Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής

Διδακτορική Διατριβή

Αυθεντικοποίηση με Χρήση Οπτικής Πληροφορίας και Διαχείριση Πρόσβασης με Δυναμικές Παραμέτρους σε Πληροφοριακά Συστήματα

Εμμανουήλ Ν. Γεωργακάκης

Πειραιάς, Φεβρουάριος 2016

.....

Εμμανουήλ Ν. Γεωργακάκης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Πληροφορικής

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Αυθεντικοποίηση με Χρήση Οπτικής Πληροφορίας και Διαχείριση Πρόσβασης με Δυναμικές παραμέτρους σε Πληροφοριακά Συστήματα

Εμμανουήλ Ν. Γεωργακάκη

Τριμελής Συμβουλευτική Επιτροπή

Επιβλέπων: **Χρήστος Δουληγέρης,** Καθηγητής Πανεπιστημίου Πειραιώς

Μέλη: **Δέσποινα Πολέμη,** Αναπληρώτρια Καθηγήτρια Πανεπιστημίου Πειραιώς

Δημήτριος Βέργαδος, Επίκουρος Καθηγητής Πανεπιστημίου Πειραιώς

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την 26η Φεβρουαρίου 2016.

Χρήστος Δουληγέρης Καθηγητής Πανεπιστημίου Πειραιώς	**Δέσποινα Πολέμη** Αναπληρώτρια Καθηγήτρια Πανεπιστημίου Πειραιώς	**Δημήτριος Βέργαδος** Επίκουρος Καθηγητής Πανεπιστημίου Πειραιώς
Βασίλειος Χρυσικόπουλος Καθηγητής Ιονίου Πανεπιστημίου	**Αντώνιος Ανδρεάτος** Καθηγητής Σχολής Ικάρων	**Παναγιώτης Κοτζανικολάου** Επίκουρος Καθηγητής Πανεπιστημίου Πειραιώς
	Κωνσταντίνος Πατσάκης Λέκτορας Πανεπιστημίου Πειραιώς	

Αφιερώνεται στην μητέρα μου

Πανεπιστήμιο Πειραιώς
Τμήμα Πληροφορικής Εμμανουήλ Ν. Γεωργακάκης

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Χρήστο Δουληγέρη ο οποίος με εμπιστεύτηκε και μου έδωσε την ευκαιρία να εκπονήσω την παρούσα διατριβή. Η καθοδήγηση, η υπομονή και η υποστήριξη που μου παρείχε είναι παροιμιώδης. Η ευστροφία και η επιστημονική σκέψη που τον διακρίνει αποτέλεσε διαρκή πηγή έμπνευσης κατά την εκπόνηση της διατριβής μου ενώ το προσωπικό του ήθος αποτελεί έμπνευση και πρότυπο για την πορεία της ζωής μου.

Θα ήθελα να ευχαριστήσω ιδιαίτερα και τους καθηγητές που απαρτίζουν την τριμελή επιτροπή μου, τους κ. Βεργαδο και κα Πολέμη με τους οποίους είχα την τύχη να συνεργαστώ ιδιαίτερα στενά όλα αυτά τα χρόνια.

Πολύτιμη για την αρτιότητα της διατριβής ήταν και η συνεισφορά από τα μέλη της επταμελούς μου επιτροπής κ. Βασίλειο Χρυσικόπουλο, κ. Αντώνιο Ανδρεάτο, κ. Παναγιώτη Κοτζανικολάου και κ. Κωνσταντίνο Πατσάκη.

Επιπλέον, θα ήθελα να εκφράζω την ευγνωμοσύνη μου στους Στέφανο Νικολιδάκη και Νίκο Κομνηνό που συνεργάστηκαν μαζί μου σε σημαντικό μέρος των ερευνητικών προσπαθειών που παρουσιάζονται στο παρόν κείμενο.

Σημαντικοί άνθρωποι με τους οποίους μπόρεσα να μοιραστώ προβληματισμούς και σκέψεις -οργανωμένες ή μη- είναι πολλά από τα στελέχη της περιβόητης «208» (ή αλλιώς Εργαστήριο Διαδικτυακών και Τηλεπικοινωνιακών Συστημάτων, Υπηρεσιών και Ασφάλειας) και ιδίως ο Αγάπιος Αβραμίδης.

Ιδιαίτερες ευχαριστίες στην σύντροφο και σύζυγό μου Μαρίνα Χατζηχαραλάμπους για την κατανόηση που επέδειξε και την υποστήριξη που μου παρείχε στην διάρκεια της δύσκολης αυτής πορείας. Τέλος, ευχαριστώ ολόψυχα την οικογένειά μου για την αμέριστη συμπαράσταση και υποστήριξη που μου παρείχαν.

Φεβρουάριος, 2016

Εμμανουήλ Ν. Γεωργακάκης

.

.

Περίληψη

Τα σημερινά πληροφοριακά συστήματα χαρακτηρίζονται από αυξημένη πολυπλοκότητα και την ανάγκη να εξυπηρετούν ταυτόχρονα πολλαπλούς χρήστες με διαφορετικές απαιτήσεις. Σε κάθε περίπτωση, κοινή απαίτηση όλων των σύγχρονων πληροφοριακών συστημάτων είναι η προστασία της πληροφορίας κατά τη διακίνησή της μέσα σε αυτά.

Προαπαιτούμενο για την επιτυχή προστασία των πόρων ενός συστήματος είναι η αυθεντικοποίηση των χρηστών από αποκτούν πρόσβαση σε αυτό και κατόπιν η εφαρμογή κανόνων διαχείρισης πρόσβασης όπου καθορίζεται τι δικαιώματα κατέχει ο κάθε χρήστης.

Η πιο διαδεδομένη μέθοδος αυθεντικοποίησης, παρά τα προβλήματα που παρουσιάζει, είναι η χρήση κωδικών πρόσβασης. Ωστόσο, η ανθρώπινη ικανότητα να απομνημονεύουμε οπτική πληροφορία έχει δώσει το έναυσμα για έντονη ερευνητική δραστηριότητα στην αυθεντικοποίηση με χρήση γραφικών κωδικών ως μια πιο αξιόπιστη εναλλακτική λύση στους κωδικούς κειμένου. Όμως, τα μοντέλα γραφικών κωδικών παρουσιάζουν όχι μόνο προβλήματα αποδοχής χρήσης από τους χρήστες αλλά και ζητήματα ασφάλειας. Κατανοώντας τις αδυναμίες αυτές η παρούσα διατριβή προτείνει ένα καινοτόμο μοντέλο αυθεντικοποίησης το Novel Authentication with Visual Information (NAVI), το οποίο είναι βασισμένο σε οπτική πληροφορία και το οποίο παρέχει υψηλού επιπέδου ασφάλεια. Το προτεινόμενο σύστημα αυθεντικοποίησης χρησιμοποιεί ως διαπιστευτήρια την διαδρομή που επιλέγει ένας χρήστης σε έναν προκαθορισμένο χάρτη. Στη διατριβή αυτή, πραγματοποιείται ανάλυση της ασφάλειας που παρέχει το NAVI σε θεωρητικό επίπεδο και επιπλέον αναπτύχθηκε μια πρότυπη υλοποίηση με την οποία πραγματοποιήθηκαν δοκιμές χρηστών για την αξιολόγηση της ευκολίας χρήσης και της ασφάλειας του παραγόμενου κωδικού. Επιπλέον, ζητήθηκε από τους χρήστες που συμμετείχαν στις δοκιμές να απαντήσουν σε ένα ερωτηματολόγιο αξιολόγησης προκειμένου να ληφθεί υπόψη η γνώμη τους σε μια σειρά από ζητήματα που αφορούν την υλοποίηση του NAVI.

Εφόσον έχει πιστοποιηθεί ότι ένας χρήστης είναι αυτός που υποστηρίζει ότι είναι θα πρέπει να του αποδωθούν τα κατάλληλα δικαιώματα πρόσβασης. Η πλειοψηφία των μοντέλων ελέγχου πρόσβασης που έχουν αναπτυχθεί βασίζονται στην υπόθεση ότι τα δικαιώματα πρόσβασης των χρηστών μπορεί να καθοριστούν εκ των προτέρων. Ωστόσο, σε ένα σύγχρονο περιβάλλον συχνά προκύπτουν καταστάσεις έκτακτης ανάγκης που οδηγούν σε αιτήματα πρόσβασης που δεν έχουν προβλεφθεί από τις συνήθεις διαδικασίες. Έχοντας εντοπίσει την ανάγκη αυτή προτείνουμε ένα καινοτόμο μοντέλο διαχείρισης πρόσβασης το Dynamic Spatio Temporal EMergency Role Based Access Control (DSTEM-RBAC), το οποίο βασίζεται στο μοντέλο διαχείρισης πρόσβασης με ρόλους (Role Based Access Control – RBAC). Το DSTEM-RBAC λαμβάνει υπόψη του χρονικούς και χωρικούς περιορισμούς αλλά το σημαντικότερο είναι ότι προσφέρει έναν ελεγχόμενο και ασφαλή τρόπο για να παρακαμφθούν οι στατικές πολιτικές ασφαλείας

χρησιμοποιώντας δυναμικές πληροφορίες για να καταλήξει σε μια απόφαση κατ' εξαίρεση πρόσβασης η οποία θα παρακάμπτει την στατική πολιτική ασφαλείας που εφαρμόζεται.

Στο προτεινόμενο μοντέλο η ιεραρχία των ρόλων αναπαρίσταται ως ένας κατευθυνόμενος γράφος με βάρη, όπου κάθε ρόλος αποτελεί έναν κόμβο. Οι αποστάσεις μεταξύ των κόμβων είναι μια παράμετρος-κλειδί για την προτεινόμενη διαδικασία της κατ' εξαίρεση πρόσβασης. Επί της ουσίας, η απόσταση μεταξύ ρόλων σε συνδυασμό με τους χρονικούς και τους χωρικούς περιορισμούς και η δυναμική πληροφορία καθορίζουν την κατ' εξαίρεση πρόσβαση. Οι δυναμικές πληροφορίες που λαμβάνονται υπόψη αποτελούνται από την τοποθεσία του χρήστη, το επίπεδο ασφαλείας και το επίπεδο έκτατης ανάγκης που βρίσκεται ο οργανισμός καθώς και το επίπεδο των κινδύνων από το διαδίκτυο. Η προτεινόμενη αρχιτεκτονική , η οποία είναι επί της ουσίας μια επέκταση του XACML, αναλύεται σε βάθος και παρουσιάζεται μια πρότυπη υλοποίηση με στόχο να αναδειχθεί η εφαρμοσιμότητα του προτεινόμενου μοντέλου στον χώρο της υγείας.

Επιπλέον, παρέχεται και μια μεθοδολογία για την αξιολόγηση της συμπεριφοράς των χρηστών έτσι ώστε να είναι εφικτό να βελτιστοποιηθεί η παραμετροποίηση που έχει εφαρμοστεί και να εντοπιστεί μια πιθανή κατάχρηση της λειτουργικότητας της κατ' εξαίρεση πρόσβασης. Τέλος, πραγματοποιήθηκε μια έρευνα σε δύο κλινικές ως μελέτες περίπτωσης για την αξιολόγηση των αναγκών που υπάρχει για κατ' εξαίρεση προσβάσεις.

Abstract

Modern information technology systems are characterized by increased complexity and by the obligation to support multiple concurrent users with different needs. In all cases it is a common requirement for all information systems to protect the information stored and managed by them.

In order to be able to successfully protect the resources of a system it is a prerequisite to authenticate users prior to granting them access and enforcing access controls rules thereafter so as to determine what resources and information each user is allowed to access.

The most widely used authentication method used, despite the well-known issues that it faces, is text passwords. Nevertheless, the human ability to remember and recall visual information has been the trigger for intense research in the field of graphical passwords authentication as a more reliable alternative against text-based passwords. However, graphical passwords suffer from user acceptance issues and security weaknesses.

Having identified these shortcomings, in this thesis we present a novel authentication scheme, namely the Novel Authentication with Visual Information (NAVI), based on visual information that generates strong and secure passwords. NAVI utilized as users' credentials the route a user selects in a predefined map. We present a security analysis of NAVI at a theoretical level and we have implemented a prototype that was provided to a number of users in order to evaluate its ease of use and its real-life password generated strength. In addition to that, the users who participated in the aforementioned experiment have answered a questionnaire regarding NAVI's functionality and implementation.

Once a user has been successfully authenticated appropriate access rights should be granted to him. The majority of access control models has been based on the assumption that the users' access rights can be defined a priori. However, in a modern and complex environment emergency and unpredictable situations arise very often, leading to access requests that have not been foreseen by the standard procedures in place. Having identified such a need, we introduce a novel access control model, namely the Dynamic Spatio Temporal EMergency Role Based Access Control (DSTEM-RBAC) which has been based upon the Role Based Access Control (RBAC) model. DSTEM-RBAC takes into account spatiotemporal restrictions and more importantly it provides controllable and secure means to override the defacto security policy of an organization by utilizing static and dynamic information in order to reach a decision whether emergency access should be allowed.

In DSTEM_RBAC, the Role hierarchy is represented as a directed graph with weights, where each role is a node. The distance between nodes is the key parameter for the

proposed emergency access process. In essence, the distance between roles combined with spatiotemporal restrictions and dynamic information determine whether emergency access should be granted. The dynamic information consists of the user's location, its level of trust, the organization's threat level, the organization's emergency status and the internet threats risk level.

The proposed architecture, as implemented in DSTEM-RBAC, is an extension of XACML. A prototype implementation of the model is presented in order to highlight its applicability in the healthcare environment.

In addition to that a methodology was developed to assess the users' behavior so as to provide the means to optimize the DTSTEM-RBAC parameter configuration and also to provide a methodology to detect possible abuses of the emergency access functionality. Finally, a survey was performed in two clinics as a case study for the emergency access process.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

ΠΕΡΙΕΧΟΜΕΝΑ ΠΙΝΑΚΩΝ

ΓΛΩΣΣΑΡΙΟ

Ακρωνύμια	Αγγλικοί Όροι	Ελληνικοί Όροι
	Accountability	Λογοδοσία
	Administrator	Διαχειριστής
	Authentication	Αυθεντικοποίηση
	Authorization	Εξουσιοδότηση
	Availability	Διαθεσιμότητα
ACM	Access Control Matrix	Πίνακας Ελέγχου Πρόσβασης
ACL	Access Control Lists	Λίστες Ελέγχου Πρόσβασης
BTG	Break The Glass	Σπάσιμο Γυαλιού
	Browsers	Φυλλομετρητές
	Brute force attacks	Επιθέσεις δια της Βίας
CL	Capability lists	Λίστες Δυνατοτήτων
	Chinese Wall Security Policy	Πολιτική Κινέζικου Τείχους
	Confidentiality	Εμπιστευτικότητα
	Credentials	Διαπιστευτήρια
DoF	Degrees of Freedom	Βαθμοί Ελευθερίας
DoS	Denial of Service	Άρνηση Υπηρεσίας
	Dictionary Attacks	Επιθέσεις Λεξικού
DAC	Discretionary Access Control	Διακριτικός Έλεγχος Πρόσβασης
DDoF	Dynamic Degrees of Freedon	Δυναμικοί Βαθμοί Ελευθερίας
	Graphical passwords	Κωδικοί Γραφικών
	Guessing attacks	Επιθέσεις Εικασίας
	Identification	Ταυτοποίηση
.	Integrity	Ακεραιότητα

ISP	Internet Service Provider	Πάροχος Υπηρεσιών Διαδικτύου
IDS	Intrusion Detection System	Σύστημα Ανίχνευσης Διείσδυσης
IPS	Intrusion Prevention System	Σύστημα Παρεμπόδισης της Διείσδυσης
	Keyloggers	Καταγραφείς Πληκτρολογίου
LAN	Local Area Network	Τοπικό Δίκτυο
MAC	Mandatory Access Control	Υποχρεωτικός Έλεγχος Πρόσβασης
	Non repudiation	Μη Αποποίηση Ευθυνών
ΛΣ (OS)	Operating System	Λειτουργικό Σύστημα
	User Name	Όνομα Χρήστη
	Passwords	Κωδικοί Ασφαλείας
	Password key space	Χώρος Κωδικών
	Password key subspace	Υποχώρος Κωδικών
	Privacy	Ιδιωτικότητα
	Recall Based	Βασισμένοι στην Ανάκληση
	Recognition Based	Βασισμένοι στην Αναγνώριση
RBAC	Role Based Access Control	Έλεγχος Πρόσβασης Βασισμένος σε Ρόλους
	Route Password	Κωδικός Διαδρομής
	Screenshot	Στιγμιότυπο Οθόνης
	Shoulder surfing	Περιήγηση Ώμου
	Social engineering	Κοινωνική Μηχανική
	Spyware	Λογισμικό Υποκλοπής
	State Machine	Μηχανή Καταστάσεων
SQL	Structured Query Language	Δομημένη Γλώσσα Ερωτημάτων
	Text based Passwords	Κωδικοί Ασφαλείας Κειμένου

	Token	Τεκμήριο
	Triggers	Εναύσματα
VPN	Virtual Private Network	Εικονικό Ιδιωτικό Δίκτυο
VA	Vulnerability Assessment	Αξιολόγηση Ευπαθειών
	Web	Ιστός
WAN	Wide Area Network	Δίκτυο Ευρείας Περιοχής

1. Εισαγωγή

1.1. Ασφάλεια και Απαιτήσεις Ασφάλειας

Στόχος της ασφάλειας πληροφοριών είναι η προστασία των πολύτιμων πόρων ενός οργανισμού. Η διασφάλιση της ασφάλειας των πληροφοριών επιτυγχάνεται μέσα από την επιλογή και εφαρμογή κατάλληλων μηχανισμών συμβάλλοντας στην εκπλήρωση των στόχων του οργανισμού, προστατεύοντας τους οικονομικούς πόρους, τη φήμη, τα πνευματικά δικαιώματα, τους εργαζομένους, τα υλικά και τα άυλα περιουσιακά στοιχεία καθώς και διασφαλίζοντας τη νομική συμμόρφωση με το ισχύον κανονιστικό πλαίσιο.

Συχνά θεωρείται ότι η υλοποίηση μηχανισμών ασφαλείας παρεμποδίζει τη λειτουργία ενός οργανισμού, επειδή επιβάλλει αυστηρούς κανόνες και διαδικασίες οι οποίες επιφέρουν φόρτο σε χρήστες, διαχειριστές και συστήματα. Η ασφάλεια πληροφοριών πράγματι επιφέρει φόρτο εργασίας αλλά το να θεωρείται εμπόδιο για την ομαλή λειτουργία ενός οργανισμού οφείλεται στη μη κατάλληλη χρήση και υλοποίηση των μηχανισμών αυτών για τον οργανισμό. Οι κανόνες ασφαλείας οφείλουν να λειτουργούν προς όφελος της επιχείρησης, να υποστηρίζουν την εύρυθμη λειτουργία της και να συμβάλλουν στην κερδοφορία της. Η ασφάλεια πληροφοριών συχνά πλέον αντιμετωπίζεται ως επιχειρηματικό εργαλείο και παράγοντας διαφοροποίησης από ανταγωνιστικές υπηρεσίες/οργανισμούς.

Η πιο συνήθης προσέγγιση για να οριστεί η ασφάλεια ενός συστήματος είναι η διατήρηση της Εμπιστευτικότητας (Confidentiality), της Ακεραιότητας (Integrity) και της Διαθεσιμότητας (Availability):

- Η εμπιστευτικότητα αναφέρεται στην αποτροπή της, από πρόθεση ή χωρίς, μη εξουσιοδοτημένης αποκάλυψης πληροφορίας ή πόρων.
  - ◊ Απώλεια εμπιστευτικότητας μπορεί να συμβεί με πολλούς τρόπους, όπως για παράδειγμα κατά την εσκεμμένη διαρροή πληροφοριών από κακόβουλη ενέργεια ή κατά την εσφαλμένη ανάθεση δικαιωμάτων πρόσβασης σε χρήστες ενός οργανισμού.
  - ◊ Η εμπιστευτικότητα διασφαλίζεται με χρήση πρωτοκόλλων ασφαλείας κατά τη μεταφορά δεδομένων, με υπηρεσίες ελέγχου και ταυτοποίησης χρηστών καθώς και με κρυπτογράφηση των δεδομένων κατά την αποθήκευση τους.
  - ◊ Το αντίθετο της εμπιστευτικότητας είναι η γνωστοποίηση (Disclosure).
- Η ακεραιότητα αναφέρεται στην αξιοπιστία της πληροφορίας ή/και των πόρων, τη μη τροποποίηση δεδομένων από μη εξουσιοδοτημένους χρήστες αλλά και την επιτρεπόμενη τροποποίηση των δεδομένων από εξουσιοδοτημένους χρήστες και διαδικασίες.
  - ◊ Παράδειγμα απώλειας της ακεραιότητας σε επίπεδο λογισμικού αποτελεί η εισαγωγή κακόβουλου κώδικα σε κάποια εφαρμογή ή στο λειτουργικό

σύστημα. Σε επίπεδο δεδομένων η τροποποίηση δεδομένων συχνά οδηγεί σε οικονομικές απώλειες μέσω απάτης.

- ◊ Η ακεραιότητα εξασφαλίζεται με τη χρήση τειχών προστασίας, λογισμικό το οποίο παρακολουθεί την ακεραιότητα των δεδομένων και του λογισμικού καθώς και με μηχανισμούς ανίχνευσης παρείσφρησης.
- ◊ Το αντίθετο της ακεραιότητας είναι αλλοίωση (Alteration).

- Η διαθεσιμότητα αναφέρεται στην αξιόπιστη και έγκαιρη πρόσβαση σε δεδομένα και υπολογιστικούς πόρους από τους κατάλληλους χρήστες. Δηλαδή η εξασφάλιση της απρόσκοπτης λειτουργίας του συστήματος.
  - ◊ Απώλεια της διαθεσιμότητας μπορεί να συμβεί μετά από κάποια φυσική καταστροφή, όπως μετά από μια πυρκαγιά, ή από κακόβουλες ενέργειες όπως από επιθέσεις άρνησης υπηρεσίας (Denial of Service Attacks – DoS).
  - ◊ Η διαθεσιμότητα εξασφαλίζεται με περιορισμένη ανοχή σφαλμάτων, με τη χρήση αντιγράφων ασφαλείας, με τη χρήση τειχών προστασίας με τον έλεγχο πρόσβασης χρηστών και με διαδικασίες αντιμετώπισης περιστατικών ασφαλείας.
  - ◊ Το αντίθετο της διαθεσιμότητας είναι η καταστροφή (Disaster).

Το παραπάνω τρίπτυχο είναι ευρέως αποδεκτό και χρησιμοποιείται κατά κόρον για την αξιολόγηση του επίπεδου ασφαλείας ενός πληροφοριακού συστήματος. Οι έλεγχοι ασφαλείας που πραγματοποιούνται συχνά περιστρέφονται γύρω από την διατήρηση αυτών των ιδιοτήτων.

Ωστόσο μια πιο ολοκληρωμένη προσέγγιση στην ασφάλεια πληροφοριών θα πρέπει να περιλαμβάνει και τις ακόλουθες έννοιες.

- *Ταυτοποίηση (Identification)*: Η δυνατότητα αναγνώρισης της ταυτότητας ενός χρήστη σχετίζεται με τις διαδικασίες της αυθεντικοποίησης και της εξουσιοδότησης.
- *Αυθεντικοποίηση (Authentication)*: Η πιστοποίηση της ταυτότητας ενός χρήστη εξασφαλίζει ότι ο χρήστης είναι αυτός που διατείνεται ότι είναι.
- *Λογοδοσία (Accountability)*: Η ικανότητα ενός συστήματος να μπορεί να αποδώσει τις ενέργειες που έχουν πραγματοποιηθεί σε συγκεκριμένο άτομο ή σύστημα.
- *Μη Αποποίηση Ευθυνών (nonrepudiation)*: Να μην μπορεί κάποιος να αρνηθεί μια ενέργεια που έχει εκτελέσει.
- *Εξουσιοδότηση (Authorization)*: Αφορά στα δικαιώματα που έχουν εκχωρηθεί σε έναν χρήστη και επιτρέπουν τη χρήση ενός υπολογιστικού πόρου. Μετά την επιτυχή αυθεντικοποίηση ενός χρήστη καθορίζει τα επίπεδα εξουσιοδότησης και τα δικαιώματα πρόσβασης που θα πρέπει να αποδοθούν.
- *Ιδιωτικότητα (Privacy)*: Η έννοια αυτή καθορίζει το επίπεδο εμπιστευτικότητας που διαθέτει ένας χρήστης στο σύστημα, καθώς και το επίπεδο προστασίας του απορρήτου που διατίθεται στο χρήστη από το σύστημα.

Ένα σύστημα για να είναι ασφαλές θα πρέπει να έχει την δυνατότητα να γνωρίζει την ταυτότητα του χρήστη που αποκτά πρόσβαση στις παρεχόμενες υπηρεσίες και πόρους. Στην πράξη, οι δύο βασικοί λόγοι που είναι πολύτιμη η αυθεντικοποίηση είναι το γεγονός ότι αφενός η ταυτότητα του χρήστη είναι μια σημαντική παράμετρος στον καθορισμό

των δικαιωμάτων πρόσβασης και αφετέρου ώστε να μπορούν να διατηρούνται αρχεία καταγραφής με τις ενέργειες των χρηστών.

Η αυθεντικοποίηση για να είναι αποτελεσματική θα πρέπει αφενός να είναι εύχρηστη για τον τελικό χρήστη και αφετέρου να παρέχει υψηλό επίπεδο αξιοπιστίας.

Για την αυθεντικοποίηση των χρηστών μπορεί να χρησιμοποιηθούν βιομετρικά στοιχεία, κάποιο ειδικό τεκμήριο (token), ψηφιακά πιστοποιητικά αλλά και, οι πιο διαδεδομένοι, κωδικοί πρόσβασης. Η αυθεντικοποίηση μιας μηχανής με μια μηχανή πραγματοποιείται με κωδικούς πρόσβασης ή πιο συχνά με ψηφιακά πιστοποιητικά ή κάποιο άλλο μηχανισμό βασισμένο στην κρυπτογραφία.

Έχοντας αυθεντικοποιηθεί σε ένα σύστημα ο χρήστης έχει το δικαίωμα να δημιουργήσει αρχεία, να αποκτήσει πρόσβαση σε πληροφορία κτλ. Τους τελικούς χρήστες δεν τους ενδιαφέρει να γνωρίζουν τους μηχανισμούς που υλοποιούνται ούτε και οι χαμηλού επιπέδου λεπτομέρειες υλοποίησης των πολιτικών ασφαλείας. Οι χρήστες επιθυμούν να αποκτήσουν πρόσβαση στους πόρους που χρειάζονται για να εκτελέσουν τις εργασίες τους.

Ανάλογα με τις ιδιαιτερότητες του υπολογιστικού περιβάλλοντος και τους χρήστες που χρειάζονται πρόσβαση σε πόρους έχει προταθεί και υλοποιηθεί πληθώρα από μοντέλα διαχείρισης πρόσβασης. Δεδομένου ότι πλέον τα υπολογιστικά συστήματα έχουν γίνει πιο πολύπλοκα και έχουν διεισδύσει στην ζωή μας έχει παρουσιαστεί η ανάγκη της διαχείρισης πρόσβασης με πιο δυναμικές μεθόδους.

1.2. Αντικείμενο και συμβολή της διατριβής

Αντικείμενο μελέτης της παρούσας διατριβής είναι η αυθεντικοποίηση (ποιος είσαι;) και κατόπιν η διαχείριση πρόσβασης (τι μπορείς να κάνεις;) υπό το πρίσμα των προκλήσεων που έχουν ανακύψει ως συνέπεια της αυξανόμενης χρήσης των πληροφοριακών συστημάτων σε πολλές πτυχές της καθημερινής μας ζωής.

Την περιοχή έρευνας της διατριβής αποτελούν η αυθεντικοποίηση με χρήση γραφικών κωδικών πρόσβασης και η διαχείριση πρόσβασης με χρήση ρόλων σε καταστάσεις έκτακτης ανάγκης. Η αυθεντικοποίηση αποτελεί προαπαιτούμενο για την υλοποίηση κανόνων διαχείρισης πρόσβασης και την απόδοση δικαιωμάτων πρόσβασης σε χρήστες.

Όσον αφορά την αυθεντικοποίηση των χρηστών παραμένουμε σε μεγάλο βαθμό εξαρτημένοι από την χρήση κωδικών ασφαλείας, οι οποίοι, παρά τις γνωστές αδυναμίες τους, παραμένουν το κυρίαρχο μέσο αυθεντικοποίησης καθώς υπάρχει έλλειψη αξιόπιστων και εύχρηστων εναλλακτικών λύσεων. Από την άλλη, τα υπάρχοντα μοντέλα εξουσιόδοτησης και διαχείρισης πρόσβασης δεν μπορούν να ανταποκριθούν ικανοποιητικά σε περιπτώσεις που το περιβάλλον είναι δυναμικό.

Οι δύο πυλώνες στους οποίους βασίζεται η έρευνα που παρουσιάζεται είναι οι ακόλουθοι:

- Η ανάπτυξη μιας καινοτόμου μεθόδου αυθεντικοποίησης η οποία παρέχει ασφάλεια και αξιοπιστία υψηλού επιπέδου ενώ παραμένει εύχρηστη και φιλική στον τελικό χρήστη

- Η ανάπτυξη ενός μοντέλου διαχείρισης πρόσβασης το οποίο θα εμπεριέχει λειτουργικότητα για τη διαχείριση εξουσιοδοτήσεων σε καταστάσεις εκτάκτου ανάγκης λαμβάνοντας υπόψη της δυναμικές παραμέτρους

Η μέθοδος αυθεντικοποίησης που προτείνεται αποτελεί μέρος της οικογένειας των γραφικών κωδικών ασφαλείας. Η ανθρώπινη ικανότητα να απομνημονεύει αποτελεσματικότερα οπτικές πληροφορίες έχει αποτελέσει το έναυσμα για την ανάπτυξη μοντέλων αυθεντικοποίησης που εκμεταλλεύονται αυτή ακριβώς την ιδιότητα. Στην προτεινόμενη μέθοδο αυθεντικοποίησης (Novel Authentication with Visual Information - NAVI) ο χρήστης καλείται να δημιουργήσει μια διαδρομή σε έναν προκαθορισμένο χάρτη και κατόπιν να αναπαραγάγει τη διαδρομή αυτή κατά το στάδιο της αυθεντικοποίησής του.

Η συμβολή της διατριβής στον τομέα της αυθεντικοποίησης συνοψίζεται στις ακόλουθες περιοχές:

- Πρόταση καινοτόμου μοντέλου αυθεντικοποίησης, το οποίο είναι βασισμένο σε οπτική πληροφορία και η θεωρητική θεμελίωσή του.
- Πρότυπη υλοποίηση του καινοτόμου μοντέλου αυθεντικοποίησης..
- Αξιολόγηση της ασφάλειας του παραγόμενου κωδικού του NAVIσε θεωρητικό επίπεδο και σύγκρισή του με παραδοσιακούς κωδικούς κειμένου και με άλλα μοντέλα γραφικών κωδικών
- Δοκιμή χρηστών για την αξιολόγηση της ευκολίας χρήσης.
- Δοκιμή χρηστών για την αξιολόγηση του παραγόμενου κωδικού.
- Έρευνα χρηστών (ερωτηματολόγιο) για την αξιολόγηση διαφόρων παραμέτρων χρήσης του NAVI.

Η διαχείριση πρόσβασης με χρήση ρόλων αποτελεί ένα ευρέως διαδεδομένο μοντέλο με πληθώρα υλοποιήσεων σε πληροφοριακά συστήματα και με ενεργό ερευνητικό έργο από την αρχική του πρόταση μέχρι και σήμερα. Βασισμένοι στο RBAC (Role Based Access Control) αναπτύξαμε το DSTEM-RBAC - ένα μοντέλο που εμπεριέχει της βασικές αρχές του RBAC εμπλουτισμένες με δυνατότητες επιβολής χρονικών και χωρικών περιορισμών καθώς και με μια καινοτόμο μέθοδο απόδοσης δικαιωμάτων πρόσβασης σε χρήστες σε καταστάσεις έκτακτης ανάγκης κάνοντας χρήση των ιεραρχιών των ρόλων. Οι ρόλοι αναπαρίστανται ως κατευθυνόμενοι γράφοι και οι αποστάσεις μεταξύ τους σε συνδυασμό με μια σειρά δυναμικών παραμέτρων καθιστούν δυνατή την ελεγχόμενη απόδοση δικαιωμάτων σε καταστάσεις έκτακτης ανάγκης.

Η συμβολή της διατριβής στον τομέα της διαχείρισης πρόσβασης συνοψίζεται στις ακόλουθες περιοχές:

- Πρόταση καινοτόμου μοντέλου διαχείρισης πρόσβασης το οποίο είναι βασισμένο σε ρόλους που λαμβάνει υπόψη χρονικούς και χωρικούς περιορισμούς διαχείρισης πρόσβασης καθώς και την ιεραρχία ρόλων σε καταστάσεις έκτακτης ανάγκης.
- Επέκταση της λειτουργικότητας διαχείρισης πρόσβασης σε καταστάσεις έκτακτης ανάγκης με χρήση δυναμικών παραμέτρων.
- Πρότυπη υλοποίηση του καινοτόμου μοντέλου διαχείρισης πρόσβασης.
- Έρευνα χρηστών (ερωτηματολόγιο) από τον χώρο της υγείας για την αξιολόγηση των αναγκών πρόσβασης σε έκτακτες περιστάσεις.

- Μεθοδολογία αξιολόγησης της χρήσης του μηχανισμού πρόσβασης σε καταστάσεις έκτακτης ανάγκης και μεθοδολογία παραμετροποίησης του μοντέλου.
- Παρουσίαση περίπτωσης μελέτης με χρήση των παραμέτρων και των λειτουργιών του DSTEM-RBAC.

1.3. Δομή της Διατριβής

Στο τρέχον κεφάλαιο παρουσιάστηκαν οι ερευνητικές περιοχές που αποτελούν το αντικείμενο της διατριβής και εν συνεχεία οι ερευνητικοί στόχοι και η προσφορά της διατριβής. Το πρώτο κεφάλαιο καταλήγει με την παρουσίαση της δομής του υπολοίπου της διατριβής.

Στο δεύτερο κεφάλαιο, πραγματοποιείται μια παρουσίαση των κυρίαρχων μοντέλων διαχείρισης πρόσβασης και εν συνεχεία παρουσιάζεται αναλυτικά το RBAC καθώς και παραλλαγές και βελτιώσεις του. Τέλος, παρουσιάζονται και υπάρχοντα μοντέλα ελέγχου πρόσβασης σε καταστάσεις εκτάκτου ανάγκης.

