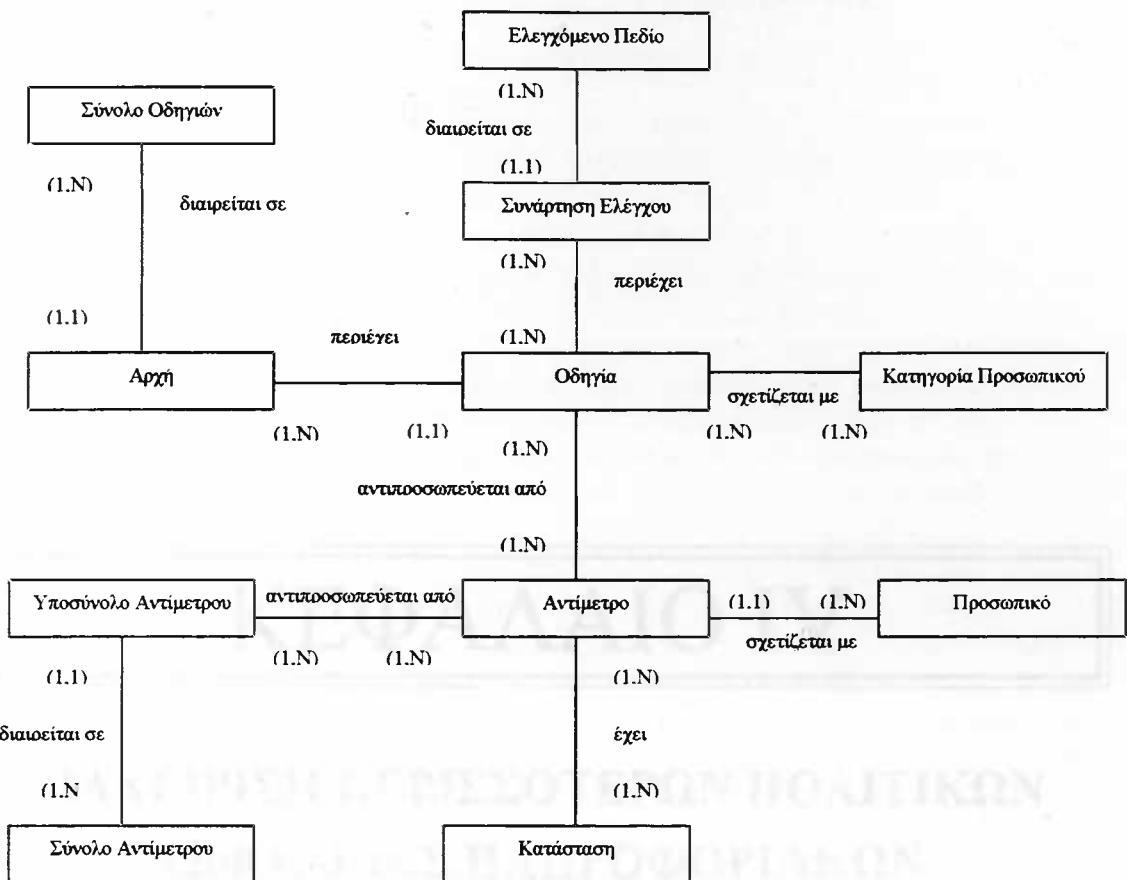
**ΣΧΗΜΑ 3.8. Το πλαίσιο IBAG σε αντιστοιχία με τα επίπεδα ανάπτυξης ασφαλούς πληροφοριακού συστήματος.**

Το εργαλείο *SIDERO* (Security Information Database Experimental Reference Centre Outcome), αποτέλεσε ένα από τα προϊόντα που μας ενδιαφέρουν. Η προσπάθεια ήταν να αναπτυχθεί ένα προτότυπο σύστημα που θα βοηθήσει τους διαχειριστές ασφάλειας να διαχειριστούν τη διαδικασία σχεδίασης και υλοποίησης, ολοκληρώνοντας τις επιμέρους εργασίες.

Το σχ. 3.9. δείχνει το Μοντέλο Οντοτήτων για το σύστημα. Στη Βάση Δεδομένων του ανάλογου σχεσιακού μοντέλου εισήχθηκαν τα προϊόντα προηγούμενων φάσεων, αρχές, οδηγίες και αντίμετρα, μαζί με σχετικά στοιχεία για τον οργανισμό. Το υπάρχον εργαλείο έχει γραφική διεπαφή.

Οι χρήσεις του εργαλείου αυτού βρίσκονται υπό συνεχή διερεύνηση. Μπορεί, ωστόσο, κάποιος να παρατηρήσει τα εξής σημεία:

- Το εργαλείο μπορεί να χρησιμοποιηθεί για την ανάπτυξη πολιτικής ασφάλειας για ένα σύστημα, με τη δημιουργία λ.χ. υποεφαρμογών οι οποίες θα δέχονται σε φόρμες εισαγωγής στοιχεία και θα παράγουν αναφορές διαφόρων τύπων και ως προς διάφορες παραμέτρους ή θέματα, προς χρήση σε συζητήσεις με στελέχη της διοίκησης για τη διαμόρφωση πολιτικής.
- Επίσης, δεδομένου του ότι το εργαλείο εμπεριέχει τις συσχετίσεις μεταξύ αρχών-οδηγιών και αντίμετρων, είναι δυνατή η ιχνηλάτηση κάθε υλοποιηθέντος αντιμέτρου με την πολιτική ασφάλειας.
- Η εποπτεία αποτελεί μία άλλη διαδικασία που μπορεί το εργαλείο να επικουρήσει. Περιλαμβάνει δε την παραγωγή αναφορών των αρχών-οδηγιών που δεν έχουν καλυφθεί από αντίμετρα (παρατηρήστε ότι τα αντίμετρα έχουν το χαρακτηριστικό "κατάσταση").
- Το εργαλείο απεικονίζει, με κατάλληλη ενημέρωση, κάθε στιγμή τις υπάρχουσες συσχετίσεις ασφάλειας στον οργανισμό. Μπορεί, κατ' αυτόν τον τρόπο, να χρησιμεύσει σαν στοιχείο συνεπούς, συνεχούς και ευέλικτης τεκμηρίωσης και εποπτείας της πολιτικής ασφάλειας.



ΣΧΗΜΑ 3.9. Το μοντέλο οντοτήτων-συσχετίσεων του εργαλείου SIDERΟ.

ΠΗΓΗ: [FLI-1997]

## ΚΕΦΑΛΑΙΟ IV

### ΔΙΑΧΕΙΡΙΣΗ ΠΕΡΙΣΣΟΤΕΡΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

#### 4.1 Οι εξελίξεις που συνθέτουν το περιβάλλον της ασφαλούς επικοινωνίας και διαλειτουργικότητας Πληροφοριακών Συστημάτων

Τεχνολογία Επικοινωνιών, Ασφαλής Διαλειτουργικότητα

Οι εξελίξεις οι οποίες έθεσαν το θέμα της διαλειτουργικότητας (interoperability) μεταξύ Πληροφοριακών Συστημάτων υπήρξαν αποτέλεσμα της γενικότερης επανάστασης στις επικοινωνίες (communications) η οποία τελέστηκε πριν αρκετά χρόνια και της οποίας την εξέλιξη συνεχίζουμε να παρακολουθούμε ως τις μέρες μας. Θα λέγαμε μάλιστα ότι η πρόδος στις επικοινωνίες αποτέλεσε τη δύναμη ώθησης, έτσι ώστε να γίνει δυνατή και εύκολη η επίτευξη στόχων και η ικανοποίηση αναγκών που τα ίδια τα Πληροφοριακά Συστήματα απαίτησαν, δημιουργησαν ή έφεραν στην επιφάνεια. Η εισβολή των Πληροφοριακών Συστημάτων σε πλήθος και ποικιλία τομέων άγγιξε φυσιολογικά το θέμα της επικοινωνίας μεταξύ οντοτήτων, βασικού συστατικού της επιχειρηματικής και καθημερινής ζωής και πρακτικής. Εξάλλου, οι ανάγκες και οι δυνατότητες, που υπήρξαν κύημα της Πληροφορικής, εστίασαν κατά πολύ το επίκεντρό τους στην καταμέριση και αποκέντρωση των εργασιών που έλεγχαν ή πραγματοποιούσαν, γεγονός που αποτελεί γενικότερη παρατήρηση στη διαχείριση εργασιών. Ο διαχωρισμός της επικοινωνίας από τη διαλειτουργικότητα είναι σχετικά σαφής. Μπορούμε να παρατηρήσουμε για το σκοπό αυτό ότι η επίτευξη επικοινωνίας προηγείται της διαλειτουργικότητας χρονολογικά, γεγονός που υποδεικνύει εμμέσως πλην σαφώς ότι κατά παρόμοιο τρόπο και πρακτικά προϋποτίθεται η ύπαρξη επικοινωνίας για την επίτευξη διαλειτουργικότητας. Έτσι, σε μία αυστηρά απόλυτη εκτίμηση, η επικοινωνία δεν περιλαμβάνει τη διαλειτουργικότητα, ενώ η δεύτερη απαιτεί την πρώτη.

Σε κάθε σύστημα επικοινωνίας απαιτείται η ύπαρξη ενός πρωτοκόλλου που την επιτυγχάνει. Κάποιος συγκεκριμένος τρόπος συνομιλίας χρειάζεται ακόμη και στην περίπτωση που τα συνομιλούντα μέρη έχουν αρκετά σημεία κοινά στην υποδομή που χρησιμοποιούν για το σκοπό αυτό. Ο εντοπισμός ενός κοινού τρόπου επικοινωνίας γίνεται μέσω διαπραγμάτευσης. Ωστόσο δεν θα μπορούσαμε να μην παρατηρήσουμε ότι όσο πιο υψηλό είναι το επίπεδο της επικοινωνίας (κοινώς, επικοινωνία σε επίπεδο εφαρμογής), τόσο αυξημένες και πολύπλοκες είναι οι ανάγκες και τόσο περισσότερο απομακρυνόμαστε από το σύνολο των κοινών σημείων, με αποτέλεσμα τα σημεία σύγκρουσης να είναι όχι μόνο πολλά και σύνθετα, αλλά επίσης να είναι δύσκολα στον εντοπισμό ή στην πρόβλεψή τους. Είναι βέβαια προφανές ότι τα προβλήματα αυτά δημιουργούνται κατά πρώτον λόγω της έλλειψης σχεδιαστικών αρχών στην ανάπτυξη των συστημάτων. Η αναρχία που έχει επικρατήσει στον τομέα της ανάπτυξης Πληροφοριακών Συστημάτων είναι γνωστή και δικαιολογεί απόλυτα την έξαρση και εντατικοποίηση των προσπαθειών προτυποποίησης σε διάφορους τομείς. Όπως χαρακτηριστικά αναφέρεται στο [GON-1994], το Υπουργείο Άμυνας - των Ηνωμένων Πολιτειών της Αμερικής εκτιμά ότι λειτουργούν υπ' αυτό πάνω από 10.000 δίκτυα παγκοσμίως, τα περισσότερα από τα οποία δεν μπορούν να υποστηρίζουν εφαρμογές που απαιτούν διαλειτουργικότητα.

Το θέμα της ασφάλειας στις επικοινωνίες αποτελεί ένα από τα πιο ενδιαφέροντα πεδία έρευνας. Κάθε προσπάθεια επίλυσης των σχετικών προβλημάτων δεν μπορεί παρά να λάβει υπόψη την άποψη της ασφαλούς διαλειτουργικότητας. Μάλιστα δεν θα ήταν πλεονασμός αν υποστηρίζαμε ότι το ουσιαστικό θέμα, ο

στόχος, είναι η επίτευξη ασφάλειας στη διαλειτουργικότητα και όχι στην επικοινωνία. Η ασφάλεια εντούτοις καλύπτει τόσες πτυχές στη λειτουργία ενός συστήματος, πτυχές οι οποίες διασταυρώνονται και αλληλεπιδρούν, ώστε προστίθονται επιπλέον προβλήματα προς επίλυση.

Συμπερασματικά, θα λέγαμε ότι η ασφαλής διαλειτουργικότητα αποτελεί ταυτόχρονα ανεπίλυτο πρόβλημα και μέγιστο ζητούμενο της σύγχρονης εποχής της Ψηφιακής Τεχνολογίας και της Πληροφορίας.

## 4.2 Ασφαλής διαλειτουργικότητα, σύνθεση και συμβατότητα πολιτικών ασφάλειας Πληροφοριακών Συστημάτων

Αυτονομία, Ασφάλεια, Πολυπλοκότητα, NP-complete προβλήματα

Ο σκοπός μας στην παράγραφο αυτή θα είναι να ορίσουμε κατά το δυνατό την έννοια της ασφαλούς διαλειτουργικότητας. Οι αναφορές μας, ωστόσο, δεν θα είναι αναλυτικές, αλλά θα περιοριστούν στην παράθεση γεγονότων (facts). Ο αναγνώστης μπορεί να αναζητήσει τις αποδείξεις των παρακάτω θεωρημάτων, λημμάτων, κ.λπ. στο [GON-1994].

Οι αρχές οι οποίες πρέπει να ισχύουν σε συνθήκες διαλειτουργικότητας συστημάτων είναι οι εξής δύο:

- **Αρχή της αυτονομίας:** Κάθε πρόσβαση η οποία επιτρέπεται σε κάποιο ατομικό (individual) σύστημα πρέπει να επιτρέπεται και σε συνθήκες ασφαλούς διαλειτουργικότητας.
- **Αρχή της ασφάλειας:** Κάθε πρόσβαση η οποία απαγορεύται σε ένα ατομικό σύστημα πρέπει να απαγορεύεται επίσης σε συνθήκες διαλειτουργικότητας μεταξύ συστημάτων.

Θεωρούμε ότι το σύστημά μας αποτελείται από μονάδες (αντικείμενα, χρήστες, μηχανές, κ.λπ.) και ότι η ασφάλειά του εκφράζεται από μία μήτρα ελέγχου προσπέλασης. Η προσπάθειά μας εντοπίζεται στην οριοθέτηση της έννοιας της ασφαλούς διαλειτουργικότητας και στον καθορισμό του βαθμού πολυπλοκότητας εντοπισμού των παραβιάσεων ασφάλειας, που μπορούν να συμβούν σε συνθήκες διαλειτουργικότητας και της εξάλειψης αυτών, διατηρώντας ένα συγκεκριμένο βαθμό διαλειτουργικότητας. Ειδικότερα, θεωρούμε ότι κάθε υποκείμενο έχει δικαίωμα πρόσβασης σε ένα μόνο αρχείο. Καλούμε το υποκείμενο και το αντίστοιχο αρχείο οντότητα. Ο ορισμός της ασφάλειας σε ένα τέτοιο σύστημα είναι ο εξής:

### © ΟΡΙΣΜΟΣ !

Ένα ασφαλές σύστημα περιγράφεται από μία μήτρα ελέγχου προσπέλασης της μορφής  $G = \langle V, A \rangle$  όπου  $V$  είναι ένα σύνολο οντοτήτων και  $A$  είναι μία δυαδική σχέση "access" στο  $V$  η οποία είναι αντιμεταθετική, μεταβατική και αντισυμμετρική.

Γραφικά, μπορούμε να παραστήσουμε το σύστημά μας σαν έναν κυκλικό κατεύθυνόμενο γράφο, όπου  $V$  είναι το σύνολο των κόμβων και  $A$  είναι το σύνολο των τόξων. Ισχύει ότι δύο κόμβοι  $u$ ,  $v$  συνδέονται από το τόξο  $(u, v)$  αν και μόνον αν η σχέση  $A$  περιέχει τη δυαδική σχέση " $u$  access  $v$ ", ενώ η κατεύθυνση του τόξου είναι αυτή που δηλώνεται από τη σχέση. Παρόμοια, μία σχέση προσπέλασης  $access(u, v)$  είναι νόμιμη στο  $G$  αν και μόνον αν υπάρχει ένα κατεύθυνόμενο τόξο από το  $u$  στο  $v$ . Ο συμβολισμός είναι  $(u, v) \in G$ .

Υποθέτουμε ότι έχουμε  $n$  ασφαλή συστήματα,  $G_i = \langle V_i, A_i \rangle$ ,  $i=1,2,\dots,n$  και για απλότητα υποθέτουμε ότι όλες οι οντότητες έχουν διαφορετικά μεταξύ τους ονόματα, δηλαδή  $V_i \cap A_j = \emptyset$ ,  $i \neq j$ . Προκειμένου να παραστήσουμε συνθήκες διαλειτουργικότητας θεωρούμε μοιράσματα πληροφορίας (information sharing) μεταξύ οντοτήτων διαφορετικών συστημάτων και ορίζουμε τις αντιστοιχίσεις μεταξύ των οντοτήτων, σε όρους σχέσεων προσπέλασης:

### Ο ΟΡΙΣΜΟΣ II

Επιτρεπτή σχέση προσπέλασης είναι μία δυαδική σχέση  $F$  στο  $\cup_{i=1}^n V_i$ , όπου  $\forall (u, v) \in F$  ισχύουν  $u \in V_i$ ,  $v \in V_j$ , και  $i \neq j$ .

### Ο ΟΡΙΣΜΟΣ III

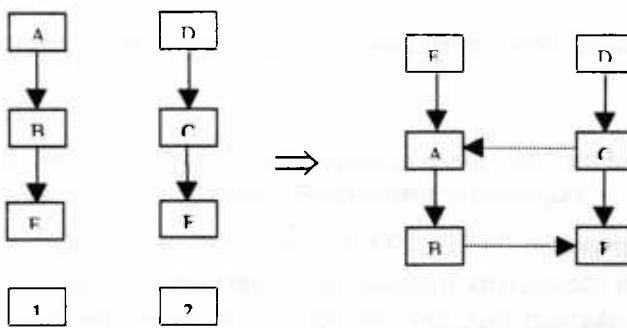
Περιοριστική σχέση προσπέλασης είναι μία δυαδική σχέση  $R$  στο  $\cup_{i=1}^n V_i$ , όπου  $\forall (u, v) \in R$  ισχύουν  $u \in V_i$ ,  $v \in V_j$ , και  $i \neq j$ .

Αντιλαμβανόμαστε ότι οι δύο παραπάνω σχέσεις αντιστοιχούν σε θετικές και αρνητικές τιμές μίας μήτρας ελέγχου προσπέλασης.

### Ο ΟΡΙΣΜΟΣ IV

Έστω ότι έχουμε επικοινωνούντα συστήματα που περιγράφονται από την μήτρα  $Q = \langle W, B \rangle$ . Η διαλειτουργικότητα  $Q$  είναι ασφαλής αν και μόνον  $W \cap B = \emptyset$  -όπου  $R$  η περιοριστική σχέση κάθε ατομικού συστήματος- και  $\forall (u, v) \in V$  ισχύει ότι  $(u, v) \in A_i$  -όπου  $A$  η δυαδική σχέση "access" κάθε ατομικού συστήματος  $i$ - αν και μόνον  $(u, v) \in B$ .

Έστω τώρα ότι έχουμε τα συστήματα του σχήματος 4.1. Η έναρξη επικοινωνίας κατά τον τρόπο που υποδεικνύεται από το σχήμα, μπορεί να επηρεάζει την  $R$  του συστήματος αυτού, για παράδειγμα γεννιέται η έμμεση πρόσβαση του  $B$  στο  $A$ , δηλαδή συγκρούεται η  $R$  του ενός συστήματος με την  $F$  του άλλουν.



ΣΧΗΜΑ 4.1. Προβλήματα ασφαλούς διαλειτουργικότητας

### Ο ΠΡΟΒΛΗΜΑ

Η προσπάθεια πρέπει να εστιαστεί στην εύρεση μίας σχέσης "access",  $F$ , που δεν θα επιτρέπει αυτές τις παραβιάσεις. Δηλαδή εύρεση μίας  $Q = \langle W, B \rangle$ , όπου

$W = \bigcup_{i=1}^n V_i$ ,  $B = \subseteq (\bigcup_{i=1}^n A_i \cup F) - R$ , έτσι ώστε η  $Q$  να είναι ασφαλής διαλειτουργικότητα.

Γενικά γνωρίζουμε ότι η εκτίμηση της ασφάλειας (security evaluation), την οποία εξασφαλίζει μία μήτρα προσπέλασης δεν είναι αποφασίσιμο πρόβλημα, ενώ στην καλύτερη περίπτωση είναι NP-complete. Μπορούμε λοιπόν να κάνουμε μία αρχική εκτίμηση ότι τα προβλήματα που ξεκινούν από αυτή τη βάση θα είναι επίσης NP-complete. Τα ακόλουθα συμπεράσματα αποδεικνύονται:

### ⌚ ΘΕΩΡΗΜΑ I - Εκτίμηση ασφάλειας

Η εύρεση της  $(\bigcup_{i=1}^n A_i \cup F) - R$  έτσι ώστε αυτή να είναι ασφαλής μπορεί να επιτευχθεί σε πολυωνυμικό χρόνο.

Διαπιστώνουμε εντούτοις ότι η λύση που βρίσκεται δεν είναι η βέλτιστη, από την άποψη ότι δεν αντιστοιχεί σε πραγματικές συνθήκες ή ότι δεν επιτυγχάνεται διαλειτουργικότητα. Ορίζουμε για το σκοπό αυτό μία συνθήκη "βέλτιστης διαλειτουργικότητας" ως τη μέγιστη διακίνηση πληροφορίας και επαναδιατυπώνουμε το πρόβλημα I έτσι ώστε να περιλαμβάνει και αυτήν.

### ⌚ ΘΕΩΡΗΜΑ II - Ασφαλής διαλειτουργικότητα με μέγιστη διακίνηση πληροφορίας

Η επίτευξη μέγιστης ασφαλούς διαλειτουργικότητας είναι NP-complete πρόβλημα.

#### ⌚ ΛΗΜΜΑ I

Η εύρεση προσεγγιστικού αλγόριθμου για την επίτευξη μέγιστης ασφαλούς διαλειτουργικότητας είναι NP-complete πρόβλημα.

Μπορούμε να αλλάξουμε την έννοια της προηγούμενης συνθήκης, θέτοντας ως νέα αυτήν της επίτευξης μέγιστου αριθμού νομίμων προσπελάσεων στη μήτρα ελέγχου προσπέλασης. Η συνθήκη αυτή υπονοεί ότι θα έχουμε μέγιστη διακίνηση πληροφορίας.

### ⌚ ΘΕΩΡΗΜΑ III - Ασφαλής διαλειτουργικότητα με μέγιστο αριθμό νομίμων προσπελάσεων

Η επίτευξη μέγιστης ασφαλούς διαλειτουργικότητας είναι NP-complete πρόβλημα.

#### ⌚ ΛΗΜΜΑ II

Η εύρεση προσεγγιστικού αλγόριθμου για την επίτευξη μέγιστης ασφαλούς διαλειτουργικότητας είναι NP-complete πρόβλημα.

Υπάρχει όπως αναφέρεται στο [GON-1994] μία περίπτωση (όπου ο γράφος είναι ακυκλικός) όπου τα παραπάνω προβήματα επιλύονται σε πολυωνυμικό χρόνο. Το επόμενο προς συζήτηση θέμα, εφόσον υπάρχει μία περίπτωση που μπορεί να συζητηθεί ή να διερευνηθεί έτσι ώστε να δώσει και άλλες παρόμοιες περιπτώσεις, είναι το θέμα της πολυπλοκότητας όταν πρόκειται να περιλάβουμε στην ανάλυσή μας πολλά ενοποιημένα συστήματα (federated systems). Μπορούμε, με άλλα λόγια, να επεκτείνουμε συμπεράσματα για ένα και δύο συστήματα σε περισσότερα συστήματα. Πρόκειται για ένα σύνθετο πρόβλημα το οποίο αναφέρεται σαν πρόβλημα της "σύνθεσης" (composability). Αποδεικνύεται ότι:

⌚ **ΘΕΩΡΗΜΑ IV** - Ασφαλής διαλειτουργικότητα σε ομόσπονδα συστήματα (federated systems)<sup>19</sup>.

Η επίτευξη ασφαλούς διαλειτουργικότητας επιτυγχάνεται όταν κάθε σύστημα είναι ασφαλές.

⌚ **ΘΕΩΡΗΜΑ V** - Μέγιστη ασφαλής διαλειτουργικότητα σε ομόσπονδα συστήματα (federated systems).

Η επίτευξη μέγιστης ασφαλούς διαλειτουργικότητας επιτυγχάνεται όταν κάθε σύστημα είναι ασφαλές στο μέγιστο βαθμό.

⌚ **ΛΗΜΜΑ III**

Η ιδιότητα της "σύνθεσης" (composability) ισχύει σε περιπτώσεις όπου η δομή που σχηματίζεται από τα ατομικά συστήματα ακολουθεί διάρθρωση δένδρου.

Οι προσπάθειες που έχουν γίνει στον τομέα αυτό είναι αρκετές. Εντούτοις η δυσκολία του προβλήματος είναι τέτοια που δεν έχει επιτρέψει την παραγωγή λύσεων που είναι εφαρμόσιμες σε πραγματικές καταστάσεις. Οι λύσεις αυτές αφορούν για παράδειγμα συστήματα με ίδιους ή συμβατούς μηχανισμούς ασφάλειας ή αγνοούν τα έμμεσα κανάλια επικοινωνίας (covert channels) που δημιουργούνται. Καμία επίσης λύση δεν περιλαμβάνει τον εντοπισμό -πόσο μάλλον την εξάλειψη- των ρηγμάτων ασφάλειας που δημιουργούνται. Είναι φανερό ότι κάθε προσπάθεια εφαρμογής των λύσεων που δίδονται θα αποδειχθεί ανεπιτυχής σε πραγματικές συνθήκες.

Σχετικό με το τελευταίο αυτό θέμα της σύνθεσης είναι και εκείνο της "συμβατότητας" (compatibility) μεταξύ πολιτικών ασφάλειας. Όπως ορίζεται στο [HIN-1994] "δύο πολιτικές ασφάλειας είναι συμβατές όταν οι στόχοι τους δεν συγκρούνται σε κάποια αλληλεπίδραση". Οι πολιτικές ασφάλειας αντιμετωπίζονται σαν συγκεκριμένες, τυπικά ορισμένες ιδιότητες που ελέγχουν τη συμπεριφορά ενός συστήματος. Προκειμένου να οριστεί περαιτέρω τυπικά το πρόβλημα, διερευνείται η φύση του προβλήματος και υπομέρους πεδία ορισμού του. Ο τρόπος που τα τελευταία ορίζονται προσπαθεί να περιλάβει σχετικά θέματα, το σημαντικότερο των οποίων είναι το περιβάλλον (με την ευρεία έννοια) των συστημάτων. Επ' αυτών των υπομέρους πεδίων ορίζεται η συμβατότητα, ακολουθώντας μία προσέγγιση και

<sup>19</sup> Ένα ομόσπονδο σύστημα\* μπορεί να θεωρηθεί σαν μία συλλογή κατανεμημένων, διαφορετικών ή μερικώς αυτόνομων συστημάτων, τα οποία συντονίζονται από ένα κεντρικό σύστημα που ονομάζεται ομόσπονδο. Τα συστήματα αυτά χαρακτηρίζονται από τα ακόλουθα κυρίως γνωρίσματα:

- **Ατέλεια (Partiality):** εντοπίζεται στο γεγονός ότι τα συστήματα μπορεί να είναι ημιπλήρη (στην αρχιτεκτονική και τη λειτουργικότητά τους, κ.λπ.).
- **Πλεονασμό (Redundancy):** εντοπίζεται στον τρόπο με τον οποίο ίδια στοιχεία αντιμετωπίζονται με διαφορετικές απόψεις από διαφορετικά συστήματα στην επανάληψη πληροφορίας ή πόρων και στις αλληλεξαρτήσεις και συσχετίσεις μεταξύ στοιχείων διαφορετικών συστημάτων.
- **Αυτονομία (Autonomy):** εντοπίζεται στη διαφορετικότητα του τρόπου σχεδιασμού, αρχιτεκτονικής, εννοιολογικών σχημάτων, κ.λπ. μεταξύ των συστημάτων.

\*Σημειώστε ότι οι πληροφορίες αυτές δεν αποτελούν ορισμό, αλλά συλλέχθησαν από κείμενα διαθέσιμα στο διαδίκτυο.

μέθοδο παρόμοια με αυτήν που παρουσιάστηκε για τη διαλειτουργικότητα.

#### 4.3 Έννοια της "μεταπολιτικής" ασφάλειας σε Πληροφοριακά Συστήματα

Μεταπολιτική, Διαχείριση, Οργάνωση, Έλεγχος, Συντονισμός Πολιτικών Ασφάλειας

Από τη βιβλιογραφία που συλλέχθηκε για τις ανάγκες αυτής της νοηματικής ενότητας, μπορούμε να πούμε ότι ένα από τα κείμενα περιγράφει πολύ καλά την έννοια της "μεταπολιτικής" ασφάλειας σε Πληροφοριακά Συστήματα. Το κείμενο αυτό [HOS-1992a] θα χρησιμοποιηθεί ως κύρια αναφορά για την ενότητα αυτή.

Το πρόθεμα "μετα-" μπορούμε να το συναντήσουμε σε διάφορες επιστήμες, μεταξύ αυτών και σε άλλους κλάδους της Πληροφορικής, όπως για παράδειγμα στις Βάσεις Δεδομένων. Γενικά, το πρόθεμα χρησιμοποιείται προκειμένου να συνθέσει έννοιες που βοηθούν στην περιγραφή ή δήλωση άλλων εννοιών. Στην περίπτωσή μας η "μεταπολιτική" δηλώνει ένα από τα παρακάτω:

- Ένα σύνολο κανόνων για μία πολιτική ασφάλειας, που προσδιορίζουν το είδος της πολιτικής, τα συστατικά της στοιχεία, το πεδίο εμβέλειάς της, τα όργανα που τη διαχειρίζονται, τη διαδικασία αλλαγής ή προσαρμογών της και τις ενδεχόμενες σχέσεις μεταξύ των υπο-πολιτικών που τη συνθέτουν.
- Ένα σύνολο κανόνων που συντονίζουν την εφαρμογή περισσότερων πολιτικών, περιλαμβανομένων των στοιχείων διαχείρισης αυτών, επίλυσης των ενδεχόμενων συγκρούσεων, κ.λπ.

Από τα παραπάνω μπορεί να φανεί ότι η χρησιμότητα των μεταπολιτικών είναι σημαντική εφόσον μπορούν να συμβάλλουν στα ακόλουθα:

- Περιγραφή της δομής της πολιτικής ασφάλειας και των συσχετίσεων μεταξύ των συστατικών της στοιχείων
- Παροχή διευκρινίσεων επί του νοήματος ή της φιλοσοφίας της πολιτικής, των υποκείμενων υποθέσεων και πεποιθήσεων που την επηρεάζουν
- Έλεγχο των αλλαγών ή προσαρμογών αυτής
- Συνεπαγόμενη ευελιξία στη διαχείριση της πολιτικής
- Ευκολία στη διαχείριση περισσότερων πολιτικών
- Ευκολία στην αυτοματοποιημένη διαχείριση μίας αλλά και περισσότερων πολιτικών

Τα τελευταία δύο στοιχεία που αναφέραμε παρουσιάζουν το μεγαλύτερο ενδιαφέρον. Πρέπει όμως να τονίσουμε (γεγονός που αποτελεί και την κατευθυντήρια γραμμή αυτής της μελέτης και δικαιολογεί την ύπαρξη του προηγούμενου κεφαλαίου), ότι είναι η άρτια και κατάλληλη περιγραφή των μεμονωμένων πολιτικών που θα αποτελέσει το εναρκτήριο σημείο για τη διερεύνηση του τρόπου εφαρμογής των αποτελεσμάτων της στην αυτοματοποιημένη διαχείριση μίας ή περισσότερων πολιτικών.

Μπορούμε όμως να δούμε αναλυτικότερα όλα τα παραπάνω πριν αναλύσουμε αυτούς τους τρόπους προσέγγισης των μεταπολιτικών, παραθέτοντας παραδείγματα ορισμένων ειδών μεταπολιτικών που μπορούμε να χρησιμοποιήσουμε.

Παραθέτουμε καταρχήν ένα παράδειγμα περιγραφής μίας πολιτικής, προκειμένου να δείξουμε ότι υπάρχουν στοιχεία που αφορούν τις πολιτικές και μπορούν να αποτελέσουν δομικά στοιχεία μίας μεταπολιτικής:



POLICY NAME: Simple Security Property

POLICY TYPE: Access Control Subpolicy

AUTHORITY: Secretary of Defence

CHANGE PROCESS: DoD with consultation of the Armed Services

APPLICATION DOMAIN: All times to all systems which contain USA military documents

DOMAIN INTERFACES: May relate to NATO and SEATO ...

INFORMAL STATEMENT OF POLICY: No user or process representing a user may read data of a higher classification level than the user's clearance level.

EXCEPTIONS: Users or processes with downgrading privilege are excepted

RELATED AUDIT POLICIES:

Security relevant events must be auditable

Attempted violations must be auditable

Any violation must be alarmed

Every use of downgrading privilege must be audited

OTHER RELATED POLICIES:

Users must identify themselves and be authenticated at login

PRECEDENCE RULES:

This policy has priority over any other access control policy

FORMAL STATEMENT OF POLICY:

S Subject: User, process, active entity

O Object: File, passive entity

CR Clearance

CL Classification

May\_Read (S,O)

Begin

If CR(S) >= CR(O)

Then May\_Read = YES

Else

If downgrade(S) = YES

Then May\_Read = YES

If Audit(May\_Read) = YES

Then write\_audit\_record

end

OTHER: ...

#### ΣΗΜΑ 4.2. Δομημένη περιγραφή μίας Πολιτικής Ασφάλειας

ΠΗΓΗ: [HOS-1992a]

Μια τέτοια μεταπολιτική που περιγράφει μία πολιτική μπορούμε να θεωρήσουμε ότι δίνει κάποια "ερμηνεία" στα στοιχεία της δεύτερης. Ας δούμε ορισμένα στοιχεία που συνθέτουν μία τέτοια μεταπολιτική:

Policy description metapolicy	Data type	Length	Criticality	Changes signer	Modifier
Policy name	Alphanumeric	20	30	Secretary of ...	System Administrator of ... ...
Policy type	Alphanumeric	5	30	None	System Administrator of ... ...
Authority	Alphanumeric	30	50	Secretary ...	...
Start date	Date	6	20	President of ...	...
Expiration date	Date	6	25	...	...
Informal model	Alphanumeric	900	20	...	...
Formal model	Some Language type	1500	40	Security officer of ...	System Administrator of ... and Security Officer
Etc.	...	...	...	...	...

ΠΗΓΗ: [HOS-1992a]

Μία μεταπολιτική που περιγράφει τις υπο-πολιτικές που τη συνθέτουν, περιγράφει τις συσχετίσεις μεταξύ αυτών, προσδιορίζει τις σημαντικές πολιτικές, τη σχετική σειρά εκτέλεσή τους, τις προτεραιότητες, κ.λπ., ως εξής:

Policy Relationship	Policy 1	Policy 2
Policy names	MAC	DAC
Relationship (Parent/Child/Colleague)	Colleague	Colleague
Execute (With/Before/After/Not)	Before	After
Precedence Level in this Relationship	100	50
Criticality of relationship	80	
Creator of relationship	Somebody	
Authorised modifiers of relationship	Somebody	
Etc	...	...

ΠΗΓΗ: [HOS-1992a]

Μία μεταπολιτική μπορεί να περιγράφει τους περιορισμούς επί μιας πολιτικής. Οι περιορισμοί αυτοί μπορεί να αφορούν γενικές περιπτώσεις (για παράδειγμα περιορισμοί που θέτει η ημερομηνία λήξεως της πολιτικής, ή περιορισμοί ανάλογα με τις αλλαγές της ώρας), αλλά επίσης και ειδικές περιπτώσεις όπως αν επιβάλλεται και πώς να αλλάξει η πολιτική σε περιόδους κρίσεως της επιχείρησης ή τεταμένου ανταγωνισμού, κ.λπ.

Η μεταπολιτική οργάνωσης και ελέγχου της πολιτικής περιλαμβάνει στοιχεία που περιγράφουν το νομικό καθεστώς της δεύτερης (π.χ. στοιχεία ισχύως, διανομής, αλλαγής, οργανωτικές διατάξεις που την επιβάλλουν, κ.λπ.), στοιχεία πιστοποίησης αυτής, δήλωση της σχέσης της πολιτικής με την οργανωτική δομή του οργανισμού και άλλα.

POLICY NAME: Organization Control

POLICY TYPE: Metapolicy

AUTHORITY: Policy Center of ...

CHANGE PROCESS: Two Security Officers with written approval from the Policy Center of ...

UNDERLYING POLICY:

POLICY NAME: Access Control to digital documents of economics nature

SOURCE OF POLICY: Executive order ...

LEGAL STATUS OF POLICY: Mandated by the organization



POLICY PEDIGREE:

OWNER: ...

CREATOR: ...

DATE CREATED: ...

EXPIRATION DATE: ...

REVIEWERS: ...

ASSURANCE:

POLICY CRITICALITY: High

ASSURANCE LEVEL: B3

POLICY EVALUATOR: Greek Center of Policy Evaluation

APPROVAL PROCESS:

AUTHORITY: President of the organization

APPROVING DEPARTMENTS: Economics Dept., Public Realations Dept., Information Systems Dept.

APPRONAL SEQUENCE: Information Systems Dept., Economics Dept., Public Realations Dept., President of the organization

POLICY IMPLEMENTATION:

EFFECTIVE DATE: ...

APPLICATION SCOPE: All organizational depts.

MODIFICATION:

AUTHORIZATION BY: President of the organization

MODIFICATION BY: Security Officer

LAST MODIFICATION ON: ...

DISTRIBUTION:

DISTRIBUTION TYPE: Unlimited

PUBLICATION DATA:

PUBLISHER: Public Relations Dept.

POLICY USED IN:

DEPARTMENTS: Every organizational Dept.

**ΣΧΗΜΑ 4.3. Μεταπολιτική Οργάνωσης και Ελέγχου Πολιτικών Ασφάλειας.**

ΠΗΓΗ: [ΗΟΣ-1992a]

Η μεταπολιτική περιγραφής εξειδικευμένων πολιτικών μπορεί να βοηθήσει στις περιπτώσεις όπου συγκεκριμένες περιοχές του συστήματός μας εφαρμόζουν διαφορετικές πολιτικές ασφάλειας. Μία τέτοια μεταπολιτική μπορεί να συντεθεί από την περιγραφή των διαφορών των πολιτικών, αλλά και του τρόπου συσχέτισης και σύνδεσης αυτών.

Η μεταπολιτική συντονισμού πολλαπλών πολιτικών αντιστοιχεί στις περιπτώσεις όπου χρειάζεται να επικοινωνήσουν συστήματα με διαφορετικές πολιτικές. Εξάλλου μία μεταπολιτική περιγραφής των διεπαφών μεταξύ πεδίων εμβέλειας πολιτικών μπορεί να φανεί χρήσιμη και στις δύο τελευταίες περιπτώσεις.

Οι τρόποι με τους οποίους μπορούμε να παραστήσουμε μεταπολιτικές πρόκειται να παρουσιαστούν στα ακόλουθα.

#### 4.4 Μέθοδοι διαχείρισης πολλαπλών πολιτικών ασφάλειας

Μηχανή Μετάθεσης Καταστάσεων. Συνδιασμός Πολιτικών Ασφάλειας. Διαβάθμιση Πολιτικών Ασφάλειας. Σύγκρουση Πολιτικών Ασφάλειας. Εξέλιξη Πολιτικών Ασφάλειας. Κουντωδοί. Άλγεβρικά Μοντέλα. Άλγεβρα Boole. Μήτρα Επίλυσης Σύγκρουσης. Μήτρα Συνεργασίας. Γλώσσες Αναπαράστασης Γνώσης. Θεωρία Ασαφών Συνόλων

##### 4.4.1 Η μηχανή πολλαπλών πολιτικών ασφάλειας

Η πρώτη προσέγγιση που παρουσιάζουμε ανήκει στους πρωτεργάτες της μελέτης του θέματος που εξετάζουμε και συγκεκριμένα στον D.E.Bell [BEL-1994].



Πρωταρχικά διακρίνονται οι διάφορες πολιτικές σε τέσσερις κατηγορίες:

- πολιτικές ασφάλειας σε επίπεδο οργανισμού (organizational), οι οποίες υπάρχουν συνήθως σε μορφή γραπτού λόγου και καλύπτουν όλο τον οργανισμό
- εννοιολογικά διατυπωμένες πολιτικές ασφάλειας (conceptual), οι οποίες χρησιμοποιούν διάφορες αφηρημένες έννοιες ή σχήματα προκειμένου να αναπαραστήσουν κάποια πολιτική του προηγουμένου είδους
- ανεπτυγμένες με αφηρημένο σχεδιασμό πολιτικές ασφάλειας (abstract design), όπου η πολιτική έχει μεταφραστεί σε ένα ανάλογο σχέδιο το οποίο επιδέχεται υλοποίηση
- υλοποιημένες πολιτικές ασφάλειας (implemented design), οι οποίες υφίστανται στο στάδιο της υλοποίησης

Η μοντελοποίηση της "μηχανής πολλαπλών πολιτικών" (multipolicy machine) περιλαμβάνει τις ενότητες ορισμού του εννοιολογικού πλαισίου, ορισμού των εννοιών συνδυασμού και σύγκρουσης πολιτικών και ορισμού των εννοιών προτεραιότητας, διαβάθμισης και εξέλιξης πολιτικών. Οι αντίστοιχοι ορισμοί είναι οι ακόλουθοι:

### ⌚ ΟΡΙΣΜΟΣ I

Το σύστημα (μηχανών πολλαπλών πολιτικών) μοντελοποιείται σαν μία υπολογιστική μηχανή μεταθέσεων, με διάφορες αρχικές καταστάσεις από τις οποίες μεταβαίνουμε σε νέες καταστάσεις μέσω εκτελέσεων έγκυρων αποφάσεων μετά από αιτήσεις. Μία πολιτική ασφάλειας αναπαρίσταται ως η τιμή ενός υπολογισμού (ο υπολογισμός αφορά μία τριπλέτα <αρχικές καταστάσεις, αίτηση, απόφαση>)

$$P: (R, D, Z) \rightarrow V$$

### ⌚ ΟΡΙΣΜΟΣ II

Έστω πολιτικές  $P_A, P_B$ . Ο συνδυασμός τους (combination) είναι μία συνάρτηση

$$C_{A,B}: (V_A \times V_B) \rightarrow V$$

Η συνάρτηση αυτή αντιστοιχίζει σε κάθε υπολογισμό μία αποδεκτή τιμή από το  $V$  συνδυάζοντας τις τιμές που ανήκουν στα  $V_A, V_B$  χρησιμοποιώντας τη συνάρτηση  $C$ .

Η έννοια της σύγκρουσης πολιτικών παραπέμπει στις έννοιες της εξασθένισης (attenuation) της πολιτικής και στην έννοια της αποκλιμάκωσης ή επίλυσης της σύγκρουσης (conflict resolution).

### ⌚ ΟΡΙΣΜΟΣ III

Η εξασθένιση της πολιτικής αντιπροσωπεύεται από μία συνάρτηση

$$\alpha: V \rightarrow P(V)$$

όπου  $v \in \alpha(v) \quad \forall v \in V$ . Η εξασθένιση δηλαδή δίνει ένα αποδεκτό σύνολο τιμών  $v \in \alpha(v)$  για την πολιτική, οι οποίες αποτελούν μη-συγκρουόμενες τιμές με την  $v$ .

### ⌚ ΟΡΙΣΜΟΣ IV

Δεδομένων δύο πολιτικών  $P_A, P_B$  και των εξασθενίσεών τους  $\alpha_A$  και  $\alpha_B$ , η πολιτική  $P_A$  δεν συγκρούεται με την πολιτική  $P_B$  αν ισχύει ότι κάθε τιμή  $v$  αποδίδει τη  $P_B$  ανήκει στο σύνολο τιμών της  $\alpha_A$ .

## Ξ ΟΡΙΣΜΟΣ V

Ένας συνδυασμός  $C_{A,B}$  δύο πολιτικών  $\Pi_A$  και  $\Pi_B$  επιλύει συγκρούσεις μεταξύ τους αν δεν συγκρούεται με καμία από τις  $\Pi_A$  και  $\Pi_B$ .

## Ξ ΟΡΙΣΜΟΣ VI

Έστω μία μηχανή πολλαπλών πολιτικών. Η προτεραιότητα (precedence) μίας πολιτικής, από το σύνολο των πολιτικών της μηχανής, είναι μία συνάρτηση  $\rho$  η οποία αντιστοιχίζει σε κάθε υπολογισμό μία τιμή από ένα σύνολο  $T$ , διατεταγμένο μέσω του τελεστή  $>=$ .

Κατά παρόμοιο τρόπο ορίζεται και η διαβάθμιση (order) μεταξύ πολιτικών ασφάλειας.

## Ξ ΟΡΙΣΜΟΣ VII

Έστω διατεταγμένο μέσω του τελεστή  $>=$  σύνολο πολιτικών  $\sigma = (\Pi_1, \dots, \Pi_N)$ . Η διαβάθμιση των πολιτικών είναι μία συνάρτηση  $\rho'$  η οποία αντιστοιχίζει σε κάθε πολιτική του συνόλου μία τιμή  $i$ ,  $i \in \{1, 2, \dots, n\}$ .

Θέματα εξέλιξης (evolution) και αλλαγής (change) αντιμετωπίζονται χρησιμοποιώντας τις διαδικασίες εισαγωγής και διαγραφής πολιτικών καθώς και τις έννοιες της διαβάθμισης και της προτεραιότητας, μέσω των οποίων επιλύονται και προβλήματα σύγκρουσης (conflict) πολιτικών.

### 4.4.2 Εφαρμογή της Θεωρίας Ασαφών Συνόλων στη διαχείριση πολλαπλών πολιτικών ασφάλειας

Η H.Hosmer διατείνεται ότι η "Θεωρία Ασαφών Συνόλων ή Ασαφής Λογική" (Fuzzy Sets Theory/ Fuzzy Logic) μπορεί να εφαρμοστεί [HOS-1993] στο πεδίο της ασφάλειας Πληροφοριακών Συστημάτων. Προκειμένου να παρουσιάσουμε τον τρόπο με τον οποίο η ιδέα αυτή υποστηρίζεται, θα αναφερθούμε καταρχήν συνοπτικά σε βασικές αρχές του παραδείγματος αυτού.

Η θεωρητική των Ασαφών Συνόλων θεμελιώθηκε από τον Lofti Zadeh αλλά και πολλούς άλλους ενώ πρωτοεμφανίστηκε στην δεκαετία του '60. Περιλαμβάνει ένα σύνολο από έννοιες, τεχνικές και θεωρήματα, τα οποία είναι σχεδιασμένα κατά τρόπο που να αντιμετωπίζουν την ανακρίβεια και την ασάφεια της πραγματικότητας. Η εφαρμογή της σε συστήματα που χαρακτηρίζονται από δομική πολυπλοκότητα και σε προβλήματα για τα οποία δεν είναι δυνατό να εφευρεθεί ένας αλγόριθμος κατάλληλος να τα επιλύσει, όπως επίσης και σε συστήματα που αλληλεπιδρούν με τον άνθρωπο ή στα οποία ο άνθρωπος έχει εκτεταμένη εμπλοκή, είναι ενδεδειγμένη.

Η παραδοχή ότι η πραγματικότητα είναι εγγενώς ανακριβής και πολύπλοκη αποτελεί το απαραίτητο σημείο εκκίνησης για τη χρήση αυτής της θεωρητικής. Η διαπίστωση ότι η έννοια της "τάξης" ή "κατηγορίας" (class) είναι μία κατεξοχήν ασαφής έννοια είναι ιδιαίτερα σημαντική. Γνωρίζουμε ότι η κατηγοριοποίηση των εκάστοτε υπό μελέτη στοιχείων συστημάτων βοηθάει σημαντικά στην κατανόηση πολύπλοκων καταστάσεων. Πρέπει ωστόσο να αναγνωρίσουμε ότι οι "τάξεις" που δημιουργούμε λειτουργούν μάλλον ως αντιπρόσωποι κάποιας τάξης στοιχείων, ευρύτερης και σχετικά περισσότερο ανομοιογενούς. Ο άνθρωπος εντούτοις προτιμά να ορίζει κάποιες σταθερές (οι οποίες ονομάζονται "πρωτότυπα" (prototypes))

προκειμένου να διατηρεί μία απλή και εύκολα κατανοητή άποψη μιας περισσότερο περίπλοκης πραγματικότητας. Αυτό σημαίνει ότι αν μελετήσουμε αναλυτικά τα υπομέρους στοιχεία που υποστηρίζουμε ότι ανήκουν σε μία τάξη, θα διαπιστώσουμε ότι υπό δεδομένες συνθήκες κάποια από αυτά ανήκουν λιγότερο ή περισσότερο στη συγκεκριμένη τάξη. Με κάποια διαφορετική διατύπωση, θα λέγαμε ότι θα ήταν εξαιρετικά χρήσιμο να μπορούσαμε να απεικονίζαμε αντές τις διακυμάνσεις έτσι ώστε να είμαστε περισσότερο ακριβείς και ενέλικτοι στην απεικόνιση κάποιων εξειδικευμένων και περίπλοκων λειτουργιών. Έτσι, για παράδειγμα, η "ακεραιότητα" αντιπροσωπεύει για μας μία έννοια δεδομένου περιεχομένου. Σε πραγματικές καταστάσεις ωστόσο μπορούμε να αντιμετωπίσουμε την ακεραιότητα με διαφορετικές εννοιολογικές υφές, σε συνδυασμό με κάποια άλλη έννοια, κ.λπ.

Ένα Ασαφές Σύνολο είναι κατά τον Zadeh [HOS-1993]

"... is a class with unsharp boundaries, that is a class in which the transition from membership to non-membership is gradual rather than abrupt"<sup>20</sup>.

Έτσι, τα μέλη ενός τέτοιου συνόλου συμμετέχουν στο σύνολο αυτό "σε κάποιο βαθμό". Ο βαθμός αυτός καθορίζεται λιγότερο ή περισσότερο αυθαίρετα ανάλογα με την περίσταση. Από την άλλη, ένα Σαφές Σύνολο (Crisp Set) είναι ένα Ασαφές Σύνολο όπου ο βαθμός ιδιότητας μέλους καθορίζεται με τέτοιο τρόπο (ανήκει δηλαδή σε ένα ορισμένο διάστημα τιμών), ώστε είναι ακριβές ποιά στοιχεία ανήκουν στο σύνολο και ποιά όχι. **Η αρχή που διέπει τη θεωρητική αυτή είναι η αρχή του "μέτρου" (measure) και όχι η αρχή της "απαρίθμησης" (count).** Έτσι, μπορούμε επίσης να υποστηρίξουμε ότι η αρχή της συνέχειας ενός πεδίου τιμών (*continuum*) αποτελεί μία επίσης χρήσιμη έννοια.

Αντιμετωπίζοντας θέματα ασφάλειας σε αυτό το πλαίσιο, παρατηρούμε για παράδειγμα ότι η TCB (Trusted Computing Base) του TCSEC είναι ένα Σαφές Σύνολο. Αν θεωρούσαμε την TCB σαν Ασαφές Σύνολο, θα μπορούσαμε να ορίσουμε επίσης βαθμούς συμμετοχής διαφόρων στοιχείων στο σύνολο αυτό, ανάλογα με την εμπιστοσύνη ή την ασφάλεια κάθε στοιχείου. Μία τέτοια αντιμετώπιση ίσως να καθιστούσε τη μελέτη αυτών των θεμάτων ευκολότερη και σίγουρα περισσότερο ενέλικτη. Εξάλλου, η έννοια του δικαιώματος είναι μία "κατεξοχήν" έννοια, δηλαδή ένα στοιχείο έχει ή δεν έχει κάποιο δικαίωμα. Ο ορισμός αυτός κάνει δύσκολη την απεικόνιση ενδιάμεσων καταστάσεων, όπως το γεγονός ότι κάποιο στοιχείο έχει κάποιο δικαίωμα υπό κάποιες προϋποθέσεις ή σε κάποιες χρονικές στιγμές και τι χάνει όταν αυτές οι συνθήκες δεν τηρούνται.

Η χρησιμότητα της θεωρίας των Ασαφών Συνόλων είναι επίσης ιδιαίτερα προφανής όσον αφορά την εφαρμογή της στην περίπτωση της ασφαλούς διαλειτουργικότητας Πληροφοριακών Συστημάτων. Αναλυτικότερα, η χρησιμότητα αυτή διίσταται στη χρήση των ακόλουθων τεχνικών:

- **Ασαφείς Περιορισμοί (Fuzzy constraints):** θεωρούμε έναν στόχο σαν ένα Ασαφές Σύνολο του οποίου τα στοιχεία ανήκουν σε ένα ορισμένο (επιθυμητό) διάστημα τιμών.

<sup>20</sup> Σε ελεύθερη μετάφραση: "...μία τάξη (class) με μη καλά ορισμένα όρια, δηλαδή μία τάξη όπου η μετάβαση από την ιδιότητα μέλους αυτής στην ιδιότητα μη-μέλους είναι σταδιακή παρά μονοσήμαντα ορισμένη και άμεσα εμπίπτουσα".

- **Ασαφής Θεωρία Αποφάσεων (Fuzzy Decision Making):** θεωρούμε μία απόφαση ως επιλεκτέα από ένα σύνολο εναλλακτικών. Εξάλλου με βάση την "αρχή της συνέχειας" η λογική μπορεί να μετασχηματιστεί και να αποτελείται από ένα ευρύτερο σύνολο λογικών αποτελεσμάτων (π.χ. ΑΛΗΘΕΣ, ΣΧΕΔΟΝ ΑΛΗΘΕΣ, ΨΕΥΔΕΣ, κ.λπ.) και ανάλογο σύνολο τελεστών.
- **Τροποποιητές (Modifiers):** μπορούμε να θεωρήσουμε τους τροποποιητές σαν "τελεστές" που επενεργούν σε ένα Ασαφές Σύνολο, ορίζοντας διαβαθμίσεις σε διάφορες ιδιότητες που χαρακτηρίζουν τα στοιχεία αυτού.
- **Λεκτικές Μεταβλητές (Linguistic variables):** όπως έχουμε σημειώσει αρκετές φορές, η λεκτική διατύπωση γεφυρώνει το χάσμα μεταξύ των αντιλήψεων για την πραγματικότητα και των τυπικών της αναπαραστάσεων. Η αντιμετώπισή τους από τη θεωρία αυτή είναι ενδεδειγμένη.
- **Διαβαθμίσεις (Degrees and Graduations):** μπορούμε εύκολα με χρήση των βαθμών ιδιότητας μέλους να ορίσουμε διάφορες έννοιες οι οποίες στην πράξη είναι δύσκολο να διαχειριστούν λόγω των πολλών περιπτώσεων που ενδέχεται να αντιμετωπίσουμε (π.χ. Graded covert channels bandwidth, degrees of assurance, graded TCB modules, κ.λπ.).

Οι παραπάνω παρατηρήσεις κάνουν κατανοητό ότι η εφαρμογή του παραδειγματισμού αυτού μπορεί να επιτρέψει ανάλογες ευκολίες και στην τυποποίηση πολιτικών ασφάλειας, όπου πολλά θέματα είναι ασαφή. Μάλιστα, όπως είδαμε, διατηρούμε την ευελιξία να ορίζουμε με ακρίβεια κάποια στοιχεία αν αυτό κρίνεται σημαντικό. Η εφαρμογή αυτού του είδους της λογικής είναι καταλυτική για τη διαδικασία επίλυσης συγκρούσεων (conflict resolution process). Παραπέμπουμε τον αναγνώστη στις έννοιες που χρησιμοποιήθηκαν από τις βάσεις κανόνων (κεφ. III) για τη διευθέτηση παρόμοιων θεμάτων, όπου η εφαρμογή αυτής της λογικής είναι ενδεδειγμένη. Επίσης, μπορούμε να θεωρήσουμε υπό αυτό το πρίσμα τη μοντελοποίηση τμημάτων των συστημάτων ως αυτομάτων μεταβάσεων κατάστασης, όπου η μετάβαση σε κάποια κατάσταση εξαρτάται από κάποιες μη καλά ορισμένες αποφάσεις. Οι αποφάσεις αυτές μπορεί σε κάποια εκδοχή να παίρνονται μετά από ψηφοφορία εμπιστοσύνης σε ασαφώς ορισμένες εναλλακτικές<sup>21</sup>.

Η εφαρμογή των τεχνικών αυτών μπορεί να οδηγήσει τον ερευνητή σε ένα πραγματικό πανόραμα εννοιολογικών ορισμών και μοντέλων. Εξάλλου η χρήση της θεωρητικής σε διάφορους ερευνητικούς τομείς επαληθεύει τη χρησιμότητά της. Ωστόσο, δεν θα πρέπει να παραλείψουμε να σημειώσουμε ότι **η ευελιξία που προσφέρει η μεθοδολογία αυτή επιφέρει και αντίστοιχο κόστος διαχείρισης των παραγόμενων σχημάτων**. Συχνά, τα ευέλικτα και λειτουργικά σχήματα απαιτούν επίσης υψηλής ποιότητας στη σύλληψή τους μεθόδους και προγράμματα διαχείρισης.

#### 4.4.3 Υποστήριξη πολλαπλών πολιτικών ασφάλειας βασισμένη σε κουντωδούς

Στο κεφάλαιο III αναλύσαμε τον τρόπο με τον οποίο η έννοια του κουντωδού και το παράδειγμα της Τεχνολογίας Λογισμικού μπορούν να υποστηρίξουν την

<sup>21</sup> Ο αναγνώστης παραπέμπεται για σχετικά παραδείγματα: α) στο [ΑΠΟ-1995] σελ. 127 δίνεται μία τεχνική ψηφοφορίας προκειμένου για το συντονισμό των αλληλεπιδράσεων μεταξύ πολλών διαφορετικών μερών, σε μη αξιόπιστο τηλεπικοινωνιακό περιβάλλον, με τρόπο ώστε να διατηρούνται κανόνες ορθότητας και ακεραιότητας και β) στα [HOS-1993], [HOS-1992a].

τυποποίηση και αυτοματοποίηση πολιτικών ασφάλειας. Στη συγκεκριμένη προσπάθεια εντάσσεται και ένα πλαίσιο για τη διαχείριση περισσότερων πολιτικών ασφάλειας. Οι αρχές που διέπουν την όλη προσπάθεια έχουν παρουσιαστεί στο σχετικό κεφάλαιο που προηγήθηκε, ισχύουν και όσον αφορά αυτή την ενότητα και συνίσταται η παραπομπή σε αυτό προς υπενθύμιση των βασικών στοιχείων.

Στη μεθοδολογία που ακολουθείται για τις ανάγκες συντονισμού περισσότερων πολιτικών πραϋποθέτουμε το στάδιο της "μετάφρασης" της πολιτικής ασφάλειας στο κοινό μορφότυπο που διαχειρίζεται, επί του παρόντος, το πλαίσιο (Μοντέλο του Δικτυώματος, Lattice). Ο όρος "μεταπολιτική" χρησιμοποιείται από το παρόν πλαίσιο για το σκοπό της διαχείρισης περισσότερων πολιτικών που πρέπει να συνυπάρξουν σε ένα σύστημα ή να συνομιλήσουν στην επικοινωνία συστημάτων, ως μηχανισμός που ελέγχει τις πολιτικές ασφάλειας.

Αναλυτικότερα, το πλαίσιο επεξεργάζεται την έννοια του μοντέλου πολιτικής ασφάλειας ως τη βασική έννοια πάνω στην οποία δομούνται τα υπόλοιπα στοιχεία. Η αφαίρεση (abstraction) κινείται σε δύο άξονες: αυτόν της έκφρασης-σημασιολογίας της πολιτικής, στον οποίο ανήκουν διάφοροι τύποι μοντέλων αναπαράστασης και αυτόν της αναπαράστασης-υλοποίησης αυτής.

Η οικογένεια μοντέλων που χρησιμοποιείται περιλαμβάνει τα ακόλουθα [ΚΥΗ-1995]:

- **Μοντέλο των Δικτυώματος**, το οποίο εξυπηρετεί όπως προαναφέραμε την αναπαράσταση των πολιτικών με έναν κοινό τρόπο για σκοπούς χειρισμού και υλοποίησης.
- **Μοντέλα Εμπειρων Συστημάτων**, βασικά με τη μορφή βιοηθητικών εργαλείων, τα οποία χρησιμοποιούνται για να διευκολύνουν την ανάπτυξη και την ταχεία προτοτυποποίηση (rapid prototyping) των πολιτικών ασφάλειας.
- **Άλγεβρικά Μοντέλα**, τα οποία πρωτίστως μας ενδιαφέρουν και τα οποία χρησιμοποιούνται για τον καθορισμό και τη δήλωση των δομών που περιγράφουν τις πολιτικές ασφάλειας και παράλληλα εκφράζουν τη σημασιολογία αυτής. Με άλλα λόγια, περιγράφουν λειτουργικά την πολιτική, αλλά χρησιμοποιούνται προκειμένου να υποστηρίζουν τη διαχείριση περισσότερων πολιτικών ασφάλειας. Τα μοντέλα αυτά έχουν αποδειχθεί επιτυχή για περιγραφή προδιαγραφών (specification) συστημάτων που πρόκειται να αυτοματοποιηθούν.

Ας αναφερθούμε λοιπόν αναλυτικότερα στην τελευταία αυτή κατηγορία. Μία άλγεβρα **A** αποτελείται από ένα σύνολο τύπων **T**, ένα σύνολο λειτουργιών επ' αυτών των τύπων **O** και προαιρετικά ένα σύνολο αξιωμάτων. Το ζεύγος  $\Sigma = (T, O)$  αποκαλείται "υπογραφή στο **A**" (signature). Το  $\Sigma$  με το σύνολο των αξιωμάτων συνθέτουν το σύνολο που καθορίζει τις προδιαγραφές. Στο κεφάλαιο III παρακολουθήσαμε πώς αυτός ο συμβολισμός χρησιμοποιήθηκε προκειμένου να προδιαγράψει και να περιγράψει πολιτικές ασφάλειας. Για την υποστήριξη μεταπολιτικών οι έννοιες που χρησιμοποιούνται ανήκουν στη Θεωρία Συνόλων και είναι τα σύνολα (*sets*), οι συναρτήσεις (*functions*) και οι σχέσεις (*relations*), ενώ τα επίπεδα στα οποία τις εφαρμόζουμε έχουν ως εξής:

**I. Το επίπεδο πολιτικής:** Κάθε πολιτική έχει ή χαρακτηρίζεται από τα ακόλουθα στοιχεία:

- **Μοναδικό Αναγνωριστικό**, για σκοπούς αυθεντικοποίησης της πολιτικής. Το σύνολο όλων των πολιτικών δηλώνεται με  $P$ .
- **Τύπο**, ο οποίος ορίζεται με βάση κοινά χαρακτηριστικά που εντοπίστηκαν σε διάφορες πολιτικές, για παράδειγμα πολιτικές ελέγχου προσπέλασης. Το σύνολο των τύπων είναι το  $T$  και η συνάρτηση που αντιστοιχίζει πολιτικές (αναγνωριστικά) με τύπους είναι η,

type:  $P \rightarrow T$

- **Ορισμό διεπαφής**, που καθορίζει τις μεθόδους με τις οποίες η πολιτική επικοινωνεί. Για την περιγραφή τους χρησιμοποιούνται "αλγεβρικές υπογραφές" (algebraic signatures).
- **Υλοποίηση πολιτικής**, η οποία περιλαμβάνει τα τυπικά μοντέλα,  $FM$  που εκφράζουν την πολιτική.
- **Πιστοποιητικά**, τα οποία δηλώνουν τις εξουσιοδοτημένες οντότητες (άτομα, οργανισμούς) που δικαιούνται να συμμετέχουν στην ανάπτυξη και διαχείριση του συγκεκριμένου επιπέδου.

Policy Name:	$P$
Policy Type:	$T$
Policy Interface:	algebraic signature
Policy Implementation:	SET OF $FM$
Certificates	

**ΣΧΗΜΑ 4.4. Ορισμός του Επιπέδου Πολιτικής**

ΠΗΓΗ: [ΚΥΗ-1995]

**II. Το επίπεδο Μοντέλων:** Για κάθε μοντέλο διατηρούνται τα εξής στοιχεία:

- **Οικογένεια**, με βάση κοινά στοιχεία στη γλώσσα που χρησιμοποιείται και η οποία συμβολίζεται με  $F$ , ενώ η συνάρτηση αντίστοιχης είναι η,  
*family:  $FM \rightarrow F$*
- **Τυπική αναπαράσταση του μοντέλου**, που υποδεικνύει τη σημασιολογία του. Το σύνολο των τυπικών παραστάσεων είναι το  $M$  και η αντίστοιχη συνάρτηση η  
*model:  $FM \rightarrow M$*
- **Υλοποίηση μοντέλου**, για την οποία χρησιμοποιούνται οι κουστώδοι. Το σύνολό τους συμβολίζεται με  $CC$ .
- **Πιστοποιητικά**, τα οποία δηλώνουν τις εξουσιοδοτημένες οντότητες (άτομα, οργανισμούς) που δικαιούνται να συμμετέχουν στην ανάπτυξη και διαχείριση του συγκεκριμένου επιπέδου.