Στο τρίτο κεφάλαιο, περιγράφεται το προτεινόμενο μοντέλο STEM-RBAC για έλεγχο της πρόσβασης σε καταστάσεις εκτάκτου ανάγκης. Κατόπιν παρουσιάζεται και η επέκταση αυτού η οποία περιλαμβάνει δυναμικές παραμέτρους, το DSTEM-RBAC. Παρουσιάζεται ως περίπτωση μελέτης το περιβάλλον της υγείας όπου και αναλύονται οι παράμετροι του μοντέλου. Τέλος, παρουσιάζονται τα αποτελέσματα έρευνας που πραγματοποιήθηκε σε κλινικές για την αξιολόγηση της χρησιμότητας χρήσης μοντέλων ελέγχου πρόσβασης σε καταστάσεις εκτάκτου ανάγκης.

Στο τέταρτο κεφάλαιο, παρουσιάζεται μια ανάλυση των κωδικών πρόσβασης όσον αφορά στην ασφάλειά τους και τα συνήθη προβλήματα που αντιμετωπίζουν. Επιπλέον, παρουσιάζονται οι κύριες προτάσεις γραφικών κωδικών πρόσβασης με τα πλεονεκτήματά τους αλλά και τα ζητήματα προς επίλυση που παραμένουν. Τέλος, επιχειρείται μια ανάλυση και σύγκριση της εντροπίας μεταξύ του προτεινόμενου μοντέλου και άλλων γνωστών μοντέλων αυθεντικοποίησης. Η εντροπία αποτελεί το μέτρο που καθορίζει την τυχαιότητα και, συνεπώς, την ασφάλεια, των κωδικών πρόσβασης (κλασικών και γραφικών).

Στο πέμπτο κεφάλαιο, αναλύεται το προτεινόμενο μοντέλο γραφικών κωδικών ασφαλείας, με ονομασία Πρότυπη Αυθεντικοποίηση με χρήση Οπτικής Πληροφορίας - Novel Authentication using Visual Information (NAVI). Περιγράφεται αναλυτικά το μοντέλο, η μέθοδος αυθεντικοποίησης, ο τρόπος υπολογισμού του κωδικού και παρουσιάζεται η υλοποίηση που έχει πραγματοποιηθεί. Επιπρόσθετα, παρουσιάζεται η αξιολόγηση του NAVI. Η αξιολόγηση βασίζεται σε τρεις άξονες: στην αξιολόγηση από τελικούς χρήστες μέσω ερωτηματολογίου, στην ανάλυση των αποτελεσμάτων από τις προσπάθειες των χρηστών να αυθεντικοποιηθούν και, τέλος, στην αξιολόγηση του πόσο

ισχυροί είναι οι κωδικοί πρόσβασης που δημιουργούνται με βάση την εκτιμώμενη παραγόμενη εντροπία.

Στο έκτο κεφάλαιο συνοψίζονται τα αποτελέσματα της έρευνας που παρουσιάστηκαν στο πλαίσιο της διατριβής καθώς και τα σχετικά συμπεράσματα. Τέλος, δίδονται οι κατευθύνσεις της μελλοντικής έρευνας στον ερευνητικό αυτό χώρο και πιθανές επεκτάσειστων προτεινόμενων λύσεων.

2. Διαχείριση Πρόσβασης

2.1. Πολιτικές και Μοντέλα Ελέγχου Πρόσβασης

Καθώς εξελίσσονται τα πληροφοριακά συστήματα, διαφοροποιούνται και οι ανάγκες για τη διαχείριση της πρόσβασης των χρηστών (*υποκείμενο*) σε πόρους του εκάστοτε συστήματος (*αντικείμενο*).

Στο παρόν κεφάλαιο θα παρουσιαστούν τα πιο διαδεδομένα μοντέλα ελέγχου πρόσβασης συμπεριλαμβανομένου και του κυρίαρχου στο χώρο της διαχείρισης πρόσβασης μοντέλου, του RBAC. Συγκεκριμένα για το RBAC θα παρουσιαστούν και μια σειρά από επεκτάσεις που έχουν προταθεί. Τέλος, γίνεται αναφορά στα μοντέλα πρόσβασης σε καταστάσεις εκτάκτου ανάγκης γνωστά και ως μοντέλα για *Σπάσιμο Του Γυαλιού (Break The Glass – BTG)*.

2.1.1. Πίνακες Πρόσβασης

Ένας βασικός τρόπος απεικόνισης των δικαιωμάτων πρόσβασης είναι μέσω της χρήσης *πινάκων ελέγχου πρόσβασης (access control matrices*) [L74], [GD72]. Τα δικαιώματα πρόσβασης ορίζονται με την μορφή ενός πίνακα δύο διαστάσεων όπου καταγράφονται οι πιθανές καταστάσεις του ελέγχου πρόσβασης.

Κάθε σειρά του πίνακα αποτελεί ένα υποκείμενο ενώ κάθε στήλη αντιπροσωπεύει ένα αντικείμενο. Στα κελιά καταγράφονται τα δικαιώματα. Ο πίνακας μπορεί να περιγραφεί με ένα σύνολο τριπλετών. Μια τριπλέτα (Υ, Α, Δ) περιγράφει μία κατάσταση όπου το Υ είναι το υποκείμενο το οποίο έχει το δικαίωμα Δ στο αντικείμενο Α. Τα δικαιώματα που καταγράφονται σε ένα πίνακα πρόσβασης είναι για παράδειγμα δικαιώματα *Ανάγνωσης (Read), Γραφής (Write), Εκτέλεσης (Execute)* και *Ιδιοκτησίας (Ownership)*. Το δικαίωμα της Ιδιοκτησίας καθορίζει τη δυνατότητα ενός υποκειμένου να αλλάζει τα δικαιώματα πρόσβασης σε ένα αντικείμενο.

Στον Πίνακας 1: Πίνακας Πρόσβασης παρουσιάζεται ένα απλό παράδειγμα πίνακα πρόσβασης με τρία υποκείμενα και τέσσερα αντικείμενα όπου καθορίζεται τι ενέργειες επιτρέπονται από κάθε υποκείμενο σε κάθε αντικείμενο λ.χ. R: read, W: write, O: own, E: execute.

Πίνακας 1: Πίνακας Πρόσβασης

	Αντικείμενο 1	**Αντικείμενο 2**	**Αντικείμενο 3**	**Αντικείμενο 4**
Υποκείμενο 1		O	E	
Υποκείμενο 2	R	R,W,E		R
Υποκείμενο 3	O	E,R		R,W

Υποκείμενο 1		O	E	

Σε ένα σύστημα μπορεί να συμβούν πολλές αλλαγές στα δικαιώματα πρόσβασης των αντικειμένων, το οποίο αντιστοιχεί σε μεταβάσεις από μία κατάσταση του πίνακα σε μία άλλη. Η κατάσταση ενός πίνακα πρόσβασης είναι η εικόνα των δικαιωμάτων πρόσβασης τα οποία αυτός παρουσιάζει σε μία δεδομένη χρονική στιγμή.

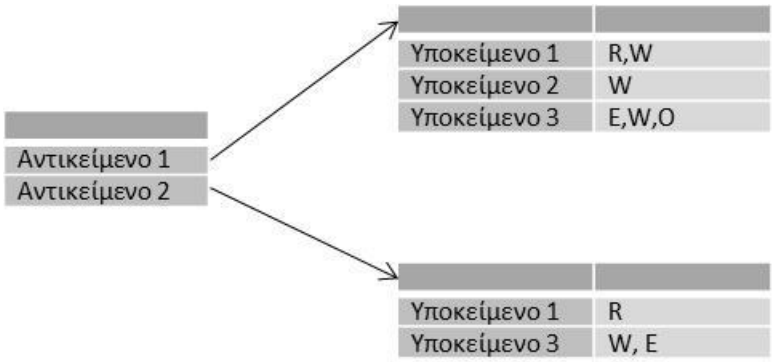
Η απλή δομή των δύο διαστάσεων και η ευκολία κατανόησής της είναι τα βασικά πλεονεκτήματα χρήσης των πινάκων πρόσβασης. Ωστόσο ο πίνακας ελέγχου πρόσβασης δεν κλιμακώνεται εύκολα με την αύξηση του μεγέθους των χρηστών ή / και των πόρων του συστήματος. Σε ένα μεγάλο σύστημα με πολλούς χρήστες και πολλά αντικείμενα, ο πίνακας ελέγχου πρόσβασης θα ήταν πολύ μεγάλος σε μέγεθος και θα περιείχε πολλά άδεια κελιά. Εξαιτίας αυτής της μη προσαρμοστικότητάς τους και της δυσκολίας διαχείρισής τους σε αλλαγές μεγέθους κλίμακας (non scalability), συχνά χρησιμοποιούνται στην πράξη παραλλαγές του πίνακα πρόσβασης: οι λίστες ελέγχου πρόσβασης και οι λίστες δυνατοτήτων που παρουσιάζονται παρακάτω.

2.1.2. Λίστες Ελέγχου Πρόσβασης

Οι λίστες ελέγχου πρόσβασης (Access Control Lists- ACL) αποτελούν λίστες με δικαιώματα που χαρακτηρίζουν κάποιο συγκεκριμένο αντικείμενο. Κάθε αντικείμενο συνδέεται με μία λίστα ελέγχου πρόσβασης η οποία περιλαμβάνει τα υποκείμενα καθώς και τις προσβάσεις που αυτά έχουν πάνω στο αντικείμενο [HFK06]. Επομένως, σε μια λίστα, κάθε καταχώριση περιλαμβάνει δύο πεδία: το υποκείμενο και τις προσβάσεις-λειτουργίες που είναι εξουσιοδοτημένο το υποκείμενο να εκτελέσει στο αντικείμενο.

Το βασικό πλεονέκτημα των λιστών ελέγχου πρόσβασης είναι ότι καθιστούν εύκολη και γρήγορη την εύρεση των χρηστών που έχουν πρόσβαση σε ένα αντικείμενο, καθώς και των λειτουργιών που οι τελευταίοι μπορούν να επιτελέσουν πάνω στο αντικείμενο, ελέγχοντας τη λίστα του αντικειμένου. Επιπλέον, επιτρέπουν την εύκολη ανάκληση της πρόσβασης σε ένα αντικείμενο μέσω της απλής διαγραφής της αντίστοιχης καταχώρισης της λίστας [SS94].

Μειονεκτούν όμως σε σχέση με τους πίνακες στην περίπτωση που θέλουμε να προσδιορίσουμε όλες τις προσβάσεις ενός υποκειμένου στο σύστημα οπότε και θα πρέπει να ελεγχθεί η ACL κάθε αντικειμένου. Στην Εικόνα 1, παρουσιάζεται μια απεικόνιση μιας απλής λίστας ελέγχου πρόσβασης. Όπου φαίνεται για δύο αντικείμενα σε ποια υποκείμενα έχουν πρόσβαση, και τα ακριβή δικαιώματά τους.



Εικόνα 1. Λίστα Ελέγχου Πρόσβασης

Ένα επιπλέον πλεονέκτημα που προσφέρουν οι λίστες ελέγχου πρόσβασης είναι ότι μπορεί να περιοριστεί το μέγεθός τους συνδέοντας το κάθε αντικείμενο με ομάδες χρηστών που έχουν κοινή πρόσβαση σε αυτό αντί με κάθε έναν μεμονωμένο χρήστη της ομάδας [FKC07].

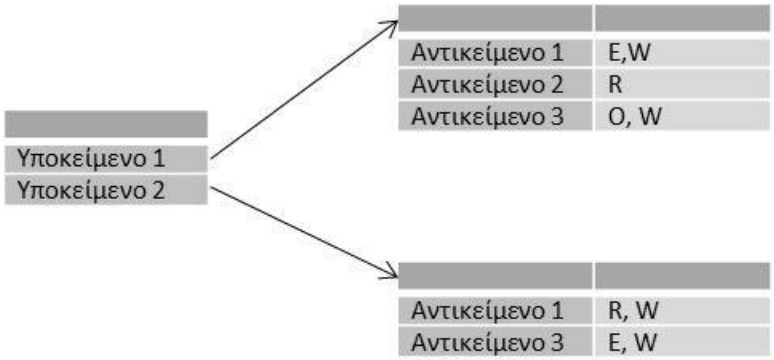
Τα παραπάνω πλεονεκτήματα των λιστών ελέγχου πρόσβασης τις καθιστούν κατάλληλες για την υλοποίηση αντικειμενοστρεφών πολιτικών όπως του *διακριτικού ελέγχου πρόσβασης (DAC - Discretionary Access Control*).

2.1.3. Λίστες Δυνατοτήτων

Εάν χρησιμοποιήσουμε τον πίνακα ελέγχου πρόσβασης ανά γραμμή παίρνουμε συγκεντρωμένα όλα τα δικαιώματα πρόσβασης ενός υποκειμένου. Η δομή αυτή καλείται λίστα δυνατοτήτων και κάθε στοιχείο της, που λέγεται Δυνατότητα, προσδιορίζει ένα αντικείμενο και όλα τα δικαιώματα πρόσβασης που έχει το υποκείμενο πάνω σε αυτό [FKC07]. Επομένως, κάθε υποκείμενο συνδέεται με μια λίστα δυνατοτήτων που αποθηκεύει για κάθε αντικείμενο στο σύστημα τις λειτουργίες που το υποκείμενο είναι εξουσιοδοτημένο να εκτελέσει [SS94]. Η πρόσβαση σε ένα αντικείμενο επιτρέπεται μόνο αν το υποκείμενο το οποίο τη ζητά έχει δυνατότητα για το αντικείμενο αυτό.

Οι λίστες Δυνατοτήτων (Capability lists) διευκολύνουν την επισκόπηση και την εύρεση όλων των προσβάσεων που έχει ένα υποκείμενο με απλή εξέταση της λίστας δυνατοτήτων του. Ωστόσο, δεν είναι εύχρηστες εάν επιθυμούμε να εντοπίσουμε τους χρήστες που έχουν πρόσβαση σε ένα αντικείμενο καθώς απαιτείται έλεγχος της λίστας δυνατοτήτων κάθε υποκειμένου. Επιπρόσθετα, είναι δύσκολη η ανάκληση της άδειας πρόσβασης σε ένα αντικείμενο [B03].

Μία απεικόνιση της λίστας δυνατοτήτων παρουσιάζεται στην Εικόνα 2, όπου φαίνεται για δύο υποκείμενα ποια αντικείμενα έχουν πρόσβαση σε αυτά, καθώς και τα ακριβή δικαιώματά τους.



Εικόνα 2. Λίστα Δυνατοτήτων

2.1.4. Διακριτικός Έλεγχος Πρόσβασης

Η πολιτική Διακριτικού Ελέγχου Πρόσβασης αποτελεί ένα μέσο περιορισμού της πρόσβασης στα αντικείμενα με βάση την ταυτότητα των υποκειμένων ή και των ομάδων στις οποίες ανήκουν τα υποκείμενα. Οι έλεγχοι πρόσβασης είναι διακριτικοί με την έννοια ότι ένα υποκείμενο που έχει συγκεκριμένη άδεια πρόσβασης σε ένα αντικείμενο μπορεί να μεταβιβάσει την άδεια αυτή (άμεσα ή έμμεσα) σε οποιοδήποτε άλλο χρήστη [DOD85].

Πρόκειται για τον πιο συνηθισμένο μηχανισμό ελέγχου πρόσβασης που δίνει τη δυνατότητα στους χρήστες του συστήματος να επιτρέπουν ή να απαγορεύουν την πρόσβαση των υπολοίπων χρηστών στους πόρους που αυτοί ελέγχουν. Επομένως, στην πολιτική DAC έχουμε ελεύθερη διακίνηση της πληροφορίας και οι κανόνες της πολιτικής καθορίζονται αποκλειστικά και μόνο από τους ιδιοκτήτες της πληροφορίας [NCSC87].

Όπως προκύπτει από τα παραπάνω, για να μπορέσουμε να παράσχουμε το μηχανισμό DAC χρειαζόμαστε την έννοια της «ιδιοκτησίας» των αντικειμένων, όπου «ιδιοκτήτης» ενός αντικειμένου είναι αυτός που μεταβιβάζει ή ανακαλεί δικαιώματα προσπέλασης σε άλλους χρήστες-υποκείμενα. Συνήθως, «ιδιοκτήτης» ενός αντικειμένου είναι ο δημιουργός του ο οποίος έχει και τον πλήρη έλεγχο της πρόσβασης σε αυτό [FKC07].

Ένας μηχανισμός DAC αφήνει στη διακριτική ευχέρεια του χρήστη που έχει κάποιο συγκεκριμένο δικαίωμα προσπέλασης πάνω σε ένα αντικείμενο τη δυνατότητα να το μεταβιβάσει σε κάποιο άλλο χρήστη ή να το ανακαλέσει από αυτόν χωρίς να απαιτείται η διαμεσολάβηση του διαχειριστή του συστήματος [NCSC87]. Ο πιο συνηθισμένος μηχανισμός για την υλοποίηση της πολιτικής DAC είναι μέσω της χρήσης των λιστών ελέγχου πρόσβασης (ACLs). Ειδικότερα, κάθε αντικείμενο συνδέεται με μία ACL που βασίζεται στο διακριτικό έλεγχο πρόσβασης, δηλαδή περιέχει τους χρήστες και τις ομάδες των χρηστών στις οποίες έχει επιτρέψει πρόσβαση ο ιδιοκτήτης του αντικειμένου καθώς και τις επιτρεπτές λειτουργίες που μπορούν να επιτελέσουν σε αυτό.

Έχουν προταθεί αρκετές παραλλαγές του DAC. Θα παρουσιάσουμε συνοπτικά τις πιο σημαντικές:

- Αυστηρό DAC (Strict DAC): μόνο ο «ιδιοκτήτης» του αντικειμένου μπορεί να παραχωρήσει άδεια πρόσβασης στο αντικείμενο. Η ιδιοκτησία δε μπορεί να μεταβιβαστεί σε άλλο χρήστη.
- Φιλελεύθερο DAC (Liberal DAC) Ο ιδιοκτήτης του αντικειμένου μπορεί να αναθέσει την «εξουσία»- ιδιότητα που έχει να παραχωρεί άδεια προσπέλασης και σε άλλους χρήστες.

Στην περίπτωση του φιλελεύθερου DAC ενδέχεται να υπάρχει η δυνατότητα ο ιδιοκτήτης του αντικειμένου να μπορεί να μεταβιβάσει τη δυνατότητα που έχει να παραχωρεί άδεια προσπέλασης στο αντικείμενο σε ένα άλλο χρήστη ο οποίος όμως δεν μπορεί να τη μεταβιβάσει περαιτέρω (μεταβίβαση πρώτου επιπέδου – one level grant). Στην περίπτωση μεταβίβασης δευτέρου επιπέδου (two- level grant) ένας χρήστης που έχει λάβει από τον ιδιοκτήτη του αντικειμένου άδεια προσπέλασης σε αυτό μπορεί να την μεταβιβάσει σε ένα τρίτο χρήστη. Δεν μπορεί να γίνει όμως περαιτέρω μεταβίβαση. Αντίστοιχα, στην περίπτωση πολυεπίπεδης μεταβίβασης (multilevel grant) οποιοσδήποτε χρήστης έχει λάβει άδεια προσπέλασης σε ένα αντικείμενο μπορεί να την μεταβιβάσει σε οποιοδήποτε άλλο χρήστη χωρίς να υπάρχει περιορισμός στις μεταβιβάσεις.

Οι πολιτικές DAC αποτελούν μια ευρέως διαδεδομένη μέθοδο ελέγχου πρόσβασης εξαιτίας της μεγάλης ευελιξίας που προσφέρουν και της εύκολης εξοικείωσης των χρηστών με αυτές.

Παρά τη διαδεδομένη χρήση τους οι πολιτικές DAC έχουν ένα σημαντικό μειονέκτημα: δεν μπορούν να ελέγξουν και να διασφαλίσουν τη ροή της πληροφορίας σε ένα σύστημα καθώς η παραχώρηση του δικαιώματος ανάγνωσης είναι μεταβατική, συνεπώς η διάδοση της πληροφορίας δεν ελέγχεται και δεν επιβάλλεται κανένας περιορισμός στη χρησιμοποίηση της πληροφορίας από τη στιγμή που κάποιος χρήστης αποκτήσει πρόσβαση σε αυτή.

2.1.5. Υποχρεωτικός Έλεγχος Πρόσβασης

Οι πολιτικές ασφάλειας που ορίζονται για συστήματα που χρησιμοποιούνται για την προσπέλαση και τη διαχείριση απόρρητων ή άλλων ευαίσθητων πληροφοριών θα πρέπει να προβλέπουν τρόπους εφαρμογής αυστηρών κανόνων ελέγχου πρόσβασης. Για την κάλυψη τέτοιων αναγκών αναπτύχθηκε η Πολιτική Πολλαπλών Επιπέδων (Multi-Level Security Policy) ή αλλιώς Πολιτική Υποχρεωτικού Ελέγχου Πρόσβασης (Mandatory Access Control).

Ο έλεγχος προσπέλασης βασίζεται στην άμεση σύγκριση της εξουσιοδότησης του χρήστη σε ό,τι αφορά την πληροφορία που ζητά να έχει πρόσβαση καθώς και της ταξινόμησης της πληροφορίας, καθώς και σε φυσικούς ή άλλους περιβαλλοντολογικούς

παράγοντες. Οι κανόνες υποχρεωτικού ελέγχου πρόσβασης πρέπει να εκφράζουν με ακρίβεια τους κανόνες και τις γενικές πολιτικές οι οποίες πρέπει να υλοποιηθούν [DOD85].

Η εφαρμογή της πολιτικής είναι υποχρεωτική για όλες τις οντότητες του πληροφοριακού συστήματος. Για όλους τους πόρους και τις πληροφορίες του συστήματος καθορίζονται ετικέτες ασφάλειας που δηλώνουν το βαθμό ευαισθησίας ή διαβάθμισης σύμφωνα με τη κρισιμότητα και τον βαθμό εμπιστευτικότητας τους [DS07].

Οι πολιτικές MAC λόγω του «αυστηρού» και πολύ τυπικού ύφους του ελέγχου πρόσβασης που παρέχουν χρησιμοποιούνται κατά κύριο λόγο σε περιβάλλοντα όπου γίνεται διαχείριση κρίσιμων δεδομένων λ.χ. σε στρατιωτικά πληροφοριακά συστήματα, συστήματα δηλαδή όπου βρίσκει κατά κόρον εφαρμογή η αρχή του «*γνωρίζω-ό,τι-χρειάζεται» (need-to-know)*. Στα συστήματα αυτά, η πληροφορία διαβαθμίζεται ως *αταξινόμητη (unclassified –U), εμπιστευτική (confidential – C), μυστική (secret –S), και άκρως μυστική (top secret – TP).* Οι χαρακτηρισμοί αυτοί αποτελούν τα στοιχεία ενός ιεραρχικού μοντέλου που μπορεί να απεικονιστεί με την εξής συσχέτιση επιπέδων: TS ≥ S ≥ C ≥ U καθορίζοντας με αυτό τον τρόπο τα επίπεδα ασφάλειας. Πέραν αυτών, μπορεί να αναφέρονται και μη ιεραρχικοί χαρακτηρισμοί (κατηγορίες), π.χ. “NUCLEAR”. Μία ετικέτα, λοιπόν, αποτελείται από ένα επίπεδο ασφάλειας και μία κατηγορία ενώ μπορούμε να πούμε ότι υπερτερεί μιας άλλης στην περίπτωση που το επίπεδο ασφάλειάς της είναι μεγαλύτερο ή ίσο από αυτό της άλλης ετικέτας και ο χαρακτηρισμός της κατηγορίας της περικλείει την κατηγορία της άλλης [FKC07], [DS07].

Αντίστοιχα, ορίζονται και επίπεδα ασφάλειας για τους χρήστες του συστήματος που ορίζουν σε ποιες πληροφορίες και πόρους έχουν άδεια να αποκτήσουν πρόσβαση και με ποιον τρόπο (R-W-E). Η πρόσβαση επιτρέπεται μόνο σε χρήστες με συγκεκριμένα επίπεδα εξουσιοδότησης ή άδεια χρήσης και μόνο εφόσον ικανοποιούνται οι παρακάτω βασικοί κανόνες:

- Το επίπεδο ασφάλειας που αντιστοιχεί στο χρήστη που ζητά άδεια πρόσβασης θα πρέπει να είναι τουλάχιστον ίσο με το βαθμό διαβάθμισης της πληροφορίας.
- Η άδεια προσπέλασης στην πληροφορία δε θα οδηγήσει σε υποβιβασμό της ετικέτας ασφάλειας της πληροφορίας. Δηλαδή, δεν θα δοθεί η δυνατότητα αυτή να εγγραφεί σε πληροφορία χαμηλότερου επιπέδου με αποτέλεσμα να αλλάξει ο βαθμός ευαισθησίας της.

Αλλαγές στις ετικέτες ασφάλειας μπορούν να κάνουν μόνο οι διαχειριστές του συστήματος και όχι οι ιδιοκτήτες των αρχείων. Με αυτό τον τρόπο, το επίπεδο ασφάλειας σε ό,τι αφορά την προσπέλαση στην πληροφορία από τους χρήστες είναι το μέγιστο δυνατό αφού περιορίζονται οι ενέργειες που μπορούν να εκτελέσουν οι χρήστες [FKC07]**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**.

Αντιπροσωπευτικότερο μοντέλο της πολιτικής του Υποχρεωτικού Ελέγχου Πρόσβασης αποτελεί το μοντέλο Bell – La Padula.

2.1.6. Μοντέλο Bell – La Padula

Το μοντέλο Bell – La Padula [BP76], [B05] είναι ένα φορμαλιστικό μοντέλο που αποτυπώνει την πολιτική Υποχρεωτικού Ελέγχου Πρόσβασης. Το μοντέλο αναπτύχθηκε από τους David Elliot Bell και Len La Padula. Σκοπός του ήταν η αποτύπωση ενός μαθηματικού μοντέλου που θα περιγράφει την έννοια της ασφάλειας σε ένα σύστημα.

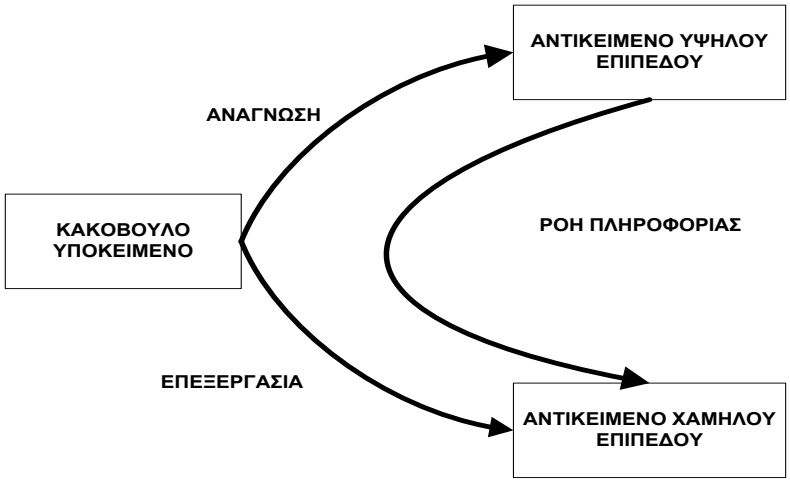
Το μοντέλο βασίζεται στην αρχή ότι το σύστημα βρίσκεται σε μία ασφαλή κατάσταση όπου ικανοποιούνται όλοι οι κανόνες που ορίζει η πολιτική και κάθε μετάβαση του συστήματος σε μία άλλη κατάσταση εξασφαλίζει ότι και η νέα κατάσταση θα είναι επίσης ασφαλής. Έτσι, το σύστημα παραμένει ασφαλές σε κάθε περίπτωση.

Το μοντέλο Bell – La Padula ορίζει δύο ιδιότητες υποχρεωτικού ελέγχου και μία ιδιότητα διακριτικού ελέγχου:

Απλή Ιδιότητα Ασφάλειας

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα ανάγνωσης ενός αντικειμένου αν η ετικέτα ασφάλειας του υποκειμένου υπερτερεί της ετικέτας ασφάλειας του αντικειμένου.

Αρχικά η ιδιότητα αυτή φαίνεται αρκετή ώστε να εξασφαλίσει την ασφάλεια του συστήματος. Αυτό που δεν προβλέπεται, όμως, στην απλή ιδιότητα ασφάλειας είναι η περίπτωση όπου ένα υποκείμενο μπορεί να «διαβάσει» μία πληροφορία (αντικείμενο) ενός επιπέδου ικανοποιώντας τη συνθήκη που τέθηκε με τις ετικέτες και στη συνέχεια να τη «γράψει» ως περιεχόμενο σε ένα αντικείμενο χαμηλότερου επιπέδου. Με αυτό τον τρόπο η πληροφορία πλέον αλλάζει επίπεδο ασφάλειας και μπορεί να είναι προσβάσιμη από χρήστες που κανονικά δε θα έπρεπε να έχουν αυτή τη δυνατότητα. Γραφική απεικόνιση αυτής της διαδικασίας παρουσιάζεται στην Εικόνα 3 όπου φαίνεται η διαρροή της πληροφορίας προς έναν κακόβουλο χρήστη. Αυτό ακριβώς το κενό έρχεται να καλύψει η επόμενη ιδιότητα.



Εικόνα 3. Το «κενό» της Απλής Ιδιότητας

Ιδιότητα*

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα εγγραφής σε ένα αντικείμενο αν η ετικέτα ασφάλειας του αντικειμένου υπερτερεί της ετικέτας ασφάλειας του υποκειμένου. Η Ιδιότητα* ικανοποιείται όταν σε κάθε κατάσταση εάν ένα υποκείμενο έχει άδεια ανάγνωσης σε ένα αντικείμενο επιπέδου ασφάλειας Α και ταυτόχρονα άδεια εγγραφής σε ένα αντικείμενο επιπέδου ασφάλειας Β (όπου Α>Β) τότε το επίπεδο Β υπερισχύει του Α.

Αυτό που θα πρέπει να σημειωθεί σε αυτό το σημείο είναι ότι η Ιδιότητα * δεν αφορά έμπιστα υποκείμενα, τα οποία θεωρείται ότι δεν πρόκειται να μεταβιβάσουν πληροφορία σε χαμηλότερα επίπεδα ακόμη και αν αυτό είναι δυνατό. Με την ικανοποίηση και των δύο ιδιοτήτων αυτό που πετυχαίνουμε είναι να έχουμε εγγραφή-προς-τα-επάνω (write-up) και ανάγνωση-προς-τα-κάτω (read-down) και, κατά συνέπεια, αποτρέπεται η διαρροή πόρων, π.χ. ευαίσθητων πληροφοριών ή κακόβουλου λογισμικού προς τα λιγότερο ασφαλή επίπεδα.Εικόνα 3. Το «κενό» της Απλής Ιδιότητας

Διακριτική Ιδιότητα Ασφάλειας

Για την εφαρμογή της ιδιότητας αυτής χρησιμοποιείται μήτρα προσπέλασης για το διακριτικό έλεγχο της προσπέλασης. Η πρόσβαση επιτρέπεται μόνο αν υπάρχει αντίστοιχη εγγραφή στη μήτρα πρόσβασης.

Τα μειονεκτήματα που εμφανίζει το μοντέλο Bell – La Padula έγκεινται κυρίως στο ότι δεν είναι ευέλικτο αλλά ούτε και εύκολα προσαρμόσιμο σε εμπορικές εφαρμογές. Επιπλέον, δεν εξασφαλίζει την ασφάλεια στην περίπτωση μεταφοράς κακόβουλου λογισμικού προς τα πιο πάνω επίπεδα αφού ένας χρήστης μπορεί να μεταφέρει πληροφορία σε ανώτερα επίπεδα η οποία όμως μπορεί να είναι απλά κακόβουλο λογισμικό. Όντας ένα ιεραρχικό μοντέλο αντιμετωπίζει τα αντίστοιχα προβλήματα και δεν ικανοποιείται πάντα η αρχή του «γνωρίζω ό,τι χρειάζεται». Χαρακτηριστικό παράδειγμα αποτελεί το γεγονός ότι κάθε χρήστης γνωρίζει την ύπαρξη κάθε αντικειμένου, ασχέτως των δικαιωμάτων πρόσβασης που έχει σε αυτό, πράγμα το οποίο δεν είναι επιθυμητό σε πολλές περιπτώσεις. Τέλος, το μοντέλο αυτό, όπως και γενικά η πολιτική πολλών επιπέδων ασφάλειας, δεν προβλέπει την προστασία από μη εξουσιοδοτημένη αλλαγή της πληροφορίας, παρά μόνο την εμπιστευτικότητα της πληροφορίας [SS94] **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**.

2.1.7. Μοντέλο Biba

Το μοντέλο Biba δεν εστιάζει μόνο στην προστασία της εμπιστευτικότητας αλλά και στον έλεγχο της μη εξουσιοδοτημένης τροποποίησης της πληροφορίας και, κατά συνέπεια, στην διατήρηση της ακεραιότητάς της [B77]. Το μοντέλο Biba αποτελεί συμπλήρωμα του μοντέλου Bell – La Padula. Το όνομά του οφείλεται στον Kenneth J. Biba ο οποίος και το ανέπτυξε και αναφέρεται στη βιβλιογραφία ως μοντέλο ακεραιότητας του Biba (Biba Integrity Model).

Κατ' αντιστοιχία με το μοντέλο Bell – La Padula, τόσο τα υποκείμενα όσο και τα αντικείμενα χαρακτηρίζονται από ετικέτες ακεραιότητας. Το μοντέλο Biba ορίζει και αυτό περιορισμούς στα δικαιώματα ανάγνωσης και γραφής ανάλογα με την ιεραρχία των επιπέδων ακεραιότητας των οντοτήτων. Συγκεκριμένα, ορίζονται η Ιδιότητα Απλής Ασφάλειας και η Ιδιότητα* καθώς και οι ιδιότητες Ενεργοποίησης του επεκταμένου μοντέλου και η ιδιότητα του δακτυλίου:

Απλή Ιδιότητα Ασφάλειας

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα ανάγνωσης ενός αντικειμένου αν η ετικέτα ακεραιότητας του αντικειμένου υπερτερεί της ετικέτας ασφάλειας του υποκειμένου.

Ιδιότητα*

Ένα υποκείμενο επιτρέπεται να έχει δικαίωμα εγγραφής σε ένα αντικείμενο αν η ετικέτα ακεραιότητας του υποκειμένου υπερτερεί της ετικέτας ασφάλειας του αντικειμένου.