Model Family:	$F$
Formal Model:	$FM$
Model Implementation:	SET OF $CC$
Certificates	

**ΣΧΗΜΑ 4.5. Ορισμός του επιπέδου Μοντέλων**

ΠΗΓΗ: [ΚΥΗ-1995]

**III. Το επίπεδο των Στιγμιοτύπων πολιτικών ασφάλειας:** Κάθε πολιτική που εκφράζεται από κάποιο μοντέλο υλοποιείται από ένα ή περισσότερα στιγμιότυπα κλάσεων κουστωδών, ενώ τα στοιχεία που χαρακτηρίζουν τα στιγμιότυπα αυτά είναι:

- Ημερομηνία έναρξης
- Ημερομηνία λήξης
- Πεδίο Εμβέλειας, το οποίο η πολιτική ελέγχει. Τα πεδία εμβέλειας μπορούν να οριστούν με βάση διάφορα κριτήρια, όπως ιεραρχικά κατ' αντιστοιχία με την οργανωτική δομή του οργανισμού ή προκειμένου να αντιπροσωπεύουν εργασίες (tasks), κ.λπ. Το σύνολο τους είναι το D, ενώ η συνάρτηση αντιστοίχισης είναι η  $domain: CC \rightarrow D$
- Το σύνολο όλων των στιγμιοτύπων μιας πολιτικής ασφάλειας δηλώνεται με CI.
- Πιστοποιητικά, τα οποία δηλώνουν τις εξουσιοδοτημένες οντότητες (άτομα, οργανισμούς) που δικαιούνται να συμμετέχουν στην ανάπτυξη και διαχείριση του συγκεκριμένου επιπέδου.

Instance Domain: <i>D</i>
Start Date:
Expire date
Instance Implementation: SET OF <i>CI</i>
Certificates

**ΣΧΗΜΑ 4.6. Ορισμός του επιπέδου Στιγμιοτύπων Πολιτικών Ασφάλειας**

ΠΗΓΗ: [ΚΥΗ-1995]

Η έννοια της **μεταπολιτικής** χρησιμοποιείται, όπως είδαμε, για την περιγραφή των πολιτικών ασφάλειας, ενώ πρέπει να σημειώσουμε ότι αντιμετωπίζεται στο πλαίσιο σαν πολιτική της οποίας το πεδίο εμβέλειας περιλαμβάνει αντικείμενα τύπου "πολιτική". Επίσης η μεταπολιτική χρησιμοποιείται με την μορφή που είδαμε και σε συνδυασμό με τον ορισμό κάποιων επιπλέον στοιχείων για σκοπούς προσδιορισμού συγκρούσεων και συνεργασίας μεταξύ πολιτικών. Τα επιπλέον στοιχεία ορίζονται ως εξής:

### ■ **Μήτρα Συγκρούσεων**

Η Μήτρα Συγκρούσεων διαχειρίζεται περιπτώσεις κατά τις οποίες περισσότερα του ενός στιγμιότυπα πολιτικών ασφάλειας ενεπλέκονται σε μία απόφαση. Ορίζεται η εξής "**σχέση κυριαρχίας**" των πολιτικών:

$dominates: \subset CI \times CI$

σύμφωνα με την οποία η μεταπολιτική μπορεί να επιλέξει την κυριαρχούσα πολιτική, χωρίς επέμβαση άλλου μέρους/οντότητας. Η έννοια αυτή υλοποιείται μέσω μίας μήτρας, ορισθείσας ως

*Conflict Resolution Matrix: (CI × CI) → CRF*

η οποία αντιστοιχίζει ένα ζεύγος πολιτικών σε μία συνάρτηση επίλυσης συγκρούσεων. Η συνάρτηση αυτή μπορεί να είναι, επί του παρόντος, είτε η προηγηθείσα συνάρτηση κυριαρχίας των πολιτικών είτε οι συναρτήσεις *and* και *or*.



## ■ **Μήτρα Συνεργασίας**

Η Μήτρα Συνεργασίας ρυθμίζει επίσης σχέσεις μεταξύ των πολιτικών σε όρους διαβάθμισης. Ορίζεται η "σχέση προτεραιότητας"

$$\text{precedes: } \subset CI \times CI$$

σύμφωνα με την οποία η μεταπολιτική μπορεί να επιλέξει την πολιτική ή εκτέλεση της οποίας πρέπει να έχει προηγηθεί, χωρίς επέμβαση άλλου μέρους/οντότητας. Η έννοια αυτή υλοποιείται μέσω μίας μήτρας, ορισθείσας ως

$$\text{Cooperation Matrix: } (CI \times CI) \rightarrow CPF$$

η οποία αντιστοιχίζει ένα ζεύγος πολιτικών σε μία συνάρτηση συνεργασίας.

Οι περιπτώσεις στις οποίες μπορεί να εμφανιστεί ανάγκη για τη χρήση των παραπάνω σχέσεων είναι κατ' αντιστοιχία αυτή όπου δύο πεδία εμβέλειας επικαλύπτονται και αυτή κατά την οποία οι εφαρμογές εντός ενός πεδίου εμβέλειας αλληλεπιδρούν με εφαρμογές εκτός αυτού.

Ο τρόπος με τον οποίο περαιτέρω υποστηρίζονται μεταπολιτικές περιλαμβάνει μία άλγεβρα που χρησιμοποιείται πρωτίστως για σκοπούς υποστήριξης της σχεδιαστικής αρχής του "ελέγχου" (verification) του συστήματος [BRY-1997]. Η άλγεβρα αυτή είναι αντίστοιχη της άλγεβρας *Boole* και χρησιμοποιείται προκειμένου να ελέγξει συσχετίσεις σύγκρισης (comparison) και συνδυασμού (combination) πολιτικών, αποσκοπώντας στον προσδιορισμό του αντίκτυπου (impact) αλλαγών που μπορεί να γίνουν, επί του υπάρχοντος σχήματος των πολιτικών. Η σημασιολογία καθεμίας από τις δύο αυτές έννοιες περιλαμβάνει τον ορισμό εννοιών όπως:

- Όσον αφορά τη Σύγκριση Πολιτικών:
  - Σχέση ισοτιμίας (equivalent to) μεταξύ πολιτικών
  - Σχέση ανισότητας (stronger than) μεταξύ πολιτικών και συνεπώς ορισμό ιεραρχιών
- Όσον αφορά το Συνδυασμό Πολιτικών:
  - Σχέση συναλήθευσης (τελεστής "and")
  - Σχέση ετεροαλήθευσης (τελεστής "or")
  - Σχέση άρνησης (τελεστής "not")

Αναγνωρίζεται, τέλος, τόσο η ανάγκη για τη δημιουργία ενός φοιαρμαλιστικού πλαισίου γενικής εφαρμογής για την κάλυψη των παραπάνω δύο εννοιών, όσο και η πολυπλοκότητα αυτής της εργασίας. Επίσης η έννοια της "σύνθεσης" πολιτικών ασφάλειας αντιμετωπίζεται μερικώς.

### **4.4.4 Υποστήριξη πολλαπλών πολιτικών ασφάλειας βασισμένη σε αναπαράσταση με γλώσσες γνώσης**

Η μοντελοποίηση πολιτικών ασφάλειας που βασίστηκε σε γλώσσες αναπαράστασης γνώσης, στην οποία αναφερθήκαμε στο κεφάλαιο III, διατείνεται ότι μπορεί να υποστηρίξει τη διαχείριση περισσότερων πολιτικών ασφάλειας.

Τα θέματα που πρέπει να διερευνηθούν προκειμένου για την υποστήριξη αυτής της προσέγγισης εστιάζονται βασικά στην ανάλυση των πεδίων ασφάλειας, της αξιολόγησης των αγαθών και της φιλοσοφίας κάθε πολιτικής ασφάλειας. Η ανάλυση στο εννοιολογικό επίπεδο έχει ως σκοπό τον εντοπισμό διαφορών που προκύπτουν

όταν οι πολιτικές αναπτύσσονται από διαφορετικές ομάδες. Η **διαφορετικότητα** που μπορεί να εντοπιστεί περιλαμβάνει τόσο περιπτώσεις ασυμφωνιών σε όρους κλασικής λογικής (για παραδείγματα βλ. [ΚΟΚ-1997b] και [ΗΟΣ-1992a]), όσο και περιπτώσεις σημασιολογικής ετερογένειας (προβλήματα ομωνύμων και συνωνύμων). Η ανάλυση των προβλημάτων που μπορούν να παρουσιαστούν αναφορικά με τα πεδία ασφάλειας, αφορά τα κλασικά σε όλες σχεδόν τις προσεγγίσεις θέματα επικάλυψης, γειτνίασης, συμπεριήψης, κ.λπ. πεδίων και τα συναφή προβλήματα. Η αξιολόγηση κάποιου αγαθού έχει ιδιαίτερη σημασία κυρίως όσον αφορά την μεταφορά του μέσω επικοινωνιακής σύνδεσης σε κάποιο άλλο πεδίο, όπου το ίδιο αγαθό αξιολογείται διαφορετικά και συνεπώς λαμβάνει λιγότερη ή περισσότερη προστασία. Τέλος, η ανάλυση των φιλοσοφιών που διέπουν τις πολιτικές ασφάλειας είναι ένα θέμα μεγάλης σημασίας, εφόσον μία διαφορά στον τομέα αυτό μπορεί να μας απαλλάξει από περαιτέρω ανάλυση. Βέβαια η διερεύνηση των συγκεκριμένων αυτών θεμάτων είναι ιδιαίτερα πολύπλοκη, αν σκεφτούμε μάλιστα ότι ο τρόπος με τον οποίο μπορούν να αναπαρασταθούν και μοντελοποιηθούν οι φιλοσοφίες είναι το πρωταρχικό ανεπίλυτο πρόβλημα.

Γενικά μπορούμε να πούμε ότι σε εννοιολογικό επίπεδο υιοθετούνται οι απόψεις σχετικά με τις μεταπολιτικές που παρουσιάστηκαν στο κεφάλαιο 4.3. Όσον αφορά την αναπαράσταση των μεταπολιτικών στο συγκεκριμένο πλαίσιο μέσω της γλώσσας *TELLOS*, δίνεται μία περιληπτική άποψη. Παρουσιάζουμε ενδεικτικά κάποια παραδείγματα:

TELL CLASS MetapolicyElement IN PolicyElementMetaClass

/\*ορισμός ενός στοιχείου "μεταπολιτική"\*/

WITH

Attributes

Title:String;  
Owner:Authority;  
Assurance:AssuranceClass;  
Author:Person;  
Distribution:DistributionLevel

END

TELL CLASS Precedes

/\*ορισμός κατηγορήματος προτεραιότητας\*/

COMPONENTS [CLASS, PRECEDES, CLASS]

IN AttributeClass

TELL CLASS PolicyPrecedence IN PolicyElementMetaClass ISA MetapolicyElement

/\*ορισμός προτεραιότητας μεταξύ κλάσεων\*/

WITH

Attributes

Domain:Domain;  
Precedes  
High:PolicyElement;  
Low:PolicyElement;

IntegrityConstraint

/\* δεν επιτρέπονται συγκρούσεις προτεραιότητας εντός ενός ή μεταξύ επικαλυπτόμενων πεδίων \*/

:\$(∀ x,y,z / PolicyElement)( ∀ p,q / Proposition)

x = p.Precedes.High ∧ y = p.Precedes.Low ∧ y = q.Precedes.High ∧

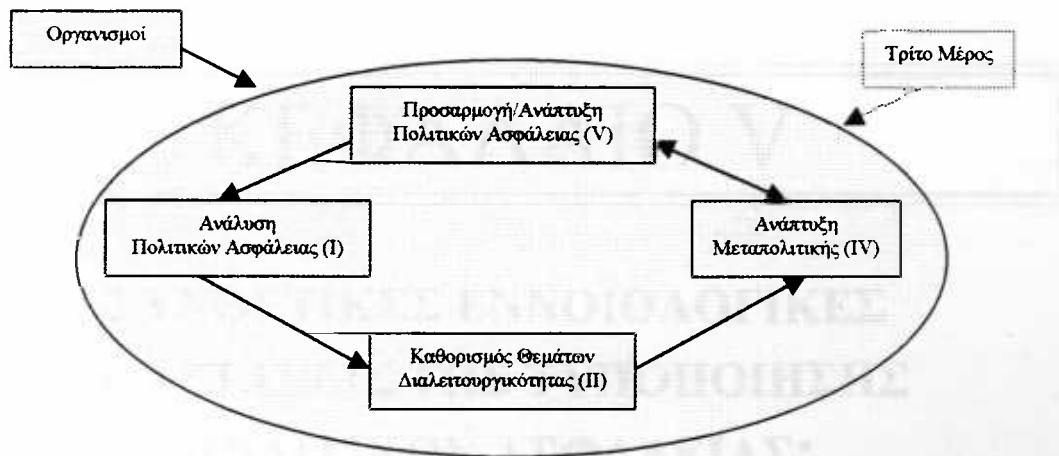
z = q.Precedes.Low ∧ p.Domain = q.Domain ⇒

```
( $\exists r / \text{PolicyPrecedence}$ )  $x = r.\text{Precedes.High} \wedge y = r.\text{Precedes.Low} \wedge$ 
 $r.\text{Domain} = p.\text{Domain} \$$ 
/* όλες οι προτεραιότητες πρέπει να δηλώνονται ρητά (όχι π.χ. μέσω μεταβατικών
σχέσεων) */
:$ ( $\forall x,y,z / \text{PolicyElement}$ ) ( $\forall p / \text{Proposition}$ )
 $x = p.\text{Precedes.High} \wedge y = p.\text{Precedes.Low} \Rightarrow$ 
 $\neg(\exists q / \text{Proposition}) x = q.\text{Precedes.Low} \wedge y = q.\text{Precedes.High} \wedge$ 
 $(p.\text{Domain} = q.\text{Domain} \vee q.\text{Domain}.IsIncluded = p.\text{Domain}) \$$ 
```

END

ΠΗΓΗ: [ΚΟΚ-1997b]

Συμπληρωματικά, προτείνεται και τεκμηριώνεται μία μεθοδολογία ανάπτυξης μεταπολιτικών για πολιτικές ασφάλειας Πληροφοριακών Συστημάτων. Η μεθοδολογία αυτή αποτελείται από τέσσερις φάσεις, όπως φαίνεται στο σχήμα:



**ΣΧΗΜΑ 4.7. Φάσεις της μεθοδολογίας ανάπτυξης μεταπολιτικών ασφάλειας**

ΠΗΓΗ: [ΚΟΚ-1997b]

Κάθε φάση έχει ορισμένα αποτελέσματα. Τα αποτελέσματα αυτά επεξεργάζονται σύμφωνα με ορισμένες μεθόδους από κάθε φάση προκειμένου να αναπτυχθούν τα επόμενα προϊόντα. Έτσι η φάση της ανάλυσης πολιτικών ασφάλειας παράγει δομημένες πολιτικές ασφάλειας και η φάση της ανάλυσης διαλειτουργικότητας συνεπάγεται τον ορισμό των σχετικών θεμάτων και προβλημάτων. Αυτά τα προϊόντα και μία συγκεκριμένη μέθοδος οδηγούν στην επεξεργασία των υπαρχουσών πολιτικών και ενδεχομένως στη δημιουργία νέων, ενώ τα μέχρι τούδε αποτελέσματα χρησιμοποιούνται με κάποια άλλη μέθοδο για τον ορισμό μεταπολιτικών ασφάλειας.

## ΚΕΦΑΛΑΙΟ V

### **ΣΥΝΘΕΤΙΚΕΣ ΕΝΝΟΙΟΛΟΓΙΚΕΣ ΔΙΑΣΤΑΣΕΙΣ ΤΗΣ ΤΥΠΟΠΟΙΗΣΗΣ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ: ΣΥΣΧΕΤΙΣΕΙΣ ΠΡΟΕΚΤΑΣΕΙΣ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ**

## 5.1 Εισαγωγή

Η ανάλυση στην οποία έχουμε μέχρι τώρα επιδοθεί, όχι μόνο παρουσίασε βασικές απόψεις αναφορικά με την τυποποίηση πολιτικών ασφάλειας, αλλά επίσης μας εισήγαγε και εξοικείώσε με έννοιες βασικές, οι οποίες αποτελούν απαραίτητο ιστορικό προκειμένου να προχωρήσουμε σε περαιτέρω θεωρητικούς σχολιασμούς.

Στο κεφάλαιο αυτό θα επιχειρήσουμε να αναπτύξουμε κριτήρια σε επίπεδο που αυτά θα προσφέρουν ένα κατάλληλα προετοιμασμένο πεδίο για τη δημιουργία μίας μεθοδολογίας για Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων. Για το σκοπό αυτό, απαιτείται να εξετάσουμε τις θεωρητικές βάσεις που μπορούν να αποτελέσουν υποδομή για την εργασία αυτή. Η εφαρμογή των θεωρητικών αυτών στοιχείων μας είναι ήδη οικεία. Ωστόσο, όπως ο αναγνώστης θα διαπιστώσει, είναι εξαιρετικά ενδιαφέρουσα η αντιμετώπιση των σχετικών θεμάτων σε επίπεδο αμιγούς θεωρητικής παρουσίασης.

## 5.2 Μοντέλα ασφάλειας Πληροφοριακών Συστημάτων

### Μοντέλα Ασφάλειας, Επιστημονικά Εργαλεία

Η νοηματική αυτή ενότητα θα προσπαθήσει να αναλύσει την έννοια των Μοντέλων Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων και να διερευνήσει τη σχέση αυτών με τις μεθοδολογίες και μεθόδους έτσι όπως οι τελευταίες αναλύθηκαν στο κεφάλαιο III αυτής της εργασίας.

Μία πρώτη παρατήρηση αποτελεί η διαπίστωση ότι το θέμα που θα επεξεργαστούμε είναι σχετικά δύσκολο. Εμπλέκει τόσο γενικές επιστημονικές αναζητήσεις όσο και συσχετίσεις με συγεκριμένα πεδία εφαρμογής. Η λέξη "μοντέλο" χρησιμοποιείται ποικιλοτρόπως σε διάφορα επιστημονικά πεδία. Είναι μάλιστα αυτός ο τρόπος χρήσης της -η ποικιλοτροπία- που καθιστά την προσπάθειά μας σε αυτό το σημείο δύσκολη. Η ποικιλοτροπία συνιστά υπερφόρτωση της λέξης με πολλά νοήματα και συνεπώς χαρακτηριστικά, απαιτήσεις και χρησιμότητες, με αποτέλεσμα να προσπαθούμε να ασχοληθούμε με μία προβληματική, ας επιτραπεί ο όρος, έννοια. Έτσι, η απομυθοποίηση της λέξης αποτελεί το εναρκτήριο σημείο αυτής της προσπάθειας.

Τα μοντέλα αποτελούν εργαλεία σχεδόν όλων των επιστημών. Όπως σημειώνεται στο [BEL-1988] όμως, μετά από ανάλυση των χρήσεων των μοντέλων, καταλήγουμε σε δύο κύριους ρόλους αυτών:

- Τα μοντέλα χρησιμοποιούνται σαν αφαιρετικές εικόνες της πραγματικότητας και αναπτύσσονται κατά τρόπο που διευκολύνει τον αναλυτή, αφενός στη μελέτη κάποιου θέματος επ' αυτής της πραγματικότητας και αφετέρου στην κατασκευή νέων δομών των συστημάτων της πραγματικότητας.
- Τα μοντέλα αναπτύσσονται προκειμένου να συμπεριλάβουν σε ένα πλαίσιο ένα σύνολο αξιωμάτων το οποίο θα χρησιμοποιηθεί προς επίδειξη των αληθειών που αντιπροσωπεύουν αυτά τα αξιώματα. Αυτή η έννοια χρησιμοποιείται κατά κόρον από την επιστήμη των Μαθηματικών.

Εξάλλου, τα ακόλουθα χαρακτηριστικά αποτελούν **κριτήρια συνέπειας** ενός μοντέλου:



- Ακριβής περιγραφή των φαινομένων που μελετώνται.
- Παροχή γενικών μηχανισμών για την ανάλυση των φαινομένων αυτών.
- Παροχή μηχανισμών για εξειδικευμένη ανάλυση και επαγωγή είτε αποδείξιμων είτε αποδεικτέων συμπερασμάτων.

Οι χρήσεις και τα χαρακτηριστικά των μοντέλων στις επιστήμες της Φυσικής, των Μαθηματικών, της Χημείας καθιστούν τα μοντέλα περισσότερο ώς αντικείμενα στήριξης της ίδιας της επιστήμης (foundations), παρά ως εργαλεία για κάποιο σκοπό. Η χρήση του όρου στο πεδίο της Ανάλυσης των Πληροφοριακών Συστημάτων και ειδικότερα της Ασφάλειας των Πληροφοριακών Συστημάτων δεν είναι εντούτοις η ίδια. Τουλάχιστον, μπορούμε να σημειώσουμε ότι η χρήση της έννοιας αυτής κατ' αυτό ακριβώς τον τρόπο προκειμένου για την ασφάλεια μπορεί να δημιουργήσει παρερμηνείς. Εξάλλου, είναι προφανές ότι η χρήση ενός όρου από διάφορες επιστήμες δεν δικαιολογεί και ταυτόσημες ερμηνείες ή απαρτήσεις, αναφορικά με τον όρο, μεταξύ διαφορετικών πεδίων. Σαφώς ρόλο σε αυτό παίζουν οι εξής παράγοντες:

- Το νέο της ηλικίας της επιστήμης και
- Η φύση του αντικειμένου της μελέτης, των ιδιοτήτων, δηλαδή, ασφάλειας ενός πληροφοριακού συστήματος. Το Πληροφοριακό Σύστημα δεν αποτελεί φαινόμενο του πραγματικού κόσμου, με τον ίδια έννοια που ορίζεται λ.χ. ένα φυσικό φαινόμενο. Έτσι, η αντίληψη των τρόπων με τους οποίους μπορεί να διερευνηθεί και επεξεργαστεί το αντικείμενο αυτό, εξαρτώμενη από τη σημαντικότητα που έχει κάθε λειτουργική άποψη του πληροφοριακού συστήματος για κάθε ομάδα ατόμων που εμπλέκονται στη μελέτη, μπορεί να διαφέρει αρκετά κατά περίπτωση.

Το ιστορικό ανάπτυξης διαφόρων γνωστών μοντέλων στο χώρο της ασφάλειας Πληροφοριακών Συστημάτων δείχνει ότι τα μοντέλα αυτά κάλυψαν δύο αντικείμενα:

- Σταδιακό ορισμό της έννοιας της ασφάλειας, με βάση τον ενστικτώδη ορισμό της, έτσι ώστε να τηρηθεί το χαρακτηριστικό της "πληρότητας" (completeness) του ορισμού και
- Έλεγχο της ορισμείσης ασφάλειας με τη δημιουργία μοντέλων πολιτικών ασφάλειας, έτσι ώστε να τηρηθεί το χαρακτηριστικό της "ορθότητας" (soundness) του ορισμού<sup>22</sup>.

Οι παραπορήσεις αυτές υποδεικνύουν τον τρόπο με τον οποίο πρέπει να αντιμετωπίσουμε τα μοντέλα ασφάλειας Πληροφοριακών Συστημάτων. Δεν θα πρέπει να παραβλέψουμε να σημειώσουμε το γεγονός εντούτοις ότι δεν έχει μέχρι σήμερα αναπτυχθεί ένα μοντέλο το οποίο περιλαμβάνει όλα τα χαρακτηριστικά της ... ενοτικτώδων αντίληψης της ασφάλειας. Πολύ περισσότερο δε, δεν υπάρχει κάποιο μοντέλο πολιτικής ασφάλειας το οποίο θα αποδείξει την εγκυρότητα κάποιου τέτοιου ορισμού.

Οι προσεγγίσεις που αναπτύχθηκαν στο κεφάλαιο III, δεν αποβλέπουν προφανώς σε έλεγχο κάποιων ορισμών. Αντίθετα, κάνουν χρήση κάποιων υπαρχόντων ορισμών, ως αντιλήψεων της έννοιας της ασφάλειας, και αποσκοπούν

<sup>22</sup> Κατ' αντιστοιχία και όπως χαρακτηριστικά σημειώνεται στο [BEL-1988]: "...every derivable formula of the model is valid", "... every valid formula is derivable".

στο να τυποποιήσουν ένα ολοκληρωμένο πλαίσιο που θα καλύπτει τον ορισμό σχετικών εννοιών και θα παρέχει μεθόδους για την ανάπτυξη συστημάτων που θα ενσωματώνουν αυτούς τους ορισμούς. Όλη αυτή η προσπάθεια όμως, υπό τους περιορισμούς ενός συγκεκριμένου περιβάλλοντος αναφοράς, έστω ευρύτερου, έτσι όπως αυτό διαμορφώνεται στο εκάστοτε Πληροφοριακό Σύστημα, συμπεριλαμβανομένων των απόψεων που διέπουν το σύστημα αυτό και του ίδιου του περιβάλλοντός του. Το γεγονός αυτό προκύπτει βάσει της φύσεως του αντικειμένου, όπως προηγουμένως σημειώσαμε. Έτσι τα μοντέλα ασφάλειας χρησιμοποιούνται ως εργαλεία στις προσεγγίσεις που περιγράψαμε, ενώ οι ίδιες οι προσεγγίσεις έχουν το χαρακτήρα προσπάθειας διαμόρφωσης μίας βάσης αναφοράς για την επιστήμη της ασφάλειας των Πληροφοριακών Συστημάτων.

### 5.3 Η πολιτική ασφάλειας εντός του περιβάλλοντός της: Μοντελοποίηση του οργανισμού ως προς την πολιτική ασφάλειας

Πληροφοριακό Σύστημα, Αντικειμενοστράφεια, Οργανισμός, Πρότυπα Ασφάλειας,  
Μεθοδολογικό Πλαίσιο

Το Πληροφοριακό Σύστημα αποτελεί την πρώτη πηγή άντλησης δεδομένων για την δημιουργία της πολιτικής ασφάλειας. Αποτελεί κυρίως το σύστημα αναφοράς και για το λόγο αυτό η πολιτική ασφάλειας οφείλει να λαμβάνει υπόψη της τα στοιχεία του περιβάλλοντος αυτού που αποτελούν νευραλγικά σημεία για την πορεία δημιουργίας της.

Σε προηγούμενες ενότητες μελετήσαμε ποικίλους τρόπους τυποποίησης των πολιτικών ασφάλειας για Πληροφοριακά Συστήματα. Διερευνήσαμε εξάλλου τη σχέση μοντέλων πολιτικών ασφάλειας και μοντέλων ασφάλειας. Σημαντική ειδοποιός διαφορά μεταξύ τους αποτελεί το γεγονός ότι **τα πρώτα εμπεριέχουν σαφώς και εξαρτώνται από την έννοια του συστήματος αναφοράς, του περιβάλλοντος επί τον οποίον εφαρμόζεται η πολιτική ασφάλειας**. Έτσι, είναι λογικό και επόμενο η μεθοδολογία που ακολουθείται για τη δημιουργία της πολιτικής ασφάλειας να προβλέπει μεθόδους οι οποίες θα λαμβάνουν υπόψη τους, θα επεξεργάζονται κατάλληλα και θα συσχετίζουν τα απαραίτητα στοιχεία που συνθέτουν το περιβάλλον αναφοράς με την πολιτική ασφάλειας.

Προκειμένου για την μελέτη των στοιχείων του Πληροφοριακού Συστήματος που σχετίζονται με την ασφάλεια μπορούμε να χρησιμοποιήσουμε διάφορες μεθόδους. Μάλιστα μπορούμε να αναζητήσουμε κάποιες απόψεις σχετικές με τη διαδικασία αυτή στην περιγραφή των μεθοδολογιών τυποποίησης των πολιτικών ασφάλειας. Έτσι το σύστημα μπορεί να μοντελοποιείται:

- Σαν υπολογιστικό σύστημα αποτελούμενο από υποσυστήματα υποκειμένων-αντικειμένων από τα οποία καθένα εκτελεί διαφορετικές λειτουργίες (βλ. μεθόδους τυποποίησης που στηρίζονται σε κανόνες, σελ. 26).
- Ως ένα αντικειμενοστραφές σύστημα αποτελούμενο από αντικείμενα με έμφαση στις λειτουργίες από τις οποίες ελέγχονται ή λειτουργίες που αυτά μπορούν να επιτελέσουν (βλ. προσέγγιση τυποποίησης που αποδίδει έμφαση στις λειτουργικές απαιτήσεις των χρηστών, σελ. 40).
- Ως ένα αντικειμενοστραφές περιβάλλον με αλληλεπιδρώντα και αμοιβαία υποπτευόμενα αντικείμενα (βλ. τη μεθοδολογία που στηρίζεται στις αρχές της

Τεχνολογίας Λογισμικού, σελ.46).

- Ως ένα πληροφοριακό σύστημα αποτελούμενο από οντότητες, με έμφαση σε στοιχεία πεποιθήσεων, αξιών και υποθέσεων που συνθέτουν την κουλτούρα του οργανισμού (βλ. προσπάθεια τυποποίησης που στηρίζεται σε γλώσσες αναπαράστασης γνώσης, σελ. 61).
- Με την έννοια που κατέχει ως τμήμα ολόκληρου του οργανισμού, με έμφαση στις υπηρεσίες -και όχι στη συμπεριφορά όπως συνήθως γίνεται- που παρέχει σε αυτό το πλαίσιο (βλ. μοντελοποίηση βασισμένη στη θεωρία των "Έλλογων Δράσεων", σελ. 65).
- Παρομοίως, χρησιμοποιώντας επίπεδα και δομές ευθύνης στα δομικά σχήματα οργανισμών (βλ. [BAC-1996], [STR-1993] και [POT-1995]).
- Χρησιμοποιώντας μεθόδους ή έννοιες μοντελοποίησης επικινδυνότητας και ανάλογα προτυποποιημένα<sup>23</sup> δομικά σχήματα για τον οργανισμό (βλ. αυτοματοποίηση της διαχείρισης πολιτικών βασιζόμενη στο πλαίσιο IBAG, σελ. 70, όπως επίσης και το [AND-1994]).
- Σαν μηχανή μετάθεσης καταστάσεων, μία δημοφιλή επιλογή που χρησιμοποιείται άλλωστε και σε συνδυασμό με πολλές άλλες.