Ιδιότητα ενεργοποίησης του επεκταμένου μοντέλου

Ένα υποκείμενο μπορεί να ενεργοποιήσει ένα άλλο υποκείμενο μόνο αν η ετικέτα ακεραιότητάς του υπερτερεί της ετικέτας ακεραιότητάς του άλλου.

Ιδιότητα δακτυλίου

Ένα υποκείμενο έχει δικαίωμα ανάγνωσης για όλα τα αντικείμενα, ανεξαρτήτως της ετικέτας ακεραιότητάς του. Μπορεί, όμως, να τροποποιεί αντικείμενα για τα οποία η ετικέτα ακεραιότητάς του υπερτερεί των αντικειμένων καθώς και να ενεργοποιεί υποκείμενα των οποίων η ετικέτα ακεραιότητάς τους υπερτερεί της δικής του.

Ειδικότερα, η ετικέτα ακεραιότητας μπορεί να έχει τις τιμές Κρίσιμη (Crucial – C), Πολύ Σημαντική (Very Important – VI), Σημαντική (Important), οι οποίες ακολουθούν τη συσχέτιση C >VI> I. Έτσι, τα δικαιώματα ανάγνωσης και εγγραφής παρέχονται σε ένα υποκείμενο αν ικανοποιούνται οι ιδιότητες που αναφέρθηκαν και πετυχαίνουμε εγγραφή-προς-τα-κάτω (write-down) και ανάγνωση-προς-τα-επάνω (read-up) [B77].

Αυτό που θα πρέπει να σημειωθεί είναι ότι οι ετικέτες ασφαλείας που αναφέρθηκαν προηγουμένως (μοντέλο Bell – La Padula) και οι ετικέτες ακεραιότητας δεν είναι έννοιες ταυτόσημες. Οι πρώτες καθορίζουν τα επίπεδα εμπιστευτικότητας περιορίζοντας τη ροή των πληροφοριών, ενώ οι τελευταίες αναστέλλουν την τροποποίηση αυτών.

Το μοντέλο Biba υποστηρίζει τόσο πολιτικές υποχρεωτικού όσο και διακριτικού ελέγχου. Η πολιτική που αναφέρθηκε παραπάνω αποτελεί μια Αυστηρή Πολιτική Ακεραιότητας (Strict Integrity Policy).

2.1.8. Πολιτική Κινέζικου Τείχους

Οι David Brewer και Michael Nash παρουσίασαν μία θεωρία που μπορεί να χρησιμοποιηθεί για την υλοποίηση δυναμικά μεταβαλλόμενων δικαιωμάτων πρόσβασης και η οποία ονομάζεται Πολιτική Κινέζικου Τείχους(Chinese Wall Security Policy) [BN89]. Πρόκειται για μία πολιτική που αφορά εμπορικές εφαρμογές και διαχειρίζεται θέματα σύγκρουσης συμφερόντων που σχετίζονται με αναλυτές που παρέχουν συμβουλευτικές υπηρεσίες σε μια επιχείρηση.

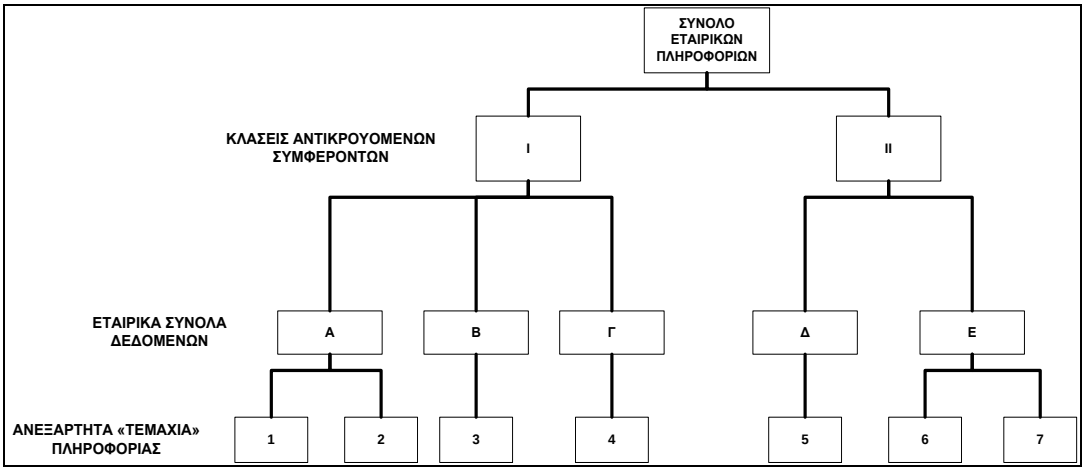
Ένας σύμβουλος, ο οποίος εργάζεται για λογαριασμό μιας εταιρείας, αποκτά πρόσβαση σε ευαίσθητες και σημαντικές πληροφορίες της εταιρείας και οφείλει να διατηρήσει την εμπιστευτικότητα των πληροφοριών αυτών. Αυτό σημαίνει ότι δεν πρέπει να έχει τη δυνατότητα να παρέχει συμβουλευτικές υπηρεσίες σε μία ανταγωνιστική της πρώτης εταιρεία. Αν αποκτήσει πρόσβαση σε σημαντικές και κρίσιμες πληροφορίες και της ανταγωνιστικής εταιρείας τότε αποκτά ένα σημαντικό ανταγωνιστικό πλεονέκτημα το οποίο μπορεί να χρησιμοποιήσει για προσωπικό του όφελος, γεγονός το οποίο δεν είναι θεμιτό.

Στόχος της πολιτικής του Κινέζικου Τείχους είναι ο εντοπισμός και η προφύλαξη της ροής πληροφοριών που μπορούν να οδηγήσουν σε συγκρούσεις συμφερόντων. Σε αντίθεση με το μοντέλο Bell – La Padula, η πρόσβαση στις πληροφορίες δεν περιορίζεται από τα ίδια τα χαρακτηριστικά της πληροφορίας**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Τα δικαιώματα πρόσβασης του χρήστη δημιουργούνται δυναμικά ανάλογα με τις πληροφορίες στις οποίες έχει ήδη πρόσβαση.

Το Μοντέλο Κινέζικου Τείχους αποτελεί την υλοποίηση της Πολιτικής Κινέζικου Τείχους. Με βάση το μοντέλο αυτό όλες οι εταιρικές πληροφορίες ταξινομούνται ιεραρχικά στα παρακάτω τρία επίπεδα [BN89]:

- Στο χαμηλότερο επίπεδο βρίσκονται τα αντικείμενα τα οποία είναι ανεξάρτητα «τεμάχια» πληροφορίας που το καθένα αφορά μία εταιρεία.
- Στο ενδιάμεσο επίπεδο βρίσκονται τα Εταιρικά Σύνολα Δεδομένων (company datasets). Ως εταιρικό σύνολο δεδομένων ορίζεται το σύνολο των αντικειμένων που ανήκουν σε έναν οργανισμό/εταιρεία.
- Στο ανώτερο επίπεδο εμφανίζονται οι Κλάσεις Αντικρουόμενων Συμφερόντων (Conflict of Interest Class –COI). Σε κάθε τέτοια κλάση ανήκουν όλα τα εταιρικά σύνολα δεδομένων που αφορούν επιχειρήσεις που είναι ανταγωνιστικές μεταξύ τους, περιλαμβάνει δηλαδή το σύνολο των ανταγωνιστικών οργανισμών. Οι κλάσεις αντικρουόμενων συμφερόντων είναι αμοιβαία αποκλειόμενες μεταξύ τους. Κάθε εταιρεία ανήκει μόνο σε μία κλάση και κάθε κλάση περιλαμβάνει τουλάχιστον δύο εταιρείες.

Τα επίπεδα στα οποία ταξινομούνται ιεραρχικά όλες οι εταιρικές πληροφορίες στο Μοντέλου Κινέζικου Τείχους παρουσιάζονται σχηματικά στην Εικόνα 4.



Εικόνα 4. Σύνθεση εταιρικών πληροφοριών στο Μοντέλο Κινέζικου Τείχους

Η πληροφορία που δε θεωρείται ευαίσθητη για μία εταιρεία και γι αυτό και μπορεί να είναι προσπελάσιμη από οποιοδήποτε υποκείμενο αποκαλείται Αποστειρωμένη πληροφορία.

Αρχικά, εφόσον ο σύμβουλος δεν έχει διαβάσει κάποια πληροφορία για κάποιον οργανισμό είναι ελεύθερος να αποκτήσει πρόσβαση σε οποιαδήποτε πληροφορία επιθυμεί και για οποιοδήποτε οργανισμό αφού δεν υπάρχει σύγκρουση συμφερόντων, εκτός κι αν περιορίζεται από κάποια άλλη πολιτική, όπως π.χ. από την πολιτική MAC. Μετά την αρχική του επιλογή για πρόσβαση στα αντικείμενα μιας εταιρείας, δημιουργείται για το σύμβουλο ένα Κινέζικο Τείχος για όλα τα δεδομένα που βρίσκονται στην ίδια κλάση αντικρουόμενων συμφερόντων με τα δεδομένα που βρίσκονται εντός του Τείχους του. Ο σύμβουλος έχει παρόλα αυτά τη δυνατότητα να αποκτήσει πρόσβαση σε οποιοδήποτε άλλα δεδομένα εφόσον αυτά ανήκουν σε διαφορετική κλάση, μεταβάλλοντας έτσι το Κινέζικο Τείχος του ώστε να περιλαμβάνει και το νέο σύνολο δεδομένων.

Όπως και στο μοντέλο Bell – La Padula έτσι και στο Μοντέλο Κινέζικου Τείχους ορίζονται οι παρακάτω δύο ιδιότητες οι οποίες προσδιορίζουν τα δικαιώματα ανάγνωσης και γραφής.

Απλή Ιδιότητα Ασφάλειας

*Ένα υποκείμενο επιτρέπεται να έχει πρόσβαση σε ένα αντικείμενο μόνο αν ισχύουν τα παρακάτω****Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.****:*

Το αντικείμενο ανήκει στο ίδιο σύνολο εταιρικών δεδομένων με ένα αντικείμενο που ήδη έχει προσπελάσει το υποκείμενο

Το αντικείμενο ανήκει σε μια διαφορετική κλάση δηλαδή το υποκείμενο δεν έχει ήδη προσπελάσει ένα άλλο αντικείμενο της ίδιας κλάσης αντικρουόμενων συμφερόντων.

Εννοείται ότι η αποστειρωμένη πληροφορία μπορεί να «διαβαστεί» από οποιοδήποτε υποκείμενο.

Ιδιότητα*

Ένα υποκείμενο μπορεί να έχει δικαίωμα εγγραφής σε ένα αντικείμενο αν:

Επιτρέπεται η πρόσβαση σε αυτό σύμφωνα με την Απλή Ιδιότητα Ασφάλειας

Δεν επιτρέπεται η ανάγνωση κάποιου μη αποστειρωμένου αντικειμένου το οποίο ανήκει σε διαφορετικό σύνολο εταιρικών δεδομένων με αυτό στο οποίο ζητάμε δικαίωμα εγγραφής. Αυτό εξασφαλίζει ότι η ευαίσθητη πληροφορία μπορεί να ρέει από ένα αντικείμενο σε ένα άλλο αν και τα δύο ανήκουν στην ίδια εταιρία.

2.1.1. Μοντέλο Harrison, Ruzzo, Ullman

Οι M. A. Harrison, W. L. Ruzzo and J. D. Ullman παρουσίασαν ένα μοντέλο που επικεντρώνεται στη δυνατότητα αλλαγής των δικαιωμάτων προσπέλασης, και στη δημιουργία ή στη διαγραφή υποκειμένων και αντικειμένων ορίζοντας συστήματα εξουσιοδότησης. Αποτελεί ένα φορμαλιστικό μοντέλο που βασίζεται στους πίνακες ελέγχου πρόσβασης [HR76]**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**.

Τα στοιχεία του μοντέλου είναι ένα σύνολο αντικειμένων (O), ένα σύνολο υποκειμένων (S), ένας πίνακας πρόσβασης (A), ένα σύνολο εντολών (C) και ένα σύνολο διαδικασιών – λειτουργιών (P). Η κατάσταση του συστήματος σε κάθε δεδομένη στιγμή καθορίζεται από τα στοιχεία των (S,O,A) ενώ οι αλλαγές στην κατάσταση και η μετάβαση σε μία άλλη γίνονται μέσω των εντολών του συνόλου C.

Το μοντέλο ορίζει έξι πρωτογενείς διαδικασίες [HR76]:

- Δημιουργία Αντικειμένου (Create Object)
  Ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο αντικείμενο.
- Δημιουργία Υποκειμένου (Create Subject)
  Ένα υποκείμενο μπορεί να δημιουργήσει ένα νέο υποκείμενο.
- Καταστροφή Αντικειμένου (Destroy Object)
  Ένα αντικείμενο μπορεί να διαγράψει ένα αντικείμενο.
- Καταστροφή Υποκειμένου (Destroy Subject)
  Ένα υποκείμενο μπορεί να διαγράψει ένα υποκείμενο.
- Προσθήκη Δικαιώματος (Add Access Right)
  Ο ιδιοκτήτης ενός αντικειμένου καθορίζει τα δικαιώματα προσπέλασης οποιουδήποτε υποκειμένου επί του αντικειμένου.
- Διαγραφή Δικαιώματος (Delete Access Right)
  Με τη διαδικασία αυτή ο ιδιοκτήτης ενός αντικειμένου διαγράφει τα δικαιώματα προσπέλασης οποιουδήποτε υποκειμένου επί του αντικειμένου.

Η δομή μιας εντολής (command – c) ορίζει μία σειρά από ελέγχους – υποθέσεις προκειμένου να εκτελεστεί η διαδικασία (ή οι διαδικασίες) που ορίζει το κυρίως μέρος της εντολής.

***Πρώτος* Ορισμός (Διαρροή ενός δικαιώματος)**: *Λέμε ότι μία εντολή c διαρρέει το δικαίωμα r από μία κατάσταση, αν κατά τη διάρκεια της εκτέλεσης της c για κάποιες αρχικές παραμέτρους της κατάστασης, η εκτέλεση της βασικής λειτουργίας που ορίζει η εντολή (προφανώς της μορφής Add Access Right) προσθέτει το δικαίωμα r στο κατάλληλο κελί του πίνακα πρόσβασης, το οποίο δεν περιείχε το r ακριβώς πριν την εκτέλεση της πρωτογενούς λειτουργίας.*

***Δεύτερος* Ορισμός**: *Δεδομένου ενός πίνακα A και μίας αρχικής κατάστασης αυτού, λέμε ότι ο A δεν είναι ασφαλής ως προς το δικαίωμα r αν και μόνο αν υπάρχει μια σειρά εντολών που να επιτρέπουν τη μετάβαση του A σε μία νέα κατάσταση στην οποία το r διαρρέει* [TN13].

Το πιο προφανές παράδειγμα διαρροής δικαιώματος είναι αν η ίδια η εντολή περιέχει μία διαδικασία που αναιρεί την εισαγωγή του δικαιώματος στον πίνακα ελέγχου πρόσβασης (Delete Access Right). Φυσικά θα πρέπει να υπάρχουν δικαιώματα που διαρρέουν, διαφορετικά ο πίνακας δε θα άλλαζε ποτέ**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**.

Το πρόβλημα της ασφάλειας στο μοντέλο των Harrison – Ruzzo – Ullman έγκειται στο να αποδειχθεί τελικά αν ο πίνακας πρόσβασης A είναι ασφαλής ως προς ένα δικαίωμα *r* για ένα σύνολο εντολών *C*. Το πρόβλημα αυτό έχει αποδειχθεί ότι είναι υπολογιστικά δύσκολο στη γενική περίπτωση. Μπορεί να λυθεί μόνο στην περίπτωση κατά την οποία η εντολή περιέχει στο κυρίως μέρος της μία μόνο λειτουργία.

2.1.2. Μοντέλο Clark - Wilson

Το μοντέλο Clark-Wilson [DW87] προορίζεται για εμπορικά συστήματα και παρέχει μία δομημένη μεθοδολογία για έλεγχο προσπέλασης. Οι Clark και Wilson διαπίστωσαν ότι η εμπιστευτικότητα είναι μεν αρκετά σημαντική για τις εμπορικές εφαρμογές αλλά ιδιαίτερο βάρος σε τέτοιου τύπου εφαρμογές πρέπει να δίνεται στην ακεραιότητα της πληροφορίας.

Το μοντέλο ορίζει δύο ειδών δεδομένα: τα δεδομένα περιορισμένου τύπου (Constrained Data Items – CDI) και τα δεδομένα μη περιορισμένου τύπου (Unconstrained Data Items – UDI). Επίσης, ορίζει δύο ειδών διαδικασίες: τις διαδικασίες επαλήθευσης ακεραιότητας (Integrity Verification Procedures – IVP) και τις διαδικασίες συναλλαγής (Transaction Procedures).

Οι Clark και Wilson στο πλαίσιο της εξασφάλισης της ακεραιότητας της πληροφορίας προτείνουν δύο βασικές αρχές στις οποίες στηρίζουν και το μοντέλο τους [DW87].:

Η αρχή της καλά σχηματισμένης συναλλαγής (Well-formed Transaction)

Κάθε ολοκληρωμένη ενέργεια αποτελείται από διαδικασίες που εκτελούνται από εξουσιοδοτημένους χρήστες με τέτοιο τρόπο ώστε το σύστημα να μεταβαίνει από μία συνεπή κατάσταση σε μία νέα, επίσης, συνεπή. Ένας χρήστης δε θα πρέπει να διαχειρίζεται τα δεδομένα αυθαίρετα αλλά μόνο με περιορισμένους τρόπους που εξασφαλίζουν την ακεραιότητά τους.

Η αρχή του διαχωρισμού των καθηκόντων (Separation of Duty – SoD)

*Σύμφωνα με αυτή την αρχή, σκοπός είναι να εξασφαλιστεί η εξωτερική συνέπεια των δεδομένων: η συμφωνία του αντικειμένου-δεδομένου του συστήματος με το αντικείμενο του πραγματικού κόσμου που αυτό αντιπροσωπεύει. Έμμεσα, αυτό μπορεί να επιτευχθεί με το χωρισμό των διαδικασιών σε τμήματα όπου το κάθε ένα από αυτά εκτελείται από διαφορετικό πρόσωπο****Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.****.*

Ίσως το πιο χαρακτηριστικό παράδειγμα εφαρμογής για την κατανόηση του μοντέλου αυτού είναι μία τραπεζική εφαρμογή όπου καταγράφονται διάφορες συναλλαγές. Έτσι, η αρχή της καλά σχηματισμένης συναλλαγής έγκειται στο ότι πρέπει να χρεώνονται και να πιστώνονται σωστά τα ποσά έτσι ώστε να μην υπάρχουν διαφορές ενώ ο διαχωρισμός των καθηκόντων επιτυγχάνεται με την απαίτηση να πραγματοποιήσει μέρος της συναλλαγής (ή έστω την τελική έγκρισή της) ο προϊστάμενος του εκάστοτε χρήστη- εργαζόμενου της τράπεζας.

2.1.3. Μοντέλο Domain-Type Enforcement (DTE)

Το μοντέλο Domain-Type Enforcement (DTE) [TP97] υλοποιεί κανόνες υποχρεωτικού ελέγχου πρόσβασης προκειμένου να μεσολαβήσει στην πρόσβαση μεταξύ τομέων και τύπων. Κάθε υποκείμενο σχετίζεται με μία ετικέτα *τομέα (domain)* ανάλογα με τη λειτουργία του και κάθε αντικείμενο με ένα *τύπο (type)* ανάλογα με τις απαιτήσεις ακεραιότητας του αντικειμένου. Εμφανίζονται δύο τύποι αδειών πρόσβασης: άδειες πρόσβασης από τομέα σε τομέα (domain-domain permissions) και άδειες πρόσβασης από τομέα σε τύπο (domain-type permissions). Για κάθε ένα τύπο άδειας πρόσβασης υπάρχει και ένας αντίστοιχος πίνακας πρόσβασης που τον αναπαριστά. Ο πίνακας ελέγχου πρόσβασης τομέα-τομέα (domain-domain access control table DDAT) είναι ένας διδιάστατος πίνακας που για κάθε ζευγάρι τομέων παρουσιάζει μια εγγραφή με τα δικαιώματα πρόσβασης μεταξύ αυτών. Ομοίως, ο πίνακας ελέγχου πρόσβασης τύπου τομέα (domain-type access control table DTAT) αποθηκεύει για κάθε ζευγάρι τομέα-τύπου μία εγγραφή με τα αντίστοιχα δικαιώματα πρόσβασης. Το σύνολο των εγγραφών των δύο αυτών πινάκων αποτελούν τη βάση δεδομένων DTE για ένα συγκεκριμένο υπολογιστικό περιβάλλον.

Υπάρχουν αρκετές ομοιότητες μεταξύ του DTE και του RBAC με αποτέλεσμα να μπορεί το μοντέλο αυτό να υλοποιεί πολιτικές που εκφράζονται από ένα μοντέλο RBAC.

2.2. Βασικό RBAC και Αρχικά Μοντέλα

Τα κλασικά μοντέλα ελέγχου πρόσβασης όπως οι Λίστες Ελέγχου Πρόσβασης και ο Διακριτικός Έλεγχος Πρόσβασης έχουν χρησιμοποιηθεί εκτενώς σε πληθώρα υλοποιήσεων και σε πολλά διαφορετικά περιβάλλοντα. Ωστόσο, τα προαναφερθέντα μοντέλα και οι τεχνικές που εφαρμόζουν δεν έχουν τη δυνατότητα να εφαρμόσουν μια σειρά από απαιτήσεις ασφαλείας που έχουν προκύψει ως αποτέλεσμα της αυξανόμενης χρήσης αλλά και της εξάρτησης κρίσιμων υπηρεσιών από πληροφοριακά συστήματα και, επιπλέον, δεν ανταποκρίνονται επαρκώς στην κλιμάκωση σε πιο σύνθετες συνθήκες.

Το μοντέλο Ελέγχου Πρόσβασης με Ρόλους (Role Based Access Control - RBAC) προσφέρει το πλεονέκτημα ότι απλοποιεί σημαντικά το διαχειριστικό κόστος με την χρήση ιεραρχιών, ρόλων και περιορισμών για να οργανώσει αποτελεσματικά τα δικαιώματα και τους σχετικούς πόρους.

Το μοντέλο RBAC είναι από τα πιο ευρέως διαδεδομένα μοντέλα που χρησιμοποιούνται σε εφαρμογές, λειτουργικά συστήματα και βάσεις δεδομένων. Επιπλέον, έχει αποτελέσει το αντικείμενο έντονης ερευνητικής μελέτης και ανάπτυξης προκειμένου να εξελιχθούν οι δυνατότητές του ώστε να περιλαμβάνει χρονικούς και γεωγραφικούς περιορισμούς, ροές εργασίας κτλ.

2.2.1. Εισαγωγή στο RBAC

Το μοντέλο ελέγχου πρόσβασης βασισμένο σε ρόλους αποτέλεσε μια μεγάλη καινοτομία στον τρόπο διαχείρισης των δικαιωμάτων πρόσβασης. Στο μοντέλο αυτό, εισάγονται για πρώτη φορά έννοιες όπως ο ρόλος και ο δυναμικός διαχωρισμός των καθηκόντων.

Η ανάθεση δικαιωμάτων ξεφεύγει πλέον από το χρήστη / υποκείμενο και γίνεται με ρόλους. Παράλληλα, γίνεται αναφορά σε κληρονομικότητα δικαιωμάτων μέσα από ιεραρχίες ρόλων καθώς και σε δυναμική ενεργοποίηση ρόλων στο πλαίσιο συνεδριών. Όλες αυτές οι έννοιες αναλύονται στη συνέχεια με την παρουσίαση των τεσσάρων βασικών συνιστωσών του μοντέλου RBAC, οι οποίες είναι [W03]:

- Βασικό RBAC (RBAC0)
- Ιεραρχικό RBAC (RBAC1)
  - ◊ Γενικές Ιεραρχίες
  - ◊ Περιορισμένες Ιεραρχίες
- Περιορισμένο RBAC ($RBAC_2$)
  - ◊ Στατικός Διαχωρισμός Καθηκόντων
  - ◊ Δυναμικός Διαχωρισμός Καθηκόντων
- Συμμετρικό RBAC ($RBAC_3$).

Η ιστορία του RBAC ξεκινάει το 1992 όταν οι Ferraiolo και Kuhn πρότειναν ένα νέο μοντέλο ελέγχου πρόσβασης [FK92] που αποτελούσε μία διαφορετική προσέγγιση

στον τρόπο διαχείρισης των δικαιωμάτων πρόσβασης των χρηστών. Παρακάτω παρουσιάζεται η πορεία του μοντέλου και πώς χρονολογικά αποδίδεται η ανάπτυξή του σύμφωνα με το NIST [NIST15].

- 1992 – Οι David Ferraiolo και D. Richard Kuhn ορίζουν το μοντέλο RBAC το οποίο καθορίζει πρόσβαση μόνο μέσω ρόλων, ιεραρχιών και περιορισμών [FK92].
- 1994 – Η IBM παρουσιάζει στην Ευρώπη την πρώτη εφαρμογή που βασίζεται στο RBAC κάνοντας ειδική αναφορά στους Ferraiolo και Kuhn.
- 1995 – Οι Ferraiolo, Cugini και Kuhn επεκτείνουν το αρχικό μοντέλο ορίζοντας τύπους διαχωρισμού καθηκόντων [FCK95].
- 1997-1998 – Οι εταιρείες Sybase, Secure Computing και Siemens ανακοινώνουν την προώθηση προϊόντων RBAC τα οποία αναφέρεται ότι στηρίζονται άμεσα στο μοντέλο των Ferraiolo-Kuhn.
- 1997 – Η Secure Computing ενσωματώνει το μοντέλο Ferraiolo-Kuhn RBAC model στο καθολικό σύστημα διοίκησης και ελέγχου του Αμερικανικού Υπουργείου Αμύνης (US DoD Global Command and Control System).
- 1997 – Μέσα ένα άρθρο του Osborn καθορίζεται η σχέση μεταξύ του RBAC και των Πολιτικών Ασφαλείας Πολλαπλών Επιπέδων Υποχρεωτικού Ελέγχου Πρόσβασης (MLS/MAC) [O97].
- 2000 – Ορίζεται το ενοποιημένο μοντέλο RBAC και γίνεται το πρότυπο RBAC (standard) από τους Sandhu, Ferraiolo, Kuhn [SFK00].
- 2004 – Το American National Standards Institute / International Committee for Information Technology Standards (ANSI/INCITS) υιοθετεί την πρόταση των Sandhu, Ferraiolo και Kuhn για το RBAC και το αναγνωρίζει ως ένα κοινά αποδεκτό βιομηχανικό πρότυπο [ANSI04].

Η εξέλιξη του μοντέλου φυσικά δε σταματάει στο 2004. Τα πλεονεκτήματά του το καθιστούν ένα ευρέως διαδεδομένο μοντέλο ελέγχου πρόσβασης ειδικά στον εμπορικό κόσμο, σε εφαρμογές λογισμικού κτλ. Με την επίσημη καθιέρωσή του ως πρότυπο οριοθετείται μια νέα εποχή όπου πλέον στο μοντέλο αρχίζουν να προστίθενται στοιχεία που διευκολύνουν τις εκάστοτε ανάγκες των οργανισμών και των συστημάτων πληροφορικής. Συνεχώς αναπτύσσονται παραλλαγές και επεκτάσεις οι οποίες όμως στηρίζονται κατά κύριο λόγο στο πρότυπο όπως αυτό καθιερώθηκε το 2004. Τα μειονεκτήματά του και οι ελλείψεις του ερευνώνται μέχρι και σήμερα προσφέροντας νέες προκλήσεις για την περαιτέρω εξέλιξή του.

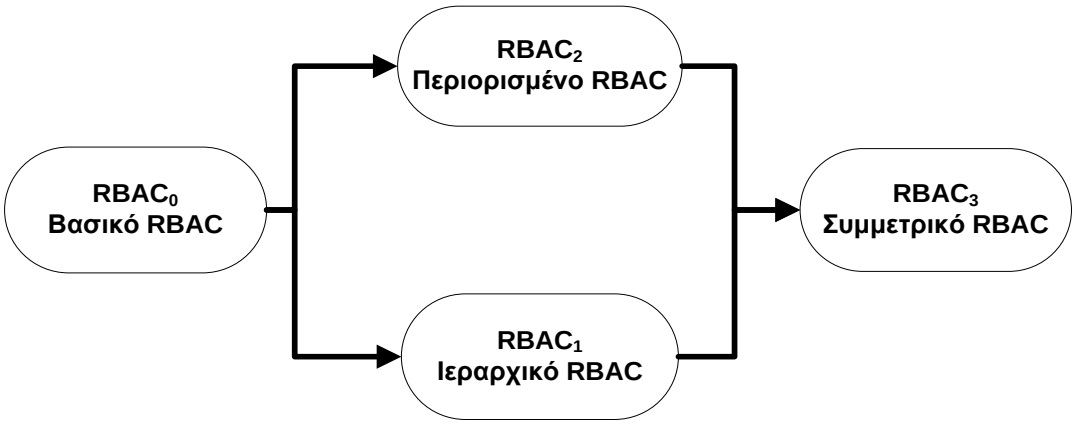
2.2.2. Βασικό RBAC

Το *Βασικό RBAC* ενσωματώνει τα βασικά και απαραίτητα χαρακτηριστικά που συναντάμε σε όλα τα συστήματα RBAC, όπως φαίνεται και στην Εικόνα 5. Προσδιορίζει τον ελάχιστο αριθμό στοιχείων, συνόλων και σχέσεων μεταξύ αυτών που είναι υποχρεωτικά και θεμελιώδη προκειμένου να επιτευχθεί ένα σύστημα ελέγχου πρόσβασης βασισμένο σε ρόλους.

Στο *Βασικό RBAC* περιλαμβάνονται πέντε βασικά στοιχεία:

- οι χρήστες, Users - *U*
- οι ρόλοι, Roles - *R*
- τα αντικείμενα, Subjects - *S*
- τα δικαιώματα πρόσβασης, Permissions – *P*
- Οι σύνοδοι, Sessions - S

Ο όρος «χρήστης» αναφέρεται σε μια ανθρώπινη οντότητα αν και μπορεί να επεκταθεί και να συμπεριλάβει μηχανήματα, δίκτυα ή έξυπνους αυτόνομους πράκτορες (agents). Ο «ρόλος» αποτελεί μια επιχειρησιακή θέση ή λειτουργία στα πλαίσια ενός οργανισμού και σχετίζεται με τις εξουσιοδοτήσεις, τα δικαιώματα και τις υποχρεώσεις που παραχωρούνται στο χρήστη στον οποίο ανατίθεται ο ρόλος. Ως «δικαίωμα πρόσβασης» νοείται η εξουσιοδότηση να εκτελεστεί μια ενέργεια σε ένα αντικείμενο του συστήματος και, τέλος, η «λειτουργία» είναι μια ενεργός διεργασία η οποία, όταν προκληθεί, εκτελεί μια ενέργεια για το χρήστη. Οι τύποι των ενεργειών και των αντικειμένων που περιλαμβάνονται στο RBAC εξαρτώνται από τον τύπο του συστήματος στο οποίο θα υλοποιηθεί ο βασισμένος σε ρόλους έλεγχος πρόσβασης.



Εικόνα 5. Βασικές συνιστώσες μοντέλου RBAC

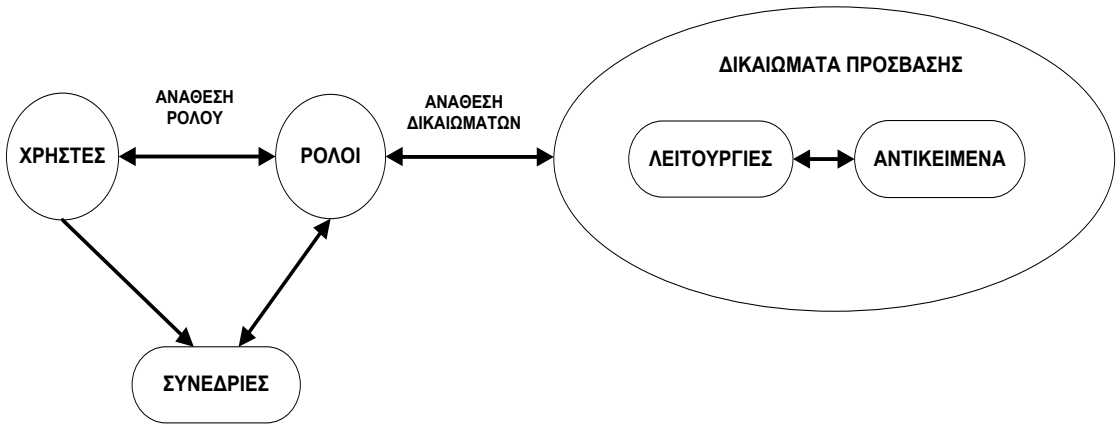
Οι διαχειριστές του συστήματος σε έναν οργανισμό προσδιορίζουν τις απαιτήσεις πρόσβασης στους πόρους με βάση τις επιχειρησιακές λειτουργίες που εκτελούνται και, στη συνέχεια, δημιουργούν ρόλους για διάφορες θέσεις εργασίας εντός του οργανισμού. Σύμφωνα με το Βασικό Μοντέλο RBAC, στους χρήστες ανατίθενται ρόλοι ανάλογα με τις αρμοδιότητες, τα καθήκοντα, τις εξουσιοδοτήσεις και τις υποχρεώσεις που έχουν στο πλαίσιο της εργασίας τους. Επιπλέον, τα δικαιώματα πρόσβασης ανατίθενται στους ρόλους αντανακλώντας τη βασική πολιτική που ακολουθεί ο οργανισμός καθώς και τους κανονισμούς που διέπουν τη λειτουργία του, είτε πρόκειται για εσωτερικούς κανονισμούς είτε για οδηγίες και νόμους του ευρύτερου περιβάλλοντος στο οποίο αυτός λειτουργεί.

Οι βασικές σχέσεις που ορίζονται στο RBAC είναι οι ακόλουθες:

- UA $\subseteq$ UxR είναι μια σχέση που αναθέτει χρήστες σε ρόλους (πολλά-προς-πολλά)
- PA $\subseteq$ PxR είναι μια σχέση που αναθέτει Δικαιώματα Πρόσβασης σε Ρόλους (πολλά-προς-πολλά)

Είναι σημαντικό να τονίσουμε ότι σε ένα σύστημα RBAC τα δικαιώματα πρόσβασης σχετίζονται με ρόλους, οι χρήστες είναι μέλη ρόλων και, επομένως, αποκτούν τα δικαιώματα πρόσβασης των ρόλων αυτών [SFK00]**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Τα δικαιώματα πρόσβασης δεν ανατίθενται απευθείας και ατομικά στο χρήστη αλλά μέσω του ρόλου του. Το θεμελιώδες αυτό χαρακτηριστικό των συστημάτων RBAC είναι και αυτό που τους προσφέρει μεγάλη ευελιξία και διαχειριστική ευκολία στο πλαίσιο των συνεχώς μεταβαλλόμενων και εξελισσόμενων οργανωτικών λειτουργιών καθώς σε περίπτωση μεταβολών αυτό που χρειάζεται είναι να διαγράφονται τα παλαιά δικαιώματα πρόσβασης ενός ρόλου και να του ανατίθενται νέα. Επιπλέον, σε περίπτωση ανάληψης νέων καθηκόντων από ένα χρήστη είναι εύκολη η ανάκληση των υφιστάμενων ρόλων του και η ανάθεση νέων ρόλων βάσει των νέων απαιτήσεων της εργασίας του.

Το Βασικό Μοντέλο RBAC που περιγράψαμε παρουσιάζεται συνοπτικά στην Εικόνα 6.



Εικόνα 6. Βασικό μοντέλο RBAC

Το Βασικό Μοντέλο καθορίζει ότι η ανάθεση ρόλων στους χρήστες και η ανάθεση δικαιωμάτων πρόσβασης στους ρόλους είναι δύο σχέσεις πολλά-προς-πολλά (many-to-many). Αυτό σημαίνει ότι ένας χρήστης σχετίζεται με έναν ή περισσότερους ρόλους, ένας ρόλος μπορεί να ανατεθεί σε έναν ή περισσότερους χρήστες, ένα δικαίωμα πρόσβασης μπορεί να ανατεθεί σε έναν ή περισσότερους ρόλους και ο κάθε ρόλος σχετίζεται με ένα ή περισσότερα δικαιώματα πρόσβασης.

Οι χρήστες μπορούν να ενεργοποιούν ταυτόχρονα περισσότερους από έναν ρόλους και να εξασκούν ταυτόχρονα τα δικαιώματα πρόσβασης των πολλαπλών αυτών

ρόλων. Η συνεδρία είναι μια αντιστοίχιση του χρήστη σε, πιθανά, πολλαπλούς ρόλους. Για παράδειγμα, ο χρήστης εκκινεί μία συνεδρία στο πλαίσιο της οποίας ενεργοποιεί ένα υποσύνολο των ρόλων που του έχουν ανατεθεί **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Κάθε συνεδρία σχετίζεται αποκλειστικά με ένα και μόνο χρήστη, ενώ ένας χρήστης μπορεί να έχει ταυτόχρονα ανοιχτές παραπάνω από μία συνεδρίες. Τα δικαιώματα πρόσβασης του χρήστη ισούνται με το άθροισμα όλων των δικαιωμάτων πρόσβασης των ενεργών ρόλων του χρήστη σε όλες τις ενεργές συνεδρίες του [ANSI04]**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**.

- user: S→U είναι μια συνάρτηση που αντιστοιχεί Συνόδους σε Χρήστες
- role: S→2R είναι μια συνάρτηση που αντιστοιχεί κάθε Σύνοδο σε ένα σύνολο Ρόλων.

Η δυνατότητα που δίνεται στους χρήστες να έχουν ταυτόχρονα ανοιχτές παραπάνω από μία συνεδρίες καθεμία από τις οποίες έχει ενεργοποιημένο ένα διαφορετικό συνδυασμό ρόλων υποστηρίζει την αρχή του ελαχίστου προνομίου (least privilege). Σύμφωνα με την αρχή αυτή, δεν θα πρέπει να δίνονται παραπάνω δικαιώματα παρά μόνο αυτά που είναι απαραίτητα [SCFY96]**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Ένας χρήστης στον οποίο έχουν ανατεθεί πολλαπλοί ρόλοι ενεργοποιεί οποιοδήποτε υποσύνολο των ρόλων που χρειάζεται για να ολοκληρώσει την εργασία του. Συνοψίζοντας, το βασικό μοντέλο διέπεται από τους παρακάτω τρεις βασικούς κανόνες **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**FK92]:

- *Κανόνας 1:* Ανάθεση ρόλου (Role assignment): Ένας χρήστης μπορεί να εκτελέσει μία λειτουργία μόνο αν του έχει ανατεθεί κάποιος ρόλος. Επομένως, όλοι οι ενεργοί χρήστες απαιτείται να έχουν κάποιο ενεργό ρόλο. Οι διεργασίες της αναγνώρισης και της αυθεντικοποίησης δε νοούνται ως λειτουργίες.
- *Κανόνας 2:* Εξουσιοδότηση ρόλου (Role authorization): Ο ενεργός ρόλος ενός χρήστη πρέπει να είναι εξουσιοδοτημένος για το συγκεκριμένο χρήστη από το διαχειριστή ασφαλείας του συστήματος. Σε συνδυασμό με τον Κανόνα 1 εξασφαλίζεται ότι οι χρήστες αναλαμβάνουν μόνο ρόλους για τους οποίους είναι εξουσιοδοτημένοι.
- *Κανόνας 3:* Εξουσιοδότηση συναλλαγής (Transaction authorization): Ένας χρήστης μπορεί να εκτελέσει μια λειτουργία μόνο αν η λειτουργία αυτή είναι εξουσιοδοτημένη για κάποιον από τους ενεργούς ρόλους του χρήστη. Σε συνδυασμό με τους Κανόνες 1 και 2, ο κανόνας αυτός εξασφαλίζει ότι οι χρήστες θα πραγματοποιήσουν μόνο λειτουργίες για τις οποίες είναι εξουσιοδοτημένοι.

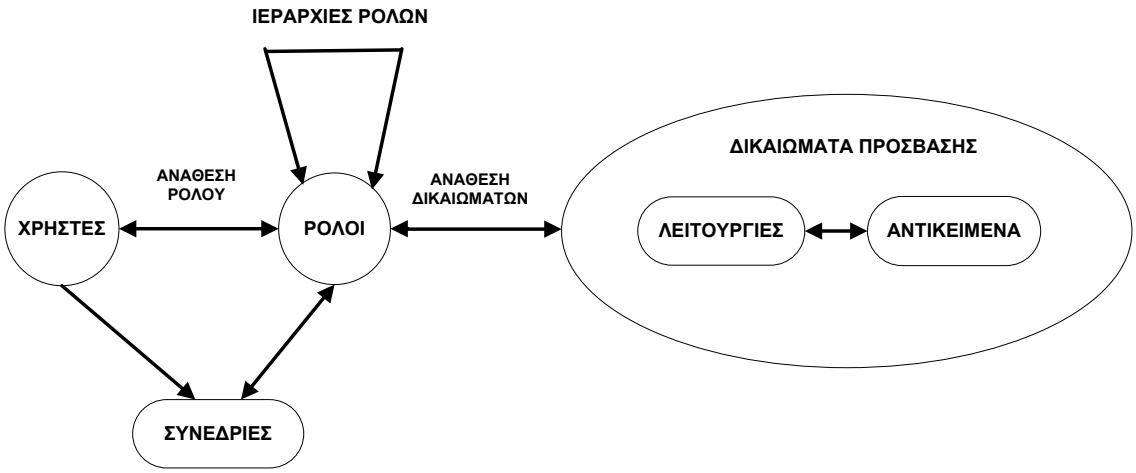
Τέλος, στο βασικό RBAC υποστηρίζεται η επανεξέταση ανάθεσης ρόλων σε χρήστες. Είναι σημαντικό να μπορεί να υποστηρίζεται η αλλαγή στους ρόλους που ανατίθενται σε ένα χρήστη. Αυτό είναι σημαντικό γιατί στην πλειονότητα των περιπτώσεων, αυτό που μεταβάλλεται στον άξονα του χρόνου είναι τα καθήκοντα του χρήστη και, κατά συνέπεια, αλλάζουν και οι ρόλοι που του ανατίθενται ώστε να αντανακλούν τη νέα δραστηριότητά του.

2.2.3. Ιεραρχικό RBAC

Στην προσπάθεια να προστεθούν νέες δυνατότητες στον τομέα της διαχείρισης των δικαιωμάτων πρόσβασης των χρηστών, η βάση του RBAC άρχισε σιγά-σιγά να εμπλουτίζεται. Έτσι, το επόμενο χαρακτηριστικό που βρίσκει εφαρμογή είναι η χρήση των ιεραρχιών και η επέκταση στο $RBAC_1$.

Ετυμολογικά, ως ιεραρχία ορίζεται *η ταξινόμηση οντοτήτων με βάση κριτήρια αξίας και σπουδαιότητας*. Αντίστοιχα, η ιεραρχία των ρόλων στο μοντέλο ελέγχου πρόσβασης που βασίζεται σε αυτούς αποτελεί τη μερική διάταξη που καθορίζει σχέσεις υπεροχής μεταξύ των ρόλων.

- $RH \subseteq R \times R$ είναι η ιεραρχία των Ρόλων, που είναι μια μερικώς διατεταγμένη σχέση



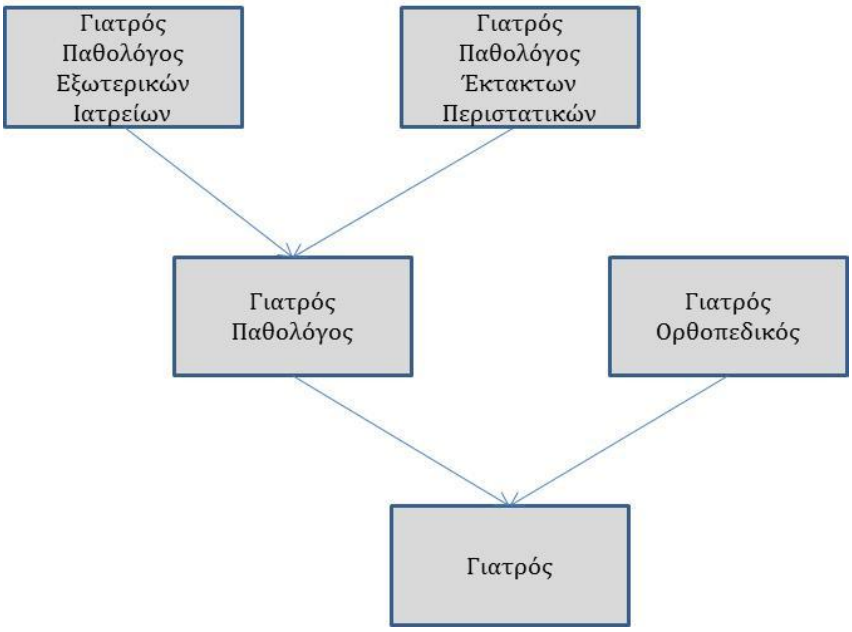
Εικόνα 7. Ιεραρχικό RBAC

Όπως υποδεικνύει και το όνομά του, το ιεραρχικό μοντέλο στηρίζεται στις ιεραρχίες και στα πλεονεκτήματα που αυτές προσδίδουν στη διαχείριση της πρόσβασης. Σε αντίθεση με τις «επίπεδες» δομές ρόλων, οι ιεραρχίες δημιουργούν συσχετίσεις μεταξύ των ρόλων που ξεφεύγουν από την απλή ανάθεση ρόλων στους χρήστες και από τον απλό καθορισμό των δικαιωμάτων. Ο πιο κοινός και αποδοτικός τρόπος απεικόνισης των ιεραρχιών είναι με τη χρήση μιας δενδροειδούς δομής. Στην Εικόνα 7 παρουσιάζεται συνοπτικά το RBAC με την εισαγωγή των ιεραρχιών.

Το βασικό κίνητρο για τη δημιουργία ιεραρχιών προήλθε από τον επιχειρηματικό κόσμο και από την ιδέα ότι στο πλαίσιο ενός οργανισμού ή μιας επιχείρησης κάποιοι ρόλοι έχουν συχνά επικαλυπτόμενα δικαιώματα. Χαρακτηριστικό παράδειγμα αποτελούν οι εργαζόμενοι σε ένα νοσοκομείο. Ας υποθέσουμε ότι στο πλαίσιο της οργανωτικής δομής μίας κλινικής έχουμε τον τομέα της γενικής παθολογικής ο οποίος χωρίζεται στα εξής δύο τμήματα: Εξωτερικά ιατρεία και έκτακτα περιστατικά. Τόσο ο γιατρός που δέχεται ασθενείς στα εξωτερικά ιατρεία με προκαθορισμένα ραντεβού όσο και ο γιατρός που

δέχεται έκτακτα περιστατικά πρέπει να έχουν π.χ. το δικαίωμα να βλέπουν αλλά και να καταχωρούν – ενημερώνουν τα στοιχεία των ασθενών στο σύστημα. Το γεγονός αυτό μπορεί να οδηγήσει στη δημιουργία ενός γενικού ρόλου που περικλείει αυτά τα δικαιώματα και που ανατίθεται σε κάθε εργαζόμενο που προσλαμβάνεται στην γενική παθολογική ανεξαρτήτως της θέσης του. Σε ό,τι αφορά όμως τα περαιτέρω καθήκοντά τους που διαφοροποιούνται εξαιτίας τις εξειδίκευσης της εργασίας τους αυτά αποτελούν δικαιώματα που ανατίθενται στους ξεχωριστούς ρόλους που αφορούν το κάθε τμήμα. Εάν δεν είχαμε την ιεραρχία τότε αναγκαστικά θα έπρεπε να επαναληφθεί η ανάθεση των κοινών δικαιωμάτων σε κάθε ένα ρόλο που εμφανίζεται στον τομέα. *Ο ρόλος αυτός που δημιουργείται με τα κοινά δικαιώματα δύο (ή περισσότερων) άλλων ρόλων που ναι μεν έχουν κοινά δικαιώματα αλλά ο ένας δεν αποτελεί υποσύνολο του άλλου ονομάζεται συνδετικός ρόλος (connector).* Το συνδετικό ρόλο τον κληρονομούν όσοι έχουν αυτά τα δικαιώματα.

Στην Εικόνα 8, απεικονίζεται με τη μορφή ανεστραμμένου δένδρου η ιεραρχία των ρόλων του παραδείγματος που περιγράφηκε παραπάνω.

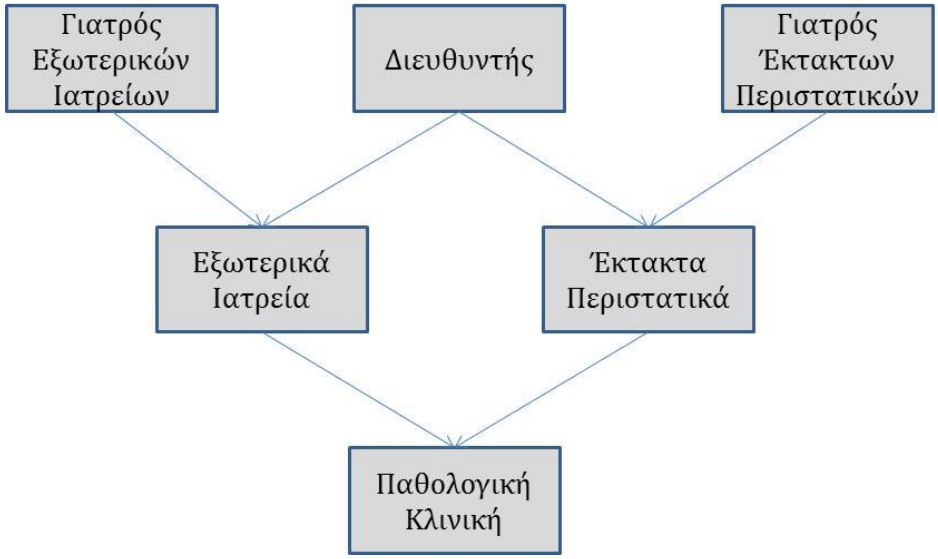


Εικόνα 8. Ιεραρχία ρόλων με τη μορφή ανεστραμμένου δένδρου

Θα πρέπει να αναφερθεί ότι δεν είναι απαραίτητο σε έναν οργανισμό να είναι όλοι οι ρόλοι μέλη μιας κοινής ιεραρχίας. Ο σκοπός της ιεραρχίας είναι μέσω της κληρονομικότητας να μειωθεί το διαχειριστικό κόστος που προκύπτει από την επανάληψη της ανάθεσης δικαιωμάτων και όχι να περιοριστεί μέσα σε αυστηρά πλαίσια η δομή του οργανισμού. Η διάταξη των ρόλων οδηγεί στη δημιουργία ρόλων χαμηλών επιπέδων και αντίστοιχα ρόλων υψηλών επιπέδων οι οποίοι συνδέονται με τέτοιο τρόπο ώστε να υποστηρίζεται η μεταβατική ιδιότητα των δικαιωμάτων των ιεραρχιών του

μοντέλου. Αυτό που γίνεται είναι ότι οι ρόλοι των υψηλότερων επιπέδων κληρονομούν τα δικαιώματα των ρόλων χαμηλότερων επιπέδων με τους οποίους αυτοί σχετίζονται άμεσα ή έμμεσα. Θα πρέπει να σημειωθεί ότι οι ρόλοι των χαμηλότερων επιπέδων είναι πιο γενικοί σε αντίθεση με αυτούς των υψηλότερων επιπέδων οι οποίοι είναι πιο εξειδικευμένοι και πιο «δυνατοί». Στο πλαίσιο της κληρονομικότητας, τη μεταβατική ιδιότητα στα συστήματα που υποστηρίζουν ιεραρχίες ρόλων αντανακλούν τόσο τα δικαιώματα όσο και ο αριθμός των χρηστών – μελών των εκάστοτε ρόλων. Στις ιεραρχίες των ρόλων το πλήθος των δικαιωμάτων και ο αριθμός των χρηστών στους οποίους αυτοί ανατίθενται ακολουθούν αντίθετες πορείες καθώς κοιτάζουμε μία ιεραρχία ρόλων με τη μορφή δένδρου [ANSI04], [SFK00]. Έτσι στο παράδειγμά μας, στο ρόλο του Γιατρού των εξωτερικών ιατρείων έχουν ανατεθεί λιγότερα δικαιώματα σε σχέση με αυτά του ρόλου του γιατρού των έκτακτων περιστατικών αλλά ο αριθμός των χρηστών που ανήκουν στο ρόλο αυτό είναι μεγαλύτερος σε σχέση με αυτόν των εξωτερικών ιατρείων.

Το πρόβλημα που δημιουργείται με την κληρονομικότητα είναι ότι οι ρόλοι των υψηλών επιπέδων μπορεί τελικά να θεωρούνται και υψηλού ρίσκου εξαιτίας των πολλών δικαιωμάτων που τελικά έχουν κληρονομώντας και όλα αυτά των προγόνων τους. Προκειμένου να αποφευχθεί κάτι τέτοιο δίνεται η δυνατότητα δημιουργίας ιδιωτικών ρόλων (private). Στο παράδειγμα της κλινικής, αν θεωρήσουμε την δομή της Εικόνας 9, ο διευθυντής κληρονομεί τόσο τα δικαιώματα από τα εξωτερικά ιατρεία όσο και από τα έκτακτα περιστατικά. Αυτό όμως του δίνει πολλές δυνατότητες, πράγμα που μπορεί να θεωρηθεί και μειονέκτημα καθώς σε περίπτωση κακόβουλης ενέργεια θα μπορούσε εν δυνάμει να πληγεί η αξιοπιστία του συστήματος. Έτσι, δημιουργώντας δύο ιδιωτικούς ρόλους, έναν για κάθε τομέα αντίστοιχα, επιτρέπουμε να κληρονομήσει ο διευθυντής το μεγαλύτερο μέρος των δικαιωμάτων των ρόλων «Γιατρός Εξωτερικών Ιατρείων» και «Γιατρός Έκτακτων Περιστατικών» αλλά κάποια δικαιώματα κληρονομούνται μόνο στους αντίστοιχους ιδιωτικούς ρόλους. Με αυτό τον τρόπο περιορίζεται η «δύναμη» του ρόλου του Διευθυντή. Με άλλα λόγια με τη χρήση των ιδιωτικών ρόλων μπορούμε να επιτύχουμε περιορισμό της κληρονομικότητας των δικαιωμάτων [SFK00].



Εικόνα 9. Ιεραρχία ρόλων με χρήση ιδιωτικού ρόλου

Παρόλο που το διαχειριστικό κόστος για τη σχεδίαση ενός συστήματος είναι πιο υψηλό με τη χρήση ιεραρχιών, τα πλεονεκτήματα που προκύπτουν για τη μετέπειτα χρήση, διαχείριση και ανακατανομή των δικαιωμάτων αντισταθμίζουν το κόστος και οδηγούν στην καλύτερη σχεδίαση της πολιτικής διαχείρισης δικαιωμάτων πρόσβασης των χρηστών.

Στο RBAC ορίζονται δύο ειδών ιεραρχίες [ANSI04]:

- Γενικές Ιεραρχίες Ρόλων (General Role Hierarchies)
- Περιορισμένες Ιεραρχίες Ρόλων (Limited Role Hierarchies).

Οι Γενικές Ιεραρχίες Ρόλων αποτελλούνται από αυθαίρετες διατάξεις ρόλων που επιτρέπουν την πολλαπλή κληρονομικότητα δικαιωμάτων και χρηστών μεταξύ των ρόλων που συμμετέχουν στην ιεραρχία**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Με άλλα λόγια ο κάθε ρόλος έχει τη δυνατότητα να κληρονομεί δικαιώματα από περισσότερους του ενός προγόνους. Με αυτή τη δυνατότητα δημιουργούνται οι λεγόμενοι *συνδυαστικοί ρόλοι (combiner roles)*. Οι ρόλοι αυτοί συνδυάζουν μέρος των δικαιωμάτων δύο περισσοτέρων ρόλων-πηγών. Έτσι η απεικόνιση των γενικών ιεραρχιών, εξαιτίας της μεγάλης ευελιξίας και ελευθερίας που παρέχουν, γίνεται κατά κύριο ρόλο μέσα από περίπλοκες δομές διαγραμμάτων που ξεφεύγουν από τα πλαίσια του δένδρου.

Οι Περιορισμένες Ιεραρχίες Ρόλων αποτελούν υποσύνολο των γενικών ιεραρχιών. Οι δομές απεικόνισής τους είναι απλούστερα δένδρα τα οποία περιορίζουν τους άμεσους απογόνους σε αυστηρά και μόνο ένα. Παρόλο που μπορεί να μην υποστηρίζουν την πολλαπλή κληρονομικότητα, έχουν σίγουρα ένα σημαντικό συγκριτικό πλεονέκτημα έναντι των «επίπεδων» δομών ρόλων στη διαχείριση αυτών.

Αν και οι Γενικές Ιεραρχίες αντιπροσωπεύουν πιο ρεαλιστικά τις περίπλοκες δομές των οργανισμών και των επιχειρήσεων, οι Περιορισμένες Ιεραρχίες είναι αυτές που φαίνεται να έχουν ευρύτερη χρήση. Ο λόγος που συμβαίνει αυτό έγκειται στο ότι παρά τους περιορισμούς που θέτουν είναι πιο απλές στην απεικόνιση αλλά και την κατανόησή τους. Άλλωστε οι δομές δένδρων, μέσα από τις οποίες αναλύονται, χρησιμοποιούνται ήδη σε πάρα πολλά συστήματα διαχείρισης (π.χ. αρχείων και φακέλων) και είναι γενικά αποδεκτές και ευρέως κατανοητές.

2.2.4. Περιορισμένο RBAC

Η έννοια του *διαχωρισμού των καθηκόντων* θέτει επιπλέον περιορισμούς στη διαχειριστική δομή του μοντέλου πρόσβασης RBAC και γι' αυτό το λόγο συναντάται στη βιβλιογραφία ως *περιορισμένο RBAC (Constrained RBAC)*.

Σύμφωνα με το ANSI [ANSI00] η αρχή του διαχωρισμού των καθηκόντων ορίζεται ως εξής: *Διαίρεση των ευθυνών που αφορούν «ευαίσθητες» πληροφορίες ώστε καμία μονάδα που ενεργεί ατομικά να μην μπορεί να βάλει σε κίνδυνο την ασφάλεια του συστήματος επεξεργασίας δεδομένων.*

Με άλλα λόγια, ο πιο απλός τρόπος για να αντιληφθούμε το τι σημαίνει διαχωρισμός καθηκόντων είναι να σκεφτούμε μία λειτουργία η οποία είναι μεγίστης σημασίας για το σύστημά και της οποίας η μη-σωστή εκτέλεση μπορεί να έχει πολύ αρνητικές συνέπειες για τον οργανισμό. Θα πρέπει να σημειωθεί ότι η μη-σωστή εκτέλεση μπορεί να προκύψει είτε από λάθος ενέργεια του χρήστη είτε από κάποια κακόβουλη απόπειρα επέμβασης στο σύστημα. Προκειμένου να αποφευχθεί κάτι τέτοιο γίνεται επιμερισμός της λειτουργίας σε δύο ή περισσότερους ρόλους με τέτοιο τρόπο έτσι ώστε η ολοκλήρωσή της να απαιτεί την υλοποίηση επιμέρους τμημάτων-μερών της λειτουργίας από όλους τους εμπλεκόμενους ρόλους**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Το κύριο πλεονέκτημα του διαχωρισμού των καθηκόντων είναι ότι περιορίζεται σε πολύ σημαντικό βαθμό ο κίνδυνος της κακόβουλης ενέργειας στο σύστημα καθότι για να επιτευχθεί κάτι τέτοιο απαιτείται πλέον συντονισμένη ενέργεια όλων των ρόλων στους οποίους έχει επιμεριστεί η ευθύνη. Επιπλέον, καθίσταται ευκολότερος ο έλεγχος και ο εντοπισμός τυχόν λαθών αφού εμπλέκονται περισσότεροι από ένας χρήστες. Ο διαχωρισμός των καθηκόντων βρίσκει πολύ συχνά εφαρμογή στον στρατιωτικό τομέα όπου για πολλές κρίσιμες ενέργειες απαιτείται η ταυτόχρονη ενέργεια δύο διαφορετικών ατόμων προκειμένου, για παράδειγμα, να οπλιστούν συστήματα επίθεσης.

Στο περιορισμένο RBAC διακρίνουμε δύο μεθόδους διαχωρισμού των καθηκόντων:

- Στατικός Διαχωρισμός Καθηκόντων (Static Separation of Duty), και
- Δυναμικός Διαχωρισμός Καθηκόντων (Dynamic Separation of Duty).

Η κύρια διαφορά των δύο μεθόδων είναι η χρονική στιγμή εφαρμογής του διαχωρισμού. Ο Στατικός Διαχωρισμός Καθηκόντων θέτει περιορισμούς τη στιγμή της ανάθεσης ενός ρόλου σε ένα χρήστη σε αντίθεση με τον Δυναμικό Διαχωρισμό Καθηκόντων όπου οι περιορισμοί τίθενται όταν οι χρήστες χρησιμοποιούν ενεργά το σύστημα [FKC07].

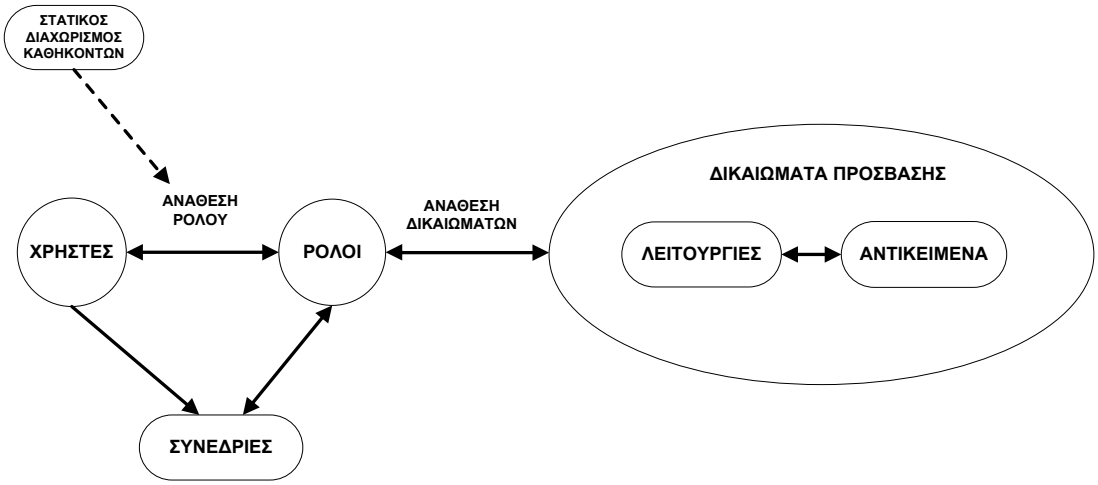
Όσο οξύμωρο και αν ακούγεται, σε πολλούς οργανισμούς ο διαχωρισμός των καθηκόντων χρησιμοποιείται για την επιβολή πολιτικών σύγκρουσης συμφερόντων. Απώτερος σκοπός είναι ο περιορισμός των χρηστών προκειμένου να μην αποκτήσουν υψηλό επίπεδο εξουσίας ειδικά σε θέσεις ισχύος και διοίκησης όπου τα δικαιώματα των χρηστών μπορεί να είναι πολλά και, κατά συνέπεια, καθίσταται πιο εύκολη και «προκλητική» η επιτέλεση μιας κακόβουλης ενέργειας.

Σύγκρουση συμφερόντων μπορεί να προκύψει όταν ο χρήστης αποκτά εξουσιοδότηση για δικαιώματα πρόσβασης που σχετίζονται με δύο ή περισσότερους αντικρουόμενους ρόλους. Ο Στατικός Διαχωρισμός Καθηκόντων αποτελεί μια λύση στην σύγκρουση συμφερόντων καθώς επιβάλλει περιορισμούς στην ανάθεση ρόλων στους χρήστες. Αυτό στην πράξη σημαίνει ότι εάν ένας χρήστης είναι εξουσιοδοτημένος για ένα ρόλο, τότε απαγορεύεται να του ανατεθεί ένας δεύτερος ρόλος ο οποίος έχει συγκρουόμενα με τον πρώτο δικαιώματα πρόσβασης. Οι δύο αυτοί ρόλοι ονομάζονται αμοιβαία αποκλειόμενοι ρόλοι. Επομένως, σύμφωνα με το Στατικό Διαχωρισμό Καθηκόντων σε ένα χρήστη μπορεί να ανατεθεί ένας ρόλος μόνο όταν αυτός ο ρόλος δεν είναι αμοιβαία αποκλειόμενος με οποιονδήποτε από τους ήδη υπάρχοντες ρόλους του χρήστη [ANSI04]. Ο έλεγχος αυτός πραγματοποιείται τη στιγμή της ανάθεσης του ρόλου στο χρήστη όπως απεικονίζεται και στην Εικόνα 10.

Μπορούμε να ορίσουμε το Στατικό Διαχωρισμό Καθηκόντων ως ένα ζευγάρι (σύνολο ρόλων, ν), όπου σε κανένα χρήστη δε μπορεί να ανατεθούν ταυτόχρονα ν ρόλοι από το σύνολο αυτό. Στις περισσότερες των περιπτώσεων το ν=2, οπότε και σε κάθε χρήστη μπορεί να ανατεθεί ένας και μόνος ρόλος από το σύνολο αυτό. Όμως από τον ορισμό αυτό προκύπτουν πολλές πολιτικές Στατικού Διαχωρισμού Καθηκόντων ανάλογα με το συνδυασμό των ρόλων για τους οποίους περιορίζεται η ανάθεση στους χρήστες. Για παράδειγμα, μπορούν να περιορίσουν ένα χρήστη από το να μπορεί να γίνει μέλος οποιουδήποτε συνδυασμού δύο ή περισσοτέρων ρόλων από το σύνολο των ρόλων σε μια περίπτωση ενώ σε μια άλλη να τον περιορίσουν από το να μπορεί να του ανατεθεί κάποιος ρόλος από ένα προκαθορισμένο σύνολο ρόλων.

Επανερχόμενοι στο παράδειγμα του Νοσοκομείου, μια περίπτωση σύγκρουσης συμφερόντων και διαχωρισμού καθηκόντων εμφανίζεται στη διαδικασία έγκρισης και χορήγησης προμηθειών, εξοπλισμού και φαρμακευτικού υλικού. Η αίτηση και η δημιουργία μιας παραγγελίας εξοπλισμού πραγματοποιούνται από το τμήμα της παθολογικής ενώ στη συνέχεια η έγκριση δίδεται από τον προϊστάμενο του τμήματος προμηθειών. Οι δύο αυτοί ρόλοι είναι αμοιβαία αποκλειόμενοι καθώς εάν ο ίδιος

υπάλληλος πραγματοποιούσε τόσο τη παραγγελία όσο και την έγκρισή της, αυτό σημαίνει μεγάλη συγκέντρωση δύναμης και εξουσίας σε αυτόν και ελλοχεύει τον κίνδυνο της απάτης. Επομένως, δε μπορεί να πραγματοποιεί όλες τις παραπάνω διαδικασίες ο ίδιος εργαζόμενος.



Εικόνα 10 Περιορισμένο RBAC με Στατικό Διαχωρισμό Καθηκόντων

Ο Στατικός Διαχωρισμός Καθηκόντων είναι εύκολα υλοποιήσιμος στο πλαίσιο ενός συστήματος RBAC. Είναι, όμως, αρκετά περιοριστικός και πολλές φορές δύσκολα εφαρμόσιμος σε μικρούς οργανισμούς που απασχολούν μικρό αριθμό ατόμων. Στις περιπτώσεις αυτές καθίσταται δύσκολος ο καθορισμός των αμοιβαία αποκλειόμενων ρόλων καθώς δεν υπάρχει επαρκής αριθμός εργαζόμενων για να πραγματοποιήσουν όλες τις αμοιβαία αποκλειόμενες λειτουργίες.