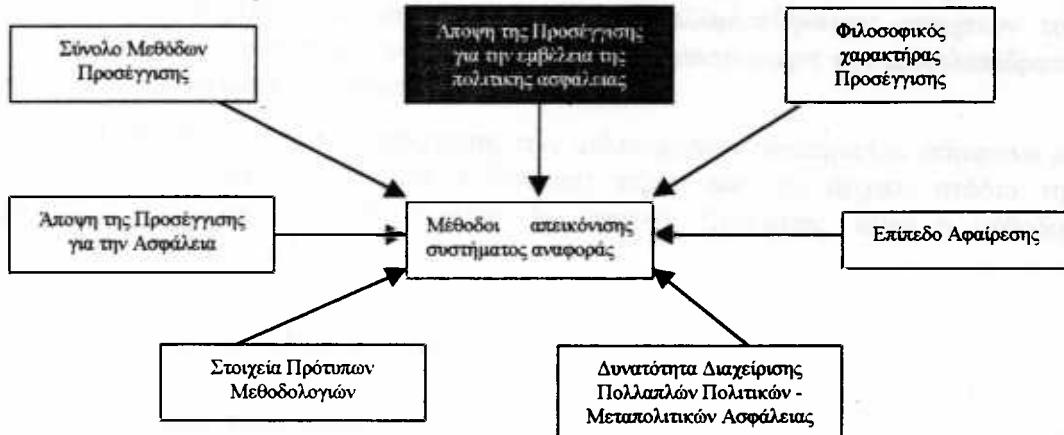
Η παράθεση αυτή, είναι εύκολο να παρατηρήσουμε ότι δεν διέπεται από κανένα κριτήριο. Διότι είναι βέβαια αναμφισβήτητο ότι παραλείπονται ορισμένα στοιχεία που προσδιορίζουν την άποψη που κάθε φορά υιοθετείται από την εκάστοτε προσέγγιση. Η διαπίστωση αυτή εξακριβώνεται αν επανελέγξουμε τις αντίστοιχες αναφορές. Ετσι, μπορούμε να σημειώσουμε τις διαστάσεις (ενίστε παραδείγματα) σύμφωνα με τις οποίες προσδιορίζουμε ή οριοθετούμε κάθε προσέγγιση αναφορικά με την άποψη που υιοθετεί για το σύστημα αναφοράς. Συνοπτικά, κάθε προσέγγιση υιοθετεί μία μέθοδο απεικόνισης του συστήματος η οποία:

- Εξυπηρετεί την αναπαράσταση στοιχείων του συστήματος που αφενός θεωρούνται σημαντικά και αφετέρου υποβοηθούν την αναπαράσταση και συσχέτιση με αυτά εννοιών ασφάλειας. Για παράδειγμα, η αντικειμενοστράφεια θεωρείται από κάποιες προσεγγίσεις ότι μοντελοποιεί επαρκώς τα σύγχρονα αποκεντρωμένα περιβάλλοντα από λειτουργική άποψη και ταυτόχρονα μπορεί να ενσωματώσει επαρκώς τη σημαντική για την ασφάλεια έννοια του "ρόλου".
- Παρέχει ευελιξία αναφορικά με τη μελέτη στοιχείων διαχείρισης πολλαπλών πολιτικών ή απεικόνισης μεταπολιτικών.
- Συνθέτει ένα ορθολογικό και μεθοδολογικό πλαίσιο με το σύνολο των τεχνικών που χρησιμοποιεί (για παράδειγμα, τα χρησιμοποιούμενα γραφικά μοντέλα για την απεικόνιση εννοιών συνεργάζονται αρμονικά με τις τυπικές γλώσσες καθορισμού προδιαγραφών που προδιαγράφουν αυτές τις έννοιες).
- Επεξεργάζεται το υλικό της σε επίπεδο αφαίρεσης ίδιο ή προσαρμόσιμο με αυτό στο οποίο αντιμετωπίζουν τις ίδιες ή άλλες διαστάσεις, που μελετώνται, οι υπόλοιπες τεχνικές της μεθοδολογίας. Αυτό σημαίνει ότι μπορούν να υπάρχουν τρόποι απεικόνισης του συστήματος αναφοράς κατά επίπεδα ανάλογα με τα επίπεδα αφαίρεσης που ακολουθεί η προσέγγιση.
- Προσημειώνει σαφώς την γενικότερη φιλοσοφική αντίληψη αναφορικά με το

<sup>23</sup> Για το ρόλο των προτύπων στη διαμόρφωση πολιτικών ασφάλειας βλ. επίσης [FER-1996].

Πληροφοριακό Σύστημα και την ασφάλεια. Έτσι, ενδέχεται να τονίζει λειτουργικές απόψεις του συστήματος, δίνοντας έμφαση σε υπηρεσίες ή συμπεριφορές, να ασχολείται με το υπολογιστικό σύστημα, το Πληροφοριακό Σύστημα ή με τον οργανισμό σαν ολότητα, κ.λπ.

Οι παραπάνω διαπιστώσεις φαίνονται γραφικά στο ακόλουθο σχήμα:



Συμπερασματικά, θα λέγαμε ότι οι υπάρχουσες μεθοδολογίες αναπαράστασης αυτού που ονομάζουμε σύστημα αναφοράς, αφενός επηρεάζουν τα μοντέλα ασφάλειας και πολιτικών ασφάλειας και αφετέρου αναπτύσσονται επηρεαζόμενα από τα πρώτα σε μία διαρκή διαδικασία ανατροφοδότησης (feedback) των αντίστοιχων πεδίων γνώσης.

## 5.4 Οι αντικειμενικές εκφραστικές δυνατότητες των τυπικών περιγραφικών μεθόδων

Τυπικές Περιγραφικές Μέθοδοι, Μοντέλα, Σημασιολογία, Συντακτικό, Μαθηματικοποιημένα Μοντέλα Συστημάτων, Αξιωματικές Περιγραφές, Γραφικές Περιγραφές

### 5.4.1 Εισαγωγή

Εκτιμούμε ότι η παράγραφος αυτή αποτελεί ένα από τα σημαντικότερα θεωρητικά μέρη αυτής της εργασίας. Οι τυπικές μέθοδοι αποτελούν το βασικό αντικείμενο μελέτης της εργασίας μας και είναι το σημείο εκκίνησης για κάθε αναφορά σε τεχνικές και πρακτικές εφαρμογές. Με άλλα λόγια οι τυπικές μέθοδοι αντιμετωπίζονται από την εργασία αυτή σαν "το ήμισυ του παντός". και γι' αυτό το λόγο η σημαντικότερη προσπάθεια αφιερώθηκε στη μελέτη της εφαρμογής τους. Ωστόσο, είναι ευνόητο ότι ο χαρακτήρας της εργασίας αυτής δεν θα επέτρεπε την

του νοήματος είναι δυνατόν να έχουν υπάρξει πολλαπλοί. Ο όρος που θα χρησιμοποιούμε στην παράγραφο που τους αφιερώνεται αποκλειστικά είναι "Τυπικές Περιγραφικές Μέθοδοι" (ΤΠΜ). Οι ΤΠΜ αποτελούν σημαντικό εργαλείο της επιστήμης της Πληροφορικής και κυριαρχούν στο χώρο της μελέτης των Πληροφοριακών Συστημάτων και της Τεχνολογίας Λογισμικού. **Επικονρούν την προσπάθεια αντίληψης, προσδιορισμού και περιγραφής της απλής έως - συνηθέστερα- περίπλοκης συμπεριφοράς των συστημάτων**, απόψεις των οποίων πρόκειται να αυτοματοποιήσουμε. Η συμπεριφορά αυτή αντιμετωπίζεται στην πληθώρα των περιπτώσεων από τη σκοπιά της **αλληλεπίδρασης** στοιχείων του συστήματος ή των συστημάτων μεταξύ τους, με σημαντικότερη την αλληλεπίδραση ορισμένων στοιχείων με το συστατικό "άνθρωπος".

Ο προσδιορισμός της υπόστασης των μελετώμενων συστημάτων σύμφωνα με τις αρχές της Νοητικής (Cognitive Science) περνά από το αρχικό στάδιο της έκφρασης μέσω απλού λόγου (verbal description). Εντούτοις, αυτή η μέθοδος περιγραφής χαρακτηρίζεται ως:

- Μακροσκελής
- Εμπεριέχουσα Περιπτολογία
- Ημιπλήρης
- Επισφαλής παρερμηνειών
- Αδόμητη

Τα χαρακτηριστικά αυτά την καθιστούν ακατάλληλη για τους σκοπούς μας. Μολονότι θα ήταν χρήσιμη η εύρεση μίας μεθόδου κατάλληλης να διαχειριστεί τη συμμετοχή λεκτικών σχημάτων σε εγχειρήματα Information Systems Security Engineering, η προσπάθεια θα ήταν πολύ φιλόδοξη από άποψη αποτελέσματος και κόστους.

Οι ΤΠΜ μέθοδοι περιλαμβάνουν διαφόρων ειδών *Μαθηματικοποιημένα Μοντέλα Συστημάτων*, τα οποία συνοπτικά θα περιγράψουμε. Για αναλυτικότερη πληροφόρηση ο αναγνώστης μπορεί να απευθυνθεί στο [BRO-1996].

#### 5.4.2 Είδη Τυπικών Περιγραφικών Μεθόδων

##### 5.5.2.1 Μοντέλα Δεδομένων

Οι τεχνικές αυτές (Data Models) προσπαθούν να απεικονίσουν τα δεδομένα και την πληροφορία που ένα πεδίο εφαρμογής περιέχει. Προκειμένου να αντιμετωπίσουν την εγγενή τους αδυναμία να αγνοούν τις λειτουργικές-διαδικαστικές απόψεις του πεδίου μελέτης αναπτύσσουν υπομεθόδους που μελετούν όχι μόνο τα σύνολα των δεδομένων αλλά και τις μεταξύ τους συσχετίσεις και τις λειτουργίες επ' αυτών.

Από μαθηματική άποψη, ένα Μοντέλο Δεδομένων αποτελείται από μία ετερογενή άλγεβρα η οποία περιέχει ένα σύνολο *Tύπων* (*T*) και ένα σύνολο *Συναρτήσεων* (*S*), που συντονίζονται από μία *Συνάρτηση Καθορισμένης Λειτουργικότητας*:

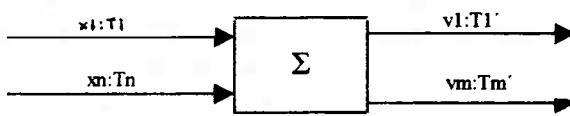
$$\text{σκλ.: } \Sigma \rightarrow T$$

Για κάθε συνάρτηση καθορίζεται το πεδίο των τύπων ορισμού και το σύνολο

των τύπων τιμών. Η τριπλέτα  $(\Sigma, T, \text{σκλ})$  αποτελεί την υπογραφή (signature) της άλγεβρας και εκφράζει το συντακτικό της μέρος. Στις περισσότερες εφαρμογές χρειάζεται να απεικονίσουμε τις καταστάσεις των στοιχείων του συστήματος. Έτσι, επεκτείνουμε την υπογραφή στην  $(T, \Sigma I, \text{σκλ})$ , όπου  $I$  είναι το σύνολο των Ιδιοτήτων των καταστάσεων. Μία συνηθισμένη τεχνική αναπαράστασης των Μοντέλων αυτών είναι τα Διεπαφά Οντοτήτων-Συγκεκριμένων.

#### 5.4.2.2 Μοντέλα Διεπαφών

Τα μοντέλα αυτά (System Component Models / Interface Models) αντιμετωπίζουν το σύστημα τμηματικά, ως αποτελούμενο από μαύρα ή διαπερατά κουτιά (black box - glass/white box) που ενσωματώνουν κάποιες λειτουργίες. Τα στοιχεία αυτά είναι αυτόνομα και επικοινωνούν με τον εξωτερικό κόσμο μέσω καναλιών εισόδου και εξόδου, τα οποία αντιπροσωπεύουν συγκεκριμένους τύπους δεδομένων, σε συγκεκριμένα χρονικά διαστήματα, όπως φαίνεται στο ακόλουθο σχήμα:



**ΣΧΗΜΑ 5.2. Μοντέλο Διεπαφών**

Έμφαση αποδίδεται στην επικοινωνία των στοιχείων, δηλαδή στις διεπαφές τους, για τις οποίες ορίζεται συντακτικό. Η σχέση

$$\delta: (I, O)$$

είναι μία απλή, αφαιρετική απεικόνιση μιας διεπαφής.

#### 5.4.2.3 Μοντέλα Κατανεμημένων Συστημάτων

Θεωρούμε ότι ένα κατανεμημένο σύστημα (Distributed System) αποτελείται από ένα σύνολο αλληλεπιδρώντων στοιχείων που καλούνται αντικείμενα (objects) ή φορείς (agents). Τα στοιχεία αυτά αντιμετωπίζονται είτε ως μαύρα είτε ως άσπρα κουτιά και επικοινωνούν μέσω καναλιών, απεικονίζονται δε σαν δίκτυα ροής δεδομένων. Έστω ν οι κόμβοι-στοιχεία του δικτύου,  $O$  τα κανάλια εξόδου και  $(I, O)$  διεπαφή. Το κατανεμημένο σύστημα  $(v, O)$  δίδεται από την αντιστοίχιση:

$$\rho: N \rightarrow \zeta, \text{ όπου } v \in N \text{ και } \zeta: (I, O)$$

η οποία συναρτά κάθε στοιχείο με μία συμπεριφορά. Τα κατανεμημένα συστήματα μπορούν επίσης να αναπαρασταθούν με διαφόρων ειδών γραφικές παραστάσεις (βλ. [BRO-1996]).

#### 5.4.2.4 Μοντέλα Διαδικασιών

Μία διαδικασία (Process) ορίζεται σαν ένα σύνολο πράξεων ο οποίες συσχετίζονται με σχέσεις παραγωγής ή πρόκλησης νέων πράξεων. Κάθε πράξη ενεργοποιείται από ένα μήνυμα (ενός συνόλου μηνυμάτων  $M$ ) και η εκτέλεσή της έχει ως αποτέλεσμα τη δημιουργία νέων μηνυμάτων. Η αποστολή ή αποδοχή μηνύματος συνιστά ένα γεγονός. Στο προηγούμενο κατανεμημένο σύστημα, μία διαδικασία μπορεί να παρασταθεί από ένα ακυκλικό δίκτυο ροής δεδομένων ( $v_i, O_i$ ) και μία συνάρτηση αποτίμησης

$\eta: chan(v_i, O_i) \rightarrow M$ , όπου  $chan(v_i, O_i)$  τα τόξα (κανάλια) του δικτύου

η οποία συναρτά κάθε τόξο του δικτύου με ένα μήνυμα. Ένα σύνολο γεγονότων και οι συναφείς συσχετίσεις παραγωγής πράξεων ορίζουν μία συμπεριφορά ή ιστορικό του συστήματος και αναπαρίστανται με Διαγράμματα Ακολουθίας Μηνυμάτων (Message Sequence Charts), Διαγράμματα Διαδικασιών (Process Charts), κ.λπ.

#### 5.4.2.5 Μοντέλα Μετάθεσης Καταστάσεων

Τα μοντέλα αυτά (State Transition Models) εστιάζουν σε περιγραφές του εσωτερικού των συστημάτων (glass box view). Θεωρούμε, κατά τον ίδιο τρόπο με τα προηγούμενα, στοιχεία του συστήματος και τις μεταξύ τους διεπαφές και ορίζουμε ένα σύνολο Καταστάσεων (State) για κάθε στοιχείο του συστήματος. Ο μηχανισμός μετάθεσης καταστάσεων (state transition machine) ορίζεται από

- ένα σύνολο αρχικών καταστάσεων  $State_0 \subseteq State$  και
- τη συνάρτηση:

$\Delta: (State \times I^*) \rightarrow (State \times O^* \rightarrow Bool)$

η οποία δίνει την έγκυρη ή άκυρη αντιστοίχιση κάποιας κατάστασης  $State$  και ενός συνόλου  $I^*$ , που αντιπροσωπεύει κανάλια εισόδου με τα αντίστοιχα μηνύματα που αυτά μεταφέρουν, σε μία άλλη κατάσταση  $State$  και ένα σύνολο καναλιών εξόδου  $O^*$ .

Γενικά, τα μοντέλα αυτά δεν είναι αιτιοκρατικά (deterministic), μπορούν να ενσωματώσουν τεχνικές απεικόνισης διαφόρων στοιχείων ή επιθυμητών χαρακτηριστικών και για το λόγο αυτό θεωρούνται ευέλικτα.

#### 5.4.3 Απαιτήσεις για τις Τυπικές Περιγραφικές Μεθόδους

Προκειμένου να αντιμετωπίσουμε το σημαντικό θέμα που θέτει ο τίτλος αυτός, πρέπει να παρατηρήσουμε ότι οι ΤΠΜ χρησιμοποιούνται για να περιγράψουν τη συμπεριφορά ενός συστήματος (χρησιμοποιώντας την έννοια της "συσχέτισης" των στοιχείων του) και οι περιγραφές αυτές μπορεί να είναι απαραίτητες σε διάφορες φάσεις, όπως στην καταγραφή απαιτήσεων, στο σχεδιασμό και στην υλοποίηση. Οι αντίστοιχες απαιτήσεις για τις ΤΠΜ πρέπει να καθοριστούν αναφορικά με τη φάση στην οποία χρησιμοποιούνται. Έτσι, μπορούμε αρχικά να υποστηρίξουμε ότι η ενελιξία στην παράσταση ποικίλων απαιτήσεων συστημάτων, αντίληψη γυρίων σε εννοιολογικό επίπεδο, είναι σημαντική για τις μεθόδους της πρώτης φάσης, ενώ η έμφαση πρέπει να δοθεί στις λειτουργικές απόψεις, που καθιστούν τα παραγόμενα

αποτελέσματα κατάλληλα για χρήση σε υπολογιστικό σύστημα, για τις επόμενες φάσεις. Ωστόσο, αναμφισβήτητα υπάρχουν ιδιότητες κοινές για όλες τις φάσεις, και αυτές συνοψίζονται στις ακόλουθες:

- Αναγνωσιμότητα
- Εκφραστικότητα
- Κατανοητότητα
- Δυνατότητα παραμετροποίησης-αφαιρετικότητας

Οι ιδιότητες τις οποίες αναφέραμε και άλλες οι οποίες μπορεί να εντοπιστούν, καλύπτονται όταν η ΤΠΜ διαθέτει τα ακόλουθα χαρακτηριστικά:

- Τυπικό συντακτικό
- Τυπική σημασιολογία
- Σαφές μοντέλο εννοιολογικής απεικόνισης συστήματος
- Μέθοδο απεικόνισης διεπαφών-επικοινωνιών
- Εκφραστικότητα και περιγραφικότητα ανάλογες με το επίπεδο των ατόμων που εμπλέκονται στη μελέτη του συστήματος
- Εργαλεία και μεθόδους μελέτης λειτουργικών απόψεων και θεμάτων υλοποίησης, τα οποία όμως παρέχουν σε επαρκή βαθμό δυνατότητες αφαιρετικότητας (abstraction-refinement)

Σχετικός με τον όρο "Τυπικές Περιγραφικές Μέθοδοι" είναι ο όρος "μοντέλο", που παραπέμπει συχνά στις γραφικές αναπαραστάσεις που χρησιμοποιούμε προκειμένου να εκφράσουμε τα νόηματα του συντακτικού που ορίζουμε. Οι τεχνικές αυτές προκύπτουν με βάση είτε αξιωματικές μεταφράσεις των συμβολισμών του συντακτικού είτε τη μετάφραση που η ίδια η τυπική άλγεβρα που χρησιμοποιούμε παρέχει. Οι γραφικές απεικονίσεις είναι ιδιαίτερα δημοφιλείς. Πρέπει όμως να παρατηρήσουμε ότι οι τυπικές μέθοδοι στις οποίες ανήκουν ανάγονται σε πλήρεις τυπικές μεθόδους όταν αποτελούνται από τυπικά ορισμένο συντακτικό και πλήρως τυπικά ορισμένη σημασιολογία. Η παρατήρηση αυτή αποτελεί τη σημαντικότερη απαίτηση για τις τυπικές μεθόδους μιας και αποτελεί επίσης την κύρια προβληματική τους περιοχή.

Πιο συγκεκριμένα, οι προσπάθειες επί της ανάπτυξης ΤΠΜ εστιάζονται στο συντακτικό, ενώ η σημασιολογία παραμελείται. Εντούτοις η σημασιολογία αποτελεί το θεωρητικό εκείνο τμήμα το οποίο τελικά θα επιδείξει ότι οι συμβολισμοί συμπίπτουν με την άτυπη διατύπωση των προβλήματος, το οποίο θα είναι τελικά δυνατό να κατανοηθεί από όλα τα συμμετέχοντα μέρη. Μάλιστα, ένα τυπικό σημασιολογικό πλαίσιο θα πρέπει, εκτός από απαιτήσεις κατανοητότητας, να είναι τέτοιο ώστε να μην περιορίζει τη χρήση διαφόρων συντακτικών τύπων -αν μάλιστα αναλογιστούμε ότι τα συντακτικά που συνήθως χρησιμοποιούνται είναι δεδομένα ή αποτελούν μίξεις κάποιων γνωστών συντακτικών- και από την άλλη να δίνει την κατάλληλη καθοδήγηση τόσο για την ερμηνεία των συντακτικών όσο και για τη χρήση συντακτικών τύπων που είναι κατάλληλοι για κάθε εφαρμογή. Η τυποποίηση της σημασιολογίας δεν πρέπει να περιορίζει λοιπόν την ευελιξία της στην αποτύπωση των χαρακτηριστικών ασφάλειας κάθε ιδιαίτερου πεδίου εφαρμογής. Επιπλέον η δυνατότητα έκφρασης εννοιών χρόνου, που έχουν ζεχωριστή σημασία στις σχετικές εφαρμογές της Τεχνολογίας Λογισμικού, αποτελεί ακάλυπτο θέμα των αναζητήσεων συντακτικών όσο και σημασιολογικών πλαισίων.

Είναι φανερό, μετά από τη συζήτηση αυτή, ότι δεν υπάρχει ένα πλήρες πλαίσιο είτε συντακτικών, είτε σημασιολογικών περιγραμμάτων. Πολύ δε περισσότερο δεν υπάρχουν προσπάθειες τυποποίησης ενός κοινού πλαισίου το οποίο θα ικανοποιεί τις ποικίλες απαιτήσεις τις οποίες θέτουν τα πολύπλοκα περιβάλλοντα εφαρμογής τα οποία προσπαθεί η Πληροφορική να καλύψει.

## 5.5 Επίπεδα αφαίρεσης, αναπαράστασης και δόμησης σε θέματα ανάλυσης συστημάτων

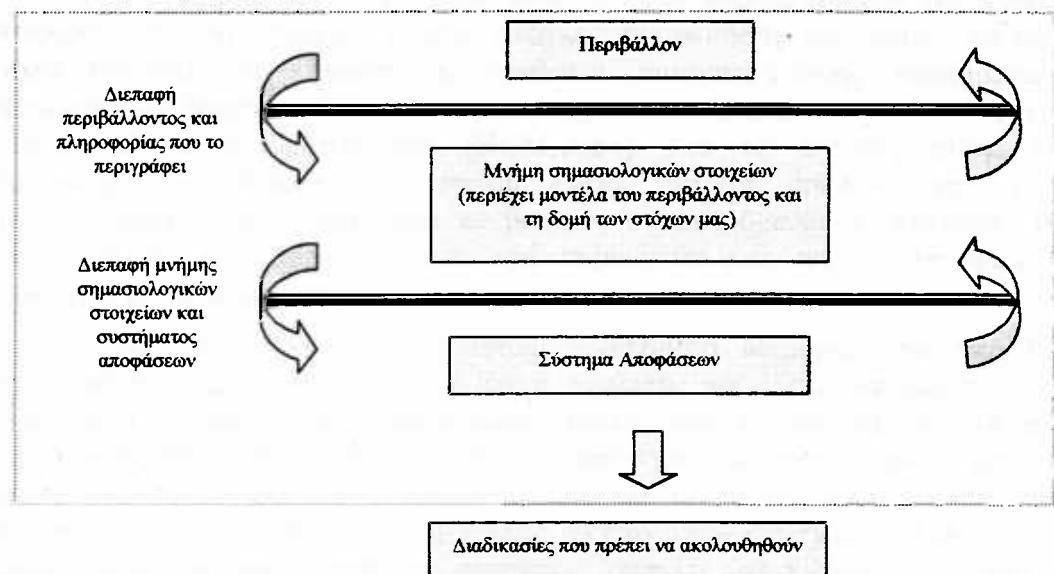
Αδόμητα Προβλήματα, Θεωρία Αποφάσεων, Νοητικές Διαδικασίες, Διαδικαστική Αβεβαιότητα, Λεκτικό, Εννοιολογικό, Λογικό, Σημασιολογικό, Περιγραφικό Επίπεδο

### 5.5.1 Σχετικά με τη δόμηση συστημάτων προβλήματα

Οι δυσκολίες που αντιμετωπίζουμε όταν προσπαθούμε να αναλύσουμε ένα σύνολο προβληματικών καταστάσεων, για τις οποίες καταρχήν ενστικτωδώς έχουμε την αντίληψη ότι μπορούν να συνθέσουν ένα σύστημα προς μελέτη, είναι σημαντικές. Η περίπτωση αυτή εμπλέκει επίσης έναν ολόκληρο κύκλο διαδικασιών λήψης αποφάσεων. Στην ενότητα αυτή θα αναφερθούμε συνοπτικά στα συναφή θέματα.

Θεωρούμε το σύνολο αυτό των προβληματικών καταστάσεων σαν ένα "μη-καλά ορισμένο" πρόβλημα, από την άποψη ότι, τόσο ο ορισμός των συστατικών του στοιχείων όσο και η αναπαράστασή του εμπεριέχουν μεγάλο ποσοστό **αβεβαιότητας**. Οι δομές που συνθέτουν τα προβλήματα αυτά συχνότατα δεν είναι προφανείς. Πρέπει αντίθετα να αναπαραχθούν μέσα από κάποιες διαδικασίες, οι οποίες θα θέσουν προτεραιότητες μέσα από μία διαδικασία καθορισμού κριτηρίων επιλογής (στο [HUM-1984] αναφέρεται σαν "decision process of criteria-experts choice", δίνοντας έμφαση στο γεγονός ότι ο ιδιοκτήτης του προβλήματος χρειάζεται τη συνδρομή ειδικών για τις διαδικασίες αυτές), προκειμένου να διαμορφώσουμε μία αφαιρετικά ολοκληρωμένη άποψη για το εν λόγω σύστημα. Οι δυσκολίες στην επιλογή αυτών των διαδικασιών ορίζουν την έννοια της "**διαδικαστικής αβεβαιότητας**" (procedural uncertainty).

Η Θεωρία Αποφάσεων προβλέπει κάποιους τρόπους επίλυσης τέτοιου είδους προβλημάτων. Μία συχνά χρησιμοποιούμενη μέθοδος είναι η "εκλογικευμένη οικονομία" (economic rationality). Η μέθοδος αυτή συνίσταται στη χρήση τυπικών μοντέλων, τα οποία βασίζονται σε κάποια δεδομένα αξιώματα. Τα αξιώματα αυτά αφορούν τις προβληματικές καταστάσεις και τον τρόπο αντιμετώπισή τους και λειτουργούν αποσυνθέτοντας την προβληματική κατάσταση και παρακολουθώντας τη συνέπεια (consistency) και την ορθότητα της μεταβατικότητας (transitivity) της όλης πορείας αποσύνθεσης. Το ακόλουθο σχήμα απεικονίζει συνοπτικά τη διαδικασία αυτή (για αναλυτικότερη περιγραφή βλ. [HUM-1984]).



ΣΧΗΜΑ 5.3. Η διαδικασία αποσύνθεσης για τη μελέτη συστημάτων.

Το Σύστημα Αποφάσεων περιέχει μεθόδους δόμησης της αδόμητης προβληματικής κατάστασης (εν πολλοίς διαγράμματα, μοντέλα, πληροφορίες συσχέτισης γεγονότων και διαδικασιών, κ.λπ.) και προσπαθεί, διατηρώντας πληροφορία σχετική με την πορεία της διαδικασίας, να καθορίσει την πιθανότητα εξάρτησης μεταξύ των αποτελεσμάτων ενεργειών διαφορετικών σταδίων αποσύνθεσης. Κατά τον τρόπο αυτό, δεν αντιμετωπίζεται επαρκώς η διαδικαστική αβεβαιότητα. Η τελευταία συσχετίζεται άμεσα με τη δομή των προβλημάτων επί των οποίων θα εφαρμόσουμε τους κανόνες αποσύνθεσης και όχι τόσο με τις ίδιες τις ενέργειες που κάνουμε για να επιλύσουμε το πρόβλημα. Οι απαιτήσεις για μία πιο ολοκληρωμένη μεθοδολογία είναι συνοπτικά οι ακόλουθες:

- Κάθε σύστημα αποφάσεων επικουρικό της διαδικασίας ανάλυσης της προβληματικής κατάστασης πρέπει να παρέχει μεθόδους συμβατές με τις ικανότητες και τη γλώσσα που μπορούν τα συμμετέχοντα μέρη να κατανοήσουν.
- Κάθε πληροφορία που γίνεται αντιληπτή ως μορφή σε κάποιο επίπεδο, αντιμετωπίζεται ως περιεχόμενο στο επόμενο.
- Κάθε απεικόνιση στοιχείου σε κάποιο επίπεδο πρέπει να υποστηρίζεται (δηλαδή να διατηρείται ως νοηματική ουσία) στα ακόλουθα επίπεδα.

Τέλος, το σύστημα αποφάσεων πρέπει να δομηθεί επί των νοητικών διαδικασιών των ατόμων που επιλύουν το πρόβλημα. Με το θέμα αυτό και την εφαρμογή του στα Πληροφοριακά Συστήματα θα ασχοληθούμε στις ακόλουθες παραγράφους.

### 5.5.2 Ανάλυση των νοητικών διαδικασιών που μετέχουν στη διαδικασία δόμησης και τυποποίησης προβλημάτων που επιδέχονται αυτοματοποίηση<sup>24</sup>

Ο στόχος μας στην παράγραφο αυτή είναι να παρουσιάσουμε ένα πλαίσιο αναφοράς, που ανταποκρίνεται στις ανάγκες τυποποίησης (οι οποίες συνήθως αναλαμβάνονται στα πλαίσια προσπαθειών αυτοματοποίησης συστημάτων), αναφορικά με θέματα καθημερινής πρακτικής, τα οποία απαιτούν και επιδέχονται κάποιου είδους αυτοματοποίηση [HUM-1984]. Για τις ανάγκες αυτής της παραγράφου υποθέτουμε ότι τέτοιου είδους θέματα ορίζουν έναν χώρο προβληματισμού, όπου δύο είναι οι βασικοί ενδιαφερόμενοι: ο αναλυτής της προβληματικής κατάστασης -άποψη που κυρίως θα μας απασχολήσει- και ο ιδιοκτήτης του προβλήματος.

Ο βασικός άξονας σε μία τέτοια προσπάθεια διαμορφώνεται από δύο αντικρουόμενες απαιτήσεις: από τη μία ο αναλυτής χρειάζεται να μελετήσει το πρόβλημα υιοθετώντας ένα συγκεκριμένο τρόπο, που προϋποθέτει ένα επίπεδο τυποποίησης προκειμένου να επιτευχθεί ο σκοπός του, ενώ ταυτόχρονα ο χρήστης απαιτεί ένα τέτοιο επίπεδο τυποποίησης που θα τον πείθει ότι αυτό που του παρουσιάζεται είναι πράγματι το πρόβλημα το οποίο τον απασχολεί. Η εύρεση της χρυσής τομής ανάμεσα σε αντές τις απαιτήσεις αποτελεί μεθοδολογικό πρόβλημα σε κάθε απόπειρα μετάβασης από μία πρακτική σε μία άλλη, όπου απαιτείται αλλαγή του τρόπου με τον οποίο οι δραστηριότητες εκτελούνται και κυρίως αλλαγή του τρόπου με τον οποίο ο ίδιος ο χώρος προβληματισμού αντιμετωπίζεται.

Ο τρόπος με τον οποίο αυτή η πρόκληση αντιμετωπίζεται εδώ, προκύπτει μέσω μελέτης των νοητικών διαδικασιών που μπορούν να στηρίζουν τη διαδικασία τυποποίησης ενός χώρου προβληματισμού. Είναι αλήθεια ότι, ενώ η γνώση που απαιτείται προκειμένου να μελετήσουμε ένα συγκεκριμένο σύστημα είναι και αυτή συγκεκριμένη, οι νοητικές διαδικασίες που ακολουθούνται είναι ίδιες στη γενική περίπτωση.

Τα στάδια νοητικών συμβολισμών που συνοδεύονται από μοντέλα αναπαράστασης του χώρου προβληματισμού είναι πέντε [HUM-1984]. Μεταξύ των πέντε σταδίων υπάρχει διαδοχική συνέπεια, ενώ κάθε στάδιο αντιπροσωπεύει διαφορετικές νοητικές διαδικασίες.

#### Στάδιο 1: Γλωσσικό επίπεδο

Περιεχόμενο	Ανακάλυψη των αντιλήψεων, των πεποιθήσεων και των επιθυμιών του ιδιοκτήτη του προβλήματος αναφορικά με την προβληματική κατάσταση.
Έκφραση	Αδόμητες προτάσεις.
Νοητικές διαδικασίες	Εκτιμάται ότι οι νοητικές διαδικασίες εντοπίζονται ακόμη και εκτός των σχετικών με τη γλωσσική έκφραση.

<sup>24</sup> Η αγγλική απόδοση -για την περίπτωση που βοηθάει την κατανόηση- για την έκφραση αυτή είναι: "Analysis of the conceptual procedures in the structuring and formalising of decision problems subject to automation".

### Στάδιο 2: Εννοιολογικό επίπεδο

Περιεχόμενο	Ο αναλυτής μαζί με τον ιδιοκτήτη του προβλήματος προσπαθούν, αναλύοντας τις προηγούμενες απόψεις, να ανακάλυψουν τα κρίσιμα σημεία του συστήματος και να δημιουργήσουν διάφορα μοντέλα που τα αναπαριστούν. Ακολουθεί ανάλυση των μοντέλων που δημιουργούνται.
Έκφραση	Μοντέλα της προβληματικής κατάστασης.
Νοητικές Διαδικασίες	Ανάλυση και σύνθεση.

### Στάδιο 3: Λογικό επίπεδο

Περιεχόμενο	Διερευνώνται οι περιορισμοί που πρέπει να εισαχθούν ή υπάρχουν στα μοντέλα του Σταδίου 3, σε σχέση με τα αντίστοιχα στοιχεία του πραγματικού κόσμου τα οποία αντιπροσωπεύουν.
Έκφραση	Οι τυπικές αναπαραστάσεις της προβληματικής κατάστασης, εμπλουτισμένες με επιπλέον περιορισμούς.
Νοητικές Διαδικασίες	Ανάλυση, παραγωγή υποθέσεων και έλεγχοι επιφρούων και συνεπειών αυτών.

### Στάδιο 4: Σημασιολογικό επίπεδο

Περιεχόμενο	Καθορίζεται ένας τυπικός τρόπος (άλγεβρα, γλώσσα και συμβολισμός) μέσω του οποίου τα προηγούμενα μοντέλα τροποιούνται προκειμένου να ακολουθούν κάποια συγκεκριμένα πρότυπα. Αυτό γίνεται από τον αναλυτή με τη βοήθεια ίσως άλλων ειδικών.
Έκφραση	Τυπικές αναπαραστάσεις (μοντέλα) της προβληματικής κατάστασης.
Νοητικές Διαδικασίες	Ορισμός τυπικών αναπαραστάσεων και διαδοχικές εκλεπτύνσεις.

### Στάδιο 5: Περιγραφικό επίπεδο

Στόχος	Ο τυπικός τρόπος αναπαράστασης που ορίστηκε στο Στάδιο 3 και εμπλουτίστηκε στο Στάδιο 4, διερμηνεύεται περαιτέρω προκειμένου να οριστούν σε τελικό στάδιο οι μηχανισμοί (ένας άλλος τυπικός τρόπος) αναπαράστασης που θα επιτρέψουν την απεικόνιση του συστήματος σε χαμηλότερο επίπεδο αφαίρεσης.
Έκφραση	Τυπικά μοντέλα αναπαράστασης (άλγεβρα) σε τελικό στάδιο προ αυτοματοποίησης.
Νοητικές Διαδικασίες	Διαδικασίες εντοπισμού στοιχείων τεχνολογίας υλοποίησης.



Παρατηρούμε ότι στην παραπάνω παράθεση δεν αναφερθήκαμε σε καμία συγκεκριμένη πρακτική. Είναι απόφαση του αναλυτή οι πρακτικές που θα επιλέξει σε κάθε στάδιο. Ας δούμε τώρα πώς η παραπάνω διαδικασία μπορεί να εφαρμοστεί στην περίπτωση δημιουργίας μοντέλων πολιτικών ασφάλειας Πληροφοριακών Συστημάτων.

### Ξ Στάδιο 1

Διερευνώνται οι κανόνες που κάθε ενδιαφερόμενο μέρος εκτιμά ότι πρέπει το σύστημα να ακολουθεί και αντίστοιχα εκτιμώνται οι ευπάθειες του συστήματος. Αυτοί οι κανόνες εκφράζουν επιθυμία για την ομαλή και βέλτιστη συμπεριφορά του συστήματος προκειμένου για την εκτέλεση των υπηρεσιών που πρέπει να προσφέρει στους χρήστες του.

### Ξ Στάδιο 2

Ο αναλυτής, έχοντας υπόψη τα αποτελέσματα του προηγούμενου σταδίου, καθώς και τη φύση της προβληματικής κατάστασης, μπορεί να εντοπίσει ή να δημιουργήσει μία γλώσσα περιγραφής της δομής της προβληματικής κατάστασης (problem structuring language<sup>25</sup>). Η επιλογή της γλώσσας έχει σημασία εφόσον αυτή αναμένεται να παράγει μία όσο το δυνατόν καλύτερη αναπαράσταση του συστήματος, και των ευπαθειών. Ένας τρόπος δημιουργίας μίας τέτοιας γλώσσας ή κριτήριο εντοπισμού της είναι ο εξής: αντιμετωπίζουμε το σύστημα σε τμήματα, καθένα από τα οποία αντιτροσωπεύει μία κρίσιμη άποψη αυτού και προσπαθούμε να αναπαραστήσουμε τα στοιχεία αυτών των τμημάτων, οντότητες και λειτουργίες, ξεχωριστά σε εννοιολογικό επίπεδο. Μπορούμε λ.χ. σε ένα σύστημα να διακρίνουμε ως ξεχωριστό το τμήμα που περιλαμβάνει τις επικοινωνίες και να ερευνήσουμε τρόπους αναπαράστασης αυτού.

### Ξ Στάδιο 3

Στο στάδιο αυτό, ο αναλυτής καλείται να δημιουργήσει ή να εντοπίσει μία άλγεβρα (*calculus*) με συμβολισμούς (*notation*) και σημασιολογία (*semantics*) προκειμένου να συμβολίσει με τυπικό τρόπο τα τμήματα που εντόπισε στο προηγούμενο στάδιο. Η όλη διαδικασία απαιτεί γνώσεις Σημειοτικής (Semiotics) και Σημασιολογίας (Semantics), προκειμένου να απεικονιστεί το πραγματικό σύστημα όπως πραγματικά είναι και ταυτόχρονα με τον καλύτερο δυνατό τρόπο για τους σκοπούς της όλης διαδικασίας. Στο στάδιο αυτό θα μπορούσαμε λ.χ. να εντοπίσουμε τρόπους αναπαράστασης του τμήματος του συστήματος που περιλαμβάνει την πρόσβαση στους πόρους του συστήματος ως μία μήτρα προσπέλασης.

### Ξ Στάδιο 4

Το στάδιο αυτό είναι μάλλον πολύπλοκο, διότι απαιτεί ανάλυση των αποτελεσμάτων του προηγούμενου σταδίου προκειμένου να ανακαλύψουμε σημαντικά σημεία του συστήματος τα οποία πρέπει να τύχουν ειδικής μεταχείρισης. Τα αποτελέσματα αυτού του σταδίου μπορεί να περιλαμβάνουν ακόμη και αλλαγή κάποιων απόψεων για την κατάσταση. Πρόκειται ουσιαστικά για τη διενέργεια μιας ανάλυσης ευαισθησίας (sensitivity analysis) στοιχείων του συστήματος που ανήκουν σε κάθε τμήμα που εντοπίσαμε στο στάδιο 2. Για παράδειγμα, θα μπορούσαν στο

<sup>25</sup> Στο [KJO-1993] αναφέρεται πώς μπορεί να δοθεί μία "πλούσια εικόνα" σχετικά με κάποια προβληματική κατάσταση και παρουσιάζεται το μοντέλο CATWOE του P.Checkland προκειμένου για την περιγραφή των υπαρχουσών απόψεων αναφορικά με την προβληματική κατάσταση.



τμήμα μελέτης των μηνυμάτων επικοινωνίας να αναλυθούν όλες οι καταστάσεις ενός μηνύματος προκειμένου να ανακαλυφθούν όλες οι περιπτώσεις κάτω από τις οποίες οι λειτουργίες επί του μηνύματος επιφέρουν αποδεκτά αποτελέσματα.

## ⇨ Στάδιο 5

Στο στάδιο αυτό καλύπτεται και ο τελευταίος "βαθμός ελευθερίας" του συστήματος που μελετάται, με το να εντοπιστεί το μηχανικό του αντίστοιχο. Ήα μπορούσαμε λ.χ. σε αυτό το στάδιο να εντοπίσουμε συγκεκριμένους αλγόριθμους κρυπτογράφησης ή πρωτόκολλα αυθεντικοποίησης.

### 5.5.3 Ένα ενδεικτικό παράδειγμα

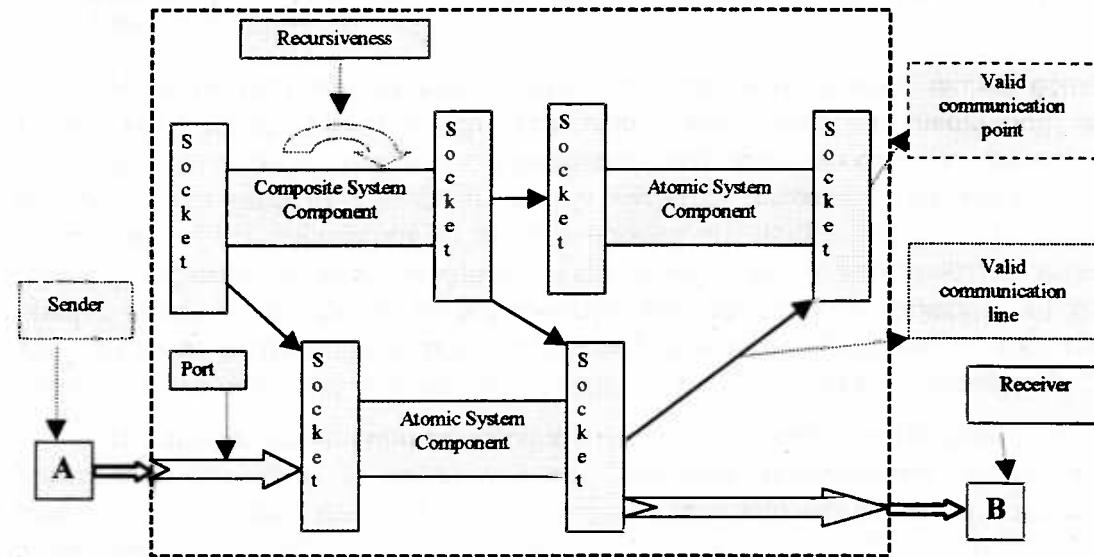
Στο [DOB-1988] προτείνονται τα βήματα για την ανάπτυξη ενός μοντέλου πολιτικής ασφάλειας για ένα σύστημα επικοινωνούντων υπολογιστών (communication system). Ανακαλύψαμε ότι ο τρόπος με τον οποίο η προτεινόμενη διαδικασία αντιμετωπίζει το σύστημα αναφοράς, είναι ανάλογος του τρόπου με τον οποίο αντιμετωπίζεται ένα πληροφοριακό σύστημα, αν γίνει εξαρχής αποδεκτό ότι το βασικό χαρακτηριστικό ενός πληροφοριακού συστήματος είναι η επικοινωνία και αλληλοσυσχέτιση μεταξύ των στοιχείων του.

Ο τρόπος με τον οποίο διεξάγεται η μελέτη περιλαμβάνει τα ακόλουθα σημεία:

1. Ορισμό του συστήματος και των εμπλεκομένων μερών.
2. Ανάλυση επικοινωνιών, δηλαδή ορισμός των τύπων επικοινωνίας που μπορούν να υπάρξουν, των μηνυμάτων και των συσχετίσεων που μπορούν να αναπτυχθούν μεταξύ των εμπλεκομένων.
3. Ορισμό των κανόνων που περιγράφουν και καθορίζουν τη συμπεριφορά των εμπλεκομένων μερών στους διάφορους τύπους επικοινωνίας που μπορούν να υπάρξουν.
4. Περιγραφή του συστήματος όπως κάθε εμπλεκόμενο μέρος το αντιμετωπίζει.
5. Ορισμό του φυσικού μοντέλου του συστήματος με ταυτοποίηση των φυσικών συνθετικών του μερών και του τρόπου που αυτά επικοινωνούν.
6. Ορισμό του λογικού μοντέλου του συστήματος με ταυτοποίηση των λογικών συνθετικών του μερών και του τρόπου που αυτά ανταλάσσουν λογικά μηνύματα.
7. Ορισμό του μοντέλου συμπεριφοράς του συστήματος σε όρους αφηρημένων ενεργειών και γεγονότων.
8. Ανάλυση των επικοινωνιών με έμφαση σε πιθανά ρήγματα επικοινωνίας.
9. Ανάλυση των ευπαθειών που μπορούν να προκύψουν σε συγκεκριμένες επικοινωνίες των εμπλεκομένων μερών με το σύστημα.
10. Ανάλυση των ευπαθειών για κάθε τύπο μηνύματος.
11. Ανάλυση του μοντέλου συμπεριφοράς για πιθανές καταστάσεις λάθους.
12. Ανάλυση του τρόπου με τον οποίο οι κανόνες που κάθε βήμα παράγει μπορούν να εφαρμοστούν.

Σε συγκεκριμένα σημεία αυτής της διαδικασίας δημιουργούνται ποικίλα μοντέλα, εκτός αυτών που αναφέρονται ρητά, που αντιπροσωπεύουν απόψεις του συστήματος. Για παράδειγμα, μπορούμε να παρουσιάσουμε ένα "μοντέλο σύνθεσης του συστήματος" από την πλευρά του αναλυτή. Το μοντέλο σύνθεσης του συστήματος πρέπει να διαχωρίζεται από το "μοντέλο δόμησης του συστήματος". Το

μεν τελευταίο αφορά αυτά καθεαυτά τα στοιχεία-μέρη δόμησης του συστήματος ενώ το πρώτο δίνει σημασία στον τρόπο με τον οποίο κάποια στοιχεία συνθέτουν ένα σύστημα. Το μοντέλο ενός επικοινωνιακού συστήματος δημιουργείται σύμφωνα με κάποιους κανόνες σύνθεσης (που ορίζουν π.χ. έγκυρα σημεία επικοινωνίας, συνθετικά μέρη του συστήματος, σημεία επικοινωνίας με το περιβάλλον, εμπλεκόμενα μέρη, κ.λ.π.).



**ΣΧΗΜΑ 5.4.** Ένα μοντέλο σύνθεσης ενός πληροφοριακού συστήματος έτσι όπως το αντιλαμβάνεται στο εννοιολογικό επίπεδο για τις ανάγκες της ανάλυσης ο αναλυτής.

Ακολούθως, μπορούμε να δημιουργήσουμε το "μοντέλο συμπεριφοράς του συστήματος". Η συμπεριφορά του συστήματος μπορεί να θεωρηθεί ότι περιγράφεται από ένα ίχνος ερεθισμάτων (stimuli) των υποδοχών (sockets) του συστήματος με ακόλουθες αντιδράσεις (responses) των συνθετικών μερών (components) αυτού. Όλες οι αποδεκτές συμπεριφορές του συστήματος, δηλαδή τετράδες του τύπου <ερέθισμα, υποδοχή, στοιχείο, αντίδραση> ορίζουν το Πεδίο Καταστάσεων του συστήματος. Κάθε στιγμή υπάρχει ένα στιγμιότυπο κάποιας τέτοιας κατάστασης και διατηρούμε έναν επιλογέα (selector) που την υποδεικνύει. Κάθε κατάσταση (συμπεριφορά) που βρίσκεται εκτός του Πεδίου Καταστάσεων αποτελεί ευπάθεια του συστήματος. Κάθε μετάβαση από μία κατάσταση εντός του Πεδίου Καταστάσεων σε μία κατάσταση εκτός αυτού, προκαλεί ένα γεγονός που ονομάζεται ρήγμα ασφάλειας. Κάθε ερέθισμα που προκαλεί ρήγμα ασφάλειας ονομάζεται απειλή. Προκειμένου να αντιμετωπίσουμε τα ρήγματα, μπορούμε να ειδάγουμε περιορισμούς στο πεδίο Καταστάσεων που τους ονομάζουμε αντίμετρα.

Από το παράδειγμα αυτό, μπορούμε να διακρίνουμε τον τρόπο με τον οποίο μπορούν να προκύψουν μέσα σε ένα μοντέλο που περιγράφει μία γενική άποψη του συστήματος, όχι μόνο βασικές έννοιες ασφάλειας για το συγκεκριμένο σύστημα, αλλά και κανόνες, οι οποίοι εκφράζουν την πολιτική ασφάλειας του συστήματος. Τέτοιου είδους έννοιες προκύπτουν σε πολλά στάδια της διαδικασίας, ενώ

παρατηρούμε από την περιγραφή των βημάτων ότι το τελευταίο στάδιο προβλέπει την περιγραφή του τρόπου εφαρμογής αυτών των κανόνων.

## 5.6 Μία αφαιρετική προσέγγιση υψηλού επιπέδου για την ανάπτυξη ασφαλών Πληροφοριακών Συστημάτων

### 5.6.1 Εννοιολογικά στοιχεία της προσέγγισης

Ιεραρχική Ανάπτυξη Ασφαλών Συστημάτων, Απαιτήσεις Ασφάλειας, Οριζόντια και Κάθετη ολοκλήρωση

Η προσέγγιση που θα μας απασχολήσει στην ενότητα αυτή ανήκει στους J.Leiwo και Y.Zheng. Απαιτεί δε την αντιμετώπιση του θέματος της τυποποίησης σε ένα υψηλότερο επίπεδο εννοιολογικής αφαιρέσης, από αυτό στο οποίο κινούμασταν έως τώρα, και μάλιστα σχετίζεται με την ανάπτυξη ασφαλών Πληροφοριακών Συστημάτων. Είναι ενδιαφέρον να παρατηρήσουμε στο σημείο αυτό πώς μπορούν διαφορετικές αφαιρετικές προσεγγίσεις να επεξεργάζονται τον ίδιο γνωστικό χώρο. Μπορεί κανείς να εκλάβει τη διαφορετικότητα των αφαιρετικών προσεγγίσεων ως προς τον τρόπο με τον οποίο αντιμετωπίζουν μεθοδολογικά το θέμα είτε ως προς τον οποίο μεθοδικά αναλύουν το θέμα είτε ως προς την εννοιολογική τους προσέγγιση.

Η παρούσα προσέγγιση υποθέτει ότι η ανάπτυξη ασφαλών Πληροφοριακών Συστημάτων ακολουθεί το παράδειγμα της "από-πάνω-προς-τα-κάτω" ανάπτυξης, υιοθετώντας επίπεδα (layers). Η ως προς επίπεδα (ή ιεραρχική) ανάπτυξη ασφαλών συστημάτων αποτελεί μία μάλλον προσφιλή τεχνική [LEI-1997], [ABR-1991]. Μάλιστα, τα επίπεδα ανάπτυξης ασφάλειας αντιστοιχίζονται με ανάλογα αφαιρετικά επίπεδα εννοιολογικών (μετα-)μοντέλων Πληροφοριακών Συστημάτων. Χρησιμοποιείται επίσης και η έννοια της μοντελοποίησης του οργανισμού ως συστήματος, ως προϋπόθεση για την εφαρμογή του πλαισίου. Παράλληλα γίνεται λόγος για μία οριζόντια άποψη στην ανάπτυξη ασφάλειας. Η άποψη αυτή, αναγνωρίζει ότι κάθε επίπεδο αποτελείται από μονάδες (units) των οποίων οι απαιτήσεις βρίσκονται καθέτως στο ίδιο αφαιρετικό επίπεδο, όμως απαιτείται οριζόντιος συντονισμός της επικοινωνίας τους.

Επίσης πρέπει να σημειώσουμε ότι η προσέγγιση αυτή δεν κάνει άμεσα λόγο για πολιτικές ασφάλειας Πληροφοριακών Συστημάτων. Υιοθετεί την έννοια των απαιτήσεων ασφάλειας, η οποία αφενός έχει μεγαλύτερο βαθμό αοριστίας και γενικότητας, αφετέρου έχει το πλεονέκτημα ότι μπορεί να καλύψει πληθώρα πραγματικών καταστάσεων, όπου η ασφάλεια κατανοείται, και συνεπώς εμφανίζεται, είτε με απλή προτασιακή μορφή δηλώσεων είτε με τη μορφή τυπικών μοντέλων απαιτήσεων.

Το μοντέλο που θα παρουσιάσουμε προσπαθεί να τυποποιήσει φορμαλιστικά τις βάσεις του, προκειμένου να προσδώσει σαφήνεια και συνέπεια σε αυτές. Εξάλλου, η προσπάθεια αυτή είναι λογική, εφόσον ένα μοντέλο που επιχειρεί να αντιμετωπίσει την ολοκλήρωση διαφόρων προσεγγίσεων πρέπει να αποδίδει με τυπικό τρόπο τις απαιτήσεις του τρόπου ολοκλήρωσης, έτσι ώστε να είναι σε θέση να ενσωματώσει περισσότερες της μίας απόψεις.



### 5.6.2 Το τυπικό μοντέλο ανάπτυξης ασφαλών Πληροφοριακών Συστημάτων

Το μοντέλο θεωρείται ως μία τετράδα της μορφής ( $L$ ,  $U$ ,  $I$ ,  $S$ ) όπου:

1.  $L = \{L_i \mid i=1, 2, \dots, N\}$  αντιπροσωπεύει το σύνολο των επιπέδων, όπου  $L_1$  είναι το υψηλότερο
2.  $U = \{u_{i,j} \mid i, j=1, 2, \dots, N; j=1, 2, \dots, count(i)\}$  αντιπροσωπεύει το σύνολο των μονάδων που συνθέτουν κάθε επίπεδο, όπου  $u_{i,j}$  είναι η  $j$  μονάδα για το  $i$  επίπεδο
3.  $I = \{I_i \mid i=1, 2, \dots, N\}$  αντιπροσωπεύει το σύνολο των απαιτήσεων ασφάλειας για το επίπεδο  $i$  (που τίθονται αποκλειστικά από το επίπεδο)
4.  $S = \{S_{i,j} \mid i, j=1, 2, \dots, N; j=1, 2, \dots, count(i)\}$  αντιπροσωπεύει το σύνολο των εξειδικευμένων απαιτήσεων ασφάλειας για τη μονάδα  $j$  του επιπέδου  $i$  (που τίθονται αποκλειστικά από τη μονάδα)

Επίσης, ορίζονται δύο σύνολα:

5.  $Parent(u_{i,j}) = \{u_{i+1,j}\}$  είναι το σύνολο όλων εκείνων των μονάδων  $u_{i+1,j}$  του προηγούμενου επιπέδου που θέτουν απαιτήσεις ασφάλειας για τη μονάδα  $u_{i,j}$
6.  $Child\{u_{i+1,j}\}$  είναι το σύνολο εκείνων των μονάδων  $u_{i+1,j'}$  των επόμενων επιπέδων για τις οποίες η μονάδα  $u_{i,j}$  θέτει απαιτήσεις ασφάλειας.

Το πλαίσιο αυτό (μοντέλο) πρέπει να ικανοποιεί τις ακόλουθες τρεις συνθήκες:

#### • ΥΠΟΘΕΣΗ I

Πληρότητα επιπέδων (Completeness of layers), η οποία υπονοεί ότι κάθε μονάδα  $u_{i,j}$  πρέπει να ανήκει οπωσδήποτε σε ένα επίπεδο:  $\forall u_{i,j} \in U \mid u_{i,j} \in \bigcup_{n=1}^N L_n$

#### • ΥΠΟΘΕΣΗ II

Μοναδικότητα επιπέδων (Uniqueness of layers), η οποία υπονοεί ότι κάθε επίπεδο είναι μοναδικό, συνεπώς κάθε μονάδα ανήκει σε ένα μόνο επίπεδο:  $\cap_{n=1}^N L_n = \emptyset$

#### • ΥΠΟΘΕΣΗ III

Μοναδικότητα μονάδων (Uniqueness of units), η οποία υπονοεί ότι κάθε μονάδα είναι μοναδική:  $\forall u_{i_1,j_1}, u_{i_2,j_2} \in U \mid (u_{i_1,j_1} = u_{i_2,j_2}) \Rightarrow ((i_1=i_2) \wedge (j_1=j_2))$

Κάθε μονάδα  $u_{i,j} \in U$  χαρακτηρίζεται και από τις συνολικές απαιτήσεις ασφάλειάς της  $R_{i,j}$ , οι οποίες προκύπτουν από τις εξειδικευμένες γι' αυτήν την μονάδα απαιτήσεις, τις απαιτήσεις του επιπέδου και τις απαιτήσεις που προκύπτουν γι' αυτήν ως αποτέλεσματα εξόδου (output) από τα ανώτερα επίπεδα:

$$R = \{S_{i,j}, I, R'_{i,I,j'} \mid u_{i,I,j'} \in Parent(u_{i,j})\}$$

Το τελευταίο αυτό στοιχείο είναι εκείνο που εξασφαλίζει την ομογενή και συνεπή κάθετη ανάπτυξη ασφαλών Πληροφοριακών Συστημάτων σε επίπεδο διαδοχικών μονάδων. Πιο συγκεκριμένα, η συνάρτηση η οποία εκφράζει την κάθετη ολοκλήρωση, δηλαδή τη "μετάφραση" μεταξύ απαιτήσεων διαδοχικών επιπέδων, είναι η ακόλουθη:

$$\tau: \{R \times S \times I\} \rightarrow R, \text{ με}$$

$$τ_{i,j}(R_{i,j}, S, I) = R'_{i+1,j'} \mid u_{i,j} \in Child(u_{i,j}) \quad (I)$$

Ωστόσο, ιδιαίτερη σημασία αποδίδεται στο θέμα της οριζόντιας



ολοκλήρωσης, η οποία αποτελεί ένα δύσκολο πρόβλημα. Μπορούμε να φανταστούμε την περίπτωση όπου περισσότερα Πληροφοριακά Συστήματα πρέπει να επικοινωνήσουν. Το θέμα της επικοινωνίας πρέπει να λάβει υπόψη του και τα προβλήματα που ενδέχεται να προκύψουν από διαφοροποιήσεις στις απαίτησεις ασφάλειας μεταξύ αυτών. Θεωρούμε σε οριζόντια τομή τα επικρινωνούντα συστήματα ως διαφορετικές μονάδες ( $u_{i,j}$ ) ενώ έχουμε εξασφαλίσει ότι καθέτως βρισκόμαστε στο ίδιο επίπεδο. Για κάθε διαφορετική απαίτηση ασφάλειας που προσδιορίζουμε σε κάθε Πληροφοριακό Σύστημα αντιστοιχίζουμε ένα αναγνωριστικό (identifier, id), έτσι ώστε η απαίτηση να συμβολίζεται με  $r_{i,j}^{id}$ . Επίσης για κάθε επίπεδο  $L_i$  δημιουργούμε το σύνολο όλων των διαφορετικών αναγνωριστικών  $ID_i = \{id\}$ . Για ένα δεδομένο επίπεδο  $L_i$  και μία δεδομένη τιμή  $id$ , η οριζόντια ολοκλήρωση είναι ο προσδιορισμός του συνόλου

$$\{ H_i^{id} \mid id \in ID_i \}$$

δηλαδή, όλων των απαίτησεων των οποίων τα αναγνωριστικά ισούνται με μία ορισμένη τιμή,

$$\forall id \in ID_i \mid H_i^{id} = \{R_{i,j}^{id} = id\}$$

και ορίζεται η ακόλουθη συνάρτηση οριζόντιας ολοκλήρωσης:

$$\rho_i: R \rightarrow R$$

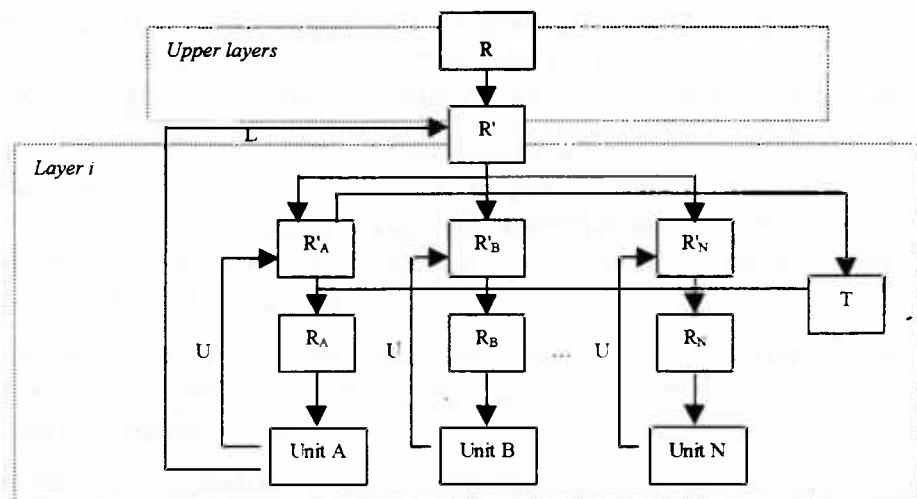
$$\rho_i(R'_{i,j}) = R_{i,j} \mid R'_{i,j} \in H_i^{id} \quad (\text{II})$$

όπου  $R'_{i,j}$  ορίζεται στην (I).

Η ολοκλήρωση των απαίτησεων γίνεται πρώτα κάθετα και ακολούθως οριζόντια, όπως δείχνει ο ακόλουθος τύπος:

$$R_{i,j} = \rho_i(\tau_{i-1,j'}(I_{i-1}, S_{i-1,j'}) \mid R_{i-1,j'} \in Parent(u_{i,j}))$$

Η σημασιολογία των τύπων αυτών φαίνεται και στο ακόλουθο σχήμα:



ΣΧΗΜΑ 5.5. Οριζόντια και κάθετη ολοκλήρωση απαίτησεων ασφάλειας.

ΠΗΓΗ: [LEI-1997]

Στο πλαίσιο που παρουσιάσαμε υπάρχουν σχετικά στατικά και σχετικά δυναμικά στοιχεία, ο οργανισμός και οι συναρτήσεις ολοκλήρωσης των απαιτήσεων ασφάλειας κατ' αντιστοιχία. Οι δεύτερες απαιτείται να αλλάζουν όταν αλλάζουν στοιχεία του οργανισμού (συμπεριλαμβανομένων των θεμάτων ασφάλειας υψηλού επιπέδου).

## 5.7 Προς την κατεύθυνση της διαμόρφωσης μιας μεθοδολογίας για Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων

### 5.7.1 Εισαγωγή

Μέχρι αυτού του σημείου, έχουμε αναφερθεί στα ακόλουθα θέματα:

- Οριοθέτηση της έννοιας της πολιτικής
- Οριοθέτηση της έννοιας της πολιτικής ασφάλειας Πληροφοριακού Συστήματος
- Ανάλυση της έννοιας της τυποποίησης πολιτικών ασφάλειας Πληροφοριακών Συστημάτων
- Μελέτη μεθοδολογιών και μεθόδων τυποποίησης πολιτικών ασφάλειας Πληροφοριακών Συστημάτων
- Ενταξη της έννοιας της διαχείρισης πολλαπλών πολιτικών ασφάλειας Πληροφοριακών Συστημάτων στη θεματολογία της εργασίας και μελέτη σχετικών μεθοδολογιών και μεθόδων
- Μελέτη βασικών θεμάτων που μορφώνουν και συμπληρώνουν τη θεματολογία μας

Αποτελεί πρόκληση στο σημείο αυτό η προσπάθεια να συλλέξουμε το πλήθος της πληροφορίας που έχουμε και να το οργανώσουμε με κριτήρια εννοιολογικά και μεθοδολογικά, έτσι ώστε να έχουμε τη δυνατότητα, αφενός να ανακαλούμε εύκολα σημεία που μας ενδιαφέρουν και αφετέρου να σχηματοποιήσουμε μία οργάνωση του υλικού σε έναν ορισμένο άξονα. Τον άξονα αυτό υποδεικνύει και ο τίτλος της ενότητας αυτής: είναι η διαμόρφωση των προδιαγραφών μιας μεθοδολογίας, για **Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων** (βλ. παράγρ. 5.7.2.2 για ανάλυση του όρου που επιλέχθηκε). Εκτιμούμε ότι η διάσταση αυτή έχει τα ακόλουθα χαρακτηριστικά, τα οποία την κάνουν ελκυστική προς μελέτη:

- Αποτελεί πεδίο το οποίο σχετικά εύκολα μπορούμε να προσεγγίσουμε εφόσον, όπως θα δείξουμε, έχουμε καλύψει τα βασικά του σημεία (αντίθετα δεν έχουμε καλύψει βασικά σημεία ώστε να προτείνουμε μία συγκεκριμένη μέθοδο τυποποίησης πολιτικών ασφάλειας για έλεγχο προσπέλασης και εμπιστευτικότητα δεδομένων, για παράδειγμα).
- Θα επέλθει ως φυσική κατάληξη αυτής της εργασίας εφόσον θα απαιτηθεί ένα είδος συνοπτικής αντιμετώπισης και οργάνωσης ενός μεγάλου όγκου πληροφοριακού υλικού.
- Η μελέτη της απαιτεί τη χρήση αυξημένων αφαιρετικών και κυρίως συνθετικών νοητικών λειτουργιών, για τις οποίες υπάρχει άφθονη πληροφορία προς επεξεργασία.
- Έχουμε τη βεβαιότητα ότι το επιστημονικό πεδίο στο οποίο έχει εμβέλεια ή από μόνη της διαμορφώνει ανήκει στα σημαντικά ανερχόμενα πεδία έρευνας για τα

επόμενα χρόνια.