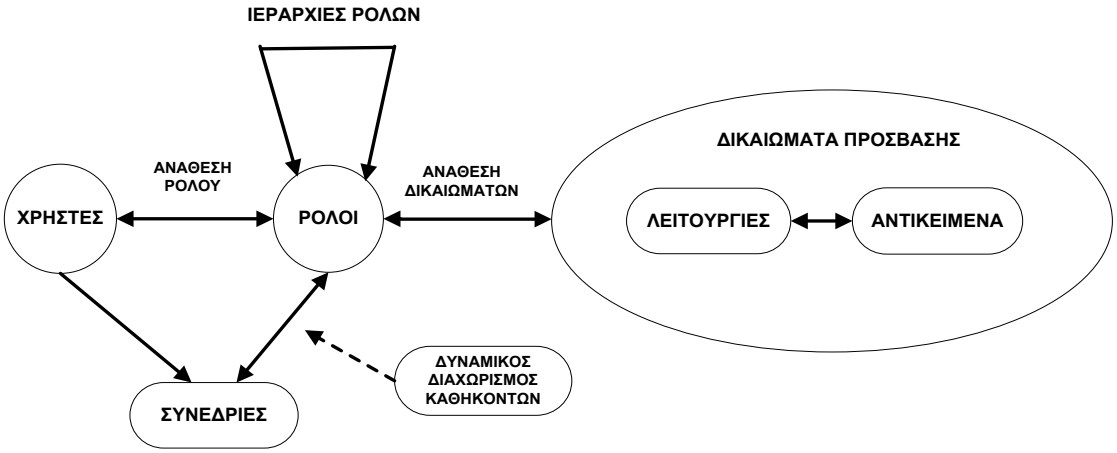
Τη λύση στη δυσκαμψία που εμφανίζει πολλές φορές ο *Στατικός Διαχωρισμός Καθηκόντων* έρχεται να φέρει ο *Δυναμικός Διαχωρισμός Καθηκόντων* ο οποίος προσδιορίζει αποκλειστικές σχέσεις όσον αφορά τους ρόλους που ενεργοποιούνται ως μέρος της συνεδρίας ενός χρήστη. Όπως και στο *Στατικό Διαχωρισμό*, σκοπός είναι ο περιορισμός των διαθέσιμων δικαιωμάτων πρόσβασης σε ένα χρήστη. Ο χρήστης εκκινεί μία συνεδρία στο πλαίσιο της οποίας μπορεί να ενεργοποιήσει ένα οποιοδήποτε υποσύνολο των εξουσιοδοτημένων για αυτόν ρόλων. Ο *Δυναμικός Διαχωρισμός Καθηκόντων* περιορίζει τη διαθεσιμότητα των δικαιωμάτων πρόσβασης θέτοντας περιορισμούς στους ρόλους που μπορεί να ενεργοποιηθούν στο πλαίσιο μιας συνεδρίας του χρήστη [ANSI04].

Σε αντίθεση με το *Στατικό Διαχωρισμό*, που παρέχει προστασία από σύγκρουση συμφερόντων πραγματοποιώντας ελέγχους την ώρα της ανάθεσης ενός ρόλου σε ένα χρήστη, ο Δυναμικός Διαχωρισμός πραγματοποιεί ελέγχους και επιβάλλει περιορισμούς την ώρα της ενεργοποίησης ενός ρόλου στο πλαίσιο μιας συνεδρίας ενός χρήστη (Εικόνα 11). Ο *Δυναμικός Διαχωρισμός Καθηκόντων* επιτρέπει την εξουσιοδότηση ενός χρήστη σε

δύο ρόλους που δεν προκαλούν σύγκρουση συμφερόντων όταν δρουν ανεξάρτητα αλλά θέτουν ζητήματα ασφαλείας όταν ενεργοποιούνται ταυτόχρονα [ANSI04], [FKC07].

Όμοια με το *Στατικό Διαχωρισμό Καθηκόντων*, θα μπορούσαμε να ορίσουμε το Δυναμικό Διαχωρισμό Καθηκόντων ως ένα ζευγάρι (σύνολο ρόλων, ν), με ν≥2, με την ιδιότητα ότι σε καμία συνεδρία του χρήστη δε θα ενεργοποιηθούν ταυτόχρονα ν ή περισσότεροι ρόλοι από το σύνολο των ρόλων**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Οι ρόλοι που δεν επιτρέπεται να ενεργοποιηθούν ταυτόχρονα ονομάζονται, και σε αυτή την περίπτωση, αμοιβαία αποκλειόμενοι ρόλοι.

Η πολύ σημαντική αρχή του ελαχίστου δικαιώματος ενισχύεται με το Δυναμικό Διαχωρισμό των Δεδομένων αφού κάθε χρήστης έχει διαφορετικά επίπεδα πρόσβασης σε διαφορετικές χρονικές στιγμές ανάλογα με το ρόλο του. Αποφεύγεται με αυτό τον τρόπο η συγκέντρωση παραπάνω δικαιωμάτων πρόσβασης από αυτά που χρειάζεται για να επιτελέσει την εργασία του με όλους τους κινδύνους που αυτό κρύβει. Επιπρόσθετα, ο χρήστης κρατάει τα δικαιώματα πρόσβασης μόνο για το χρονικό διάστημα που τα χρειάζεται για να επιτελέσει την εργασία του.



Εικόνα 11. Περιορισμένο RBAC με Ιεραρχίες και Δυναμικό Διαχωρισμό Καθηκόντων

Ο Δυναμικός Διαχωρισμός Καθηκόντων υποστηρίζει, και αυτός με τη σειρά του, την ύπαρξη ιεραρχιών και, σε αντίθεση με τον Στατικό, οι ρόλοι μπορούν να σχετίζονται ιεραρχικά μεταξύ τους μέσω κάποιας σχέσης περιορισμού (containment)**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**. Το γεγονός αυτό είναι απόλυτα συνεπές και δεν παραβιάζει τη βασική ιδιότητα του Δυναμικού Διαχωρισμού που απαγορεύει την ταυτόχρονη ενεργοποίηση ρόλων.

Υπάρχουν πολλές περιπτώσεις στις οποίες θα μπορούσαμε να χρησιμοποιήσουμε Στατικό αντί για Δυναμικό Διαχωρισμό και να πετύχουμε το ίδιο αποτέλεσμα. Η δυσκαμψία που εμφανίζει και το μεγάλο πολλές φορές κόστος που δημιουργεί η χρήση

του όμως μας οδηγεί στην επιλογή του Δυναμικού ο οποίος προσφέρει μεγάλη ευελιξία και λειτουργικότητα. Επιστρέφοντας στο παράδειγμα του νοσοκομείου, μια τέτοια περίπτωση είναι αυτή της διαδικασίας παραγγελίας υλικού. Όπως προείπαμε, απαιτούνται δύο ξεχωριστοί υπάλληλοι καθένας από τους οποίους θα αναλάβει τους αμοιβαία αποκλειόμενους ρόλους του εργαζόμενου που συμπληρώνει την αίτηση της προμήθειας και του προϊσταμένου που εγκρίνει και κάνει την παραγγελία. Χρησιμοποιώντας Στατικό Διαχωρισμό Δεδομένων και θέτοντας τους δύο αυτούς ρόλους ως αμοιβαία αποκλειόμενους προστατεύουμε τον οργανισμόα από την περίπτωση συγκέντρωσης μεγάλης εξουσίας για την υλοποίηση μιας ιδιαίτερα κρίσιμης διαδικασίας στα χέρια ενός χρήστη. Δυστυχώς στην πράξη λόγω έλλειψης προσωπικού ή άλλων αιτιών είναι δύσκολο να υπάρχουν δύο διαφορετικά άτομα που θα στελεχώσουν τους ρόλους. Στην περίπτωση αυτή η λύση προσφέρεται από το Δυναμικό Διαχωρισμό Καθηκόντων. Μπορεί ορισμένοι εργαζόμενοι να είναι εξουσιοδοτημένοι να έχουν και το ρόλο αυτού που δίνει την παραγγελία και το ρόλο αυτού που εγκρίνει αλλά απαγορεύεται να ενεργοποιήσουν τους δύο αυτούς ρόλους ταυτόχρονα στο πλαίσιο της ίδιας συνεδρίας. Συνοψίζοντας, διαπιστώνουμε ότι ο Δυναμικός Διαχωρισμός Καθηκόντων προσφέρει μεγάλη ευελιξία και ευκολία στο σύγχρονο εμπορικό και επιχειρηματικό κόσμο καθώς αντιπροσωπεύειπιο ρεαλιστικά τις δομές και τις ανάγκες των οργανισμών.

2.2.5. Συμμετρικό RBAC

Στο πλαίσιο μιας ιεραρχίας οι περιορισμοί κληρονομούνται και θα πρέπει να δίνεται μεγάλη προσοχή έτσι ώστε να διασφαλίζεται ότι η κληρονομικότητα δεν υπονομεύει τις πολιτικές του Διαχωρισμού Καθηκόντων. Ο Διαχωρισμός Καθηκόντων παρουσία Ιεραρχιών λειτουργεί με τον ίδιο ακριβώς τρόπο με τον απλό Διαχωρισμό Καθηκόντων με τη διαφορά ότι όταν επιβάλλονται οι περιορισμοί κατά την ανάθεση ενός ρόλου ελέγχονται για σύγκρουση όχι μόνο οι άμεσα ανατεθειμένοι στο χρήστη ρόλοι αλλά και οι ρόλοι που αυτός έχει κληρονομήσει.

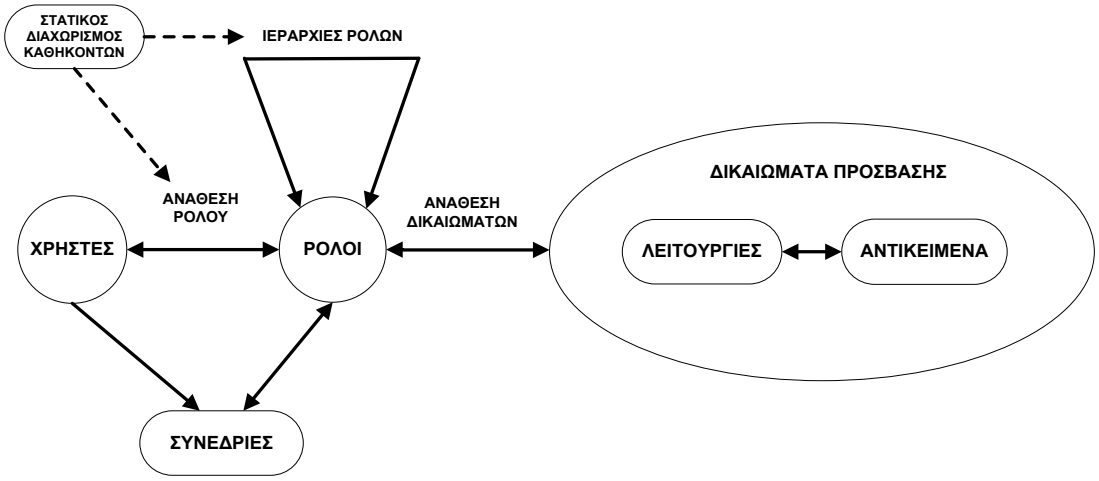
Δεδομένου ότι υποστηρίζονται οι ιεραρχίες και εδώ συναντάμε αυθαίρετες αλλά και περιορισμένες διατάξεις ορίζοντας κατ’ αυτόν τον τρόπο δύο υποεπίπεδα στο συμμετρικό RBAC.

Η επιπλέον ιδιότητα που προσφέρεται είναι η επανεξέταση της ανάθεσης αδειών σε ρόλους. Μπορούμε να το σκεφτούμε αυτό σε αντιστοιχία με την επανεξέταση ανάθεσης ρόλων σε χρήστες που υποστηρίζεται στο βασικό RBAC. Η ανάγκη για προσαρμογή των δικαιωμάτων που ανατίθενται στους ρόλους κρίνεται απαραίτητη μέσα σε έναν οργανισμό όπου οι χρήστες και οι ρόλοι τους μπορεί να αλλάζουν δυναμικά. Εάν για παράδειγμα, σκεφτούμε την πιθανή προαγωγή ενός γιατρού, τότε θα πρέπει να γίνει πολύ προσεκτική προσαρμογή των δικαιωμάτων του έτσι ώστε ούτε να καταργηθούν δικαιώματα που του είναι χρήσιμα για την εργασία του αλλά ούτε και να του δοθούν περισσότερα από όσα χρειάζονται, τηρώντας την αρχή του ελαχίστου δικαιώματος.

Μία άλλη περίπτωση στην οποία κρίνεται απαραίτητη η επανεξέταση της ανάθεσης δικαιωμάτων σε ρόλους είναι η περίπτωση όπου γίνεται αλλαγή των καθηκόντων. Στην περίπτωση του νοσοκομείου, η προσθήκη μια ειδικότητας που δεν προϋπήρχε δημιουργεί νέες λειτουργίες που θα πρέπει να πραγματοποιούν το προσωπικό (γιατροί, νοσοκόμες, γραμματειακή υποστήριξη) που θα τους ανατεθεί η λειτουργία αυτού και κατά συνέπεια η ανάθεση νέωνδικαιωμάτων στο σύστημα. Έτσι, ο διαχειριστής του συστήματος θα πρέπει να διαμορφώσει ανάλογα τους αντίστοιχους ρόλους. Ο λόγος που η ιδιότητα αυτή παρουσιάζεται στο τέταρτο και τελευταίο επίπεδο του προτύπου είναι εξαιτίας της μεγάλης δυσκολίας που παρουσιάζει η υλοποίησή της, ειδικά σε οργανισμούς μεγάλης κλίμακας όπου ο έλεγχος είναι κατανεμημένος [FKC07].

Το μοντέλο που περιγράψαμε παραπάνω είναι αυτό που δημοσιεύτηκε από το NIST και αναγνωρίστηκε ως το βασικό πρότυπο [ANSI04]. Όπως είδαμε, το μοντέλο αυτό καθορίζει τις βασικές αρχές και κανόνες που πρέπει να διέπουν τη λειτουργία των συστημάτων που βασίζονται στο RBAC και συνοπτικά παρουσιάζεται στην Εικόνα 12.

Ιδιαίτερα σημαντικό είναι να διευκρινιστεί ότι υπάρχουν αρκετά σημεία τα οποία δεν έχουν οριστεί και υιοθετηθεί με επίσημο τρόπο είτε γιατί από τη φύση τους αυτό δεν είναι δυνατό είτε γιατί δε θεωρήθηκε αναγκαία η παρουσία τους στο πλαίσιο του προτύπου.



Εικόνα 12. Συμμετρικό RBAC

Ένα από αυτά τα στοιχεία είναι η κλιμάκωση του μοντέλου. Στο πρότυπο δεν διευκρινίζεται σε κάποιο σημείο το πώς μπορεί να κλιμακωθεί το μοντέλο όσον αφορά τον αριθμό των ρόλων, τον αριθμό των δικαιωμάτων πρόσβασης ή ακόμα και το μέγεθος των ιεραρχιών. Όπως, μπορεί κανείς να αντιληφθεί, αυτό είναι σημαντικό κριτήριο στην επιλογή ενός διαχειριστικού συστήματος για μεγάλης κλίμακας επιχειρήσεις και οργανισμούς. Επιπλέον, σε ό,τι αφορά τη φύση των δικαιωμάτων, στο πρότυπο δεν καθορίζεται σαφής προσδιορισμός της. Δεν διευκρινίζεται κατά πόσο τα δικαιώματα

αφορούν ενέργειες και λειτουργίες του συστήματος σε χαμηλό επίπεδο (π.χ. δικαιώματα ανάγνωσης και γραφής σε αρχεία) ή σε πιο υψηλό επίπεδο όπου τα δικαιώματα αφορούν τις αρμοδιότητες των χρηστών(π.χ. δικαίωμα ανάληψης ή κατάθεσης στο πλαίσιο ενός τραπεζικού οργανισμού). Εκτός αυτού, το μοντέλο δεν αναγνωρίζει τα λεγόμενα *αρνητικά δικαιώματα πρόσβασης (negative permissions)*. Στο μοντέλο καθορίζεται τι μπορεί να κάνει ο χρήστης ενώ δεν δίνεται η δυνατότητα στο διαχειριστή του συστήματος να προσδιορίσει τι *δεν* μπορεί να κάνει.

Γενικά, υπάρχουν αρκετά κενά που σχετίζονται με τη διαχείριση του μοντέλου RBAC. Χαρακτηριστικό είναι ότι απουσιάζει η έννοια της εξουσιοδότησης για την επεξεργασία των ρόλων και των δικαιωμάτων. Ποιος τελικά είναι υπεύθυνος για το σχεδιασμό των ρόλων; Πώς γίνεται ο σχεδιασμός των ρόλων και ποια δικαιώματα περιλαμβάνουναυτοί οι ρόλοι; Ποιος αναλαμβάνει την ανάθεση των ρόλων αυτών στους χρήστες; Ποιος καθορίζει τον ιεραρχικό συσχετισμό των ρόλων; Όλα αυτά είναι ερωτήματα που δεν απαντώνται μέσα από το πρότυπο του NIST. Κάθε παραλλαγή που έχει αναπτυχθεί με βάση το RBAC δίνει τις δικές της απαντήσεις και λύσεις ανάλογα με την αγορά, και, συνεπώς, με την χρήση, στην οποία απευθύνεται.

Έχουμε ήδη αναφέρει ότι στο πλαίσιο του βασικού μοντέλου RBAC, δίνεται η δυνατότητα σε κάθε χρήστη να έχει περισσότερους από έναν ενεργούς ρόλους. Δεν περιγράφεται πώς γίνεται η ενεργοποίηση των ρόλων και ποιος τελικά επιλέγει ποιοι ρόλοι είναι ενεργοί σε κάθε συνεδρία (είναι προκαθορισμένοι από το σύστημα ή επιλέγει ο χρήστης). Τέλος, ένα σημαντικός παράγοντας είναι η ανάκληση των ρόλων, ο τρόπος χειρισμού της ανάκλησης και οι συνέπειες της ανάκλησης στο σύστημα. Παρόλα αυτά, το μοντέλο δε λαμβάνει υπόψη του αυτή τη συνιστώσα.

Η μη εξάρτησή του από πολιτικές το καθιστούν μοντέλο ιδιαίτερα ευέλικτο, δυναμικό και εύκολα προσαρμόσιμο στις εκάστοτε συνθήκες. Η σημαντική αυτή ιδιότητά του βοήθησε σημαντικά στη γρήγορη εξέλιξη και ανάπτυξή του από τη θεωρητική προσέγγιση στην πρακτική εφαρμογή.

Το RBAC πέρα από ένα μοντέλου ελέγχου πρόσβασης υπό την έννοια που περιγράφηκε παραπάνω, μπορεί να θεωρηθεί και ως μια προσέγγιση της διαχείρισης της συνολικής δραστηριότητας που πραγματοποιείται μέσα σε ένα περιβάλλον πληροφοριακών συστημάτων. Όπως έχουμε ήδη αναφέρει, η αρχή του διαχωρισμού των καθηκόντων, οι ιεραρχίες αλλά και ο συνδυασμός αυτών βοηθούν στην καλύτερη αναπαράσταση των επιχειρηματικών δραστηριοτήτων και, κατά συνέπεια, στην καλύτερη παρακολούθηση των διεργασιών που λαμβάνουν χώρα και στον καλύτερο έλεγχο της πρόσβασης στην πληροφορία.

Τέλος, ο χαρακτηρισμός του RBAC ως ένα γενικευμένο μοντέλο που παρέχει κεντρικό έλεγχο των πόρων, μπορεί να υποστηριχθεί από το γεγονός ότι τόσο το MAC όσο και το DAC μπορεί να υλοποιηθούν μέσω του RBAC. Φυσικά αυτό προϋποθέτει τον ορισμό κατάλληλων ρόλων, αναθέσεων και περιορισμών. Εδώ αξίζει να σημειωθεί ότι υλοποίηση

του DAC μέσω του RBAC θεωρείται αρκετά πιο περίπλοκη διαδικασία σχετικά με αυτή της υλοποίησης του MAC.

Η άλλη όψη του νομίσματος της γενίκευσης είναι ότι η μη ύπαρξη σαφώς καθορισμένων περιορισμών για παραμέτρους όπως είναι ο χρόνος και το περιβάλλον δημιουργούν ελλείψεις για την πιο άρτια λειτουργία του μοντέλου. Οι ελλείψεις αυτές ανοίγουν το δρόμο για την εισαγωγή επεκτάσεων στο βασικό μοντέλο που περιγράψαμε, οι οποίες προσδίδουν νέες λειτουργικότητες.

2.3. Επεκτάσεις του RBAC

Παρά τις ομοιότητες που παρουσιάζουν τα διάφορα πληροφοριακά συστήματα του εμπορικού κόσμου, καθένα από αυτά έχει τις δικές του ιδιαιτερότητες. Οι ιδιαιτερότητες αυτές προκάλεσαν την ανάπτυξη νέων επεκτάσεων που βασίζονται στο RBAC και οι οποίες στόχο έχουν να καλύψουν τις εξειδικευμένες ανάγκες του εκάστοτε πληροφοριακού συστήματος.

Στη συνέχεια του κεφαλαίου αυτού περιγράφονται κάποια από τα βασικότερα μοντέλα – επεκτάσεις του RBAC. Ειδικότερα αναλύονται τα:

- Μοντέλα Διαχείρισης Πρόσβασης Βασισμένα σε Ρόλους με Χρονικούς Περιορισμούς
- Μοντέλα Διαχείρισης Πρόσβασης Βασισμένα σε Ρόλους με Χωρικούς και Χρονικούς Περιορισμούς
- Μοντέλα Διαχείρισης Πρόσβασης Βασισμένα σε Ρόλους με Δυνατότητες Εξουσιοδότησης
- Μοντέλο Διαχείρισης Πρόσβασης Βασισμένα σε Ρόλους με Επίκεντρο την Ποιότητα Υπηρεσιών.

Σημειώνουμε ότι λόγω του τεράστιου πλήθους μοντέλων και επεκτάσεων που έχουν προταθεί με βάση το RBAC θα παρουσιάσουμε αναλυτικά ορισμένα από τα κυρίαρχα μοντέλα για κάθε κατηγορία και θα πραγματοποιηθεί μια πιο σύντομη ενδεικτική παρουσίαση των άλλων μοντέλων διαχείρισης πρόσβασης.

2.3.1. RBAC με Χρονικούς Περιορισμούς

Όπως έχουμε ήδη αναφέρει, το RBAC αποτελεί ένα γενικό μοντέλο, γεγονός που του δίνει την ευελιξία να μπορεί να ενσωματωθεί σε διαφορετικού τύπου πληροφοριακά συστήματα και να προσαρμοστεί στις εκάστοτε απαιτήσεις τους.

Το 2001 οι Bertino et al. [BBF01] εισάγουν για πρώτη φορά την έννοια του χρόνου στο RBAC. Έτσι προτείνουν το TRBAC (Temporal Role Based Access Control), μια επέκταση του βασικού μοντέλου που αφορά συστήματα τα οποία απαιτούν χρονικούς περιορισμούς για τον έλεγχο πρόσβασης. Ουσιαστικά περιορίζεται στη διάσταση του χρόνου η ενεργοποίηση των ρόλων και ορίζονται χρονικές εξαρτήσεις μεταξύ των ενεργοποιήσεων αυτών.

Σε πολλά συστήματα κρίνεται απαραίτητος ο περιορισμός χρήσης των πόρων όσον αφορά στο πότε μπορεί αυτός να χρησιμοποιηθεί (συγκεκριμένες ώρες μέσα στην ημέρα) αλλά και στη χρονική διάρκεια που μπορεί αυτός να χρησιμοποιηθεί. Αυτό μπορεί να επιτευχθεί με την εισαγωγή της χρονικής διάστασης στους ρόλους. Επιπλέον, σε αρκετά συστήματα απαιτούνται χρονικές εξαρτήσεις μεταξύ των ενεργοποιήσεων των ρόλων, οι οποίες δεν ικανοποιούνται στο βασικό RBAC.

Στο RBAC, σε κάθε χρήστη μπορεί να ανατεθούν περισσότεροι του ενός ρόλοι και στο πλαίσιο μιας συνεδρίας μπορεί να ενεργοποιηθεί ένα υποσύνολο αυτών. Ως ενεργοποίηση ενός ρόλου ορίζουμε τη μετάβαση από την κατάσταση «ανενεργός» στην κατάσταση «ενεργός» που οδηγεί στην απόκτηση των δικαιωμάτων πρόσβασης του ρόλου από το χρήστη. Η αντίστροφη μετάβαση ονομάζεται απενεργοποίηση. Οι καταστάσεις των ρόλων και οι μεταβάσεις μεταξύ αυτών παρουσιάζονται στην Εικόνα 13.

Εικόνα 13. Καταστάσεις ρόλων και μεταβάσεις μεταξύ αυτών στο μοντέλο TRBAC

Μία από τις βασικές λειτουργίες του TRBAC είναι η περιοδική ενεργοποίηση και απενεργοποίηση των ρόλων. Περιοδικό είναι ένα γεγονός το οποίο λαμβάνει χώρα ανά τακτούς χρόνους στα όρια ενός καθορισμένου χρονικού διαστήματος. Για την καλύτερη κατανόηση μπορούμε να αναλογιστούμε το ρόλο του εφημερεύοντος γιατρού στα έκτακτα περιστατικά σε ένα νοσοκομείο. Ο ρόλος αυτός θα πρέπει να ενεργοποιείται μόνο κατά τις ώρες λειτουργίας της εφημερίας, π.χ. μεταξύ 12:00 και6:00, και μόνο σε συγκεκριμένες ημέρες του μήνα.

Στο TRBAC υποστηρίζονται οι χρονικές εξαρτήσεις μεταξύ των ενεργοποιήσεων και των απενεργοποιήσεων των ρόλων. Για παράδειγμα, με την ενεργοποίηση του ρόλου του ειδικευόμενου γιατρού θα πρέπει ενεργοποιηθεί και ο ρόλος του προϊσταμένου του (εάν αυτός δεν είναι ήδη ενεργός). Στα πλαίσια του TRBAC, οι κανόνες που ορίζουν τις χρονικές εξαρτήσεις εκφράζονται μέσω της έννοιας των εναυσμάτων (triggers). Τα εναύσματα είναι κανόνες οι οποίοι εκτελούνται αυτόματα όταν συμβούν συγκεκριμένα γεγονότα. Έτσι, η ενεργοποίηση του ρόλου του γιατρού αποτελεί έναυσμα για την ενεργοποίηση του ρόλου του προϊσταμένου. Θα πρέπει να σημειωθεί ότι ένα έναυσμα μπορεί να ενεργοποιήσει/απενεργοποιήσει ένα ρόλο είτε άμεσα είτε μετά την πάροδο ενός σαφώς προκαθορισμένου χρονικού διαστήματος [BBF01].

Η περιοδικότητα, τα εναύσματα και οι αιτήσεις χρόνου εκτέλεσης μπορεί να οδηγήσουν πολλές φορές το σύστημα σε καταστάσεις συγκρούσεων, αφού υπάρχει πιθανότητα οι συνθήκες να οδηγούν στην ενεργοποίηση ενός ρόλου και στην ταυτόχρονη απενεργοποίησή του. Για την αποφυγή των συγκρούσεων ορίζονται προτεραιότητες και, έτσι, εκτελείται πρώτο το γεγονός με την μεγαλύτερη προτεραιότητα.
Το TRBAC επεκτείνει το βασικό RBAC προσθέτοντας τη διάσταση του χρόνου και επικεντρώνεται στην προσθήκη χρονικών περιορισμών στην ενεργοποίηση των ρόλων αλλά αφήνει ανοιχτά ζητήματα που αφορούν χρονικούς περιορισμούς στην ανάθεση ρόλων στους χρήστες και στην ανάθεση δικαιωμάτων πρόσβασης στους ρόλους.

Το TRBAC εφαρμόζει περιορισμούς στην ενεργοποίηση και στην απενεργοποίηση ενός ρόλου, αφήνοντας ανοιχτά ζητήματα τα οποία συνοψίζονται ως εξής:

- Δεν υποστηρίζει τον καθορισμό χρονικών περιορισμών στην ανάθεση ρόλων σε χρήστες και στην ανάθεση δικαιωμάτων σε ρόλους.
- Το TRBAC δεν διαχωρίζει τη δυνατότητα ενεργοποίησης ενός ρόλου από το χρήστη (role enabling) από τον ενεργό ρόλο (role activation).
- Δεν δίνει τη δυνατότητα διαχείρισης των περιορισμών (ενεργοποίησης / απενεργοποίησής τους).

τις δυνατότητες αυτές έρχεται να καλύψει το GTRBAC (Generalized Temporal Role Based Access Control)των Joshi et al. [JBLG01]. Η επέκταση αυτή ορίζει μία νέα κατάσταση στην οντότητα του ρόλου και θέτει χρονικούς περιορισμούς στις αναθέσεις ρόλων, δικαιωμάτων και χρηστών.

Στο GTRBAC σε κάθε χρήστη ανατίθενται συνήθως περισσότεροι του ενός ρόλοι. Στο πλαίσιο μιας συνεδρίας κάθε χρήστης έχει τη δυνατότητα να ενεργοποιήσει ένα υποσύνολο των ρόλων για τους οποίους είναι εξουσιοδοτημένος. Οι καταστάσεις στις οποίες μπορεί να βρεθεί ένας ρόλος είναι τρεις:

Ρόλος με δυνατότητα ενεργοποίησης (Enabled role)

Ένας ρόλος βρίσκεται στην κατάσταση αυτή όταν υπάρχουν χρήστες οι οποίοι είναι εξουσιοδοτημένοι να αποκτήσουν τα δικαιώματα του ρόλου αλλά κανένας χρήστης δεν τον έχει ενεργοποιήσει ακόμα.

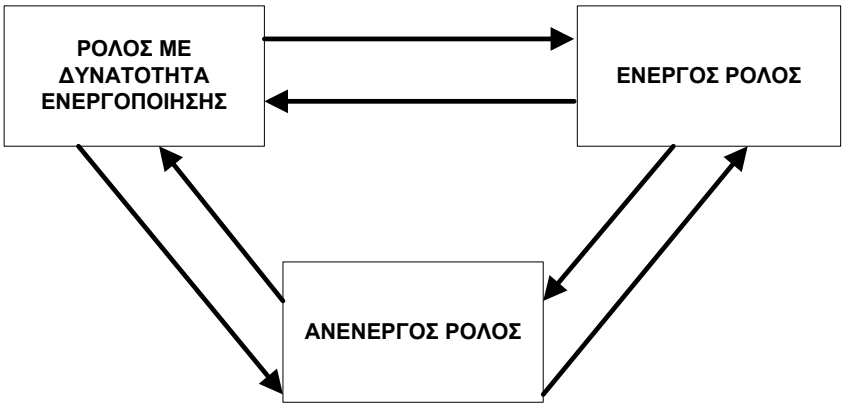
Ενεργός ρόλος (Active role)

Ένας ρόλος περνά σε αυτή την κατάσταση από τη στιγμή που τουλάχιστον ένας χρήστης τον έχει ενεργοποιήσει.

Ανενεργός ρόλος (Disabled role)

Παρόλο που ο ρόλος μπορεί να έχει ανατεθεί σε έναν ή περισσότερους χρήστες, αυτός δεν μπορεί να χρησιμοποιηθεί σε καμία συνεδρία.

Στην Εικόνα 14 παρουσιάζονται οι καταστάσεις στις οποίες μπορεί να βρεθεί ένας ρόλος καθώς και οι μεταβάσεις μεταξύ αυτών.



Εικόνα 14. Καταστάσεις ρόλων και μεταβάσεις μεταξύ αυτών στο GTRBAC

Οι κύριες κατηγορίες στις οποίες μπορεί να χωριστούν οι χρονικοί περιορισμοί είναι οι περιορισμοί διάρκειας και οι περιορισμοί περιοδικότητας. Και οι δύο αυτές κατηγορίες βρίσκουν εφαρμογή στην ανάθεση ρόλων στους χρήστες, στην ανάθεση δικαιωμάτων πρόσβασης στους ρόλους και στη δυνατότητα ενεργοποίησης ενός ρόλου. Επιπλέον, περιορισμοί διάρκειας μπορεί να εφαρμοστούν και στην ενεργοποίηση των ρόλων από τους χρήστες.

Η περιοδικότητα και οι περιορισμοί διάρκειας όσον αφορά την ανάθεση ρόλων σε ένα χρήστη έγκεινται στον περιορισμό της ανάθεσης σε συγκεκριμένες περιόδους στο πλαίσιο ενός χρονικού διαστήματος ή/και σε συγκεκριμένη χρονική διάρκεια. Ως παράδειγμα μπορεί να αναφερθεί ο ρόλος του ορκωτού ελεγκτή στο τμήμα λογιστηρίου μιας εταιρείας. Ο ρόλος αυτός απαιτείται να ανατίθεται σε χρήστες μόνο στο κλείσιμο του λογιστικού έτους και για χρονικό διάστημα 15 ημερών.

Αντίστοιχα, οι περιορισμοί αυτοί μπορεί να βρουν εφαρμογή στην ανάθεση δικαιωμάτων πρόσβασης σε ένα ρόλο. Ενδεικτικό παράδειγμα είναι το δικαίωμα δήλωσης μαθημάτων που ανατίθενται στο ρόλο του φοιτητή σε ένα Ανώτατο Εκπαιδευτικό Ίδρυμα. Το δικαίωμα αυτό το αποκτούν δύο φορές το χρόνο και για χρονικό διάστημα δύο εβδομάδων.

Ομοίως, περιορισμοί αυτής της μορφής μπορεί να οριστούν και στη διαδικασία αλλαγής της κατάστασης ενός ρόλου από Ενεργός σε Ανενεργός και το αντίστροφο. Για παράδειγμα, ο ρόλος του επισκέπτη γιατρού που παρακολουθεί τους νοσηλευόμενους σε ένα νοσοκομείο ασθενείς μπορεί να γίνει Ενεργός από τις 9 το πρωί έως τις 9 το βράδυ. Από τη στιγμή που θα ενεργοποιηθεί ο ρόλος αυτός, γίνεται αυτόματα Ενεργός για 4 ώρες ο ρόλος του ειδικευόμενου γιατρού.

Χρονικοί περιορισμοί μπορεί να τεθούν και στην Ενεργοποίηση ενός ρόλου. Στην περίπτωση αυτή, δεν μπορούμε να αναφερθούμε στην έννοια της περιοδικότητας καθώς η ενεργοποίηση ενός ρόλου είναι απόφαση του κάθε χρήστη. Μπορεί, όμως, εύκολα να

τεθούν περιορισμοί χρονικής διάρκειας. Εδώ εντοπίζονται οι παρακάτω κατηγορίες περιορισμών διάρκειας:

- Συνολική διάρκεια ενεργού ρόλου (Total Active Role Duration): Καθορίζεται η συνολική χρονική διάρκεια που ένας ρόλος μπορεί να παραμείνει ενεργός.
  - ◊ Ανά ρόλο Περιορίζεται η χρονική διάρκεια που ένας ρόλος μπορεί να παραμείνει ενεργός ανεξάρτητα από το ποιοι και πόσοι χρήστες τον έχουν ενεργοποιήσει. Όταν το άθροισμα της διάρκειας όλων των ενεργοποιήσεων φτάσει τη μέγιστη συνολική διάρκεια δεν επιτρέπεται περαιτέρω ενεργοποίηση του ρόλου.
  - ◊ Ανά ανάθεση χρήστη σε ρόλο Περιορίζεται η χρονική διάρκεια που ένας χρήστης μπορεί να ενεργοποιήσει το ρόλο. Όταν ο χρήστης υπερβεί τη διάρκεια αυτή, δεν του επιτρέπεται να τον ενεργοποιήσει ξανά.