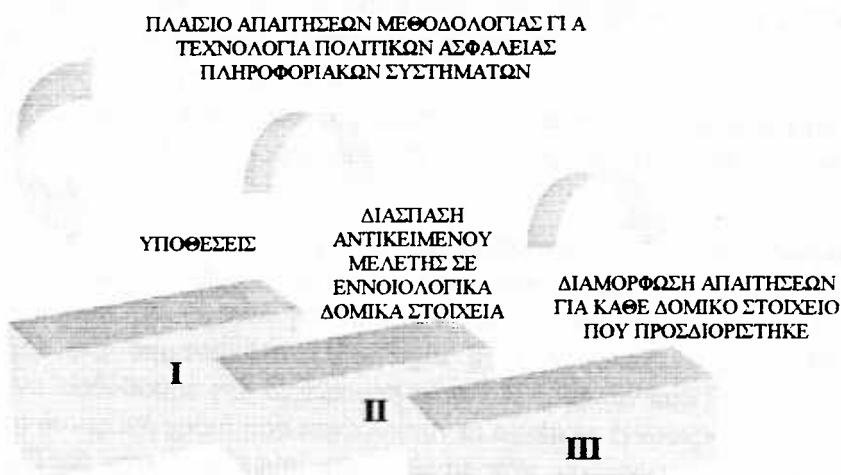
Τα χαρακτηριστικά αυτά αποτελούν και τους λόγους για τους οποίους επιλέχθηκε να πραγματοποιηθεί η μελέτη του συγκεκριμένου θέματος.

### **5.7.2 Δομικά στοιχεία του πλαισίου αναφοράς**

## Εννοιολογική Διάσπαση, Δομικά Στοιχεία, Πλάσιο, Σύντημα Μελέτης Χαρακτηριστικά Ασφάλειας, Εργαλεία, Μεθοδολογικές Πρακτικές

#### 5.7.2.1 Συνοπτική περιγραφή της προσέγγισης

Τα δομικά μέρη (διαστάσεις) που συνθέτουν την προσέγγισή μας και δομούν ένα πλαίσιο για τις απαιτήσεις της μεθοδολογίας είναι τρία. Αυτά ορίζουν επίσης ισάριθμα βήματα που θα ακολουθηθούν στον καθορισμό των απαιτήσεων, όπως παριστάνεται σχηματικά στο ακόλουθο σχήμα:



**ΣΧΗΜΑ 5.6.** Τα δομικά μέρη της προσέγγισης για τον προσδιορισμό των απαιτήσεων για τη μεθοδολογία Τεχνολογίας Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων.

Το πρώτο βήμα περιλαμβάνει τη διατύπωση ορισμένων βασικών υποθέσεων για το χαρακτήρα αυτής της προσέγγισης. Τα βήματα II και III αποτελούν το κυρίως μέρος της προσέγγισης. Τα βήματα τα οποία θα ακολουθήσουμε αναλύονται όπως περιγράφεται στα παρακάτω.

#### **5.7.2.2 Ορισμός των αντικειμένου των προβληματισμού - Διαμόρφωση υποθέσεων**

Επιλέξαμε να περιγράψουμε το πρόβλημα που μας απασχολεί με την έκφραση "απαιτήσεις μιας μεθοδολογίας για Τεχνολογία Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων". Χρειάζεται, εντούτοις, να δώσουμε προσοχή στη σημασία που ο όρος έχει για τη μελέτη αυτή. Αυτό είναι απαραίτητο διότι, στη συναφή βιβλιογραφία ο όρος μπορεί να χρησιμοποιείται με εννοιολογικές διαφοροποιήσεις.

Βασικό άξονα αναφοράς αποτελεί σαφώς η έννοια της πολιτικής ασφάλειας. Η έννοια αυτή, έρχεται να απελευθερώσει τους αυστηρούς ορισμούς και τις αναφορές στην ασφάλεια από τον στενό και ακατανόητο τεχνικό τους κλειό και να τις συνδέσει με ένα ευρύτερο περιβάλλον που καλύπτει όλο το πληροφοριακό σύστημα. Άλλωστε, το γεγονός ότι οι σύγχρονες μέθοδοι ανάπτυξης χαρακτηριστικών ασφάλειας σε πληροφοριακά συστήματα, απαιτούν τη διαμόρφωση πολιτικών ασφάλειας που λαμβάνουν υπόψη τους το σύστημα σαν ολότητα, αποτελεί ένδειξη για τη σημασία που αποδίδεται στις πολιτικές ασφάλειας. Κάτι τέτοιο δεν σημαίνει βέβαια ότι αποσπάμε την ασφάλεια από κάθε τεχνική της διάσταση. Η τυποποίηση και μαθηματικοποίηση πολλών σημείων είναι αναπόφευκτη και απαραίτητη. Ο όρος "τεχνολογία" άλλωστε παραπέμπει οπωδήποτε σε μία αυστηρή και δομημένη προσέγγιση. Εμείς θα τηρήσουμε τη συμβατότητα με αυτά τα χαρακτηριστικά, διαμορφώνοντας ένα πλαίσιο με συγκεκριμένο τρόπο και θα δίνοντάς του μία ορισμένη δομή. Αυτό που χρειαζόμαστε είναι ένα πλαίσιο το οποίο θα χρησιμεύσει ως αναφορά απαιτήσεων σχετικών με:

- Τη δημιουργία πολιτικών ασφάλειας ικανών να αντιμετωπίσουν τις πολύπλοκες απαιτήσεις που διαμορφώνουν τόσο οι χρήστες όσο και η τεχνολογία.
- Την έκφραση των πολιτικών ασφάλειας στο περιβάλλον ενός οργανισμού του οποίου τα πληροφοριακά συστήματα πρέπει να καλύψουν, ώστε τα δεύτερα να υπηρετούν τον οργανισμό αυτό.
- Την εξαγωγή της πληροφορίας μέγιστης χρησιμότητας αναφορικά με τον έλεγχο, την ανατροφοδότηση, προσαρμογή και εξέλιξη των ίδιων των πολιτικών ασφάλειας.

Επίσης, πρέπει να αναφέρουμε ότι πρόκειται για ένα **εννοιολογικό πλαίσιο**. Δεν φύλασσαν μας να δημιουργήσουμε ένα τυπικό πλαίσιο ή μία τυποποιημένη γλώσσα ορισμού απαιτήσεων για τα παραπάνω θέματα, παρόλο που κάτι τέτοιο θα αποτελούσε ένα σημαντικότατο βοήθημα στην προσπάθεια αυτή. Δεν πρόκειται συνεπώς να επιδιοθούμε στη διατύπωση κάποιων ορισμών που θα κλείσουν σε στενά πλαίσια τη δυναμική χροιά που περικλείουν οι σχετικές έννοιες και θα είναι ευάλωτοι σε ανακρίβειες στη διατύπωσή τους. Αυτό που κυρίως μας ενδιαφέρει είναι να αποδώσουμε τη σημασία που έχει η έννοια για το χώρο της ασφάλειας, δεδομένων των εξελίξεων στο πεδίο αυτό, έτσι όπως τις περιγράψαμε στο πρώτο κεφάλαιο. Μετά από την ανάλυση που έχει προηγηθεί βρισκόμαστε αντιμέτωποι με έναν όγκο πληροφορίας σχετικό με το θέμα μας. Έχουμε επίσης διαμορφώσει κάποιες απόψεις για τα σημεία που αποτελούν πηγές προβληματισμού (αν και η εκτίμηση για τη σημαντικότητα κάθε θέματος είναι σχετικά υποκειμενική, βέβαια).

Τα θέματα που μας απασχόλησαν και στα οποία θα στηριχθούμε, είναι ομολογουμένως πολλά στο πλήθος και κατά συνέπεια πρέπει να συμπεράνει κανείς ότι η μεθοδολογία μας πρέπει να καλύψει ένα πεδίο που εκτείνεται σε ένα αρκετά μεγάλο εύρος θεμάτων. Από την άλλη βέβαια, η έννοια της μεθοδολογίας είναι αρκετά γενική ώστε να επιτρέπει να επιλέξουμε ένα συγκεκριμένο επίπεδο αφαίρεσης ανάλογο των θεμάτων που θέλουμε να καλύψουμε και των πληροφοριών που έχουμε στη διάθεσή μας. Ετσι, θα επικεντρωθούμε στην οργάνωση του υλικού κατά χρήσιμο τρόπο για τους σκοπούς που αναφέρθηκαν και σε σημεία τα οποία μας απασχόλησαν περισσότερο στη μελέτη που προηγήθηκε (π.χ. τυπικές μέθοδοι, μοντέλα ασφάλειας και η συμβολή τους στη διαδικασία της Τεχνολογίας Πολιτικών Ασφάλειας, κ.λπ.).

Οι διαστάσεις που τέθηκαν ορίζουν για μας την έννοια του όρου Τεχνολογία

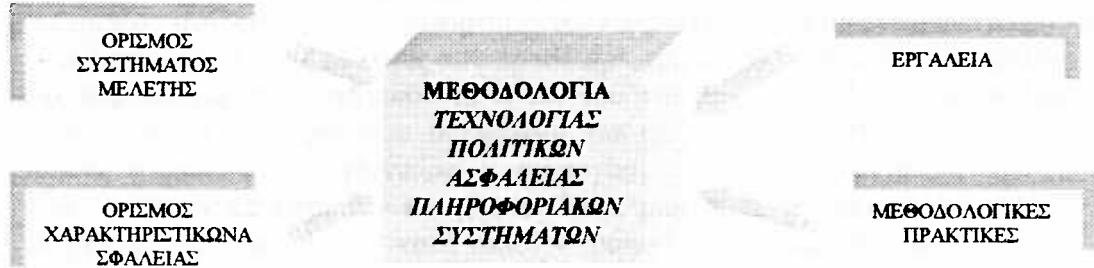
Πολιτικών Ασφάλειας Πληροφοριακών Συστημάτων. Πρόκειται λοιπόν να προδιαγράψουμε απαιτήσεις για μία μεθοδολογία που θα μελετά την ανάπτυξη και υλοποίηση των πολιτικών ασφάλειας για πληροφοριακά συστήματα, με προοπτική την αυτοματοποίηση αυτών των διαδικασιών. Για την καλύτερη κατανόηση του κειμένου χρειάζεται να αναφέρουμε τα ακόλουθα τρία σημεία:

- Η έννοια του "εννοιολογικού πλαισίου" συνεπάγεται επίσης ότι οι λέξεις αντιπροσωπεύουν τις αντίστοιχες έννοιες και δεν είναι αυστηρά ορισμένες στην επιστημονική περιοχή της Πληροφορικής.
- Ένα πλαίσιο δεν καλύπτει το σύνολο των περιπτώσεων, απαιτήσεων, χαρακτηριστικών, κ.λπ. Εποικιά, τα στοιχεία που θα παραθέσουμε δεν ορίζουν πλήρως ένα πλαίσιο. Είναι όμως αρκετά ώστε ο αναγνώστης να κατανοήσει το στόχο και τη χρησιμότητα των αποτελεσμάτων.
- Είναι σημαντικό να σημειώσουμε ότι η εξοικείωση με τα θέματα που αναπτύχθηκαν από αυτή την εργασία, δημιουργεί την υποδομή ώστε κανείς να κατανοήσει τη φιλοσοφία που διέπει την προσέγγισή μας.

### 5.7.2.3 Προσδιορισμός δομικών στοιχείων του πλαισίου

Τα δεδομένα που έχουμε μελετήσει αποτελούν σημαντικό βοήθημα για την παράγραφο αυτή. Καλούμαστε να τα χρησιμοποιήσουμε σε συνδυασμό με την αφαιρετική μας σκέψη προκειμένου να παραμετροποιήσουμε τη γνώση μας αναφορικά με τις διαστάσεις που μπορούν να σκιαγραφήσουν μία μεθοδολογία για Τεχνολογία Πολιτικών Ασφάλειας. Τα επίπεδα αφαιρεσης για το πλαίσιο μας είναι δύο και θα προχωρήσουμε ευθύς αμέσως στην παράθεση των δομικών στοιχείων.

#### ΟΡΙΣΜΟΣ ΔΟΜΙΚΩΝ ΣΤΟΙΧΕΙΩΝ: Επίπεδο αφαίρεσης I



ΣΧΗΜΑ 5.7. Το πρώτο δομικό επίπεδο του πλαισίου αναφοράς.

Το σχήμα 5.7. παρουσιάζει τα δομικά στοιχεία της μεθοδολογίας. Αριστερά στο σχήμα, υπάρχουν τα στοιχεία που χαρακτηρίζουν τη μεθοδολογία σε υψηλό επίπεδο ως επιστημονική πρακτική. Δεξιά, βρίσκονται εκείνα που άπτονται του συγκεκριμένου πεδίου μελέτης. Συνοπτικά, θα λέγαμε ότι **ο ορισμός των αντικειμένων προς μελέτη (ΣΥΣΤΗΜΑ ΜΕΛΕΤΗΣ και ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ), καθώς και ο τρόπος με τον οποίο η μεθοδολογία επιλέγει να το**

**μελετήσει (ΕΡΓΑΛΕΙΑ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ) είναι αρκετά για να προσδιορίσουν μία μεθοδολογία, διαμορφώνοντας το "προφίλ" αυτής και διαχωρίζοντάς την από άλλες μεθοδολογίες.**

Θα περιγράψουμε συνοπτικά τα στοιχεία αυτά:

### ■ ΟΡΙΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΜΕΛΕΤΗΣ

Προσδιορίζεται σαφώς το σύστημα που θα μελετηθεί. Αυτό μπορεί να είναι το πληροφοριακό σύστημα, το υπολογιστικό σύστημα, ο οργανισμός. Προσδιορίζονται αναλυτικά οι οντότητες του συστήματος αυτού και οι συσχετίσεις μεταξύ τους, αν υπάρχουν. Προσδιορίζονται οι επικοινωνίες με το περιβάλλον (αφού αυτό οριστεί), καθώς και οι λειτουργίες του συστήματος.

### ■ ΟΡΙΣΜΟΣ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

Προσδιορίζεται η έννοια της ασφάλειας για το συγκεκριμένο αυτό σύστημα. Αναλύονται τα χαρακτηριστικά ασφάλειας (ακεραιότητα (integrity), εμπιστοσύνη (trust), εμπιστευτικότητα (confidentiality), χρησιμότητα (utility), κ.λπ.), που θεωρείται ότι πρέπει να μελετηθούν για το σύστημα που ορίστηκε.

### ■ ΕΡΓΑΛΕΙΑ

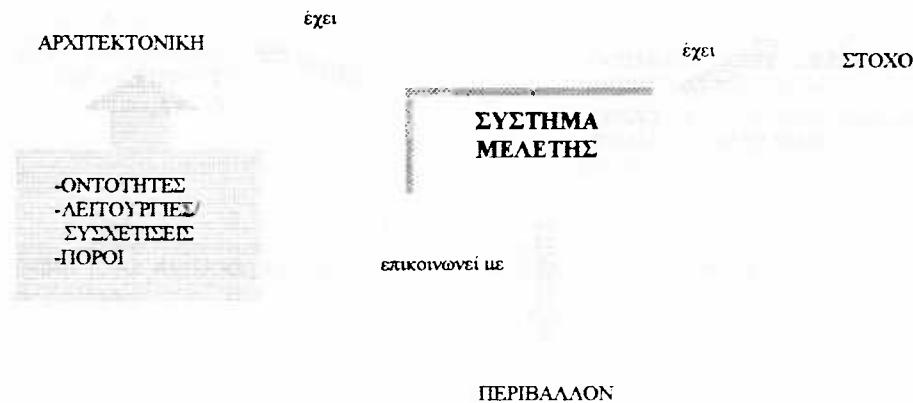
Η μεθοδολογία χρησιμοποιεί ορισμένα εργαλεία προκειμένου να μελετήσει το σύστημα και την ασφάλειά του. Αυτά μπορεί να περιλαμβάνουν: τυπικές μεθόδους ορισμού προδιαγραφών, διαγραμματικές τεχνικές, γλώσσες προγραμματισμού υψηλού ή χαμηλού επιπέδου, πρότυπα ασφάλειας, τεχνικές της τεχνολογίας λογισμικού όπως γρήγορη προτυποποίηση, κ.λπ. Αυτές οι τεχνικές είναι βασικές για τη μελέτη, γιατί μπορούν να προσδιορίσουν τυπικά τα βασικά αντικείμενα μελέτης, να αποδώσουν αφαιρετικά τις μελετώμενες έννοιες, να τις "μεταφράσουν" με τρόπους που μπορούν διάφοροι εμπλεκόμενοι να τις κατανοήσουν, κ.ά.

### ■ ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ

Χρησιμοποιούμε τον όρο αυτό προκειμένου να αναφερθούμε τόσο σε διαδικαστικές τεχνικές που χρησιμοποιούνται από τη μεθοδολογία (όπως καθορισμός της ομάδας ανάλυσης, επιλογή επιστημονικών περιοχών που κρίνονται αναγκαίες για τη μελέτη), όσο και σε επιλογές που προσδιορίζουν τη φιλοσοφία της μεθοδολογίας. Για παράδειγμα, η συστημικότητα ή μη του τρόπου ορισμού των αντικειμένων μελέτης, η κοσμοθεωρία που υιοθετείται για το ίδιο το σύστημα και η επιλογή χρήσης συγκεκριμένων τεχνικών, η συνεργασία που επιτυγχάνεται μεταξύ τους, κ.λπ., ανήκουν σε αυτή την κατηγορία. Έτσι, μπορούμε να παρατηρήσουμε ότι η κατηγορία αυτή "επεμβαίνει" κατά κάποιον τρόπο στις τρεις προηγούμενες.

Ακολουθεί στα επόμενα σχήματα η ανάλυση δευτέρου επιπέδου για κάθε ένα από τα στοιχεία που προσδιορίσαμε. Η ανάλυση δευτέρου επιπέδου θα εξειδικεύσει τα δομικά στοιχεία σε επιμέρους στοιχεία που τα προσδιορίζουν, κατά τρόπο που ο αναγνώστης μπορεί να κατανοήσει το περιεχόμενό τους.

**ΟΡΙΣΜΟΣ ΔΟΜΙΚΟΥ ΣΤΟΙΧΕΙΟΥ: ΟΡΙΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΜΕΛΕΤΗΣ**  
**Επίπεδο αφαίρεσης II**



**ΣΧΗΜΑ 5.8.** Ανάλυση δομικού στοιχείου "ΟΡΙΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ ΜΕΛΕΤΗΣ" της μεθοδολογίας.

**ΟΡΙΣΜΟΣ ΔΟΜΙΚΟΥ ΣΤΟΙΧΕΙΟΥ: ΕΡΓΑΛΕΙΑ**  
**Επίπεδο αφαίρεσης II**

ΕΡΓΑΛΕΙΑ  
ΜΕΘΟΔΟΛΟΓΙΑΣ

- ΔΙΑΓΡΑΜΜΑΤΙΚΕΣ ΤΕΧΝΙΚΕΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ
- ΤΥΠΙΚΑ ΜΟΝΤΕΛΑ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ
- ΓΛΩΣΣΕΣ ΟΡΙΣΜΟΥ ΠΡΟΔΙΑΓΡΑΦΩΝ ΑΠΑΙΤΗΣΕΩΝ ΟΡΙΣΜΕΝΟΥ ΒΑΘΜΟΥ ΤΥΠΟΠΟΙΗΣΗΣ
- (ΗΜΙ)ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΑ ΕΡΓΑΛΕΙΑ ΤΕΧΝΟΛΟΓΙΑΣ ΛΟΓΙΣΜΙΚΟΥ
- ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΑ ΠΑΚΕΤΑ ΛΥΣΕΩΝ ΠΟΙΚΙΛΟΥ ΠΕΡΙΕΧΟΜΕΝΟΥ
- ΜΕΘΟΔΟΙ ΑΝΑΛΥΣΗΣ ΠΟΙΚΙΛΩΝ ΣΤΟΧΩΝ
- ΠΡΟΤΥΠΑ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑΣ

**ΣΧΗΜΑ 5.9.** Ανάλυση δομικού στοιχείου "ΕΡΓΑΛΕΙΑ" της μεθοδολογίας.

## ΟΡΙΣΜΟΣ ΔΟΜΙΚΟΥ ΣΤΟΙΧΕΙΟΥ: ΟΡΙΣΜΟΣ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ Επίπεδο αφαίρεσης II

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ  
ΑΣΦΑΛΕΙΑΣ

- ΟΡΙΣΜΟΣ ΕΝΝΟΙΑΣ ΑΣΦΑΛΕΙΑΣ &  
ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ
- ΟΡΙΣΜΟΣ ΣΤΟΧΟΥ ΑΣΦΑΛΕΙΑΣ &  
ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

**ΣΧΗΜΑ 5.10. Ανάλυση δομικού στοιχείου "ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ" της μεθοδολογίας.**

## ΟΡΙΣΜΟΣ ΔΟΜΙΚΟΥ ΣΤΟΙΧΕΙΟΥ: ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ Επίπεδο αφαίρεσης II

ΜΕΘΟΔΟΛΟΓΙΚΕΣ  
ΠΡΑΚΤΙΚΕΣ

- ΜΕΘΟΔΟΣ ΑΝΑΛΥΣΗΣ (ΔΟΜΗΜΕΝΗ, ΑΠΟ-ΠΑΝΩ-ΠΡΟΣ-ΤΑ-ΚΑΤΩ, ΑΠΟ-ΚΑΤΩ-ΠΡΟΣ-ΤΑ-ΠΑΝΩ, Κ.Λ.Π.)
- ΣΥΤΗΜΙΚΗ Η ΣΥΣΤΗΜΑΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΣΤΗ ΜΕΛΕΤΗ
- ΟΡΙΣΜΟΣ ΟΜΑΔΑΣ ΜΕΛΕΤΗΣ
- ΕΠΙΛΟΓΗ ΧΡΗΣΗΣ ΕΠΙΚΟΥΡΙΚΩΝ ΜΕΘΟΔΩΝ ΚΑΙ ΕΡΓΑΛΕΙΩΝ ΕΥΡΕΙΑΣ ΕΠΙΣΤΗΜΟΝΙΚΗΣ ΠΡΟΕΛΕΥΣΕΩΣ
- ΧΡΗΣΗ ΑΦΑΙΡΕΣΗΣ ΣΤΗΝ ΕΙΠΕΞΕΡΓΑΣΙΑ ΤΗΣ ΕΝΝΟΙΑΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ
- ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΘΕΜΕΛΙΑΚΟΥ ΠΛΑΙΣΙΟΥ ΑΝΑΦΟΡΑΣ
- ΧΡΗΣΗ ΕΡΓΑΛΕΙΩΝ ΠΟΙΚΙΛΩΝ ΤΥΠΩΝ
- ΚΑΛΥΨΗ ΚΥΚΛΟΥ ΖΩΗΣ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

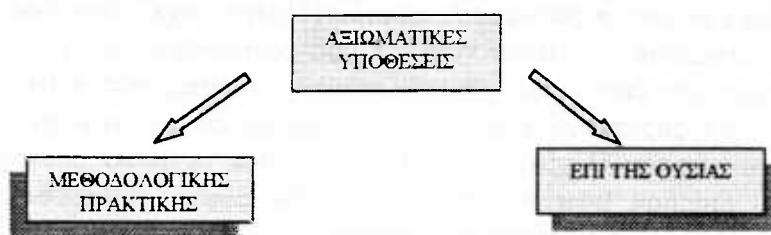
**ΣΧΗΜΑ 5.11. Ανάλυση δομικού στοιχείου "ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ" της μεθοδολογίας.**

### 5.7.2.4 Διαμόρφωση απαιτήσεων για τα δομικά στοιχεία

Ο προσδιορισμός των βασικών απαιτήσεων για κάθε δομικό στοιχείο που έχουμε ταυτοποιήσει<sup>26</sup> είναι η εργασία αυτής της παραγράφου. Είναι σημαντικό να

<sup>26</sup> Παρόλο που θεωρούμε τη σχηματική αναπαράσταση ιδιαιτέρως βοηθητική για την κατανόηση της προσέγγισής μας, δεν είναι δυνατό να τη χρησιμοποιήσουμε επαρκώς για παράθεση μεγάλου κειμένου.

τονίσουμε ότι η **εργασία των καθορισμού των απαιτήσεων θα πρέπει να εξάγει αποτελέσματα για όλη τη μεθοδολογία**. Είναι επομένως λογικό -και αναπόφευκτο- ότι σημεία απαιτήσεις να μην άπονται ειδικά κάποιου δομικού στοιχείου αλλά να αφορούν ολόκληρο το σύστημα. Τα σημεία αυτά είτε αποτελούν γενικότερες μεθοδολογικές απόψεις, είτε προκύπτουν ως συμπεράσματα που πρέπει να αποδεχτούμε από την ανάλυση που έχει γίνει. Όπως φαίνεται δε διαγραμματικά, διαχωρίζουμε τις απαιτήσεις σε **δύο κατηγορίες** και τις αντιμετωπίζουμε ως υποθέσεις: αυτές που αφορούν θέματα μεθοδολογικής πρακτικής και εκείνες που διαμορφώνονται προσδιοριζόμενες από το εκάστοτε σύστημα προς μελέτη.



ΣΧΗΜΑ 5.12. Διαχωρισμός Αξιωματικών Υποθέσεων της προσέγγισης.

Οι υποθέσεις μεθοδολογικής πρακτικής είναι οι εξής:

- Η μεθοδολογία για Τεχνολογία Πολιτικών Ασφάλειας πρέπει να ακολουθήσει δομημένη προσέγγιση συγκεκριμένης αφαιρετικής διαβάθμισης για όλα τα σχετικά θέματα (δηλαδή, τον ορισμό του συστήματος αναφοράς, της πολιτικής ασφάλειας για το σύστημα αυτό, κ.λπ.). Εκτιμάται ότι η αφαίρεση πρέπει να είναι τέτοια που να διευκολύνει την κατανόηση των σχετικών με τις πολιτικές ασφάλειας εννοιών και να έχει προοπτική προς την υλοποίηση-αυτοματοποίηση αυτών.
- Ο καθορισμός των ατόμων που μπορούν να "παρακολουθήσουν" τη μεθοδολογία πρέπει να αποτελεί διακριτή εργασία.
- Τα αποτελέσματα της μεθοδολογίας πρέπει να είναι σαφή και κατανοητά (για τα μέρη τα οποία ορίστηκαν).
- Η μεθοδολογία πρέπει να κάνει χρήση πρακτικών τέτοιων που θα αυξάνουν την ενστικτώδη αντίληψη των μερών που ορίστηκαν ως ανάγντες (enhances the intuitive understanding of the analyst).
- Η μεθοδολογία πρέπει να καλύπτει κατά το δυνατό τη γενικότητα των περιπτώσεων. Συνεπώς, πρέπει να παρέχει ένα πλαίσιο αναφοράς όλων των σημαντικών θεμάτων που μία τέτοια μεθοδολογία καλείται να επιλύσει.

Οι υποθέσεις που είναι άμεσα σχετικές με τη συγκεκριμένη προς ανάλυση κατάσταση αφορούν τις εξής απόψεις:

- Έχει καταστεί προφανές, από τις έως τώρα αναλύσεις, ότι η προβληματική κατάσταση που συνιστά το πεδίο μελέτης της εν λόγω μεθοδολογίας είναι πολύπλοκη, αφού εμπλέκει για παράδειγμα στοιχεία υπολογιστικών συστημάτων, ανθρώπινο στοιχείο, πληροφορίες και δεδομένα, καθώς και ένα ολόκληρο πλέγμα συσχετίσεων αυτών μεταξύ τους και με το περιβάλλον τους, το οποίο εμπλέκεται άμεσα ή έμμεσα στη διαμόρφωση ορισμένων εξ αυτών των σχέσεων. Με άλλα λόγια, η προβληματική κατάσταση που περιγράψαμε συνιστά ένα σύστημα,

δύσκολο καταρχήν στον καθορισμό του. **Τα προβλήματα δε, πον αφορούν συστήματα, καλούν τον αναλυτή σε συστηματική αντιμετώπιση.**

- Πρέπει να παρατηρήσουμε ότι η δυσκολία στην αντιμετώπιση μιας τέτοιας προβληματικής κατάστασης<sup>27</sup> δεν εντοπίζεται τόσο στη διερεύνηση της λογικής του τρόπου με τον οποίο επεξεργαζόμαστε τα προβλήματα. Είναι προφανές ότι στην πραγματικότητα γνωρίζουμε πώς να αντιμετωπίσουμε τα προβλήματα που ένα ρήγμα ασφάλειας λ.χ. προκαλεί, όταν συμβεί. Αυτό που απαιτείται όμως είναι να γνωρίζουμε εκ των προτέρων τη λογική που διέπει τα αντικείμενα μελέτης (βλ. αντίστοιχη παρατήρηση στην παράγρ. 5.5.1). Η τυποποίηση άλλωστε αυτή την άποψη προσπαθεί να επεξεργαστεί. Όπως θα παρατηρούσε η H. Hosmer, "*only the objects of manipulation are fuzzy, not the logic that deals with them*".
- Η μεθοδολογία Τεχνολογίας Πολιτικών Ασφάλειας πρέπει να καλύπτει τον κύκλο ζωής τόσο του συστήματος όσο και των πολιτικών ασφάλειας. Έχει καταστεί σαφές ότι η ενσωμάτωση χαρακτηριστικών ασφάλειας στο σύστημα αναφοράς πρέπει να κινείται παράλληλα με τα στάδια ανάπτυξης και λειτουργίας του συστήματος. Οι αρχές που διέπουν την ανάπτυξη Πληροφοριακών Συστημάτων τις περισσότερες φορές, εξάλλου, είναι ιδιαίτερα χρήσιμες στην ανάπτυξη ασφαλών συστημάτων (βλ. για παράδειγμα παράγρ. 5.5.3).

Για τις απαιτήσεις αυτές, **επιλέγουμε να ανήκουν στο στοιχείο "ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ" της μεθοδολογίας.**

Για το στοιχείο "ΜΕΘΟΔΟΛΟΓΙΚΕΣ ΠΡΑΚΤΙΚΕΣ" καθορίζουμε επίσης τις ακόλουθες απαιτήσεις:

- Η επιλογή των επιμέρους πρακτικών της μεθοδολογίας (μεθόδων και εργαλείων) πρέπει να είναι τέτοια που να επιτρέπει ανεξαρτησία από συγκεκριμένες εφαρμογές (δηλαδή συστήματα και πολιτικές ασφάλειας), αλλά ταυτόχρονα να είναι τόσο ευέλικτη που να μπορεί να αντιπροσωπεύσει εφαρμογές με συγκεκριμένες απαιτήσεις.
- Απαιτείται να καταβάλλεται προσπάθεια έτσι ώστε το αποτέλεσμα να αποτελεί το σημείο ισορροπίας μεταξύ της βέλτιστης λύσης και των κοστών (λειτουργικού, διαχειριστικού της διαδικασίας, συντήρησης, ελέγχων, οικονομικού, κ.λπ.) που εμπλέκονται στην όλη διαδικασία.

Θα αντιμετωπίσουμε τα δομικά στοιχεία "ΟΡΙΣΜΟΣ ΣΥΣΤΗΜΑΤΟΣ" και "ΟΡΙΣΜΟΣ ΑΣΦΑΛΕΙΑΣ" εν μέρει από κονού, εφόσον οι φάσεις αυτές σχετίζονται με σχέση αλληλεπίδρασης. Δηλαδή, η άποψη για το σύστημα διαμορφώνεται εν μέρει από την αντίληψη για την έννοια της ασφάλειας που λειτουργεί ως "αντικείμενο-στόχος" για τις μεθοδολογίες. Οι απαιτήσεις διαμορφώνονται ως εξής:

- Ο ορισμός του συστήματος πρέπει να ενσωματώνει έννοιες που θεωρούνται βασικές για τα σύγχρονα συστήματα (σε οποιοδήποτε επίπεδο αφαίρεσης ορίζουμε την έννοια του συστήματος), όπως κατανεμημένη επεξεργασία, δικτύωση, κ.λπ. και να περιλαμβάνει κατά το δυνατό το σύνολο των στοιχείων από τα οποία ένα σύστημα αποτελείται.
- Ο ορισμός της έννοιας της ασφάλειας πρέπει επίσης να λαμβάνει υπόψη του

<sup>27</sup> Να σημειωθεί ότι ο αναγνώστης πρέπει να διατηρεί τη σκέψη ότι οι προβληματικές καταστάσεις που εξετάζουμε αφορούν τη διαχείριση προβλημάτων που υφίστανται κάποιου είδους τυποποίηση και αυτοματοποίηση.