Θα πρέπει να σημειωθεί ότι ο περιορισμός της συνολικής διάρκειας είναι ανεξάρτητος του αριθμού των ενεργοποιήσεων του ρόλου.

- Μέγιστη διάρκεια ρόλου ανά ενεργοποίηση (Maximum Role Duration per Activation): Εδώ, περιορίζεται η μέγιστη διάρκεια που μπορεί ένας ρόλος να παραμείνει ενεργός ανά ενεργοποίηση.
  - ◊ Ανά ρόλο: Για τον οποιοδήποτε χρήστη έχει τη δυνατότητα να ενεργοποιήσει το ρόλο καθορίζεται μια μέγιστη διάρκεια που μπορεί αυτός ο ρόλος να παραμείνει ενεργός από τη στιγμή που ενεργοποιείται.
  - ◊ Ανά ανάθεση χρήστη σε ρόλο: Καθορίζεται η μέγιστη διάρκεια που ένας χρήστης μπορεί να διατηρήσει ενεργό ένα ρόλο από τη στιγμή που θα τον ενεργοποιήσει.

Επιπλέον, στην ενεργοποίηση ενός ρόλου μπορεί να τεθούν χρονικοί περιορισμοί που αφορούν το πλήθος των ενεργοποιήσεων αυτού του ρόλου. Αντίστοιχα με τους περιορισμούς διάρκειας, διακρίνουμε δύο κατηγορίες:

- Συνολικός αριθμός ενεργοποιήσεων
- Μέγιστος αριθμός ενεργοποιήσεων.

2.3.2. RBAC με Χωροχρονικούς Περιορισμούς

Πέρα από την εισαγωγή της έννοιας του χρόνου και των σχετικών περιορισμών εκτεταμένη έρευνα έχει πραγματοποιηθεί και στην ενσωμάτωση χωρικών περιορισμών.

Το LoT-RBAC (Location and Time-basedRBAC) [CJ05] βασίζεται στο GTRBAC για να ενσωματώσει την λογική των αναλυτικών και βασισμένων σε γεγονότα χρονικών περιορισμών.Για τους χωρικούς περιορισμούς ορίζονται οι έννοιες τις *χωρικής τοποθεσίας*, ορισμένη στον χώρο τον τριών γεωμετρικών διαστάσεων, και η έννοια των *λογικών τοποθεσιών* οι οποίες αποτελούνται από ένα σύνολο *χωρικών τοποθεσιών*. Το LoT-RBAC δεν ασχολείται με το πώς υπολογίζεται η τοποθεσία αλλά και ούτε με το πως ακριβώς απεικονίζεται η φυσική τοποθεσία π.χ. ένα σημείο, ένα σύνολο σημείων που ορίζει ένα δισδιάστατο πολύγωνο ή έναν κύκλο, ή γεωμετρική κατασκευή τριών διαστάσεων.

Οι *λογικές τοποθεσίες* είναι ένα σύνολο φυσικών *χωρικών τοποθεσιών* που μπορούν εν δυνάμει να έχουν πολλαπλές *υποστάσεις*. Η υπόσταση «πόλη» μπορεί να περιλαμβάνει οποιαδήποτε πόλη στον κόσμο.

Για κάθε τοποθεσία ορίζονται τρεις πιθανές καταστάσεις του χρήστη: να βρίσκεται εντός αυτής, εκτός αυτής και ακριβώς πάνω στο όριο που ορίζει η τοποθεσία (φυσική ή λογική).

Οι τοποθεσίες μπορεί να έχουν μεταξύ τους τις ακόλουθες σχέσεις:

- *Υποσύνολο:* Μια λογική τοποθεσία μπορεί να έχει πολλαπλά υποσύνολα.
- *Υπερσύνολο:* Μια λογική τοποθεσία μπορεί να έχει πολλαπλά υπερσύνολα.
- *Υπόσταση:* Μια λογική τοποθεσία μπορεί να έχει ένα σύνολο υποστάσεων.
- *Τύπος:* Μια φυσική τοποθεσία μπορεί να έχει πολλαπλούς τύπους χωρικής τοποθεσίας.
- Δυο τοποθεσίες μπορεί να σχετίζονται με επικαλύψεις, η μια να εμπεριέχει την άλλη, να ισούνται μεταξύ τους, να μην έχουν κοινό σημείο ή να έχουν σημεία επαφής.
- Η *Υπόσταση* ορίζει τις φυσικές χωρικές τοποθεσίες οι οποίες αποτελούν την λογική τοποθεσία.

Επιπλέον, ορίζεται και η *σχετική τοποθεσία.* Υπάρχουν περιπτώσεις όπου έχει σημασία η απόσταση από ένα σημείο ενδιαφέροντος λ.χ. 6 χλμ. δυτικά του Νοσοκομείου ή σε απόσταση 1 χλμ. (ανεξάρτητα από την κατεύθυνση) από κάποιο κινητό σημείο, λ.χ. ένα ασθενοφόρο.

Πιο συγκεκριμένα, η σχετική τοποθεσία ορίζεται από το σημείο ενδιαφέροντος, και την ανυσματική απόσταση (η οποία περιλαμβάνει την απόλυτη τιμή της απόστασης και την κατεύθυνση αυτής). Η απόσταση μπορεί να οριστεί σε μία, δύο ή και στις τρεις διαστάσεις ανάλογα τον περιορισμό που χρειάζεται να απεικονιστεί.

Με την χρήση των εννοιών *Υποσύνολο, Υπόσταση* και *Λογική τοποθεσία* που ορίστηκαν παραπάνω μπορεί να οριστούν και αντίστοιχες ιεραρχίες. Οι ιεραρχίες διαχωρίζονται σε *Φυσικές, Λογικές* και *Υβριδικές Ιεραρχίες Τοποθεσιών*:

- Ιεραρχίες φυσικών τοποθεσιών, όπου μια φυσική τοποθεσία εμπεριέχει μια άλλη
- Ιεραρχίες λογικών τοποθεσιών, όπου μια λογική τοποθεσία εμπεριέχει μια άλλη
- Υβριδική ιεραρχία, όπου μια φυσική τοποθεσία εμπεριέχει μια άλλη και μια λογική τοποθεσία εμπεριέχει μια άλλη.

Στο GTRBAC οι ρόλοι μπορεί να είναι ενεργοί, ανενεργοί και ενεργοποιημένοι ανάλογα με τους χρονικούς περιορισμούς που έχουν επιβληθεί. Οι έννοιες υιοθετούνται και στο LoT αλλά η κατάσταση ενός ρόλου εξαρτάται και από χωρικούς περιορισμούς.

Έτσι, ένας ρόλος για να είναι στην κατάσταση ενεργός θα πρέπει να πληρούνται οι χρονικοί περιορισμοί και ο χρήστης να βρίσκεται σε μια τοποθεσία στην οποία επιτρέπεται να του αποδοθεί ο συγκεκριμένος ρόλος.

Επιπλέον, και πάλι βασισμένο στο GTRBAC επεκτείνεται η έννοια των εναυσμάτων. Στο LoT τα εναύσματα σχετίζονται με την ενημέρωση του συστήματος RBAC για κάποια αλλαγή στην τοποθεσία χρήστη η οποία επηρεάζει και τα δικαιώματα πρόσβασης που αυτός μπορεί να αναλάβει. Έτσι, π.χ. στην περίπτωση που κάποιος χρήστης μετακινείται και οι περιορισμοί που έχει λόγω της σχετικής τοποθεσίας αίρονται, και έτσι, ο ρόλος είναι πλέον ενεργός για να τον αναλάβει κάποιος εξουσιοδοτημένος χρήστης.

Το Δυναμικό RBAC (Dynamic RBAC - DRBAC) προτάθηκε από τους Zhang et al. [ZP03] και αποτελεί ένα μοντέλο διαχείρισης πρόσβασης γνώσης περιεχομένου. Το υποσύνολο των ρόλων που ανατίθενται σε ένα χρήστη και οι προσβάσεις που αποδίδονται σε ένα ρόλο είναι δυναμικές και διατηρούνται σε μια μηχανή καταστάσεων (state machine). Το περιεχόμενο συλλέγεται και αυτό που κρίνεται σημαντικό αντιμετωπίζεται ως έναυσμα. Τα εναύσματα προκαλούν τις μεταβάσεις είτε της μηχανής καταστάσεων ρόλων είτε της μηχανής καταστάσεων προσβάσεων.

Στο GEO-RBAC [BCDP05] οι χωρικές οντότητες χρησιμοποιούνται για να μοντελοποιήσουν τα υποκείμενα, τη θέση του χρήστη, και τους γεωγραφικά περιορισμένα ρόλους. Οι ρόλοι ενεργοποιούνται με βάση την θέση του χρήστη. Πέραν από την φυσική τοποθεσία αποδίδεται στους χρήστες και μια λογική τοποθεσία η οποία καθορίζεται από κάποιο χαρακτηριστικό της τοποθεσίας, π.χ. δρόμος, πόλη, περιοχή. Στο GEO-RBAC ορίζεται ο *χωρικός ρόλος* ως το ζεύγος < r,e >, όπου r είναι ο *ρόλος* και e είναι η *χωρική επέκτασή* του. Η *χωρική επέκταση* καθορίζει τα χωρικά όρια στα οποία ο ρόλος μπορεί κάποιος χρήστης να εκκινήσει συνεδρία. Οι ρόλοι είναι ενεργοί και συνεπώς διαθέσιμοι στον χρήστη μόνο εάν η τοποθεσία του χρήστη περιλαμβάνεται στην χωρική επέκταση του ρόλου. Στο GEO-RBAC υποστηρίζονται και οι ιεραρχίες, όπου οι ρόλοι κληρονομούν δικαιώματα από τους προγόνους ρόλους και οι χρήστες από τους απογόνους χρήστες [BCDP05].

2.3.3. RBAC με Δυνατότητες Εξουσιοδότησης

Στο RBAC η εξουσιοδότηση καθιστά δυνατό ένας χρήστης που κατέχει έναν συγκεκριμένο ρόλο να μπορεί να αναθέσει σε κάποιον άλλο χρήστη να εκτελέσει τις ενέργειες που επιτρέπονται από τον συγκεκριμένο ρόλο. Η Εξουσιοδότηση αποτελεί καταλύτη στην λειτουργία επιχειρηματικών διαδικασιών σε ένα οργανισμό καθώς επιτρέπει την πραγματοποιήση ενεργειών κρίσιμων για την επιχείρηση εν τη απουσία αντίστοιχων αρμοδίων. Δεδομένου ότι το RBAC έχει υιοθετηθεί εκτεταμένα ήταν αναμενόμενο να έχουν προταθεί επεκτάσεις του μοντέλου οι οποίες περιλαμβάνουν δυνατότητες εξουσιοδότησης. Το βασικό πλεονέκτημα που προσφέρει η εξουσιοδότηση είναι η ευελιξία και η μείωση του διαχειριστικού φόρτου, ωστόσο τα δικαιώματα που αποδίδονται στους χρήστες δεν είναι πλέον υπό αυστηρό έλεγχο.

Η εξουσιοδότηση στο πλαίσιο των μοντέλων διαχείρισης πρόσβασης χρηστών αναφέρεται συνήθως στην ανάθεση δικαιωμάτων από έναν χρήστη σε κάποιον άλλο. Η εξουσιοδότηση δύναται να πραγματοποιηθεί και σε ευρύτερο πλαίσιο από αυτό που αναφέρθηκε. Η εξουσιοδότηση μπορεί να αναφέρεται σε σχέση χρήστη προς χρήστη, χρήστη προς σύστημα, σύστημα προς σύστημα και ακόμα και σύστημα προς χρήστη.

Ο χρήστης που μεταφέρει δικαιώματα αναφέρεται ως ο εξουσιοδοτών και ο χρήστης που λαμβάνει τα δικαιώματα πρόσβασης ως εξουσιοδοτούμενος.

Η πιο απλή μορφή εξουσιοδότησης στο RBAC είναι αυτή όπου ο χρήστης που εξουσιοδοτεί επιτρέπει στον εξουσιοδοτούμενο χρήστη να αποκτήσει έναν ρόλο και τις αντίστοιχες προσβάσεις. Ένα τέτοιο μοντέλο έχει προταθεί από τους Barka και Sandu στο [BS00] το οποίο βασίζεται στο [BSA00]. Τα δικαιώματα μπορεί είτε να μεταφερθούν είτε να αποδοθούν. Στην πρώτη περίπτωση ο εξουσιοδοτών χρήστης δεν μπορεί να χρησιμοποιήσει τα δικαιώματα πρόσβασης που έχει μεταφέρει ενώ στην περίπτωση που τα αποδίδει διατηρεί τα δικαιώματα πρόσβασής του ακέραια. Μια ακόμα περίπτωση που λαμβάνεται υπόψη είναι η δυνατότητα εξουσιοδότησης δικαιωμάτων από κάποιον χρήστη ο οποίος δεν κατέχει ο ίδιος τα δικαιώματα αυτά. Μια περίπτωση που θα ήταν χρήσιμη αυτή η προσέγγιση είναι σε ένα τμήμα ανάπτυξης λογισμικού όπου ο διευθυντής του τμήματος μπορεί να εξουσιοδοτήσει μέλη της ομάδας να αποκτήσουν πρόσβαση στον πηγαίο κώδικα συγκεκριμένων εφαρμογών. Ωστόσο, ο ίδιος δεν είναι αναγκαίο να έχει πρόσβαση.

Ένας χρήστης που του έχει αποδοθεί κάποιος ρόλος μπορεί να τον μεταφέρει με την σειρά του σε κάποιον άλλο χρήστη και να θέσει την χρονική διάρκεια της εξουσιοδότησης αυτής. Ο χρήστης που εξουσιοδοτήθηκε δεν μπορεί με τη σειρά του να εξουσιοδοτήσει κάποιον άλλο˙ αυτό ονομάζεται εξουσιοδότηση ενός βήματος.

Στην εξουσιοδότηση δύο βημάτων ο εξουσιοδοτημένος χρήστης μπορεί με την σειρά του να αποδώσει τον ρόλο σε άλλο χρήστη. Στην εξουσιοδότηση πολλαπλών βημάτων ο δεύτερος χρήστης που έλαβε εξουσιοδότηση μπορεί να εξουσιοδοτήσει και κάποιον άλλον κτλ.

Στο [WK05] προτείνεται εξουσιοδότηση χρήστη-προς-χρήστη και υποστηρίζεται εξουσιοδότηση πολλών βημάτων καθώς και περιορισμοί όταν δίδεται εξουσιοδότηση. Στην εξουσιοδότηση πολλών βημάτων όταν η εξουσιοδότηση του πρώτου βήματος ανακληθεί τότε ανακαλείται και από όλους τους υπόλοιπους χρήστες που είχε αποδοθεί με εξουσιοδότηση. Ωστόσο, εάν ο εξουσιοδοτών δεύτερου βήματος μπορούσε να δώσει την ίδια εξουσιοδότηση με άλλα μέσα ή δικαιώματα που έχει, τότε τα δικαιώματα που έχει εξουσιοδότησει δεν αναιρούνται.

Στο PBDM [ZS03] η εξουσιοδότηση μπορεί να είναι από χρήστη σε χρήστη, από ρόλο σε ρόλο ή σε προσβάσεις. Παρουσιάζονται σύνθετες περιπτώσεις εξουσιοδότησης όπου μπορεί να εξουσιοδοτηθεί ένα υποσύνολο προσβάσεων ενός ρόλου, μπορεί να επιτρέπεται ή όχι εξουσιοδότηση πολλών βημάτων, τα δικαιώματα μπορεί να

ανακαλούνται ή να έχουν συγκεκριμένη χρονική διάρκεια, και λαμβάνεται υπόψη και η κληρονομικότητα.

Όπως αναφέρθηκε παραπάνω, ένας από τους στόχους της χρήσης εξουσιοδότησης είναι η μείωση του διαχειριστικού κόστους. Εντούτοις έχουν προταθεί μοντέλα στα οποία προβλέπεται η εμπλοκή ενός διαχειριστή προκειμένου να υπάρχει αυστηρότερος έλεγχος των δικαιωμάτων πρόσβασης. Στο PBDM1 ο διαχειριστής εμπλέκεται έτσι ώστε να διαχειρίζεται τις ιεραρχίες των ρόλων και κατ' επέκταση την κληρονόμηση δικαιωμάτων πρόσβασης. Οι ρόλοι διαχωρίζονται σε δύο κατηγορίες: σε αυτούς που επιτρέπεται να γίνει εξουσιοδότηση, (*συνήθεις ρόλοι*) και σε αυτούς στους οποίους δεν επιτρέπεται (*εξουσιοδοτούμενοι ρόλοι*). Οι ρόλοι που έχουν αποκτηθεί δια μέσου εξουσιοδότησης δεν επιτρέπεται να κληρονομηθούν μέσω των ιεραρχιών που ισχύουν. Ο ρόλος του διαχειριστή είναι να παρέχει υποστήριξη και να μπορεί να μετακινήσει δικαιώματα από έναν εξουσιοδοτημένο ρόλο σε ένα συνήθη ρόλο και να ανακαλέσει έναν χρήστη από έναν *συνήθη* ή έναν *εξουσιοδοτούμενο* ρόλο.

2.3.4. RBAC με Παροχή Ποιότητας Υπηρεσίας

Ένα ασφαλές σύστημα μπορεί να μην αποδειχτεί τελικά και τόσο χρήσιμο αν δεν καταφέρει να παρέχει ένα συγκεκριμένο επίπεδο ποιότητας υπηρεσιών (Quality o fService - QoS). Στον αντίποδα, ένα σύστημα που φτάνει ένα καλό επίπεδο ποιότητας υπηρεσιών χωρίς τους κατάλληλους μηχανισμούς ασφαλείας, μπορεί εύκολα να δεχθεί επίθεση από έναν κακόβουλο χρήστη. Το σύστημα μπορεί να οδηγηθεί σε άρνηση παροχής υπηρεσιών (Denial of Service-Dos), σε εξάντληση των πόρων του από τον κακόβουλο χρήστη και, τελικά, σε πτώση της ποιότητας των υπηρεσιών. Κρίνεται λοιπόν απαραίτητος για την επιτυχία ενός συστήματος ο συνδυασμός της ασφάλειας με την ποιότητα των παρεχόμενων υπηρεσιών και αυτό μελετάται μέσα από το QRBAC [K03] .

Το QRBAC προτάθηκε από τον Kyoung-Don Kang ο οποίος μελέτησε την επέκταση αυτή για τις εφαρμογές ηλεκτρονικού εμπορίου (e-commerce). Στις εφαρμογές αυτές τόσο η ποιότητα των παρεχόμενων υπηρεσιών όσο και η ασφάλεια είναι κρίσιμοι παράγοντες για την επιτυχία τους. Στο QRBAC εισάγεται η έννοια των «ρόλων που έχουν επίγνωση της ποιότητας των υπηρεσιών» (Qos-aware roles), προσφέροντας στο διαχειριστή του συστήματος τη δυνατότητα να προσδιορίζει το αναλογούν σε κάθε ρόλο μερίδιο από τους αιτούμενους πόρους του συστήματος προκειμένου να επιτευχθεί η ζητούμενη ποιότητα υπηρεσιών. Για παράδειγμα, σε ένα σύστημα ηλεκτρονικού εμπορίου ο διαχειριστής προσδιορίζει για ένα ρόλο το αναλογούν εύρος ζώνης που αυτός χρειάζεται προκειμένου να διαχειριστεί τα αιτήματα για υπηρεσίες με το κατάλληλο επίπεδο ποιότητας, και τον μέσο χρόνο απόκρισης στα αιτήματα αυτά.

Επίσης, στο QRBAC εισάγεται η έννοια της «*κατάστασης του συστήματος*» ως μέρος του μοντέλου ελέγχου πρόσβασης. Με αυτό τον τρόπο, ο μηχανισμός ελέγχου πρόσβασης επιβλέπει άμεσα την κατάσταση του συστήματος και τη χρήση των πόρων

αυτού έχοντας τη δυνατότητα να ανιχνεύσει και να αποτρέψει πιθανή υπερφόρτωσή του και εξάντληση των πόρων του από κακόβουλους χρήστες. Επανερχόμενοι στο παράδειγμα της εφαρμογής ηλεκτρονικού εμπορίου, η χρήση του QRBAC στοχεύει στο να πετύχει μια καθορισμένη επίδοση, π.χ. ένα μέσο χρόνο απόκρισης ή ένα ανώτατο όριο χρήσης των πόρων για την αποφυγή υπερφορτώσεων. Για να το πετύχει αυτό παρακολουθείται σε τακτά χρονικά διαστήματα η επίδοση του συστήματος και η χρήση των πόρων του και όταν διαπιστωθεί υπερφόρτωση τότε μειώνεται η ποιότητα των υπηρεσιών. Για παράδειγμα, παρέχονται στους χρήστες μόνο πληροφορίες κειμένου και όχι εικόνες, χωρίζονται οι χρήστες σε κατηγορίες ανάλογα με τη σημαντικότητά τους και έτσι εξυπηρετούνται π.χ. πρώτα οι χρήστες που θέλουν να πραγματοποιήσουν μια πληρωμή και θα αποφέρουν κέρδος στην εφαρμογή.

Όπως έχουμε ήδη αναφέρει, το RBAC βασίζεται στην διατήρηση δύο σημαντικών αρχών, την αρχή του ελαχίστου προνομίου και την αρχή του διαχωρισμού των καθηκόντων. Στο QRBAC οι αρχές αυτές επεκτείνονται και υλοποιούνται με διαφορετικό τρόπο με απώτερο στόχοτην διατήρηση της ποιότητας της υπηρεσίας. Στο QRBAC, όταν ένας ρόλος καταναλώσει παραπάνω πόρους από το μερίδιο που του αναλογεί τότε θεωρείται ότι έχει παραβιαστεί η αρχή του ελαχίστου προνομίου. Αποτέλεσμα της υπερκατανάλωσης πόρων από ένα ρόλο είναι η μείωση της ποιότητας των υπηρεσιών για τους υπόλοιπους πόρους λόγω της έλλειψης πόρων. Ως συνέπεια αυτού, παραβιάζεται και η απομόνωση της απόδοσης των ρόλων αφού η απόδοση ενός ρόλου είναι άμεσα συνδεδεμένη με την απόδοση των υπολοίπων. Αυτό αντιμετωπίζεται ως πρόβλημα διαχωρισμού των καθηκόντων.

Για να επιτύχει τη διατήρηση των παραπάνω αρχών, το QRBAC προσαρμόζει δυναμικά τις άδειες πρόσβασης των ρόλων σε ό,τι αφορά τη χρήση των πόρων μειώνοντάς τους την ποιότητα των υπηρεσιών σε περίπτωση υπερφόρτωσης μέσω π.χ. μειωμένης ποιότητας εικόνας. Επιπλέον, έχει τη δυνατότητα να προσαρμόζει και να μειώνει δυναμικά το ρυθμό ενεργοποίησης των ρόλων. Για παράδειγμα, μπορεί να μειώσει των αριθμό των ρόλων που μπορούν να έχουν πρόσβαση στους πόρους του συστήματος σε μια δεδομένη χρονική στιγμή ώστε να μπορέσουν να εξυπηρετηθούν οι ρόλοι με τη μεγαλύτερη προτεραιότητα. Τέλος, δίδεται στο διαχειριστή του συστήματος η δυνατότητα να ανακαλεί όλα τα δικαιώματα πρόσβασης ενός ρόλου ο οποίος προσπαθεί να εξαντλήσει όλους τους διαθέσιμους πόρους.

2.3.5. Το RBAC στο Σύγχρονο Περιβάλλον

Οι επεκτάσεις του μοντέλου RBAC που παρουσιάστηκαν παραπάνω αποτελούν ενδεικτικά αλλά χαρακτηριστικά παραδείγματα του συνόλου των επεκτάσεων που έχουν αναπτυχθεί έως τώρα. Φυσικά δεν είναι οι μοναδικές επεκτάσεις αλλά αποτελούν τα μοντέλα που καλύπτουν σημαντικές παραμέτρους για τα πληροφοριακά συστήματα σήμερα: το χρόνο, το χώρο, την εξουσιοδότηση και την ποιότητα των υπηρεσιών.

Δεδομένης της φύσης των σύγχρονων υπολογιστικών συστημάτων, το επίκεντρο του ενδιαφέροντος είναι η παροχή υπηρεσιών. Σημαντικός παράγοντας για την επιτυχία τέτοιων συστημάτων είναι η σωστή επιβολή των χρονικών περιορισμών καθώς και η διασφάλιση της ποιότητας των υπηρεσιών. Η αυξανόμενη χρήση φορητών συσκευών (έξυπνων τηλεφώνων, tablets κτλ.) φέρνει στο προσκήνιο και την ανάγκη η τοποθεσία ενός χρήστη να λαμβάνεται υπόψη στη διαχείριση πρόσβασης.

Λόγω της συνεχούς ανάπτυξης της τεχνολογίας, της συνεχούς μεταβολής των πληροφοριακών συστημάτων και, γενικά, του περιβάλλοντος στο οποίο αυτά λειτουργούν, προκύπτουν διαρκώς νέες ανάγκες που πρέπει να καλυφθούν αλλά και νέοι περιορισμοί που πρέπει να επιβληθούν. Η κάλυψη αυτών των αναγκών θα φέρνει πάντα στο προσκήνιο νέες βελτιώσεις, νέες επεκτάσεις και πιθανόν νέα μοντέλα που θα ενσωματώνουν τα πλεονεκτήματα του RBAC, θα ξεπεράσουν τους περιορισμούς του RBAC και θα προσφέρουν νέες προοπτικές. Προς το παρόν, το RBAC παραμένει ο πρωταγωνιστής στη διαχείριση του ελέγχου πρόσβασης λόγω της ευελιξίας και της διαχειριστικής ευκολίας που προσφέρει.

2.4. Κατ’ Εξαίρεση Πρόσβαση

Τα μοντέλα και τα πλαίσια διαχείρισης πρόσβασης περιγράφουν και επιβάλλουν τον τρόπο με τον οποίο αντικείμενα και χρήστες αποκτούν πρόσβαση σε δεδομένα, πόρους του συστήματος και δικτυακές υπηρεσίες. Οι πολιτικές ελέγχου πρόσβασης διαμορφώνονται σύμφωνα με την υπόθεση ότι οι ανάγκες των χρηστών μπορεί να αναγνωριστούν και να καταγραφούν επαρκώς και, εν συνεχεία, να τους παραχωρηθούν τα κατάλληλα δικαιώματα πρόσβασης.

Σε ένα σύγχρονο περιβάλλον, όμως, συχνά προκύπτουν περιπτώσεις όπου επικρατούν καταστάσεις έκτακτης ανάγκης που με τη σειρά τους οδηγούν σε αιτήματα πρόσβασης που δεν έχουν προβλεφθεί από τις συνήθεις διαδικασίες. Η έννοια της πρόσβασης σε καταστάσεις έκτακτης ανάγκης ή κατ’ εξαίρεση πρόσβασης ή όπως συχνά αναφέρεται στην βιβλιογραφία «Σπάσιμο του Γυαλιού» (Break The Glass - BTG) περιγράφει τις περιπτώσεις όπου ένας χρήστης θα πρέπει να αποκτήσει δικαιώματα πρόσβασης σε πόρους και πληροφορίες που σε κανονικές συνθήκες θα έπρεπε να του αρνηθούν. Αυτός ο μηχανισμός είναι γνωστός ως Σπάσιμου του Γυαλιού κάνοντας τον παραλληλισμό με το σπάσιμο του γυαλιού προκειμένου να ενεργοποιηθεί ο συναγερμός σε περίπτωση φωτιάς.

Η πλειοψηφία των μοντέλων ελέγχου πρόσβασης που έχουν αναπτυχθεί βασίζεται στην υπόθεση ότι τα δικαιώματα πρόσβασης των χρηστών μπορεί να καθοριστούν εκ των προτέρων. Επιπλέον, οι ρόλοι των χρηστών και τα σχετιζόμενα δικαιώματα πρόσβασης είναι στατικά και έχουν προκαθοριστεί και, συνεπώς, οι τροποποιήσεις δεν είναι δυνατό να είναι αυτοματοποιημένες. Σε ένα μοντέρνο περιβάλλον, όπως είναι οι σύγχρονες επιχειρήσεις και οργανισμοί, είναι συχνό το φαινόμενο όπου είναι ωφέλιμο να υλοποιηθούν ευέλικτες πολιτικές ασφαλείας μιας και είναι πρακτικά αδύνατο να προβλεφθούν εκ των προτέρων όλες οι πιθανές καταστάσεις

που μπορεί να προκύψουν. Οι χρήστες μπορεί να χρειαστούν πρόσβαση σε πόρους που συνήθως δεν χρειάζονται για διάφορους λόγους όπως π.χ. όταν προκύψει μια κατάσταση έκτακτης ανάγκης.

Αυτό μπορεί να επιτευχθεί με τη χρήση ενός μηχανισμού που παρέχει κατ' εξαίρεση πρόσβαση στους χρήστες με απώτερο στόχο τη δημιουργία ενός πλαισίου ελέγχου πρόσβασης το οποίο δεν θα παρεμποδίζει ή δεν θα επιβαρύνει τις επιχειρησιακές λειτουργίες ενός οργανισμού ενώ ταυτόχρονα θα εξασφαλίζει υψηλό επίπεδο ασφάλειας και διασφάλισης της πληροφορίας.

Μια περίπτωση που αναδεικνύει την ανάγκη να παρακαμφθούν οι στατικές πολιτικές ασφαλείας είναι ο χώρος της υγείας όπου η ασφάλεια των πληροφοριών, όπως ο ηλεκτρονικός φάκελος του ασθενούς, είναι ιδιαίτερα σημαντική. Ωστόσο, το ιατρικό προσωπικό χρειάζεται πρόσβαση στην επιθυμητή πληροφορία την κατάλληλη στιγμή ώστε να μπορέσει να παράσχει στον ασθενή την καλύτερη δυνατή θεραπεία. Λόγω της φύσης του χώρου της υγείας έχει παρουσιαστεί ερευνητικό ενδιαφέρον για την ανάπτυξη μεθόδων κατ' εξαίρεση πρόσβασης.

Μία ακόμα περίπτωση όπου ενδέχεται να παρουσιαστεί ανάγκη κατ' εξαίρεση πρόσβασης είναι σε περιπτώσεις σημαντικής καταστροφής των υποδομών ενός οργανισμού όπου θα πρέπει να ενεργοποιηθούν διαδικασίες ανάκαμψης από καταστροφή. Σε περίπτωση εκτεταμένης ζημιάς χρήστες ή/και διαχειριστές θα κληθούν να εκτελέσουν ενέργειες που είναι πιθανόν να μην έχουν προβλεφθεί. Από την μια προκειμένου να συνεχισθούν οι εργασίες του οργανισμού και από την άλλη για την αποκατάσταση των ζημιών, λ.χ. εφαρμόζοντας την αρχή του διαχωρισμού καθηκόντων ο διαχειριστής του λειτουργικού συστήματος δεν έχει δικαιώματα διαχειριστή ούτε στη βάση δεδομένων ούτε και στην εφαρμογή αλλά σε μια κατάσταση ανάγκης προκειμένου να επαναλειτουργήσει ένα κρίσιμο σύστημα θα ήταν σκόπιμο ο ίδιος άνθρωπος να μπορεί να εκτελέσει διαχειριστικές εργασίες σε όλα τα επίπεδα.

2.4.1. Μοντέλα κατ' Εξαίρεση Πρόσβασης

Η νομοθεσία στις Ηνωμένες Πολιτείες της Αμερικής για την υγεία, ασφάλιση και φορητότητα (Health Insurance and Portability Act - HIPPA) [SPC04] λαμβάνει υπόψη τις ανάγκες που υπάρχουν για την κατ' εξαίρεση πρόσβαση και προτείνεται στα πλαίσια αυτά η δημιουργία προπαρασκευασμένων λογαριασμών χρηστών οι οποίοι θα χρησιμοποιούνται μόνο όταν προκύπτει ανάγκη επείγουσας πρόσβασης. Η παραπάνω προσέγγιση περιλαμβάνει χειροκίνητες διαδικασίες οι οποίες αφενός έχουν αρνητικό αντίκτυπο στην ευελιξία του σχήματος και αφετέρου εγείρουν ερωτήματα στο κατά πόσο μπορεί να αποδοθούν κατάλληλες ευθύνες (accountability).

Στο [VKGBJ09], χρησιμοποιώντας το παράδειγμα ενός σεναρίου έκτακτης ανάγκης πρόσβασης σε περιβάλλον υγειονομικής περίθαλψης αναδεικνύονται οι προκλήσεις που προκύπτουν σε ένα δυναμικό περιβάλλον με μεταβλητές καταστάσεις σε αντικείμενα και

υποκείμενα. Στο [AR10], προτείνεται μια αρχιτεκτονική, βασισμένη στο XACML (eXtensible Access Control Markup Language) για την αποτύπωση της πολιτικής πρόσβασης σε ιατρικά δεδομένα με τη χρήση φορητών συσκευών όπως έξυπνων τηλεφώνων.

Στο μοντέλο που παρουσιάζεται από τους Ardagna et al. [AVFGJS10], οι πολιτικές επιμερίζονται στις τρεις ακόλουθες κατηγορίες: συνήθης πρόσβαση, επείγουσα και BTG. Κάθε χρήστης αντιμετωπίζεται αναλόγως σε ποια από τις παραπάνω κατηγορίες ανήκει.

Στο [CZ12], παρουσιάζεται ένα μοντέλο BTG που επικεντρώνεται στην πρόσβαση σε Αρχεία Ιατρικών Δεδομένων. Για κάθε ασθενή ορίζεται μια ομάδα επικοινωνίας και όποτε προκύψει η ανάγκη πρόσβασης στα ιατρικά δεδομένα τους ασθενούς μέσω μιας διαδικασίας ψηφοφορίας λαμβάνεται η απόφαση άρνησης ή πρόσβασης στα δεδομένα.

Στο [FCFC09] παρουσιάζεται το BTG-RBAC, το οποίο, όπως υπονοεί και το όνομα του, βασίζεται στο RBAC. Οι κατ' εξαίρεση προσβάσεις αποδίδονται στους χρήστες βάση μιας προκαθορισμένης πολιτικής. Οι ρόλοι είναι προκαθορισμένοι και οι προσβάσεις ώστε να επιτραπεί BTG εξαρτώνται από τους ρόλους που κατέχει ο χρήστης. Το προτεινόμενο μοντέλο χρησιμοποιεί και την έννοια των *Υποχρεώσεων (Obligations)* [SSNDS07]. Καθορίζονται και πραγματοποιούνται οι *αυθαίρετες (arbitrary)* ενέργειες όταν ενεργοποιείται ο μηχανισμός της κατ' εξαίρεση πρόσβασης.

Η απόφαση για την απόδοση πρόσβασης ή μη λαμβάνεται από την συνάρτηση CheckBTGAccess, η οποία επιστρέφει τρεις δυνατές αποφάσεις: Άρνηση, Παραχώρηση, κατ' εξαίρεση πρόσβαση.

Το σπάσιμο του γυαλιού σημαίνει ότι αποδίδεται σε κάποιο ρόλο r δικαίωμα να αποκτήσει κατ' εξαίρεση πρόσβαση για μια συγκεκριμένη λειτουργία π.χ. για ανάγνωση (read) σε ένα αντικείμενο. Η λειτουργικότητα του BTG-RBAC υλοποιήθηκε σε μια πρότυπη εφαρμογή.

Η διαδικασία για την απόδοση κατ' εξαίρεση πρόσβασης, εφόσον ο χρήστης έχει αυθεντικοποιηθεί επιτυχώς και έχει εκκινήσει συνεδρία, έχει ως ακολούθως: Η εφαρμογή καλεί την μηχανή BTG-RBAC και περνάει τα στοιχεία της συνεδρίας, την λειτουργία που επιθυμεί να εκτελέσει ο χρήστης και το αντικείμενο στο οποίο έχει ζητηθεί πρόσβαση. Η συνάρτηση CheckBTGAccess εξετάζει εάν υπάρχει κανόνας ο οποίος επιτρέπει την πρόσβαση στο υποκείμενο. Εφόσον υπάρχει σχετική πολιτική, αποδίδεται το αιτούμενο δικαίωμα πρόσβασης. Εάν όχι, εξετάζεται εάν υπάρχει πολιτική για κατ' εξαίρεση πρόσβαση, αποδίδεται η Υποχρέωση BTG και η απόφαση κατά πόσο θα δοθεί άδεια για κατ' εξαίρεση πρόσβαση. Σε κάθε άλλη περίπτωση του αρνείται η πρόσβαση. Ο χρήστης ερωτάται εάν επιθυμεί να προχωρήσει σε σπάσιμο του γυαλιού (δίνοντας και κάποια αιτιολόγηση). Σε περίπτωση που ο χρήστης επιθυμεί να προχωρήσει, η εφαρμογή λαμβάνει τις πληροφορίες της συνεδρίας, την αιτούμενη ενέργεια (*Υποχρέωση BTG*) και το υποκείμενο. Ελέγχεται η πολιτική από την εφαρμογή ότι έχει δώσει την κατάλληλη *Υποχρέωση* και ορίζεται η κατάσταση του BTGi σε αληθή. Το BTGi είναι υπεύθυνο για την

καταγραφή της κατάστασης BTG, όπου ουσιαστικά έχει τον ρόλο κατάστασης μηχανής (state machine) για το BTG.

Κατά την απόφαση απόδοσης πρόσβασης στον χρήστη, αυτό που τελικά θα αξιολογηθεί είναι εάν η κατάσταση BTGi είναι σε κατάσταση αληθή, και κατόπιν η εφαρμογή θα λάβει τις απαραίτητες πληροφορίες της συνεδρίας και των *Υποχρεώσεων* για να δώσει τα κατάλληλα δικαιώματα πρόσβασης.

Τα μοντέλα BTG που έχουν αναφερθεί έως τώρα βασίζονται είτε στην δημιουργία κάποιας επιπλέον πολιτικής πρόσβασης για τα υποκείμενα και για τα αντικείμενα προκειμένου να επιτευχθεί η απόφαση για την κατ' εξαίρεση πρόσβαση ή στη δημιουργία μιας ξεχωριστής διεργασίας διαχείρισης πρόσβασης.

Στο [NCMD11], παρουσιάζεται το Rumpole, όπου η πολιτική BTG βασίζεται στην αναγνώριση της αιτίας για την άρνηση πρόσβασης αντί για τον αυστηρό καθορισμό κανόνων. Το εν λόγο μοντέλο λαμβάνει υπόψη του τις διαθέσιμες πληροφορίες και τις συνδυάζει με αυστηρούς κανόνες προκειμένου να καταλήξει στην απόφαση για την απόδοση πρόσβασης. Σημειώνεται ότι το Rumpole δεν αποτελεί την επέκταση κάποιου συγκεκριμένου μοντέλου, παρά δίδει ένα πλαίσιο υλοποίησης BTG.

Προκειμένου να διευκολυνθεί η αποτύπωση της διαδικασίας BTG χρησιμοποιούνται οι ακόλουθες έννοιες:

Αρμοδιότητες (Competences): Ορίζουν κατά πόσο ένα υποκείμενο έχει τις απαραίτητες δυνατότητες πρόσβασης σε πόρους χωρίς να προκαλέσει κάποια βλάβη στους πόρους του συστήματος.

Ενδυναμώσεις (Empowerments): Ορίζουν κατά πόσο υπάρχουν οι απαραίτητες συνθήκες περιεχομένου ώστε η πρόσβαση δεν θα προκαλέσει κάποια βλάβη στους πόρους του συστήματος.

Κανόνες BTG: Ορίζουν το εάν θα επιτραπεί σε ένα αντικείμενο να αποκτήσει κατ εξαίρεση πρόσβαση λαμβάνοντας υπόψη τις Αρμοδιότητες, τις Ενδυναμώσεις και τις Υποχρεώσεις που πληροί ή έχει παραβιάσει.

Ψήφισμα Ερωτήματος (Resolution Query): Ορίζει τον τρόπο με τον οποίο και κάτω υπο ποιες συνθήκες λαμβάνονται υπόψη οι κανόνες ώστε να αποφασισθεί η απόδοση κατ' εξαίρεση πρόσβασης.

Οι *Αρμοδιότητες* εμπεριέχουν την έννοια του να ανήκεις σε μια επιτρεπόμενη κατηγορία και επιχειρούν να αποτυπώσουν κατά πόσο το υποκείμενο κατέχει τις αναγκαίες αρμοδιότητες για να αποκτήσει πρόσβαση χωρίς ανεπιθύμητες συνέπειες.

Οι *Ενδυναμώσεις* εμπεριέχουν περιορισμούς ακεραιότητας οι οποίοι είναι σχετικοί για κάποιον πόρο και σχετικοί με το περιεχόμενο και αποτυπώνουν κατά πόσο η πρόσβαση που ζητείται θα πρέπει να αποδοθεί χωρίς να συνυπολογιστεί εάν το υποκείμενο έχει τις κατάλληλες αρμοδιότητες.

Οι α*ρμοδιότητες* και οι *ενσωματώσεις* εκτός από αληθείς ή ψευδείς μπορεί να είναι και άγνωστες. Όταν ένα αντικείμενο δεν κατέχει τα κατάλληλα διαπιστευτήρια είναι πιο κατάλληλο να οριστεί ως άγνωστη η κατάσταση του.

Παρομοίως, εάν ένα υποκείμενο φέρεται κατάλληλο να αποκτήσει πρόσβαση με βάση μια πολιτική και ακατάλληλο από μια άλλη τότε η κατάσταση των Αρμοδιοτήτων του είναι *αντικρουόμενη*.

Έτσι λοιπόν προτείνεται από τους συγγραφείς οι συνήθεις απαντήσεις αληθές / ψευδές να επεκταθούν και να συμπεριλαμβάνουν και τις «άγνωστη» και «αντικρουόμενη» ώστε να αποτυπωθεί με μεγαλύτερη ακρίβεια η πολιτική της κατ' εξαίρεσης πρόσβασης. Για να αποτυπωθούν πιο αναλυτικά οι παραπάνω καταστάσεις χρησιμοποιείται η Λογική BELnap [B77] η οποία ορίζει τέσσερις πιθανές καταστάσεις αλήθειας.

Το Ψήφισμα Ερωτήματος καθορίζει το πώς συνδυάζεται η γνώση που είναι διαθέσιμη για ένα αντικείμενο ώστε να αποφανθεί εάν η πρόσβαση θα αρνηθεί ή θα επιτραπεί. Επιπλέον, καθορίζει το πόσο βάρος πρέπει να δοθεί σε κάθε απόφαση και πόση γνώση είναι επαρκής ώστε η απόφαση που ληφθεί να είναι οριστική.

Οι κανόνες της κατ' εξαίρεση πρόσβασης καθορίζουν πόσα γνωρίζουμε για το εάν μια αίτηση πρόσβασης θα πρέπει να επιτραπεί ή να αρνηθεί και το Ψήφισμα Ερωτήματος καθορίζει πώς αυτή η πληροφορία θα χρησιμοποιηθεί ώστε να ορίσει στο σημείο απόφασης για την απόδοση πρόσβασης τι θα κάνει.

Η εργασία αυτή είναι η κοντινότερη με αυτή που παρουσιάζεται στην διατριβή υπό το πρίσμα ότι δεν βασίζεται σε στατικές πληροφορίες και πολιτικές. Δεν υπάρχει, όμως, κάποιο μοντέλο BTG το οποίο συνυπολογίζει με σαφήνεια παραμέτρους χωρικών και χρονικών περιορισμών καθώς και άλλων παραμέτρων όπως είναι το τρέχον επίπεδο ασφαλείας του οργανισμού στο οποίο εφαρμόζονται οι διαδικασίες BTG.

3. Δυναμική κατ' Εξαίρεση Πρόσβαση με Χωροχρονικούς Περιορισμούς

3.1. Εισαγωγή

Ο απώτερος στόχος του κεφαλαίου αυτού είναι η πρόταση ενός πλαισίου, βασισμένου στο RBAC, το οποίο λαμβάνει υπόψη χρονικούς και χωρικούς περιορισμούς αλλά το σημαντικότερο είναι ότι προσφέρει έναν ελεγχόμενο και ασφαλή τρόπο για να παρακαμφθούν οι στατικές πολιτικές ασφάλειας. Η ιεραρχία των ρόλων αναπαρίσταται ως ένας κατευθυνόμενος γράφος με βάρη, όπου κάθε ρόλος αποτελεί έναν κόμβο. Οι αποστάσεις μεταξύ των κόμβων είναι μια παράμετρος-κλειδί για την προτεινόμενη διαδικασία της κατ' εξαίρεση πρόσβασης. Επιπρόσθετα, πέραν από τους χρονικούς και τους χωρικούς περιορισμούς χρησιμοποιείται δυναμική πληροφορία για να καταλήξουμε σε μια απόφαση κατ' εξαίρεση πρόσβασης. Η προτεινόμενη αρχιτεκτονική , η οποία είναι επί της ουσίας μια επέκταση του XACML, αναλύεται σε βάθος και παρουσιάζεται με μια πρότυπη υλοποίηση με στόχο να αναδείξει την εφαρμοσιμότητα του προτεινόμενου μοντέλου στον χώρο της υγείας. Επιπλέον, παρέχεται και μια μεθοδολογία για την αξιολόγηση της συμπεριφοράς των χρηστών έτσι ώστε να είναι εφικτό να εντοπιστεί μια πιθανή κατάχρηση της λειτουργικότητας της κατ' εξαίρεση πρόσβασης. Τέλος, πραγματοποιήθηκε μια έρευνα σε δυο κλινικές ως μελέτες περίπτωσης για την προαναφερθείσα μεθοδολογία αξιολόγησης.

Το κίνητρο και ο στόχος για τη μεθοδολογία που παρουσιάζεται στο κεφάλαιο αυτό ήταν η δημιουργία ενός μοντέλου κατ' εξαίρεση πρόσβασης το οποίο:

- Λαμβάνει υπόψη χωρικούς και χρονικούς περιορισμούς
- Λαμβάνει υπόψη δυναμικές παραμέτρους
- Δεν απαιτεί την δημιουργία περαιτέρω πολιτικών
- Δεν επιφέρει σημαντικό διαχειριστικό φόρτο
- Η επίδοσή του μπορεί να αξιολογηθεί

3.2. Spatio Temporal EMergency Role Based Access Control (STEM-RBAC)

3.2.1. Βασικό RBAC

Το προτεινόμενο μοντέλο είναι βασισμένο στο RBAC96 όπως προτάθηκε από τον Sanduetal στο [SFK00] και, πιο συγκεκριμένα, στο $RBAC_1$ το οποίο αργότερα υιοθετήθηκε ως το ιεραρχικό RBAC στο πρότυπο ANSIRBAC [ANSI00].

Τα βασικά συστατικά του $RBAC_1$ είναι τα ακόλουθα:

- U, R, P και S είναι τα σύνολα των χρηστών (users – U), ρόλων (roles – R), δικαιωμάτων πρόσβασης (permissions – P) και συνόδων (sessions – S), αντίστοιχα
- $UA \subseteq U \text{x} R$ είναι μια σχέση που αναθέτει χρήστες σε ρόλους (πολλά προς πολλά)
- $PA \subseteq P \text{x} R$ είναι μια σχέση που αναθέτει Δικαιώματα Πρόσβασης σε Ρόλους (πολλά προς πολλά)
- user: $S \rightarrow U$ είναι μια συνάρτηση που αντιστοιχεί Συνόδους σε Χρήστες
- role: $S \rightarrow 2^R$ είναι μια συνάρτηση που αντιστοιχεί κάθε Σύνοδο σε ένα σύνολο Ρόλων
- $RH \subseteq R \times R$ είναι η ιεραρχία των Ρόλων, που είναι μια μερικώς διατεταγμένη σχέση

Το DSTEM-RBAC (Dynamic Spatio Temporal EMergency Role Based Access Control) αποτελεί μια επέκταση του STEM-RBAC (Spatio Temporal EMergency Role Based Access Control) [GNVD11]**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**, το οποίο παρουσιάζεται συνοπτικά στην παρούσα ενότητα.

Στο STEM-RBAC κάθε Ρόλος μπορεί να βρίσκεται σε μια από τις παρακάτω καταστάσεις:

- Ενεργός, ο οποίος δύναται να αποδοθεί στους χρήστες
- Ανενεργός, ο οποίος δεν μπορεί να αποδοθεί στους χρήστες λόγω περιορισμών π.χ. χρονικοί περιορισμοί
- Ενεργόποιημένος, ο οποίος είναι ήδη ενεργός τουλάχιστον σε μια σύνοδο.

3.2.2. Χρονικοί Περιορισμοί

Επιπλέον στοιχεία που έχουμε εισαγάγει προκειμένου να περιγραφούν οι χρονικοί και οι χωρικοί περιορισμοί είναι τα ακόλουθα:

- $R_{EN} \subseteq R$, είναι το σύνολο των ενεργοποιημένων ρόλων (enabled roles)
- $R_{ACT} \subseteq R$, είναι το σύνολο των ενεργών ρόλων is (active roles)
- $uR_{EN} \subseteq U \text{x} R_{EN} \subseteq U \text{x} R$, είναι το υποσύνολο των ενεργοποιημένων ρόλων σε σχέση με κάποιον συγκεκριμένο χρήστη.

Σε συμφωνία με τους χρονικούς περιορισμούς ένα σύνολο ρόλων R_{EN} θα είναι ενεργό. Κάθε εξουσιοδοτημένος χρήστης μπορεί να ξεκινήσει μια συνεδρία με κάποιο ρόλο που ανήκει στο R_{EN}. Κάποιος ρόλος μπορεί να είναι ανενεργός λόγω άλλων περιορισμών. Επιπλέον, για κάθε χρήστη, u, ορίζεται ένα σύνολο, uR_{EN}, το οποίο αποτελεί υποσύνολο

του R_{EN} το οποίο περιλαμβάνει τους ενεργούς ρόλους για κάθε χρήστη. Το uR_{EN} ορίζει τους ρόλους που δύναται να ενεργοποιήσει ο χρήστης.

Προκειμένου να μπορούμε να εκφράσουμε τους χρονικούς περιορισμούς ορίζουμε τις ακόλουθες παραμέτρους:

- *PE* είναι το σύνολο των περιοδικών χρονικών εκφράσεων, τα οποία εκφράζονται ως *ημερολόγια*
- $RTC \subseteq R \times PE$ είναι μια πολλά προς πολλά ανάθεση περιοδικών χρονικών εκφράσεων (χρονικοί περιορισμοί) σε ρόλους.

Προκειμένου να απεικονίσουμε αποτελεσματικά τους χρονικούς περιορισμούς θα χρησιμοποιήσουμε την έννοια των ημερολογίων όπως αυτά έχουν προταθεί από την Niezette [NS92] και των περιοδικών εκφράσεων τα οποία αργότερα ενσωματώθηκαν στους μηχανισμούς ελέγχου πρόσβασης χρησιμοποιώντας περιοδικούς χρονικούς περιορισμούς από την Bertino et al. [BBF01].

Τα ημερολόγια αποτελούνται από «κάθε ημέρα», «κάθε εβδομάδα», «Δευτέρα» κτλ. Οι περιοδικές εκφράσεις είναι ένα ζευγάρι PE=<I, P>, όπου I=[αρχή, τέλος]. Η Αρχή και το Τέλος αποτελεί ένα ζευγάρι ημερολογίου της μορφής μμ/ηη/εεεε:ωω π.χ. 01/01/2024:10, όπου το χρονικό Τέλος μπορεί να είναι απεριόριστο.

$$PE = \sum_{i=1}^{n} O_i C_i \rhd xC_d \ , \qquad (1)$$

C_d, C_1, C_2, …, C_n, είναι ημερολόγια και

$O_1 = all$, $O_i \in 2^N \cup \{all\}$, $C_i \subseteq C_{i-1}$ for i=2,…, n, $C_d \subseteq C_n$, και x ∈ IN. (2)

Το πρώτο μέρος της παραπάνω εξίσωσης (1) καθορίζει το σύνολο των αρχικών σημείων των περιόδων. Η διάρκειά τους καθορίζεται από το (2). Για παράδειγμα, η έκφραση all.years+{1,6}.months $\rhd$ 2.week αναπαριστά τα χρονικά διαστήματα τα οποία ξεκινούν την πρώτη και έκτη ημέρα κάθε μήνα, ανεξαρτήτως έτους, με χρονική διάρκεια δυο εβδομάδων.

3.2.3. Χωρικοί Περιορισμοί

Πέραν της ώρας, περιορισμοί με βάση την τοποθεσία μπορεί να επιβληθούν σε κάθε ρόλο. Οι φυσικές τοποθεσίες μπορεί να ομαδοποιηθούν καθορίζοντας μια λογική οντότητα φυσικής τοποθεσίας λ.χ. κτίρια σε διαφορετικές τοποθεσίες που ανήκουν στον ίδιο οργανισμό, ή διαφορετικά γραφεία σε ένα κτίριο που ανήκουν οργανωτικά στην ίδια διεύθυνση.

Προκειμένου να αποτυπώσουμε τους χωρικούς περιορισμούς ορίζονται οι παρακάτω έννοιες:

- L το σύνολο των φυσικών τοποθεσιών βάση των οποίων επιβάλλονται περιορισμοί τοποθεσίας
- UL η τοποθεσία του χρήστη
- $LL \subseteq LxL$ είναι το σύνολο των λογικών οντοτήτων φυσικής τοποθεσίας, που αποτελεί έναν πολλά προς πολλά ορισμόφυσικών τοποθεσιών σε λογικές οντότητες φυσικής τοποθεσίας
- $LLA \subseteq RxLL$ η ανάθεση λογικών οντοτήτων φυσικής τοποθεσίας $LLA(r_m)$ σε κάθε χρήστη που επιθυμεί να ενεργοποιήσει τον ρόλο r_m.

Οι φυσικές τοποθεσίες L ενδεικτικά μπορεί να αναφέρονται π.χ. στον δεύτερο όροφο του τομέα Β ενός κτιρίου. Ανακύπτει το ζήτημα του καθορισμού της τοποθεσίας ενός χρήστη. Το προαναφερόμενο ζήτημα δεν είναι στα πλαίσια της παρούσας διατριβής, ωστόσο θα αναφέρουμε ορισμένους από τους πιο διαδεδομένους μηχανισμούς καθορισμού της τοποθεσίας ενός χρήστη. Σε κάθε περίπτωση, η αναγνώριση της τοποθεσίας κάθε χρήστη εξαρτάται από την ειδικευμένη υλοποίηση που θα επιλεχθεί. Σε ένα νοσοκομειακό περιβάλλον όπου το νοσηλευτικό προσωπικό χρησιμοποιεί PDA ή κάποια άλλη έξυπνη συσκευή με ενσωματωμένη λειτουργικότητα GPS η ακριβής τοποθεσία μπορεί να καθοριστεί από το PDA. Στο εσωτερικό του νοσοκομείου όπου χρησιμοποιούνται κάρτες φυσικής πρόσβασης στις εσωτερικές θύρες μπορεί να καθοριστεί η τοποθεσία του χρήστη. Σε ένα πιο απλοϊκό σενάριο όπου χρησιμοποιούνται προσωπικοί υπολογιστές η τοποθεσία του χρήστη μπορεί να οριστεί από την χρησιμοποιούμενη διεύθυνση IP ή MAC (φυσική διεύθυνση υπολογιστή).

Η χρήση της φυσικής τοποθεσίας για να καθοριστούν περιορισμοί μπορεί να αποτελέσει μια ιδιαίτερα σύνθετη διεργασία σε πραγματικές συνθήκες. Για να αντιπαρέλθουμε αυτές τις δυσκολίες ορίζουμε την έννοια της Λογικής Τοποθεσίας (Logical Locations - *LL*). Στην απλούστερη των περιπτώσεων μια Λογική Τοποθεσία LL_n θα εμπεριέχει μια τοποθεσία L_m. Σε ένα πιο σύνθετο περιβάλλον η Λογική Τοποθεσία LL_n θα εμπεριέχει μια σειρά από φυσικές τοποθεσίες L_k , L_l ,L_m κτλ.

Η φυσική τοποθεσία L_1 ορίζεται ως ο πρώτος όροφος του κτιρίου Α. Ως τοποθεσία L_2 ορίζεται ο δεύτερος όροφος του κτιρίου Β. Η λογική τοποθεσία της παιδιατρικής κλινικής LL_1 αποτελείται από τις τοποθεσίες L_1 και L_2.

Στον Πίνακα 2, συνοψίζονται οι παράμετροι που ορίσαμε προκειμένου να αποτυπώσουμε και να διαχειριστούμε τους χωροχρονικούς περιορισμούς. Ως «δυναμική» ορίζουμε κάθε παράμετρο η οποία είναι μεταβλητή με τον χρόνο, όπως το σύνολο των ενεργών ρόλων. Ως «στατική» ορίζεται κάθε παράμετρος που παραμένει σταθερή εφόσον δεν διαφοροποιηθεί και η εφαρμοζόμενη πολιτική ασφαλείας όπως οι ρόλοι που έχουν οριστεί σε κάθε χρήστη. Επιπρόσθετα, κάθε παράμετρος του μοντέλου εμπίπτει σε μια από τις ακόλουθες τρεις κατηγορίες: συστατικά (*components)*, σχέσεις *(relations)* και διεργασίες (*functions)* ανάλογα με την εργασία που εκτελούν.

Πίνακας 2: Παράμετροι του STEM-RBAC

Παράμετρος	Περιγραφή	Ιδιότητα	Είδος
PE	Το σύνολο των περιοδικών εκφράσεων (PeriodicExpressions)	Στατική	Συστατικό
$RTC \subseteq$ RxPE	Μια σχέση πολλά προς πολλά, που αποδίδει περιοδικές εκφράσεις σε ρόλους	Στατική	Σχέση
RxPE	Η απόδοση περιοδικών εκφράσεων σε χρήστες για συγκεκριμένους ρόλους	Στατική	Σχέση
$R_{EN} \subseteq R$	Το σύνολο των ενεργοποιημένων ρόλων	Δυναμική	Συστατικό
$R_{ACT} \subseteq R$	Το σύνολο των ενεργώνρόλων	Δυναμική	Συστατικό
$UR_{EN} \subseteq U \times R_E$	Το υποσύνολο των ενεργοποιημένων ρόλων για έναν συγκεκριμένο χρήστη	Δυναμική	Σχέση
L	Το σύνολο των φυσικών τοποθεσιών	Στατική	Συστατικό
UL	Η τοποθεσία του χρήστη(UserLocation)	Δυναμική	Συστατικό
$LL \subseteq L \times L$	Το σύνολο των Λογικών Τοποθεσιών (LogicalLocations)	Στατική	Συστατικό
LxLL	Μια σχέση πολλά προς πολλά, που αποδίδει Φυσικές Τοποθεσίες σε Λογικές Τοποθεσίες	Στατική	Σχέση
$LLA \subseteq R \times LL$	Η απόδοση περιορισμών Λογικής Τοποθεσίας *LLA(r)* σε χρήστες που επιθυμούν να εκκινήσουν συνεδρία με το ρόλο *r*	Στατική	Σχέση
location: S→UL	Απόδοση της τοποθεσίας χρήστη για κάθε συνεδρία που εκκινείται	Δυναμική	Διεργασία

3.2.4. Ιεραρχίες Ρόλων

Στο RBAC, η ιεραρχία των ρόλων υποστηρίζει μια μερική ταξινόμηση των ρόλων ούτως ώστε να υποστηρίζεται η κληρονομικότητα των δικαιωμάτων πρόσβασης. Για να παρέχεται κατ' εξαίρεση πρόσβαση με ελεγχόμενο τρόπο θα κάνουμε χρήση των ιεραρχιών ρόλων ώστε να μπορούμε να καθορίσουμε υπό ποιες συνθήκες μπορεί ένας ρόλος να παραβιάσει την ισχύουσα πολιτική ασφαλείας.

Στην κλασική ιεράρχηση των ρόλων, ένας ρόλος θεωρείται ότι είναι ανώτερος από κάποιον άλλο εάν κατέχει όλες τις προσβάσεις του τελευταίου. Προκειμένου να διευκολύνουμε την διαχείριση της κατ' εξαίρεση πρόσβασης θα επεκτείνουμε την έννοια της ιεράρχησης των ρόλων ορίζοντας τις έννοιες της Ισχυρής Ιεραρχίας Ρόλων (*Strong Role Hierarchy - SRH)* και της Ασθενούς Ιεραρχίας Ρόλων (*Weak Role Hierarchy - WRH)*.

Η Ισχυρή Ιεραρχία Ρόλων, SRH⊆R×R, ορίζεται ως μια μερικώς διατεταγμένη σχέση που την συμβολίζουμε με >>. Λέμε ότι ένας ρόλος είναι πρεσβύτερος του ρόλου εφόσον:

α) όλα τα δικαιώματα πρόσβασης του 2 είναι προσβάσεις και του 1, β) οι χρονικοί περιορισμοί που έχουν επιβληθεί στον 1 είναι υποσύνολο αυτών που έχουν επιβληθεί στον 2 και γ) οι χωρικοί περιορισμοί που έχουν επιβληθεί στον 1 είναι υποσύνολο αυτών που έχουν επιβληθεί στον 2. Το παραπάνω μπορεί να αποδοθεί ως εξής: SRH: $r_2 >> r_1$ iff $PA(r_1) \in PA(r_2)$ && $TC(r_2) \in TC(r_1)$ &&$LLA(r_2) \in LLA(r_1)$.

Η Ασθενής Ιεραρχία Ρόλων WRH έχει εφαρμογή μόνο ανάμεσα στους **ενεργούς ρόλους,** και συνεπώς είναι πλεονασμός να λάβουμε υπόψη και τους χρονικούς περιορισμούς. Η WRH είναι δυναμική καθώς εξαρτάται από τον χρόνο. Ωστόσο λαμβάνονται υπόψη οι χωρικοί περιορισμοί. Πιο αυστηρά, η WRH ορίζεται ως εξής: WRH: $r_2 > r_1$ iff $PA(r_1) \in PA(r_2)$ && $LLA(r_2) \in LLA(r_1)$.

3.2.5. Βαθμοί Ελευθερίας

Οι βαθμοί ελευθερίας (Degrees of Freedom – DoF) είναι μια αριθμητική τιμή που ορίζεται για κάθε ρόλο. Αποδίδει την έννοια της ελευθερίας που έχει ένας ρόλος να παραβιάζει την πολιτική ασφαλείας. Ανάλογα με την τιμή του DoF ένας ρόλος μπορεί να αποκτήσει ή όχι πρόσβαση σε πόρους που κανονικά δεν δικαιούται.

3.2.6. Παράμετρος Παράκαμψης Χρονικών Περιορισμών

Μέχρι στιγμής έχουμε παραμερίσει τους χωροχρονικούς περιορισμούς. Ωστόσο, κάνοντας χρήση της WRH οι χρονικοί περιορισμοί έχουν ήδη ληφθεί υπόψη μιας και αποτελείται μόνο από τους ενεργούς ρόλους.

Ορίζουμε την παράμετρο Παράκαμψης Χρονικών Περιορισμών (TimeByPass – TBP) η οποία επιτρέπει την πρόσβαση σε πόρους που δεν θα επιτρεπόταν εάν εφαρμόζονταν οι χρονικοί περιορισμοί. Η παράμετρος TBP μπορεί να είναι είτε αληθής, όταν έχει δοθεί σε κάποιον ρόλο, είτε ψευδής εάν όχι. Επιπλέον ορίζουμε:

- $RTBP \subseteq TBP \times R$ είναι μια σχέση πολλά προς πολλά που αποδίδει την παράμετρο *Παράκαμψης Χρονικών Περιορισμών σε ρόλους.* Ο ρόλος r_m κατέχει την Παράμετρο *TBP* αν και μόνο αν $r_m \in RTBP \subseteq TBP \times R$.

3.2.7. Παράμετρος Παράκαμψης Χωρικών Περιορισμών

Ορίζουμε την παράμετρο *Παράκαμψης Χωρικών Περιορισμών (LocationByPass - LBP)* η οποία επιτρέπει σε κάποιον ρόλο να αποκτήσει πρόσβαση σε πόρους λαμβάνοντας υπόψη τους χρονικούς περιορισμούς και τους Βαθμούς Ελευθερίας αλλά αγνοεί τους πιθανούς χωρικούς περιορισμούς που υπάρχουν:

- $RLBP \subseteq LBP \times R$ είναι μια σχέση πολλά προς πολλά που αποδίδει την παράμετρο *Παράκαμψης Χωρικών Περιορισμών σε ρόλους.* Λέμε ότι στον ρόλο r_m έχει αποδοθεί η Παράμετρος *LBP* αν και μόνο αν $r_m \in RLBP \subseteq LBP \times R$.

3.2.8. Αλληλεξάρτηση Ρόλων

Λόγω της κρισιμότητας ορισμένων πληροφοριών ή/και άλλων πόρων ορισμένες προσβάσεις και ενέργειες θα πρέπει να υπόκεινται σε αυστηρότερο έλεγχο για την αποφυγή λάθους ή κακόβουλης ενέργειας. Για αυτό τον λόγο ορισμένοι ρόλοι θα ήταν σκόπιμο να εξαρτώνται από κάποιους άλλους. Η *αλληλεξάρτηση ρόλων (Role Dependency - RD)* ορίζεται ως εξής*:*

- $RD \subseteq R \times R$ είναι μια σχέση πολλά προς πολλά που σχετίζει έναν ρόλο με άλλους ρόλους. Ο ρόλος r_m εξαρτάται από τον ρόλο r_n αν και μόνο αν $r_n \in r_m D$.

3.2.9. Ανάσχεση κατ' Εξαίρεση Παραβιάσεων

Προκειμένου να υπάρχει ευελιξία αλλά και ταυτόχρονα να επιβάλλονται περιορισμοί στις προσβάσεις των ρόλων είναι χρήσιμο να εισέλθει περιορισμός στον αριθμό των προσβάσεων/πόρων που αποκτά κάποιος μέσω της διαδικασίας BTG.

Το να επιτραπεί σε κάποιον χρήστη να έχει πρόσβαση στο P_3 ενώ χρειάζεται για να εκτελέσει επιτυχώς και τις εργασίες P_4, P_5 και P_6. δεν είναι αποτελεσματικό. Από την άλλη μεριά, δεν είναι θεμιτό να γίνει κατάχρηση του BTG και κάποιος να αποκτήσει πρόσβαση στο σύνολο των πόρων που του επιτρέπεται μέσω του BTG. Ορίζουμε την παράμετρο *Ταυτόχρονων Παραβιάσεων (Simultaneous Violations - SV),* μια αριθμητική – ακέραια- τιμή η οποία δρα ως το ανώτερο όριο ταυτόχρονων παραβιάσεων της πολιτικής ασφαλείας. Οι περιορισμοί που εισάγονται από το SV εφαρμόζονται σε κάθε σύνοδο που εκκινείται.

- *Roles:* $SV \rightarrow 2^R$ είναι μια συνάρτηση η οποία αποδίδει την τιμή του SV σε ένα σύνολο ρόλων

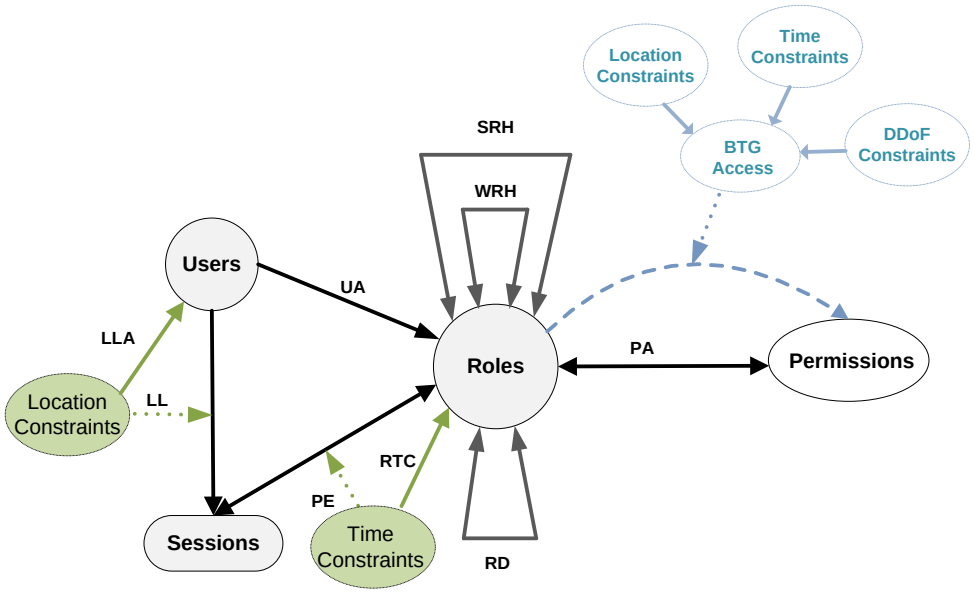
Εάν η τιμή του SV οριστεί ως μηδενική για κάποιο ρόλο τότε ουσιαστικά του στερείται κάθε δικαίωμα για απόκτηση πρόσβασης χρησιμοποιώντας τον μηχανισμό BTG.