- έννοιες που κρίνονται βασικές για τα σύγχρονα συστήματα (λ.χ. την έννοια του "ρόλου") και να καλύπτει κατά το δυνατό το σύνολο των χαρακτηριστικών ασφάλειας που κρίνονται απαραίτητα σύμφωνα με τον ορισμό του συστήματος και το στόχο της ασφάλειας.
- Ο στόχος του συστήματος και ο στόχος της ασφάλειας πρέπει να καθορίζονται σε κάθε περίπτωση, να είναι ενδεικτικοί της συστημικότητας της προσέγγισης της μεθοδολογίας, να αντικατοπτρίζουν τους αντίστοιχους στόχους των σύγχρονων συστημάτων και να είναι συμβατοί.
  - Ιδιαίτερη έμφαση πρέπει να αποδίδεται στις σχέσεις επικοινωνίας των στοιχείων που προσδιορίζονται, καθώς και στην επικοινωνία με το περιβάλλον, το οποίο πρέπει σα φώς να ορίζεται.
  - Η απεικόνιση των εννοιών του συστήματος και της ασφάλειας πρέπει να συνθέτουν μία βάση αναφοράς (core) τέτοια που:
    - Να μπορεί να λειτουργήσει ως βάση για:
      - Τον ορισμό της έννοιας του συστήματος
      - Τον ορισμό της έννοιας της ασφάλειας
      - Την υποδοχή της έννοιας της μεταπολιτικής ασφάλειας
    - Να αποτελείται από ένα σύνολο βασικών εννοιών (fundamental concepts), περιορισμένο σε μέγεθος και επιδεχόμενο παραμετροποίηση και επαναχρησιμοποίηση για διάφορες παραλλαγές στόχων επεξεργασίας του.
    - Να επιτυγχάνει σύνδεση με το ορισμένο περιβάλλον και περιεχόμενο (context).
  - Τέλος, απαιτείται όπως οι ορισμοί του συστήματος και της ασφάλειας να περιλαμβάνουν χαρακτηριστικά στοιχεία του οργανισμού ή να συνοδεύονται από αυτόνομη μεθοδολογική αντιμετώπιση του οργανισμού.

Προκειμένου για τη μελέτη αυτών των δύο δομικών στοιχείων μπορούμε επίσης να λάβουμε υπόψη μας το ακόλουθο πλαίσιο [LAP-1992]<sup>28</sup>. Το πλαίσιο αυτό προσδιορίζει τα σημεία-στόχους όπου οι απαιτήσεις πρέπει να εστιάσουν και δίνει μία συνοπτική περιγραφή για το περιεχόμενο αυτών των απαιτήσεων.

### Οι Απαιτήσεις αναφέρονται σε:

1. Περιγραφή Οργανισμού
2. Στόχους ως προς εμπιστοσύνη (trust objectives)
3. Μοντέλο εξωτερικής διεπαφής (external interface)
4. Κυρίως μοντέλο (internal model)
5. Κανόνες επιβολής απαιτήσεων κυρίως μοντέλου (rules of

### Περιγραφή Απαιτησης

- Η περιγραφή του Οργανισμού πρέπει να περιλαμβάνει τις δραστηριότητες, υπευθυνότητες και μεθόδους μέσω των οποίων επιτυγχάνονται οι συγκεκριμένοι στόχοι του οργανισμού.
- Προσδιορισμός του τι πρέπει να επιτευχθεί από έναν οργανισμό επεξεργασίας πληροφορίας, του οποίου το πληροφοριακό σύστημα είναι μέρος.
- Προσδιορισμός τόσο των στοιχείων του συστήματος όσο και του περιβάλλοντος και κατανομή υπευθυνοτήτων σχετικών με την υλοποίηση των ανωτέρω στόχων, έτσι ώστε να επιδεικνύεται πώς το σύστημα αυτό υλοποιεί τους στόχους αυτούς.
- Περιγραφή του τρόπου με τον οποίο οι παραπάνω υπευθυνότητες υλοποιούνται (are met with) από το πληροφοριακό σύστημα.
- Περιγραφή του τρόπου με τον οποίο οι παραπάνω υπευθυνότητες επιβάλλονται (are enforced) από το πληροφοριακό σύστημα.

<sup>28</sup> ... το οποίο συμπληρώνουμε με μία επιπλέον διάσταση.

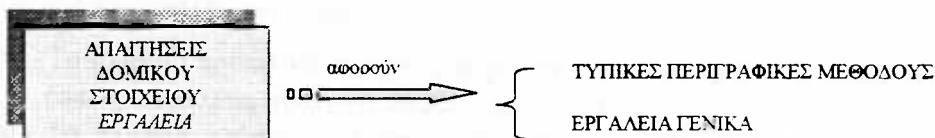


operation)

6. Λειτουργικό σχεδιασμό (functional design)
  7. Προδιαγραφές λογισμικού και υλικού (S/W, H/W specifications)
  8. Υποστήριξη διαχείρισης περισσότερων πολιτικών ασφάλειας (Multiple policies management)
- Παρόμοια με τους κανόνες επιβολής, αλλά με σχεδιαστική πληρότητα περιγράφει τη συμπεριφορά του συστήματος και των οντοτήτων αυτού που ελέγχονται.
- Λεπτομερής περιγραφή των τμημάτων λογισμικού και υλικού που επιβάλλουν, ελέγχουν ή υποστηρίζουν τα χαρακτηριστικά ασφάλειας του λειτουργικού σχεδιασμού.
- Η υποστήριξη διαχείρισης περισσότερων πολιτικών ασφάλειας αποτελεί ξεχωριστή απαίτηση, λόγω της σοβαρότητάς της δεδομένων των σύγχρονων συνθηκών και εξελίξεων.

Χαρακτηριστικά, θα λέγαμε ότι η βάση αναφοράς πρέπει να συνιστά ένα πλήρες πλαίσιο το οποίο επιτρέπει την εφαρμογή πολιτικών ασφάλειας που ανταποκρίνονται στις ανάγκες ποικίλων εφαρμογών, μέσω της εφαρμογής μηχανισμών ασφάλειας με έναν ορισμένο τρόπο.

Αναφορικά με το στοιχείο "ΕΡΓΑΛΕΙΑ" παρατηρούμε στο ακόλουθο σχήμα ότι πρέπει να διαμορφώσουμε κριτήρια που καλύπτουν γενικά αυτή την κατηγορία, καθώς και κριτήρια που άπτονται ειδικών περιπτώσεων.



ΣΧΗΜΑ 5.13. Απαιτήσεις του δομικού στοιχείου "ΕΡΓΑΛΕΙΑ".

Είναι σημαντικό να σημειώσουμε ότι κατά τη διαμόρφωση των απαιτήσεων των εργαλείων, δεν θα κριθούν οι δυνατότητες των εργαλείων στο επίπεδο των εννοιών που αναπαριστούν, αλλά στην ποιότητα της απόδοσης αυτών των εννοιών. Για παράδειγμα, τα "μοντέλα πολιτικών ασφάλειας" θα προδιαγραφούν ως εννοιολογικά μοντέλα στις απαιτήσεις του δομικού στοιχείου "ΟΡΙΣΜΟΣ ΑΣΦΑΛΕΙΑΣ" και όχι στις απαιτήσεις των "ΕΡΓΑΛΕΙΩΝ".

Οι απαιτήσεις διαμορφώνονται ως εξής:

### ■ ΓΕΝΙΚΕΣ

- Ευχρηστία (utility), δηλαδή, καταλληλότητα για το σκοπό της μελέτης του συστήματος και της ασφάλειάς του.
- Συμβολή στην αύξηση της εμπιστοσύνης στο σύστημα που προσπαθούμε να προστατεύσουμε.
- Ποιότητα (δηλαδή, ευχρηστία, ορθότητα, επιστημονική πληρότητα, κ.λπ.).
- Λειτουργικότητα.
- Ευελιξία στη συνεργασία με το σύνολο των πρακτικών και εργαλείων που χρησιμοποιούνται.

### ■ ΤΥΠΙΚΕΣ ΠΕΡΙΓΡΑΦΙΚΕΣ ΜΕΘΟΔΟΙ

Οι απαιτήσεις αναλύονται στην παράγρ. 5.4.3. Συνοπτικά επαναλαμβάνουμε ότι πρέπει να ικανοποιούνται τα ακόλουθα:



- Αναγνωσιμότητα.
- Κατανοητότητα.
- Εκφραστικότητα.
- Δυνατότητα παραμετροποίησης-αφαιρετικότητας.
- Ευελιξία στην παράσταση ποικίλων απαιτήσεων συστημάτων.
- Λειτουργική ευελιξία, που καθιστά τα παραγόμενα αποτελέσματα κατάλληλα για υλοποίηση-αυτοματοποίηση.
- Υπαρξη:
  - Τυπικού συντακτικού.
  - Τυπικής σημασιολογίας.
  - Σαφούς μοντέλου εννοιολογικής απεικόνισης συστήματος.
  - Μεθόδου απεικόνισης διεπαφών-επικοινωνιών.
- Να μην είναι περιοριστικό χρήσης διαφόρων άλλων τεχνικών και εργαλείων, αλλά να είναι καθοδηγητικό της εφαρμογής ποικίλων μέσων κατάλληλων για κάθε περίπτωση.

Ολοκληρώνοντας τις απαιτήσεις να συμπληρώσουμε με τα ακόλουθα σημεία το πλαίσιό μας:

Επιπλέον βασικά θέματα, σχετικά με ένα ενιαίο πλαίσιο περιγραφικό των μεθοδολογιών τυποποίησης και αυτοματοποίησης πολιτικών ασφάλειας, που πρέπει να μας απασχολήσουν είναι:

- Το πλαίσιο πρέπει να παρέχει μία **γλώσσα ενιαίου ορισμού σημαντικών εννοιών** (όπως ασφάλεια, πολιτική ασφάλειας, κ.λπ.)
- Το πλαίσιο πρέπει να παρέχει διεξόδους για τη **γεφύρωση του κενού μεταξύ διατύπωσης πολιτικών ασφάλειας και υλοποίησης** αυτών.
- Το πλαίσιο πρέπει επίσης να καλύψει το χάσμα που αφήνουν οι υπάρχουσες λύσεις μεταξύ της **τυποποίησης της ασφάλειας σε επίπεδο οργανισμού και των τυποποιήσεων πολιτικών ασφάλειας χαμηλού επιπέδου**.
- Η αυτοματοποιημένη διαχείριση πολιτικών ασφάλειας εισάγει επιπλέον κόστος σε όρους πόρων που απαιτούνται προκειμένου να την επιτύχουμε αλλά και να την ελέγχουμε και επιβεβαιώσουμε. **Το θέμα των κόστους απαιτείται να λάβει ιδιαίτερη προσοχή εξαρχής.** Ένας βασικός τρόπος να επιτύχουμε κάτι τέτοιο είναι η μεγιστοποίηση του ωφέλους από την χρήση κάθε τεχνικής, έτσι ώστε να καλύπτονται ταυτόχρονα περισσότερες ανάγκες (λ.χ. η υποδομή που θα δημιουργήσουμε για την τυποποίηση πολιτικών πρέπει να είναι δεκτική και της διαχείρισης των μεταπολιτικών).

## ΣΥΜΠΕΡΑΣΜΑΤΑ

Έρευνα Διαχείριση Πολιτικών Ασφάλειας Τυποποίηση Αυτοματοποίηση  
Μεθοδολογίες Πρότυπα Σημασιολογία Μεταπολιτικές Ασφάλειας

Σε μία περιοχή η οποία είναι κατεξοχήν ερευνητική, κανείς μπορεί συνεχώς να ασχολείται με νέες ιδέες. Εφόσον ο προβληματισμός σχετικά με θέματα αυτοματοποίησης διαχείρισης πολιτικών ασφάλειας είναι συνεχής, **τα συμπεράσματα μίας εργασίας που μελέτησε ορισμένες έννοιες δεν μπορεί παρά να τείνουν στη δημιουργία και όχι στην ανακεφαλαίωση**. Ετσι, η λογική μας σε αυτή την παράγραφο θα είναι η παράθεση υπό τίτλους θεμάτων που συνοψίζουν σημαντικά σημεία που θίχτηκαν.

### ① Η διαχείριση πολιτικών ασφάλειας είναι μία διαδικασία με δύο κύρια αντικείμενα ενδιαφέροντος

Οι πολιτικές ασφάλειας αποτελούν βασική έννοια στο χώρο της ασφάλειας Πληροφοριακών Συστημάτων. Το ενδιαφέρον μας κατά τη διαδικασία διαχείρισης αυτών θα πρέπει να εντοπίζεται όχι μόνο στους μηχανισμούς που προστατεύουν ένα σύστημα, αλλά και στους ανώτερους σκοπούς, στους οποίους αντοί οι μηχανισμοί "ταιριάζουν". Αυτοί οι σκοποί είναι που δένουν τους μηχανισμούς σε ένα ολοκληρωμένο σύνολο ή αποδεικνύουν την ασυμβατότητά τους.

### ② Η αυτοματοποιημένη διαχείριση πολιτικών ασφάλειας αποτελεί το ερευνητικό ξητούμενο.

Οι λόγοι οι οποίοι επιβάλλουν αυτή τη θεώρηση έχουν καταγραφεί. Ωστόσο, έγινε εμφανές από τη μελέτη αυτή ότι υπάρχουν δυσεπίλητα θέματα προς διερεύνηση. Κατά παρόμοιο τρόπο που η Τεχνολογία Λογισμικού ευφευρίσκει σταθερές αλλά προσαρμόσιμες σε κάθε εφαρμογή μεθόδους αντιμετώπισης διαφόρων θεμάτων λογισμικού, η Τεχνολογία πολιτικών ασφάλειας Πληροφοριακών Συστημάτων πρέπει να συλλέξει και να προσφέρει πρότυπους τρόπους επίλυσης των βασικών θεμάτων αυτοματοποιημένης διαχείρισης πολιτικών ασφάλειας. Τα θέματα αυτά, στο σύνολό τους, φέρνουν στην επιφάνεια την ανάγκη για εύρεση ενός πλαισίου αναφοράς (framework of reference) το οποίο θα παγιώσει (consolidate) τις απαιτήσεις που εισάγει η παραπάνω θεώρηση.

### ③ Η ανακάλυψη των τρόπων με τον οποίο αντιμετωπίζουμε την τυποποίηση-αυτοματοποίηση των πολιτικών ασφάλειας αποτελεί σημείο-κλειδί για την επιτυχία αυτής της διαδικασίας

Τα πραγματικά αντίστοιχα των εννοιών που συνθέτουν το αντικείμενο μελέτης συνιστούν αναμφισβήτητα ένα σύστημα. Μέσω της τυποποίησης επιχειρούμε να τυποποιήσουμε αυτό το σύστημα με απότερο σκοπό να παράξουμε ένα "προϊόν" διαχείρισης πολιτικών ασφάλειας. Η διαδικασία αυτή προσδιορίζεται από εναλλαγές και ανατροφοδοτήσεις μεταξύ τεχνικών πρακτικών και επιστημονικής θεωρητικής γνώσης. Αυτή ακριβώς τη διαδικασία επιχειρήσαμε να παρουσιάσουμε

στα πρώτα κεφάλαια και ανάγλυφα να περιγράψουμε στο παρόν κεφάλαιο. Χρειαζόμαστε μία γλώσσα με την οποία θα εκφράζουμε μεθοδολογικά στοιχεία της διαδικασίας τυποποίησης-αυτοματοποίησης πολιτικών ασφάλειας. Η όλη μελέτη απέδειξε ότι απαιτείται να φανούμε ιδιαίτερα προσεκτικοί με την ίδια τη **διαδικασία μετασχηματισμού των συστήματος σε οποιοδήποτε τυποποιημένο αποτέλεσμα**.

**④ Οι υπάρχουσες λύσεις προς την κατεύθυνση της συνεπούς αυτοματοποιημένης διαχείρισης πολιτικών ασφάλειας είναι ημιπλήρεις**

Το ίδιο έργο της διαχείρισης πολιτικών ασφάλειας τονίσαμε ότι είναι ιδιαίτερα περίπλοκο. Γενικά, δεν υπάρχει ενιαίος, πρότυπος τρόπος (μεθοδολογία) για την ολοκληρωμένη διαχείριση πολιτικών ασφάλειας. Υπάρχει ένα φάσμα διαστάσεων που πρέπει να λάβουμε υπόψη μας και οι υπάρχουσες λύσεις προς αυτή την κατεύθυνση δεν κατορθώνουν παρά να καλύπτουν υποσύνολα αυτών των διαστάσεων. Ο ακόλουθος πίνακας δείχνει ποιά σημεία καλύπτονται από τις υπάρχουσες λύσεις και ποιά χρειάζονται περαιτέρω μελέτη. Η κάλυψη των ερευνητικών θεμάτων μπορεί να συμβάλλει στη διαμόρφωση μιας Βασικής Υποδομής Ασφάλειας (corporate security infrastructure), που αποτελεί τη βάση για την ολοκληρωμένη αντιμετώπιση των θεμάτων διαχείρισης πολιτικών ασφάλειας. Οι διαστάσεις ενδιαφέροντος της πρώτης στήλης του πίνακα αυτού, παρουσιάστηκαν στον πίνακα της παραγρ. 5.7.2.4.

ΔΙΑΣΤΑΣΗ	ΠΑΡΑΔΟΣΙΑΚΑ ΜΟΝΤΕΛΑ (π.χ. Bell-LaPadula)	ΠΡΟΣΦΑΤΑ ΜΟΝΤΕΛΑ (βλ. κεφάλαιο III)	ΕΡΕΥΝΗΤΙΚΟ ΕΝΔΙΑΦΕΡΟΝ
1. Περιγραφή Οργανισμού		✓	✓✓
2. Στόχοι ως προς εμπιστοσύνη		✓	✓✓
3. Μοντέλο εξωτερικής διεπαφής		✓	✓✓
4. Κυρίως μοντέλο	✓✓	✓	
5. Κανόνες επιβολής απαιτήσεων κυρίως μοντέλου	✓✓	✓	
6. Λειτουργικός σχεδιασμός		✓	✓✓
7. Προδιαγραφές λογισμικού και υλικού			✓✓✓
8. Υποστήριξη διαχείρισης περισσότερων πολιτικών ασφάλειας		✓	✓✓

Ο βαθμός βέβαια στον οποία κάθε μία από τις προσεγγίσεις<sup>29</sup> που αναφέραμε

<sup>29</sup> Σαφώς, οι τίτλοι που έχουμε αποδώσει στις προσεγγίσεις που παρουσιάσαμε είναι ενδεικτικοί και μας βοηθούν να αναφερόμαστε συνοπτικά σε αυτές. Σε καμία περίπτωση δεν αποτελούν μοναδικές και καθοριστικές ενδείξεις για το περιεχόμενο των προσεγγίσεων.



στο τρίτο κεφάλαιο καλύπτει τις παραπάνω περιοχές είναι ένα δύσκολο θέμα. Η αξιολόγηση που πρέπει να κάνουμε δεν πρέπει να βασίζεται σε συγκριτικές εκτιμήσεις, αλλά να είναι αυτόνομη για κάθε προσέγγιση. Επίσης πρέπει να λάβουμε υπόψη μας τους αρχικούς στόχους κάθε προσέγγισης και με βάση αυτούς να κρίνουμε τα αποτελέσματα.

Σημαντική παράμετρο αποτελεί εξάλλου το γεγονός ότι τα θέματα που μας αποσχολούν εδώ είναι κατεξοχήν ερευνητικά. Κάτι τέτοιο σημαίνει ότι η πληθώρα των προσπαθειών βρίσκεται σε επίπεδο αρχικής έρευνας ή τουλάχιστο ότι η έρευνα βρίσκεται στο στάδιο όπου δεν έχει επικυρώσει τα αποτελέσματά της. Πολύ περισσότερο δε, πρέπει να σημειώσουμε ότι οι προσπάθειες είναι σχετικά αυτόνομες και διενεργούνται από μικρές ερευνητικές ομάδες, με αποτέλεσμα η πρόδος να είναι είτε αντικειμενικά μικρή, είτε μη δημοσιευμένη στο σύνολό της.

Όλα αυτά συνεπάγοντα, κατά την προσωπική μας άποψη, ότι δεν μπορούμε με τα στοιχεία που έχουμε στη διάθεσή μας να προβούμε σε σοβαρή κριτική. Μπορούμε όμως να περιοριστούμε στην αναγνώριση ορισμένων σημαντικών συμπερασμάτων αναφορικά με κάθε προσέγγιση, ως προς τα σημεία που παρουσιάστηκαν στον προηγούμενο πίνακα (ο αναγνώστης παρατέμπεται στις σχετικές παρουσιάσεις του τρίτου και τέταρτου κεφαλαίου).

### ⌚ Τυποποίηση πολιτικών ασφάλειας με Βάσεις Κανόνων

Στην προσέγγιση αυτή παρατηρήσαμε έμφαση στα στοιχεία "Κυρίως μοντέλο" και "Κανόνες επιβολής κυρίως μοντέλου". Σύμφωνα με τον παραπάνω πίνακα, είναι εξάλλου προφανές, η προσέγγιση αυτή προσεγγίζει στην αντιμετώπισή της τα κλασικά μοντέλα ασφάλειας. Παρόλα αυτά όμως, δεν τεκμηριώνει μαθηματικά τις απόψεις της αλλά, όπως είδαμε, χρησιμοποιεί εμπειρικές μεθόδους. Επίσης, δεν διαβλέπουμε ενδιαφέρον για το θέμα της διαχείρισης περισσότερων πολιτικών ασφάλειας. Η προσέγγιση αντιμετωπίζει, όπως σημειώθηκε, το θέμα της δημιουργίας μιας τεχνολογίας η οποία θα επιτρέπει τη βέλτιστη αποδοτικότητα από τη χρήση ασφαλών συστημάτων, μέσω της ενσωμάτωσης και εφαρμογής πολλών πολιτικών ασφάλειας, και ιδιαίτερα Πολιτικών Περιορισμών Προσπέλασης (Access Control Restriction Policies), σε ένα και μόνο σύστημα.

### ⌚ Τυποποίηση πολιτικών ασφάλειας βασισμένη στις Αρχές της Τεχνολογίας Λογισμικού

Η προσέγγιση αυτή παρουσιάζει ένα αρκετά ευρύ ερευνητικό προϊόν το οποίο καλούμαστε να εκτιμήσουμε.

Όσον αφορά τους "στόχους ως προς εμπιστοσύνη", η προσέγγιση ορίζει ότι μεταξύ των σκοπών της είναι να καθορίσει επακριβώς τους στόχους ασφάλειας ενός συστήματος". Το θέμα του "κυρίως μοντέλου" αντιμετωπίζεται μεν, αλλά δευτερευόντως από την προσέγγιση αυτή. Αυτό σημαίνει ότι δεν αποδίδεται σημασία στο ίδιο το περιεχόμενο της Πολιτικής Ασφάλειας αλλά κυρίως στους "κανόνες επιβολής του κυρίως μοντέλου", όπου ακριβώς εισάγεται και η έννοια του κουστωδού.

Στα πλαίσια του "λειτουργικού σχεδιασμού", παρόλο που δεν έχουμε στη

διάθεσή μας τις σχεδιαστικές επιλογές, θα λέγαμε ότι η προσέγγιση προσπαθεί να αποδείξει κάποια αρχική σύλληψη για την κατανομή υπευθυνοτήτων μέσα από την ανάπτυξη εφαρμογών (βλ. για παράδειγμα την εφαρμογή CWASAR και το αντίστοιχο σχήμα).

Η προσέγγιση αυτή είναι, επί του παρόντος, η μόνη που που κάνει σαφείς αναφορές σε συγκεκριμένες επιλογές υλικού και λογισμικού (λ.χ. το λειτουργικό σύστημα *BirliX* παρουσιάζεται σαν η ενδεικτική λύση υποδομής) και προσπαθεί να συνδέσει τις λύσεις που προτείνει με τις αντίστοιχες υποδομές. Ή α πρέπει να σημειώσουμε ότι πρέπει να είμαστε σε θέση, έχοντας τα κατάλληλα στοιχεία, να γνωρίζουμε τους λόγους υιοθέτησης συγκεκριμένων επιλογών επί αυτού του θέματος. Στην περίπτωση που εξαρτούν τη λειτουργικότητα από περιορισμένη εν λειτουργία υποδομή, υποβαθμίζουν τη λύση που προτείνουν. Αν όμως οι επιλογές έχουν σκοπό να διερευνήσουν κριτήρια επιλογής για ασφαλείς λύσεις, τότε είναι ορθές (ένα τέτοιο παράδειγμα είναι η αρχιτεκτονική CORBA). Ας μην ξεχνάμε ότι κάθε νέα ερευνητική προσπάθεια έχει στη διάθεσή της την επιλογή να δημιουργήσει νέα πρότυπα.

Το θέμα της διαχείρισης περισσότερων πολιτικών ασφάλειας, βρίσκεται σε αρχικά στάδια, αλλά αντιμετωπίζεται με ενδιαφέρον, όπως φαίνεται, ενώ χρησιμοποιείται για το σκοπό αυτό η ίδια σχεδιαστική επιλογή, δηλαδή ο κουστωδός.

Η προσέγγιση δεν εστιάζει στο θέμα της "περιγραφής του οργανισμού" αλλά αντιμετωπίζει μία πτυχή αυτού, λαμβάνοντας υπόψη της το θέμα του χώρου προβληματισμού στον οποίο απευθύνεται (ορίζει, θυμίζουμε ένα σύγχρονο κατανεμημένο περιβάλλον όπου τα πληροφοριακά συστήματα εκτελούν αμοιβαία υποποτευόμενες εφαρμογές, κ.λπ.). Εξάλλου, σε εξάρτηση από αυτή την έλλειψη δεν αντιμετωπίζεται επαρκώς και το θέμα της "εξωτερικής διεπαφής".

### ⌚ Τυποποίηση πολιτικών ασφάλειας με έμφαση στις λειτουργικές απαιτήσεις των χρηστών

Η παρουσίαση αυτής της προσέγγισης δεν μπορεί να υποστεί ουσιαστική κριτική, εφόσον ο απώτερος σκοπός μας ήταν να παρουσιάσουμε μία ολοκληρωμένη περίπτωση χρήσης μιας κατηγορίας τυπικών περιγραφικών μεθόδων για τυποποίηση εννοιών σχετικών με πολιτικές ασφάλειας.

Ωστόσο, μπορούμε να παρατηρήσουμε την περιορισμένη, εντούτοις χαρακτηριστική πολλών προσεγγίσεων εμμονή, στις έννοιες της ακεραιότητας σε όρους ροών πληροφορίας και του ελέγχου πρόσβασης (αναφορικά με το "κυρίως μοντέλο"). Ορισμένες επιλογές μας επιτρέπουν να εξάγουμε με επιφυλάξεις συμπεράσματα όσον αφορά το "λειτουργικό σχεδιασμό". Η προσέγγιση χρησιμοποιεί αντικειμενοστραφείς επιλογές και δίνει άμεσα σημασία σε λειτουργικές απόψεις. Θεωρεί, με άλλα λόγια, ότι ασχολείται με μία καλά καθορισμένη κατάσταση και δίνει, για το λόγο αυτό, έμφαση στις λειτουργικές απαιτήσεις του υποτιθέμενου συστήματος. Για το λόγο αυτό χρησιμοποιεί για παράδειγμα την έννοια του *Action Model*. Προσπαθεί, τέλος, να παραμετροποιήσει το περιβάλλον που τυποποιεί για να μπορεί να προσφέρει επιλογές και δίνει ως ενδεικτικό το παράδειγμα του τρόπου τυποποίησης της έννοιας του ρόλου.

### ⌚ Τυποποίηση πολιτικών ασφάλειας βασισμένη σε Γλώσσες Αναπαράστασης Γνώσης

Την προσέγγιση αυτή μπορούμε να τη σχολιάσουμε όσον αφορά τις αρχικές



διαστάσεις του πίνακα. Γενικά η προσέγγιση αυτή παρουσιάζει σε πρώιμο ερευνητικό στάδιο έναν νέο τρόπο αναπαράστασης πολιτικών ασφάλειας. Δεν αντιμετωπίζει συνεπώς ακόμη πιο πρακτικά θέματα, όπως λ.χ. υλοποίηση και συγκεκριμένες επιλογές (για παράδειγμα δεν ασχολείται με το θέμα κάποιου "κυρίως μοντέλου" ή συγκεκριμένης επιλογής υλοποίησης κάποιου πειραματικού προτοτύπου). Εστιάζει εντούτοις την προσοχή της στη δημιουργία μίας σωστής υποδομής για την τυποποίηση πολιτικών ασφάλειας, αντιμετωπίζοντας με επιμονή δύο κυρίως θέματα: "στόχοι ως προς εμπιστοσύνη" και "μοντέλο εξωτερικής διεπαφής". Με τον τρόπο αυτό καλύπτει κατ'επέκταση το θέμα "περιγραφή οργανισμού" και "διαχείριση περισσότερων πολιτικών ασφάλειας" (κατ'αντιστοιχία με τα προηγούμενα).

### • *Τυποποίηση Πολιτικών Ασφάλειας βασισμένη στη Θεωρία Ασφούς Λογικής*

Μία εξίσου φιλόδοξη και σε αρχικό ερευνητικό στάδιο προσπάθεια η οποία εστιάζει στον ίδιο ερευνητικό χώρο με την προηγούμενη: προσπαθεί να εντοπίσει το σωστό τρόπο αναπαράστασης πολιτικών ασφάλειας, και δη μεταπολιτικών ασφάλειας. Ο ορθός αυτός τρόπος θα μας επιτρέψει να παραστήσουμε εκείνα τα στοιχεία που αποτελούν τα κλειδιά για τη λύση διαφόρων προβλημάτων. Τέτοια προβλήματα είναι λ.χ. η σωστή περιγραφή των "στόχων ως προς εμπιστοσύνη" και η "περιγραφή του οργανισμού".

### • *Τυποποίηση πολιτικών ασφάλειας βασισμένη σε αρχές Ανάλυσης Επικινδυνότητας και Πρότυπα Ασφάλειας Πληροφοριακών Συστημάτων.*

Είναι προφανές ότι αυτή η περίπτωση αποτελεί μία εντελώς διαφορετική κατηγορία. Εντοπίζει το ενδιαφέρον της στη δημιουργία ενός εργαλείου το οποίο μπορεί να χρησιμοποιηθεί για την ανάπτυξη πολιτικής ασφάλειας για ένα σύστημα. Το εργαλείο μπορεί επίσης να χρησιμοποιηθεί για σκοπούς ιχνηλάτησης κάθε υλοποιηθέντος αντιμέτρου με την πολιτική ασφάλειας, εποπτείας αναφορικά με τα αντίμετρα και τέλος έχει τη δυνατότητα να απεικονίζει τις υπάρχουσες συσχετίσεις ασφάλειας στον οργανισμό.

Σύμφωνα με τα στοιχεία αυτά, το εργαλείο *SIDERØ* μπορεί να χρησιμεύσει σαν στοιχείο τεκμηρίωσης και εποπτείας της πολιτικής ασφάλειας.

Παρά το γεγονός ότι αρχικά μπορεί κανείς να δυσκολευτεί ιδιαίτερα στην εφαρμογή του πίνακά μας για την προσέγγιση αυτή, και πράγματι κάτι τέτοιο αληθεύει, δεν μπορούμε να μην παρατηρήσουμε ότι η προσέγγιση αυτή αντιμετώπισε τις δύο πρώτες διαστάσεις του πίνακα και ιδιαίτερα την πρώτη. Παραπέμπουμε στο σχετικό κεφάλαιο, όπου σημειώνουμε ότι το πρώτο πρόβλημα το οποίο αναγνωρίστηκε αφορά την ανυπαρξία μίας κοινής και συνεπούς υποδομής αναφοράς (*infrastructure*), όσον αφορά τα σημαντικά συστατικά στοιχεία του περιβάλλοντος εφαρμογής. Για το λόγο αυτό επιχειρήθηκε η κατά ιεραρχικά επίπεδα, ανάλογα με την ιεραρχική δόμηση υπευθυνοτήτων των οργανισμών, αντιμετώπιση των Πληροφοριακών Συστημάτων. Μάλιστα η αναφορά σε στοιχεία που ανήκουν στο σύστημα που αποτελεί ο εκάστοτε οργανισμός Υγείας θεωρείται μεγάλης σημασίας για την ανάπτυξη και διαχείριση των πολιτικών ασφάλειας. Προκειμένου να αντιμετωπιστεί το θέμα αυτό, αναπτύχθηκαν δύο μοντέλα, του συστήματος εφαρμογής και της πολιτικής ασφάλειας, χρησιμοποιώντας κατ'αντιστοιχία το πλαίσιο IBAG και την Ανάλυση Επικινδυνότητας, δύο εργαλεία με κοινά αποδεκτή ισχύ στο πεδίο της ασφάλειας Πληροφοριακών Συστημάτων.



## ⌚ Τυποποίηση πολιτικών ασφάλειας με έμφαση στην έννοια του οργανισμού

Όπως σημειώσαμε και κατά την παρουσίασή της, η προσέγγιση αυτή είναι σχετικά καινοτομική και σίγουρα πολύ φιλόδοξη. Αντιμετωπίζει ιδιαίτερα δύσκολα θέματα με πολύπλοκες και απαιτητικές μεθόδους. Χρησιμοποιεί εργαλεία, όπως η Θεωρία των Ελλογών Δράσεων, τα οποία απαιτούν με σειρά τους χρησιμοποίηση μεθόδων που δεν θα περιμέναμε να συναντήσουμε στο πεδίο αυτό, όπως για παράδειγμα η Ανάνυση της Λογικής Σύνταξης της Γλώσσας.

Η προσέγγιση εστιάζει τις προσπάθειές της σε δύο κύριους άξονες: ο πρώτος αφορά τις δύο πρώτες διαστάσεις του πίνακα ("περιγραφή του οργανισμού" και "στόχοι ως προς εμπιστοσύνη") και ο δεύτερος τις τρίτη και τέταρτη ("μοντέλο εξωτερικής διεπαφής" και "κυρίως μοντέλο").

Επισήμως δίνεται μεγάλη έμφαση στον οργανισμό, δηλαδή το σύστημα-στόχο. Όλες οι δομές που συνιστούν τον οργανισμό αυτό ως οντότητα πρέπει να αναγνωριστούν και να ληφθούν υπόψη σε οποιαδήποτε απόπειρα ανάλυσης του οργανισμού. Όσον αφορά τη δεύτερη διάσταση προτείνεται επίσης μία νέα αντιμετώπιση. Οι απαιτήσεις ασφάλειας ενός συστήματος θεωρούνται καταρχήν σαν μη-λειτουργικές απόψεις αυτού. Αναγνωρίζεται ότι αυτές οι μη-λειτουργικές απόψεις πρέπει τελικά να μεταφραστούν σε ορισμούς λειτουργικών απαιτήσεων για το σύστημα. Τονίζεται ότι οι μεθοδολογίες "μετάφρασης" απαιτήσεων από μη-λειτουργικές σε λειτουργικές δεν είναι τελειοποιημένες.

Οι άξονες αυτοί αλληλεπιδρούν σημαντικά κατά τον ακόλουθο τρόπο: θεωρείται ότι ο πιο ενδεδειγμένος τρόπος προκειμένου να επιτευχθεί σωστή αντιμετώπιση των απαιτήσεων ασφάλειας είναι η εις βάθους ανάλυση των απαιτήσεων ασφάλειας με επίκεντρο τον ίδιο τον οργανισμό, τέτοια ώστε να κατανοηθεί πλήρως το "νόημά" τους. Επισήμως, τα συμπεράσματα που θα προκύψουν θα είναι σε θέση να δώσουν τα βασικά στοιχεία μίας γλώσσας ορισμού απαιτήσεων ασφάλειας σε λειτουργικό επίπεδο.

## ⑤ Η συμβολή της τυποποίησης εντοπίζεται σε διάφορα σημεία, αλλά ο τρόπος χρήσης της είναι αμφιλεγόμενος.

Μία από τις σημαντικότερες αιτίες για το φαινόμενο αυτό εντοπίζεται στον τρόπο χρήσης μεθόδων τυποποίησης πολιτικών ασφάλειας. Τα διάφορα μέρη που αποτελούν τις ομάδες ενδιαφέροντος δεν έχουν ίδια αντίληψη του ρόλου, του τρόπου χρήσης, της γλώσσας και της χρησιμότητας των τυπικών μεθόδων. Το πεδίο έρευνας σε αυτό τον τομέα είναι η "σημασιολογία".

Μπορούμε να θεωρήσουμε τη σημασιολογία σαν μία συνάρτηση μετάφρασης των δεδομένων σε νόημα, μπορούμε δηλαδή να τη θεωρήσουμε σαν μηχανή πληροφορίας:

### ΠΛΗΡΟΦΟΡΙΑ: ΔΕΔΟΜΕΝΑ → ΝΟΗΜΑ

Η συνάρτηση ως μαθηματική έννοια αντιστοιχίζει ένα στοιχείο κάποιου συνόλου στο πολύ ένα στοιχείο ενός άλλου συνόλου. Τα σημεία τα οποία ενδέχεται να δημιουργήσουν προβλήματα και στα οποία συνεπώς πρέπει να εστιάσουμε είναι:

- Ότι η μετάφραση γίνεται από τον άνθρωπο και
- Ότι η μετάφραση γίνεται πάντα ως προς κάποιο ορισμένο περιεχόμενο



(context).

Συνεπώς, ο άνθρωπος και το περιεχόμενο πρέπει να αποτελούν αναπόσπαστα στοιχεία του ορισμού της πληροφορίας. Η κάλυψη των κενών που υπάρχουν στην αντιστοίχιση των περιγραφώμενων στα εννοιολογικά τους αντίστοιχα θα έλινε πολλά προβλήματα τόσο κατανόησης όσο και πρακτικά (όπως αναλύθηκε στην παράγρ. 5.4.3.).

---

**⑥ Η διαχείριση περισσότερων πολιτικών ασφάλειας αποτελεί ένα ιδιαίτερα ενδιαφέρον ερευνητικό πεδίο το οποίο μπορεί να ωθηθεί σημαντικά από την επιτυχή τυποποίηση-αυτοματοποίηση πολιτικών ασφάλειας**

---

Το θέμα της διαχείρισης πολλών πολιτικών ασφάλειας είναι ένα σημαντικό κεφάλαιο, το οποίο μπορεί να διαμορφώσει ολόκληρο πεδίο έρευνας. Οι εξελίξεις στο χώρο όχι μόνο το επιτρέπουν αλλά στην πραγματικότητα το επιβάλλουν. Ενδέχεται, κατά τις εκτιμήσεις μας, το πεδίο αυτό να γνωρίσει μεγάλη ανάπτυξη καθώς η δικτύωση των Πληροφοριακών Συστημάτων θα ολοκληρώνεται και καθώς οι χρήστες θα επιζητούν συνεχώς αυξανόμενες και εξατομικευμένες απαιτήσεις ασφάλειας.

Στο τέταρτο κεφάλαιο, αναφερθήκαμε στη διαχείριση πολλών πολιτικών ασφάλειας. Η "μεταπολιτική" κυριαρχεί ως έννοια στο χώρο αυτό. Μετά από τα παραδείγματα που εξετάσαμε, μπορούμε να εντοπίσουμε ορισμένα σημεία-κλειδιά σχετικά με την ανάπτυξη και διαχείριση πολλών πολιτικών ασφάλειας:

Για θεωρητικούς μεθοδολογικούς σκοπούς, κρίνουμε ότι η τυποποίηση πολιτικών ασφάλειας πρέπει να προηγείται της ανάλυσης σε επίπεδο μεταπολιτικών. Η διαχείριση των μεταπολιτικών είναι ένα πολύπλοκο θέμα, του οποίου η λύση έγκειται σε μεγάλο βαθμό στον τρόπο με τον οποίο έχουμε αξιολογήσει τις υποκείμενες πολιτικές, τρόπος ο οποίος πρέπει να χαρακτηρίζεται από **αυστηρή τυποποίηση** και **σημασιολογική σαφήνεια** και να υπόκειται σε **αυτοματοποίηση**. Προκειμένου να αυτοματοποιηθεί μία πολιτική ασφάλειας και να επιδέχεται διαχείριση από μεταπολιτική, απαιτείται μία ορισμένη προεργασία βασικά για τον καθορισμό εμφανών αλλά και λιγότερο προφανών και άμεσων στοιχείων σύνθεσης μιας πολιτικής, όπως είναι: Πεδίο εμβέλειας, Περιγραφή και Δομή σε όρους τυπικών και μη-τυπικών συστατικών στοιχείων, Συσχετίσεις, Στοιχεία Ελέγχου, κ.λπ., όπως περιγράψαμε στο σχετικό κεφάλαιο.

Οι μεταπολιτικές πρέπει να είναι γενικές ώστε να καλύπτουν τη γενικότητα των περιπτώσεων, στοιχείο που μπορεί να επιτευχθεί μέσω σωστής δόμησης των υποκείμενων πολιτικών, αλλά και να χαρακτηρίζονται από παραμετρικότητα για την προσαρμογή τους σε εξειδικευμένες συνθήκες.

Ενα από τα βασικότερα χαρακτηριστικά στοιχεία των μεταπολιτικών είναι ότι πρέπει να υπόκεινται σε έλεγχο και εποπτεία. Μάλιστα υποστηρίζεται ότι ο μηχανισμός που τις ελέγχει θα πρέπει να ικανοποιεί τα βασικά γνωρίσματα ενός Επόπτη (Reference Monitor).

Είναι επόμενο να υποθέσει κανείς ότι οι έννοιες και οι απαιτήσεις που η μεταπολιτική εισάγει, μπορεί να επιφέρουν επιπλέον **προβλήματα σε όρους επιπλέον κόστους** στον τρόπο με τον οποίο διαχειρίζόμαστε τις πολιτικές ασφάλειας. Μάλιστα, κάτι τέτοιο είναι σίγουρο ότι θα συμβεί όταν το θέμα της μεθοδολογίας και

των μεθόδων με τις οποίες θα προσεγγίσουμε το θέμα των μεταπολιτικών, ώστε τα πλεονεκτήματα που υποθέτουμε ότι θα μας προσφέρουν να πραγματοποιηθούν, είναι δύσκολο να εντοπιστούν. Όπως είδαμε, τα είδη των μεταπολιτικών είναι αρκετά, καλύπτοντας διάφορες ανάγκες και απόψεις διαχείρισης πολιτικών ασφάλειας. Ανάλογα με το είδος της ανάγκης που πρέπει να καλυφθεί, μπορούμε να θεωρήσουμε ότι οι μεταπολιτικές μπορούν να αναπτυχθούν ακολουθώντας το παράδειγμα της κατά στάδια ανάπτυξης των πληροφοριακών συστημάτων και κατ' αναλογία με την ανάπτυξη των πολιτικών ασφάλειας και λαμβάνοντας υπόψη τις οργανωτικές δομές των συστημάτων που θα καλύψουν. Η διερεύνηση, στο πλαίσιο αυτό, εννοιών υψηλού επιπέδου αφαιρέσης (φιλοσοφία που διέπει τις πολιτικές ασφάλειας, πεποιθήσεις, χαρακτήρας του οργανισμού, κ.λπ.) συνιστά ένα σημαντικό όσο και ανεπίλυτο θέμα.

Είναι προφανές ότι η διαδικασία ανάπτυξης μεταπολιτικών πρέπει να ξεκινά με τον καθορισμό του *εννοιολογικού σχήματος* της μεταπολιτικής. Η εργασία αυτή απαιτεί βαθιά και επίμονη ανάλυση πλήθους περιπτώσεων, όχι μόνο διότι διαφορετικά το επαγόμενο πλαίσιο δεν θα καλύπτει τη γενικότητα των περιπτώσεων, αλλά και διότι δεν υπάρχει άλλος τρόπος προκειμένου να εντοπιστεί η γλώσσα και οι τύποι, που είναι κατάλληλα να εκφράσουν τις εντοπισθείσες έννοιες. Η διαχείριση των μεταπολιτικών απαιτεί επίσης και τη δημιουργία ή τον εντοπισμό μίας αρχιτεκτονικής υποδομής κατάλληλης να υποστηρίζει τις αντίστοιχες εφαρμογές (η υποδομή αυτή πρέπει να είναι συμβατή, για παράδειγμα, με τις απαιτήσεις που θέτει η επικοινωνία των πολιτικών και ταυτόχρονα να υποστηρίζει επιπλέον χαρακτηριστικά ασφάλειας, όπως μεσολάβηση για τον έλεγχο της επικοινωνίας, κ.λπ.).

Ο αναγνώστης θα παρατηρήσει εξαρχής ότι οι μέθοδοι τυπικής παράστασης πολιτικών εφαρμόζονται και στην ανάπτυξη μεταπολιτικών. Πρέπει προφανώς να θεωρήσουμε ότι πρόκειται για επιστημονικές προσπάθειες που αλληλεπιδρούν στο γενικότερο πλαίσιο που θέτει η ανάγκη για διαχείριση πολιτικών ασφάλειας και εντείνονται ταυτόχρονα, εφόσον οι πρόοδοι στη μία μπορούν να φανούν χρήσιμες στην άλλη.

## ΜΕΤΑΦΡΑΣΕΙΣ ΟΡΩΝ

### ΑΓΓΛΙΚΟΣ ΟΡΟΣ

### ΜΕΤΑΦΡΑΣΗ ΣΤΑ ΕΛΛΗΝΙΚΑ

A

Action Model	Μοντέλο Δράσης
Action Refinement	Εξειδίκευση Πράξης
Agent	Φορέας
Aggregation	Συνένωση
Atomic Action	Ατομική Πράξη
Attenuation	Εξασθένιση

C

Classification	Κατηγοριοποίηση
Cognitive procedures	Νοητικές διαδικασίες
Composability of Security Policies	Σύνθεση πολιτικών ασφάλειας
Confidence Domain	Πεδίο Εμπιστοσύνης
Corporate Security Infrastructure	Βασική Υποδομή Ασφάλειας
Covert channel	Έμεσο κανάλι
Custodian	Κουστωδός
Compatibility of Security Policies	Συμβατότητα πολιτικών ασφάλειας

D

Deductive Mechanism	Επαγγειακός/Συμπερασματικός Μηχανισμός
Deterministic Model	Αιτιοκρατικό Μοντέλο

E

Economic rationality	Εκλογικευμένη οικονομία
Engineering	Τεχνολογία
Evolution of Security Policies	Εξέλιξη πολιτικών ασφάλειας

F

Federated systems	Ενοποιημένα συστήματα
Formal Description Techniques	Τυπικές Περιγραφικές Μέθοδοι
Formal Methods	Τυπικές Μέθοδοι Ορισμού Απατήσεων
Formal Security Policy Models	Τυπικά Μοντέλα Πολιτικής Ασφάλειας
Formal Specification Methods/Techniques	Τυπικές Μέθοδοι Ορισμού
Formalization	Τυποποίηση
Fuzzy theory	Θεωρία Ασφάλειας Συνόλων

I

Information sharing	Μοίρασμα πληροφορίας
Information Systems Security Engineering	Τεχνολογία πολιτικών ασφάλειας Πληροφοριακών Συστημάτων
Interoperability	Διαλειτουργικότητα

K

Knowledge representation language	Γλώσσα Αναπαράστασης Γνώσης
Lattice Model	Μοντέλο του Δικτυώματος

L

Modeling	Μοντελοποίηση/Διαδικασία μοντελοποίησης
Multipolicy Machine	Μηχανή Πολλαπλών Πολιτικών Ασφάλειας



	O
Order of Security Policies	Διαβάθμιση πολιτικών ασφάλειας
	P
Paradigm	Παράδειγμα
Policy structure	Δομή Πολιτικής
Precedence of Security Policies	Προτεραιότητα πολιτικών ασφάλειας
Procedural uncertainty	Διαδικαστική αβεβαιότητα
	R
Reference Monitor	Επόπτης
	S
Security Architecture	Αρχιτεκτονική Ασφάλειας
Security Policy Model	Μοντέλο Πολιτικής Ασφάλειας
Security property	Χαρακτηριστικό/Ιδιότητα ασφάλειας
Semantics	Σημασιολογία
Semiotics	Σημειωτική
Sensitivity analysis	Ανάλυση ενασθησίας
Sensitivity Labels	Επικέτες Ενασθησίας
Socket	Υποδοχή
Speech Acts Theory	Θεωρία Έλλογων Δράσεων
State Transition Machine	Μηχανή Μετάθεσης Καταστάσεων
Stimulus	Ερέθισμα
Syntax	Σύνταξη/Συντακτικό
	T
Tamperproofness	Απροσβλητότητα
Theory of Plans	Θεωρία Προγραμματισμού
Top-down approach	Προσέγγιση από-πάνω-προς-τα-κάτω
Total Mediation	Καθολική Μεσολάβηση
Trusted Computing Base	Έμπιστη Υπολογιστική Βάση
Type Definition Language	Γλώσσα Ορισμού Τύπων

## ΕΥΡΕΤΗΡΙΟ ΟΡΩΝ

### A

- Αιτιοκρατικό Μοντέλο, 105  
Ανάλυση Επικινδυνότητας, 72, 133  
Ανάλυση ευασθησίας, 111  
Αντικειμενοστράφεια, 27, 45, 51, 54, 65, 100, 132  
Απροσβλητότητα, 51  
Αρχή της ασφάλειας, 78  
Αρχή της αυτονομίας, 78  
Αρχιτεκτονική Ασφάλειας, 54  
Ασαφή Σύνολα, 85, 87, 133  
Ατομική Πράξη, 43

### B

- Βάσεις Γνώσης, 63  
Βάσεις Κανόνων, 28, 39, 89, 131  
Βασική Υποδομή Ασφάλειας, 55, 72, 130

### Γ

- Γενικευμένο Πλαίσιο για Έλεγχο Προσπέλασης, 29  
Γλώσσα Ορισμού Τύπων, 52, 56  
Γλώσσες Αναπαράστασης Γνώσης, 63, 93, 101, 132

### Δ

- Διαβάθμιση πολιτικών ασφάλειας, 32, 58, 86, 92  
Διαδικαστική αβεβαότητα, 107  
Διαλειτουργικότητα, 77, 96  
Δίκτυα Petri, 27  
Δομή Πολιτικής, 16

### E

- Εκλογικευμένη οικονομία, 107  
Έμεσο κανάλι, 81, 89  
Έμπειρα Συστήματα, 28, 90  
Έμπιστη Υπολογιστική Βάση, 39, 51, 88  
Εννοιολογικό πλαίσιο, 54, 69, 86, 119  
Ενοποιημένα συστήματα, 80  
Εξασθένιση, 86  
Εξειδίκευση Πράξης, 45  
Εξέλιξη Πολιτικών Ασφάλειας, 87  
Επαγγελματικό/Συμπερασματικό Μηχανισμός, 65  
Επόπτης, 51, 135  
Ερέθισμα, 113  
Ετικέτες Ευασθησίας, 67

### H

- Θεωρία Αποφάσεων, 107  
Θεωρία Ασαφών Συνόλων, 87, 133  
Θεωρία Έλλογων Δράσεων, 70  
Θεωρία Προγραμματισμού, 17

I

- Ιδιότητα ασφάλειας 40, 44  
Ιεραρχική Ανάπτυξη Ασφαλών Συστημάτων, 73, 114  
Ιστορικό, 70

K

- Καθολική Μεσολάβηση, 51  
Κατηγοριοποίηση, 65, 87  
Κουνταδός, 51, 89, 131

M

- Μεθοδολογικό Πλαίσιο, 100  
Μεταπολιτική, 82, 90, 126, 129, 133, 135  
Μετασύστημα, 20  
Μηχανή Μετάθεσης Καταστάσεων, 28, 39, 43, 54, 85, 101  
Μηχανή Πολλαπλών Πολιτικών Ασφάλειας, 85  
Μοίρασμα πληροφορίας, 79  
Μοντέλα Δεδομένων, 103  
Μοντέλα Διαδικασιών, 104  
Μοντέλα Διεπαφών, 103  
Μοντέλα Κατανεμημένων Συστημάτων, 103  
Μοντέλα Μετάθεσης Καταστάσεων, 104  
Μοντέλο Δικτυώματος, 51, 90  
Μοντέλο Δράσης, 131

N

- Νοητικές διαδικασίες, 106, 108  
NP-complete πρόβλημα, 78, 80

II

- Παράδειγμα, 54, 113  
Πεδίο Εμπιστοσύνης, 55  
Πολυπλοκότητα, 21, 78  
Προσέγγιση από-πάνω-προς-τα-κάτω, 42, 113  
Προτεραιότητα πολιτικών ασφάλειας, 84, 87, 93, 94  
Πρότυπα Ασφάλειας, 99, 120, 128, 132

P

- Ροή Πληροφορίας, 41, 44, 48

S

- Σημασιολογία, 90, 94, 105, 109, 127, 133  
Σημειωτική, 110  
Σύγκριση Πολιτικών Ασφάλειας, 93  
Σύγκρουση Πολιτικών Ασφάλειας, 86  
Συμβατότητα Πολιτικών Ασφάλειας, 78  
Συμπερασματικός Μηχανισμός, 65  
Συνδυασμός Πολιτικών Ασφάλειας, 86  
Σύνθεση πολιτικών ασφάλειας, 80  
Συντακτικό, 47, 101, 105, 127  
Σχέση κυριαρχίας Πολιτικών Ασφάλειας, 92  
Σχέση προτεραιότητας Πολιτικών Ασφάλειας, 93



**T**

- Τεχνική Πολιτική Ασφάλειας, 17  
Τεχνολογία Λογισμικού, 48, 100, 105, 120, 128  
Τεχνολογία πολιτικών ασφάλειας Πληροφοριακών Συστημάτων, 48, 102  
Τυπικές Μέθοδοι Ορισμού Απατήσεων Λογισμικού, 48  
Τυπικές Περιγραφικές Μέθοδοι, 101

- Υπευθυνότητα, 67, 71, 125  
Υποδοχή, 53, 112

**Φ**

- Φιλοσοφία Πολιτικής Ασφάλειας, 63, 135



## BIBLIOGRAPHY

### A. ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- [ABR-1991] M.D.Abrams & D.Bailey, "Abstraction and refinement of layered security policy", in *Information Systems Security: An integrated collection of essays*, Eds: M.D.Abrams, S.Ja Jodia & H.Podell, IEEE Computer Society Press, 1991
- [AND-1994] A.Anderson, D.Longley & L.F.Kwok, "Security Modelling for Organizations", in *Proceedings of the 2<sup>nd</sup> ACM Conference on Computer and Communications Security, Fairfax Virginia, ACM SIGSAG 1994*
- [BAC-1996] J.Backhouse & G.Dillon, "Structures of responsibility and security of information systems", *European Journal of Information Systems*, Vol.5, No.1, 1996
- [BEL-1988] E.Bell, "Concerning 'Modeling' of Computer Security", in *IEEE Symposium on Research, Security & Privacy, 1988*
- [BEL-1991] E.Bell, "Putting policy commonalities to work", in *Proceedings of the 14<sup>th</sup> National Computer Security Conference, Washington D.C, 1991*
- [BEL-1994] E.Bell, "Modeling the multipolicy machine", in *Proceedings of the 1994 New Security Paradigms Workshop, ACM SIGSAG, IEEE Computer Society Press*
- [BRO-1996] R.Gotzhein & J.Bredereke, "Formal description techniques - how formal and descriptive are they?", in *Formal description techniques in theory, application & tools, IFIP, Chapman & Hall 1996*
- [BRY-1996] C.Bryce & W.Kuhnhauser, "Security in CWASAR", *CWASAR project report, December 1996*, also available at <http://www.set.gmd.de/~khuenhsr>
- [BRY-1997a] C.Bryce, W.Kuhnhauser, R.Amouroux, M.Lopez, H.Rudnik, "CWASAR: a European Infrastructure for Secure Electronic Commerce", available at <http://www-set.gmd.de/~bryce>
- [BRY-1997b] C.Bryce, "Security engineering of lattice based policies", *10<sup>th</sup> IEEE Computer Security Foundations Workshop, Rockport, Mass., USA, June 1997*, also available at <http://www-set.gmd.de/~bryce>
- [BRY-1997c] C. Bryce, "The Skippy security engineering framework", *GMD Research Report no.1060, March 1997*, available at <http://www-set.gmd.de/~bryce>
- [CCTA-1996] CCTA, "CRAMM User Guide", *Version 3.0, April 1996, U.K.*
- [DOB-1988] J.Dobson, "Modelling real-world issues for dependable software", in *High integrity Software, Ed: C.T. Sennett, Edition Pitman 1988*
- [DOB-1989] J.E.Dodson, "A framework for expressing models of security Policy", in *IEEE Computer Society Symposium on security and privacy 1989*
- [ECK-1995] C.Eckert, "Matching securities policies to application needs", in *Information Security-The next decade, Eds I.H.P. Eloff & S.H von Solms, IFIP, Chapman-Hall 1995*
- [FER-1994] J.M.Ferris, "Using Standards as a security policy tool", *Standardsview, Vol. 2 June 1994*

- [FLI-1997] E.Flikkenschild, "The development of a security Administration Policy, using a supporting tool:SIDERO", *Central Information Processing Department, Leiden University Hospital, Working paper*
- [GON-1994] L.Gong & X.Qian, "The Complexity and Composability of Secure Interoperation", in *IEEE Symposium on Computer & Communications Security, 1994*
- [HÄR -1993] H.Härtig, O.Kowalski & W.Kuhnhauser, "The BirliX Security Architecture", *Journal of Computer Security Vol.2 No.1, 1993*, also available at <http://www.set.gmd.de/~khuenhsr>
- [HER-1986] D.B.Hertz, "Expert systems for the analysis and synthesis of strategic policy", in *Proceedings of the Economics and Artificial intelligence Conference, Eds: Jean-Louis Roos, France 1986, Pergamon Press*
- [HIN-1994] H.Hinton & E.S.Lee, "The compatibility of policies", in *Proceedings of the 2<sup>nd</sup> ACM Conference on Computer and Communications Security, Fairfax Virginia, ACM SIGSAG 1994*
- [HOS-1992a] H.Hosmer, "METAPOLICIES II", in *Proceedings of the 15<sup>th</sup> National Computer Security Conference, Baltimore, M.D, 1992*
- [HOS-1992b] H.Hosmer, "The multipolicy paradigm for trusted systems", in *Proceedings of the 1992-1993 New Security Paradigms Workshop, ACM SIGSAG, IEEE Computer Security Press*
- [HOS-1993] H.Hosmer, "Security is fuzzy, Applying the fuzzy logic paradigm to the multipolicy paradigm", in *Proceedings of the 1992-1993 New Security Paradigms Workshop, ACM SIGSAG, IEEE Computer Security Press*
- [HOW-1992] D.Howe, "Information Systems security engineering: cornerstone to the future", in *Proceedings of the 15<sup>th</sup> National Computer Security Conference, Baltimore M.D., 1992*
- [HUM-1984] P.Humphreys, "Levels of representation in structuring decision problems", *Journal of applied systems analysis vol.11, 1984*
- [IBAG-1993] Infosec Business Advisory Group, "The IBAG framework for commercial IT Security", *Version 2.0 September 1993*
- [ITSEC-1991] "Information Technology Security Evaluation Criteria", *Provisional Harmonised criteria, version 1.2, Commission of the European Communities, Belgium, Brussels*
- [KOK-1997a] S.Kokolakis, "A framework for Information Systems Security Policies Management", *Working paper, Athens University of Economics and Business*
- [KOK-1997b] S.Kokolakis & E.Kiountouzis, "Developing security metapolicies for cooperating information systems", *Working paper, Athens University of Economics and Business*
- [KUH-1995] W.Kuhnhauser & M.K.Ostrowski, "A Framework to Support Multiple Security Policies", in *Proceedings of the 7<sup>th</sup> Annual Canadian Computer Security Symposium, Ottawa, Canada 1995*, also available at <http://www.set.gmd.de/~khuenhsr>
- [KUH-1995] W.Kuhnhauser, "On Paradigms for Security Policies in Multipolicy Environments", in *Proceedings of the 11<sup>th</sup> International Information Security Conference (IFIP/SEC '95), Cape Town, South Africa 1995*.



- Chapman & Hall / also available at <http://www.set.gmd.de/~khuenhsr>*
- [LAP-1991] L.LaPadula, "Rule-Set modeling of a trusted computer system", in *Informations Systems Security: An integrated collection of essays*, Eds: M.D.Abrams, S.Ja Jodia & H.Podell, IEEE Computer Society Press, 1991
- [LAP-1992] L.J. LaPadula, "Prospect on Security Paradigms", in *Proceedings of the 1992-1993 New Security Paradigms Workshop*, ACM SIGSAG, IEEE Computer Security Press
- [LEI-1997] J.Leiwo & Y.Zheng "A formal model to aid documenting and harmonizing of Information security requirements", in *Proceedings of the 13<sup>th</sup> International Information Security Conference (IFIP/SEC '97)*, Chapman & Hall
- [MAR-1991] M.Martin, "Enterprise modeling and security policies", in *Database security IV: Status and prospects*, Eds: S.Jajodia and Landwehr, Elsevier Science Publishers B.V. (North-Holland) IFIP, 1991
- [MUM-1985] E.Mumford, "Defining system requirements to meet business needs", *The Computer Journal*, Vol.28, No.2, 1985
- [OLA-1996] D.Olawsky, T.Fine, E.Schneider, & R.Spencer, "Developing and Using a 'Policy Neutral' Access Control Policy", in *Proceedings of the 1996 New Security Paradigms Workshop*, ACM SIGSAG, IEEE Computer Security Press
- [OLS-1991] I.M.Olson & M.D.Abrams, "Information Security Policy", in *Informations Systems Security: An integrated collection of essays*, Eds: M.D.Abrams, S.Ja Jodia & H.Podell, IEEE Computer Society Press, 1991
- [OXF-1989] A.S.Hornby, "Oxford Advanced Learner's Dictionary", Oxford University Press, Fourth edition 1989
- [PAG-1989] J.Page, J.Heaney, M.Adkins & G.Dolsen, "Evaluation of security model rule bases", in *Proceedings of the 12th National Computer Security Conference*, Baltimore 1989
- [POL-1997] E.Polidorou, "Security paradigms: exploring the theoretical paths of Information Security", MSc project, Athens University of Economics and Business
- [POT-1995] D.Pottas & SH von Solms, "Aligning information security profiles with organisational profiles", in *Information Security-The next decade*, Eds I.H.P. Eloff & S.H von Solms, IFIP, Chapman-Hall 1995
- [SPI-1992] J.M.Spivey, "The Z notation, A reference Manual", Prentice Hall International Series in Computer Science Second Edition 1992
- [STR-1993] R.Strens & J.Dobson, "How responsibility modelling leads to security requirements", in *Proceedings of the 1992-1993 New Security Paradigms Workshop*, ACM SIGSAG, IEEE Computer Security Press
- [TIN-1990] T.C.Ting, "Application Information Security Semantics: A case of mental Health Delivery", in *Database Security III: Status and Prospects*, Eds: D.L.Spooner & C.Landwehr, Elsevier Science Publishers B.V. (North-Holland), IFIP, 1990
- [UNI-1996] UNILEVER, "Unilever IT Policies", Internal Report, September 1996
- [WAR-1995] A.Warman, "Developing policies, procedures and Information Systems", in

*Information Security-The next decade, Eds I.H.P. Eloff & S.H von Solms,  
IFIP, Chapman-Hall 1995*

[www-1997] Demo available at <http://devius.cs.uiuc.edu/Security/SPRF/sprf.html>

## B. ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- [ΑΠΟ-1995] Θ.Αποστολόπουλος, "Ανώτερα επίπεδα σε δίκτυα υπολογιστών", *Πανεπιστημιακές Παραδόσεις, Οικονομικό Πανεπιστήμιο Αθηνών, ΑΘΗΝΑ Φεβρουάριος 1995*
- [ΓΚΡ-1993] D.Γκρίτζαλης & Σ.Γκρίτζαλης, *Ασφάλεια λειτουργικών συστημάτων UNIX-DOS, Management & Information Technology Training Publications, ΑΘΗΝΑ 1993*
- [ΚΑΒ-1995] I.Κάβουρας, "Λειτουργικά Συστήματα, Συστήματα Υπολογιστών Τόμος Ι", *Έκδοση τρίτη, Εκδόσεις κλειδάριθμος, ΑΘΗΝΑ 1995*
- [ΚΙΟ-1993] Ε.Κιουντούζης, "Ανάλυση και σχεδιασμός συστημάτων", *Έκδοση 1η, Εκδόσεις Μπένου, ΑΘΗΝΑ 1993*