3.3. Dynamic Spatio Temporal EMergency Role Based Access Control (DSTEM-RBAC)

Προκειμένου να επιτύχουμε την ελεγχόμενη BTG πρόσβαση θα ορίσουμε την έννοια των Δυναμικών Βαθμών Ελευθερίας (Dynamic Degrees of Freedom - DDoF). Όπως το DoF έτσι και το DDoF είναι μια αριθμητική τιμή που αποδίδεται σε κάθε ρόλο και καθορίζει πόση ελευθερία δίνεται στον ρόλο για να μπορεί να παραβιάσει την πολιτική ασφαλείας.

Στην Εικόνα 15, παρουσιάζονται τα μέρη που αποτελούν το DSTEM-RBAC και οι περιορισμοί που λαμβάνονται υπόψη. Οι χρήστες, εφόσον το επιτρέπουν οι χωροχρονικοί περιορισμοί, εκκινούν μια σύνοδο με έναν συγκεκριμένο ρόλο. Η κατ' εξαίρεση πρόσβαση

σε πόρους επιτρέπεται εφόσον έχουν ληφθεί υπόψη οι περιορισμοί που αφορούν την τοποθεσία, το χρόνο, και το DDoF.



Εικόνα 15. Σύνοψη του DSTEM-RBAC

3.3.1. Δυναμικοί Βαθμοί Ελευθερίας

Οι *Δυναμικοί Βαθμοί Ελευθερίας (Dynamic Degrees of Freedom - DDoF)* αποτελούν μια επέκταση της έννοιας των στατικών Βαθμών Ελευθερίας ώστε να μπορεί να περιλαμβάνονται δυναμικές παράμετροι από το περιβάλλον. Απώτερος στόχος είναι να καταστεί εφικτό ο μηχανισμός για την απόδοση κατ' εξαίρεση πρόσβασης να είναι δυναμικός και πιο εύστοχος. Έτσι, ανάλογα με την τιμή που λαμβάνει το DDoF σε ένα χρήστη, που έχει εκκινήσει συνεδρία με κάποιο ρόλο, θα του επιτραπεί ή όχι να αποκτήσει πρόσβαση σε πόρους που υπό κανονικές συνθήκες δεν του έχουν δοθεί κατάλληλα δικαιώματα πρόσβασης.

Όποτε ένας χρήστης U που έχει εκκινήσει μια σύνοδο με τον ρόλο R αιτηθεί πρόσβαση σε κάποιον πόρο P, όπου με τα συνήθη δικαιώματά του δεν επιτρέπεται, υπολογίζεται η απόσταση του ρόλου R με τον κοντινότερο ρόλο που έχει πρόσβαση στον πόρο P. Όταν αναφερόμαστε σε απόσταση εννοούμε απόσταση γράφων, όπου κάθε ρόλος αποτελεί έναν κόμβο και η ιεραρχία καθορίζεται από το άνυσμα του γράφου.

Η συνολική τιμή του DDoF ορίζεται ως εξής:

$$DDoF = DoF + LLT + OTL - IRL - OES, \quad (3)$$

όπου:

- LLT (Logical Location Trust level) είναι το επίπεδο εμπιστοσύνης της λογικής τοποθεσίας του χρήστη
- OTL (Organization Threat Level) είναι το επίπεδο ασφάλειας που βρίσκεται ο οργανισμός
- OES (Organization Emergency Status) είναι το επίπεδο ανάγκης που βρίσκεται ο οργανισμός
- IRL (Internet Risk Level) είναι το επίπεδο των προερχόμενων από το διαδίκτυο κινδύνων.

Το DoF έχει μια σταθερή στατική τιμή που αποδίδεται σε κάθε ρόλο από τον διαχειριστή σε συμφωνία με την πολιτική ασφαλείας του οργανισμού.

Logical Location Trust level - LLT

Εάν υποθέσουμε ότι ένας χρήστης u υπόκειται σε χωρικούς περιορισμούς, και ο χρήστης βρίσκεται στην τοποθεσία $uL \in LL$. Όπου $LL=(L_1+L_2+...+L_n)$, με L_n να είναι οι τοποθεσίες που δε θέτουν περιορισμούς. Εάν με L_1 συμβολίζουμε την τοποθεσία του κέντρου μηχανογράφησης και με L_2 συμβολίζουμε την οικιακή κατοικία του χρήστη, είναι σαφές η τοποθεσία L_1 μπορεί να θεωρηθεί πιο έμπιστη. Έτσι, λοιπόν, σε κάθε τοποθεσία ή λογική τοποθεσία που χρησιμοποιούμε στο μοντέλο ορίζουμε και ένα επίπεδο εμπιστοσύνης, λ.χ. από LLT=1 στην λιγότερο έμπιστη τοποθεσία έως LLT=5 στην ασφαλέστερη.

Internet Risk Level - IRL

Είναι σύνηθες οι μεγάλοι πάροχοι υπηρεσιών ασφάλειας να δίνουν μια εκτίμηση του επιπέδου κινδύνου στο διαδίκτυο λαμβάνοντας υπόψη τους μια σειρά από παράγοντες όπως νέες κρίσιμες αδυναμίες σε πληροφοριακά συστήματα, κακόβουλες ενέργειες, επικίνδυνο κακόβουλο λογισμικό (ιούς, rootkits κτλ.), δεδομένα που συλλέγονται από αναχώματα ασφαλείας (firewalls), honeypots κτλ. Το IRLπαρέχει ένα μέτρο του ρίσκου στο οποίο εκτίθενται τα πληροφοριακά συστήματα του οργανισμού που είναι συνδεδεμένα στο διαδίκτυο.

Εάν τα πληροφοριακά συστήματα είναι πιο ευάλωτα και υπάρχει μεγαλύτερη πιθανότητα να δεχθούν κάποια επίθεση αυτό θα πρέπει να αντικατοπτρίζεται και στην διαδικασία BTG. Ο αυξημένος κίνδυνος να παραβιαστεί ένα σύστημα και, κατά συνέπεια, κάποιος λογαριασμός χρήστη θα πρέπει να μετριαστεί στην διαδικασία BTG για να περιοριστούν οι συνέπειες μια πιθανής παραβίασης ασφαλείας. Έτσι, λοιπόν, όταν υπάρχει έξαρση των διαδικτυακών κινδύνων οι δυνατότητες για κατ' εξαίρεση πρόσβαση θα πρέπει να περιορίζονται. Αυτή ακριβώς είναι και η χρησιμότητα του IRL, όσο υψηλότερος ο κίνδυνος μιας επίθεσης τόσο υψηλότερη η τιμή και του IRL και, κατά συνέπεια, τόσο πιο περιορισμένες οι δυνατότητες για προσβάσεις μέσω BTG. Η τιμή του IRL μπορεί να υπολογιστεί χρησιμοποιώντας τις ακόλουθες πηγές πληροφόρησης: IBM

threat level [IBM], Symantec Deep Sight Threat Management threatcon[SYM], AVG Internet Risk level [AVG] και Kaspersky securelist [KASP].

Organization Threat Level - OTL

Οργανισμοί που έχουν υψηλό βαθμό ωριμότητας σε ζητήματα ασφάλειας πληροφοριών και διαχείρισης ρίσκου συχνά έχουν διαδικασίες αξιολόγησης του επιπέδου έκθεσης σε ρίσκο τόσο για τα πληροφοριακά συστήματα όσο και για το σύνολο του οργανισμού. Εφόσον υλοποιείται μια τέτοια διαδικασία, το τρέχον επίπεδο έκθεσης ρίσκου θα πρέπει να συνυπολογιστεί κατά την διαδικασία χορήγησης κατ' εξαίρεση πρόσβασης.

Λόγου χάρη, εάν οι υποδομές πληροφορικής έχουν υποστεί καίριο πλήγμα και έχουν εκκινήσει διαδικασίες για ανάκαμψη από καταστροφή αυτό σημαίνει ότι ενδέχεται οι διαχειριστές των συστημάτων να χρειαστούν αυξημένα δικαιώματα για να ανταπεξέλθουν στις τρέχουσες απαιτήσεις. Τα παραπάνω συμπεριλαμβάνονται και αντικατοπτρίζονται στο Organization Threat Level (*OTL*).

Organization Emergency Status - OES

Στον αντίποδα υπάρχουν περιπτώσεις όπου η κατάσταση του οργανισμού επιβάλλει να υπάρχει περιορισμός των δυνατοτήτων BTG των χρηστών, όπως σε περιπτώσεις όπου οι υποδομές έχουν πληγεί από κακόβουλό λογισμικό. Για να ληφθούν υπόψη οι προαναφερθείσες καταστάσεις ορίζουμε το Organization Emergency Status (*OES*).

Οι τιμές που δύνανται να λάβουν οι παράμετροι που αποτελούν το DDoF είναι στην διακριτική ευχέρεια του διαχειριστή. Ο υπεύθυνος για την υλοποίηση και διαχείριση των πολιτικών ασφαλείας και την απόδοση των δικαιωμάτων πρόσβασης θα είναι και τελικά αυτός που θα καθορίσει το εύρος των τιμών αυτών. Ένα παράδειγμα τέτοιας υλοποίησης θα περιγραφεί σε παρακάτω ενότητα.

Οι παράμετροι που αποτελούν τους Δυναμικούς Βαθμούς Ελευθερίας (DDoF) συνοψίζονται στον Πίνακα 3.

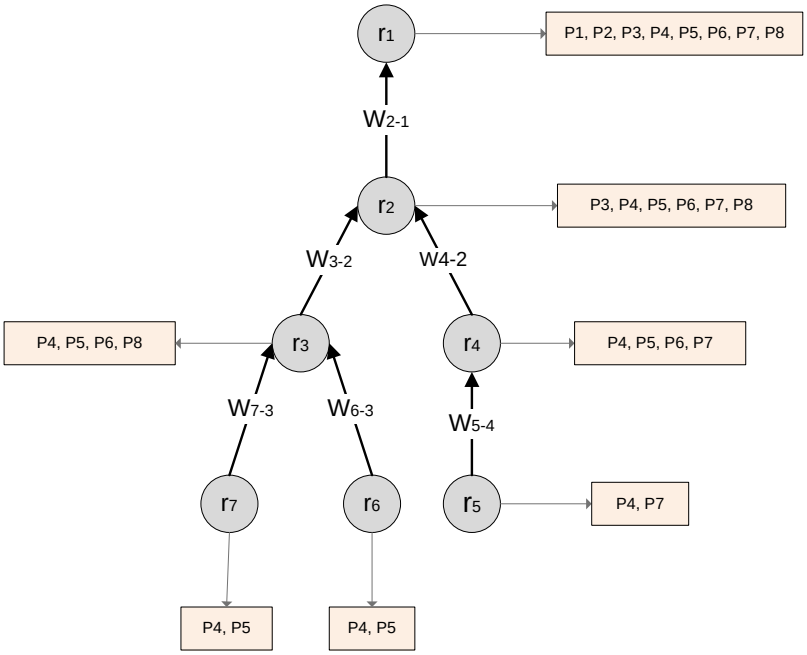
Πίνακας 3: Παράμετροι του DDoF

Παράμετρος	Περιγραφή	Ιδιότητα	Είδος
DoF	ΒαθμοίΕλευθερίας (Degrees of Freedom)	Στατική	Συστατικό
LLT	Επίπεδο Εμπιστοσύνης Λογικής Τοποθεσίας (LogicalLocationTrustlevel)	Δυναμική	Συστατικό
OTL	Επίπεδο Απειλής για τον Οργανισμό (Organization Threat Level)	Δυναμική	Συστατικό
OES	Κατάσταση Εκτάκτου Ανάγκης για τον Οργανισμό (Organization Emergency Status)	Δυναμική	Συστατικό
IRL	Διαδικτυακό Επίπεδο Κινδύνου (Internet Risk Level)	Δυναμική	Συστατικό

3.3.2. Ιεραρχίες Ρόλων ως Γράφοι

Οι ιεραρχίες των ρόλων μπορεί να αναπαρασταθούν από έναν κατευθυνόμενο γράφο που δεν περιέχει κλειστές διαδρομές - loops (κύκλους) και, πιο συγκεκριμένα, από ένα πολυδένδρο (ή κατευθυνόμενο δένδρο ή μοναδικά συνδεόμενο δίκτυο). Οι γράφοι έχουν προταθεί στην βιβλιογραφία για να αναπαραστήσουν εξολοκλήρου το μοντέλο RBAC [KMP02], ωστόσο στο DSTEM-RBAC οι γράφοι χρησιμοποιούνται με πρωτότυπο τρόπο και προκειμένου να υπηρετήσουν συγκεκριμένο στόχο, την ελεγχόμενη διαδικασία BTG.

Το πρόβλημα του εάν θα δοθεί κατ' εξαίρεση πρόσβαση ανάγεται στο ακόλουθο πρόβλημα: την εύρεση της ελάχιστης απόστασης του κόμβου (ο ρόλος με τον οποίο έχει εκκινήσει ο χρήστης σύνοδο) με τον κόμβο – στόχο (που έχει τα επιθυμητά δικαιώματα πρόσβασης) και την σύγκριση με την τιμή του DDOF. Κάθε φορά που πρέπει να ληφθεί μια απόφαση σχετική με BTG θα χρησιμοποιείται ένας γράφος G(V,A), , ο οποίος επί της ουσίας αναπαριστά την WRH. V είναι το σύνολο των κορυφών (vertices) ή κόμβων που αναπαριστούν τους ρόλους και A είναι το σύνολο των ακμών που ορίζουν τη σύνδεση μεταξύ των κορυφών. Στην Εικόνα 16, παρουσιάζεται ο γράφος G(V, A), όπου V={r_1, r_2, r_3, r_4, r_5, r_6, r_7} και A={(r_7, r_3), (r_6, r_3), (r_5, r_4), (r_4, r_2), (r_3, r_2), (r_2, r_1)}.



Εικόνα 16. Ρόλοι ως Γράφοι

3.3.3. Ελάχιστη Απόσταση και Πολυπλοκότητα

Στο παράδειγμα που εξετάσαμε δεν τίθεται θέμα πολυπλοκότητας (complexity) καθώς ήταν μια σχετικά απλή περίπτωση με λίγες παραμέτρους. Ωστόσο, σε μια σύνθετη

ιεραρχία ρόλων που αναπαρίσταται από γράφο με μεγάλο αριθμό ακμών και κόμβων ο υπολογισμός της απόστασης μεταξύ δύο κόμβων δεν είναι δεδομένο ότι θα είναι εύκολος και ότι δεν θα έχει συνέπειες στην επίδοση του συστήματος.

Η ιεραρχία ρόλων είναι ένας δίγραφος χωρίς κατευθυνόμενους κύκλους. Θα εξετάσουμε στη συνέχεια το πρόβλημα του υπολογισμού της ελάχιστης απόστασης μεταξύ δύο κόμβων για αυτή την περίπτωση. Πιο συγκεκριμένα, θα υπολογίσουμε την πολυπλοκότητα εύρεσης της ελάχιστης απόστασης (shortest path) μεταξύ των κόμβων r_i και r_j, όπου $r_i<r_j$. Προϋποθέτουμε ότι ο γράφος είναι τοπολογικά διατεταγμένος εκ των προτέρων, δηλαδή δεν υπάρχει μονοπάτι μεταξύ r_i και r_j εάν $r_i>r_j$, και ο μοναδικός τρόπος να προσεγγιστεί ο κόμβος r_j είναι να χρησιμοποιηθούν κόμβοι που είναι «μικρότεροι» από τον r_j.

Η πιο σύντομη απόσταση μεταξύ δύο κόμβων (ρόλων στην περίπτωσή μας) μπορεί να υπολογιστεί από την παρακάτω αναδρομική σχέση:

$$d(r_j) = \min\{d(r_i) + d(r_i, r_j)\}, \quad (4)$$

όπου $d(r_j)$ η απόσταση μεταξύ r_1, r_j και $d(r_i, r_j)$ είναι η απόσταση μεταξύ r_i, και r_j.

Η παραπάνω εξίσωση είναι γνωστή ως δυναμική εξίσωση προγραμματισμού (ή εξίσωση Bellman) [B57]. Χρειάζονται O(m) πράξεις για να πραγματοποιηθεί τοπολογική ταξινόμηση, και O(m) πράξεις για να υπολογιστούν οι αποστάσεις για μια δεδομένη επανάληψη. Συνεπώς, η απόσταση μεταξύ οποιωνδήποτε κόμβων μπορεί να υπολογιστεί σε χρόνικο διάστημα της τάξης του O(m). Αξίζει να σημειωθεί ότι καταγράφοντας τα *i* που ελαχιστοποιούν το δεξί σκέλος της επανάληψης, μπορούμε να ακολουθήσουμε την ανάποδη διαδικασία και να ανακατασκευάσουμε τα πιο σύντομα μονοπάτια.

3.4. Αρχιτεκτονική DSTEM-RBAC και Πρότυπη Υλοποίηση

3.4.1. Βασισμένη στην XACML

Στην ενότητα αυτή παρουσιάζεται μια αρχιτεκτονική βασισμένη στην XACML [A05]**Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.** και παρουσιάζεται μια πρότυπη υλοποίηση του DSTEM-RBAC ως διαδικτυακή εφαρμογή. Θα χρησιμοποιήσουμε τις ακόλουθες έννοιες που ορίζονται και στο XACML:

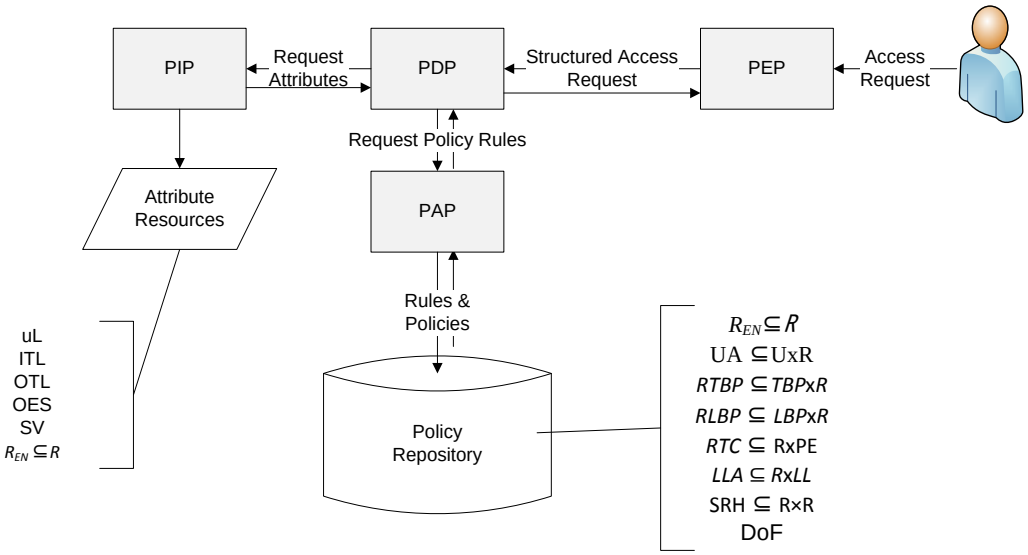
- Σημείο Εφαρμογής Πολιτικής (Policy Enforcement Point - PEP)
- Σημείο Αποφάσεων Πολιτικής (Policy Decision Point - PDP)
- Σημείο Πληροφοριών Πολιτικής (Policy Information Point - PIP)
- Σημείο Πρόσβασης Πολιτικής (Policy Access Point - PAP).

Τις έννοιες αυτές θα τις προσαρμόσουμε και θα τις επεκτείνουμε προκειμένου να ανταποκρίνονται στις απαιτήσεις μας.

Όποτε κάποιος χρήστης αιτείται πρόσβαση σε κάποιον πόρο το PEP λαμβάνει το αίτημα πρόσβασης και με τη σειρά του κάνει ένα δομημένο αίτημα πρόσβασης στο PDP. Το PDP για να μπορέσει να αποφασίσει εάν θα πρέπει να επιτραπεί η πρόσβαση χρειάζεται να συμβουλευτεί τα PIP και PAP. Το PIP είναι υπεύθυνο να προωθήσει στο PDP τις απαραίτητες πληροφορίες που σχετίζονται με δυναμικές παραμέτρους όπως πληροφορίες για την τοποθεσία του χρήστη. Το PAP είναι υπεύθυνο να ενημερώσει το PDP με τις στατικές πληροφορίες που αφορούν την ισχύουσα πολιτική πρόσβασης. Το PDP λαμβάνει και επεξεργάζεται τις πληροφορίες που έλαβε από τα PIP και PAP, προκειμένου να λάβει την απόφαση για το ποιες πολιτικές πρόσβασης πρέπει να εφαρμοστούν.

Το *PIP* έχει την ευθύνη να λάβει την τοποθεσία του χρήστη uL, τον αριθμό των παραβιάσεων υπό τη συγκεκριμένη συνεδρία (εάν υπάρχουν), το σύνολο των ενεργοποιημένων ρόλων και, τέλος, τις ακόλουθες παραμέτρους του *DDoF*: Διαδικτυακό Επίπεδο Κινδύνου (IRL), Κατάσταση Εκτάκτου Ανάγκης για τον Οργανισμό (OES) και Επίπεδο Απειλής για τον Οργανισμό (OTL).

Η συνολική αρχιτεκτονική περιγράφεται συνοπτικά στην Εικόνα 17:



Εικόνα 17. Εννοιολογικό μοντέλο Διαχείρισης Πρόσβασης

3.4.2. Υλοποίηση Εφαρμογής

Προκειμένου να αναδείξουμε την εφικτότητα και την ευκολία χρήσης της προτεινόμενης λύσης αναπτύξαμε μια πρότυπη υλοποίηση. Η σχεδίαση της αρχιτεκτονικής της εφαρμογής βασίζεται στο μοντέλο που παρουσιάζεται στην Εικόνα 17 και υλοποιήθηκε ως εφαρμογή διαδικτύου χρησιμοποιώντας php, JavaScript, JSON και το σύστημα

διαχείρισης σχεσιακών βάσεων δεδομένων mysql για την διαχείριση και αποθήκευση των δεδομένων.

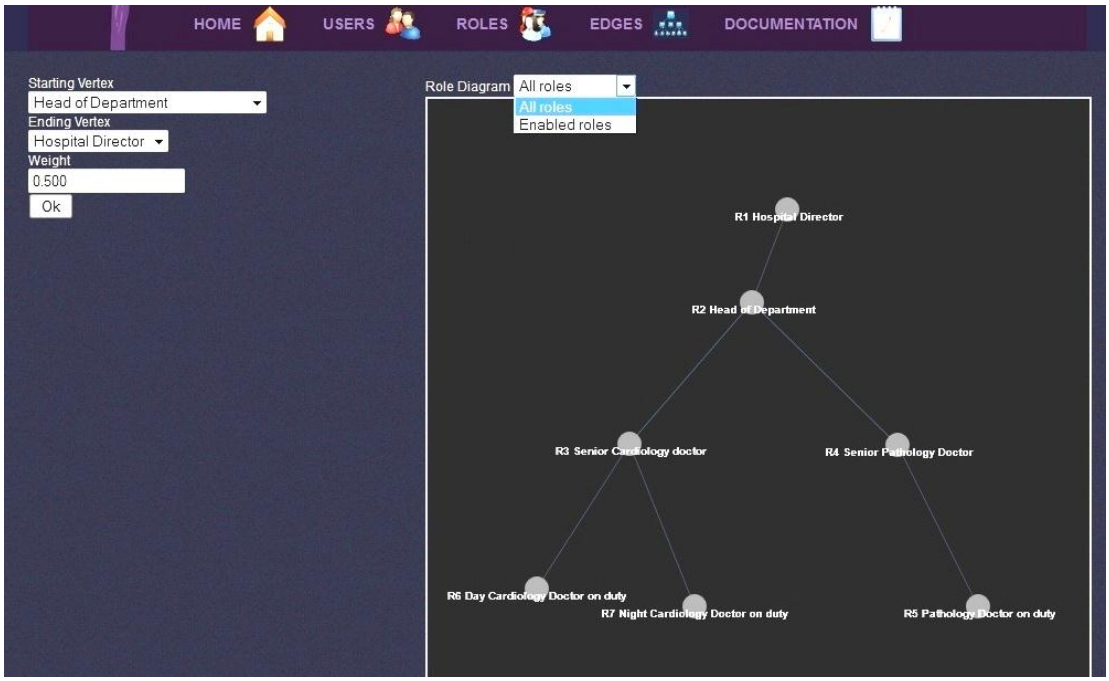
Μέσω της διεπαφής της εφαρμογής που παρέχεται, οι τελικοί χρήστες μπορούν να συνδεθούν και ανάλογα με τον ρόλο με τον οποίο εκκίνησαν τη σύνοδο σύνδεσης μπορούν να δουν, να τροποποιήσουν ή να διαγράψουν πληροφορίες. Κατά τη δημιουργία ενός χρήστη εξ ορισμού αυτός δεν έχει καθόλου δικαιώματα μέχρις ότου ο διαχειριστής να του εκχωρήσει κάποιο ρόλο. Όποτε κάποιος χρήστης προσπαθεί να προσπελάσει κάποιο πόρο που βάσει του ρόλου του δεν δικαιούται, αναδύεται ένα παράθυρο που τον ενημερώνει ότι η πρόσβαση αυτή (εάν τελικά επιτευχθεί) θα γίνει με τη διαδικασία BTG και ζητείται να επιβεβαιώσει ότι επιθυμεί να προχωρήσει. Οι όποιες ενέργειες πραγματοποιούνται από τους χρήστες με BTG διαδικασίες καταγράφονται. Η απόφαση για το εάν θα δοθεί κατ' εξαίρεση πρόσβαση πραγματοποιείται λαμβάνοντας υπόψη την τελική τιμή του DDoF, τον πόρο που αιτείται πρόσβαση και την εφαρμοζόμενη πολιτική πρόσβασης.

Στον διαχειριστή της εφαρμογής παρέχονται τα κατάλληλα εργαλεία σε γραφικό περιβάλλον για να υλοποιήσει το μοντέλο RBAC και να ορίσει τις παραμέτρους για το BTG. Ο διαχειριστής μπορεί να προσθέσει ή να τροποποιήσει ρόλους και χρήστες, καθώς και να ορίσει/καταργήσει ρόλους σε χρήστες. Επιπλέον, ορίζει την τιμή του DoF και τις τιμές που έχουν τα βάρη στους γράφους ανάμεσα στους ρόλους. Επιπλέον, μπορεί να καθοριστούν χωρικοί και χρονικοί περιορισμοί στους ρόλους. Στην συγκεκριμένη υλοποίηση, οι χωρικοί περιορισμοί βασίζονται στην δικτυακή διεύθυνση (IP) του χρήστη. Οι ενέργειες που πραγματοποιούνται χρησιμοποιώντας κατ' εξαίρεση πρόσβαση καταγράφονται σε ξεχωριστό πίνακα της βάσης δεδομένων.

Επιπλέον, παρέχεται στον διαχειριστή η δυνατότητα να έχει γραφική απεικόνιση της ιεραρχίας των ρόλων, είτε του συνόλου των ρόλων (SRH) είτε της ιεραρχίας των ενεργών ρόλων (WRH) (βλέπε Εικόνες 18 και 19).

Εικόνα 18. Αρχική σελίδα διαχειριστή

Κάθε ρόλος αποτελεί έναν κόμβο και κάθε σχέση ιεραρχίας δυνατότερου-ασθενέστερου ρόλου αποτελεί μια ακμή στον γράφο. Έτσι, για την αναπαράσταση μίας ιεραρχίας ρόλων αρκεί η δημιουργία δύο πινάκων στην βάση. Ο πρώτος πίνακας αποθηκεύει τις ιδιότητες κάθε κόμβου (id, δικαιώματα , ειδικότητα) και ο δεύτερος πίνακας αποθηκεύει τις ιδιότητες κάθε γράφου (id κόμβου εκκίνησης, id κόμβου τερματισμού, βάρος).



Εικόνα 19. Σελίδα διαχειριστή

Μεταβαίνοντας στα μενού των χρηστών και των γράφων μπορεί κανείς να παρατηρήσει αντίστοιχες λειτουργίες με αυτές των ρόλων για τη δημιουργία και την επεξεργασία τους. Σημαντικό είναι να αναφερθεί ότι κατά την δημιουργία του χρήστη και την ανάθεσή του σε έναν ρόλο δημιουργείται αυτόματα από το σύστημα ένας κωδικός πρόσβασης για την πρόσβασή του στο σύστημα. Σε περίπτωση απώλειας του κωδικού από τον χρήστη ο διαχειριστής μπορεί να επιλέξει την δημιουργία ενός νέου κωδικού από το σύστημα.

Ο χρήστης μετά την εισαγωγή και τον επιτυχή έλεγχο του ονόματος χρήστη και του κωδικού του θα μεταβεί στην αρχική σελίδα της ιατρικής κλινικής. Χρησιμοποιώντας το κεντρικό μενού στο αριστερό μέρος της σελίδας ο χρήστης μπορεί να μεταβεί στις σελίδες του κάθε τμήματος της ιατρικής κλινικής καθώς και να διαβάσει ανακοινώσεις που έχουν αναρτηθεί.

Ο χρήστης αφού μεταφερθεί στη σελίδα κάποιου τμήματος (βλέπε και Εικόνα 20) μπορεί να χρησιμοποιήσει της λειτουργίες του τμήματος αυτού εφόσον κατέχει τα κατάλληλα δικαιώματα. Οι βασικές λειτουργίες κάθε τμήματος είναι οι παρακάτω:

- Ανάγνωση ιστορικού του ασθενή
- Προσθήκη καταγραφής στο ιστορικό του ασθενή
- Αλλαγή στοιχείων καταγραφής
- Προσθήκη νέου ασθενή
- Αλλαγή στοιχείων ασθενή.

Εικόνα 20. Λειτουργίες σελίδας καρδιολογικού τμήματος

3.5. Συχνότητα Εμφάνισης κατ' Εξαίρεση Προσβάσεων

Μέχρι στιγμής έχουμε παρουσιάσει ένα ολοκληρωμένο πλαίσιο για την απόδοση κατ' εξαίρεση πρόσβασης με ελεγχόμενο τρόπο. Παρά ταύτα, υπάρχει πάντοτε η πιθανότητα κάποιος χρήστης να κάνει υπέρμετρη ή ακόμα και κακόβουλη χρήση της διαδικασίας BTG. Η ύπαρξη ενός μηχανισμού που θα εντοπίζει τέτοιες περιπτώσεις είναι αναγκαία. Σε αυτή την ενότητα θα παρουσιάσουμε μια μεθοδολογία για την αξιολόγηση της χρήσης της λειτουργικότητας του BTG.

Προκειμένου η συμπεριφορά ενός χρήστη να κατηγοριοποιηθεί ως κακόβουλη ή έστω ύποπτη θα πρέπει πρώτα να ορίσουμε ποια είναι η φυσιολογικά αποδεκτή συμπεριφορά και να ορίσουμε το κατώφλι πέραν από το οποίο η συμπεριφορά του χρήστη δεν είναι αποδεκτή. Όταν το κατώφλι αυτό ξεπερνιέται θα πρέπει να ενημερώνεται ο διαχειριστής και να εξετάζεται εάν πρέπει να ληφθούν περαιτέρω μέτρα. Μια αυτοματοποιημένη αντίδραση, π.χ. απαγόρευσης πρόσβασης και χρήσης της λειτουργικότητας BTG παρέχει ένα στιβαρό αντίμετρο απέναντι σε κακόβουλες ενέργειες, ωστόσο κάτι τέτοιο ενδέχεται να έχει δραστική επίδραση στην λειτουργία και την όλη νοοτροπία της κατ' εξαίρεση πρόσβασης. Επιπρόσθετα, το να οριστεί ένα καθολικό κατώφλι ίσως να μην είναι ρεαλιστικό καθώς ο αναμενόμενος αριθμός ενεργειών BTG εξαρτάται από μια σειρά από παράγοντες που επηρεάζουν τον οργανισμό.

Προκειμένου να μπορέσουμε να παράσχουμε μια ρεαλιστική προσέγγιση για την αξιολόγηση και χρήση του προτεινόμενου μοντέλου πρόσβασης συλλέξαμε πληροφορίες, μέσω ερωτηματολογίων, από δύο οργανισμούς παροχής υπηρεσιών υγείας. Η μια κλινική βρίσκεται στην Αθήνα, την οποία θα καλούμε κλινική Α, και η άλλη στην Θεσσαλονίκη, την οποία θα καλούμε κλινική Β. Ο στόχος των ερωτηματολογίων ήταν διττός: η συλλογή πληροφοριών για την τρέχουσα κατάσταση όσον αφορά την διαχείριση πρόσβασης και η συλλογή πληροφοριών για τη συχνότητα με την οποία παρουσιάζεται ανάγκη για κατ' εξαίρεση πρόσβαση σε δεδομένα.

Αξίζει να σημειωθεί ότι χρησιμοποιήσαμε δύο διαφορετικά ερωτηματολόγια, ένα που απευθυνόταν στο ιατρικό προσωπικό και ένα που απευθυνόταν στο τμήμα μηχανογράφησης και πληροφορικής. Για τα πλήρη ερωτηματολόγια βλέπε Παράρτημα Α - Ερωτηματολόγιο Προς Κλινικές.

Σύμφωνα με τις απαντήσεις που λάβαμε και οι δύο οργανισμοί υλοποιούν έλεγχο πρόσβασης με ιεραρχική χρήση ρόλων. Σε συνέχεια της συμπλήρωσης των ερωτηματολογίων πραγματοποιήσαμε μια συνέντευξη με το τμήμα πληροφορικής της κλινικής Α, και καταλήξαμε στο συμπέρασμα ότι τα δεδομένα που συλλέξαμε δεν είναι αξιοποιήσιμα για τους σκοπούς μας όπως τους ορίσαμε στην ενότητα αυτή. Πιο συγκεκριμένα, το ζήτημα που ανέκυψε είναι ότι στην πλειοψηφία των περιπτώσεων που ζητείται κατ' εξαίρεση πρόσβαση σε δεδομένα ασθενών πρόκειται για την συλλογή πληροφοριών χωρίς ταυτοποίηση με συγκεκριμένο ασθενή. Τα δεδομένα αυτά ζητούνται στα πλαίσια ιατρικής έρευνας. Για την διαδικασία αυτή προβλέπεται μια εσωτερική

διαδικασία για να δοθούν οι κατάλληλες εγκρίσεις. Οι περιπτώσεις μεμονωμένης κατ' εξαίρεση πρόσβασης είναι ελάχιστες και όχι αξιοποιήσιμες για τον στόχο μας. Ωστόσο οι πληροφορίες που συλλέξαμε από την κλινική Β είναι σχετικές με την κατ' εξαίρεση πρόσβαση στα πλαίσια του DSTEM-RBAC.

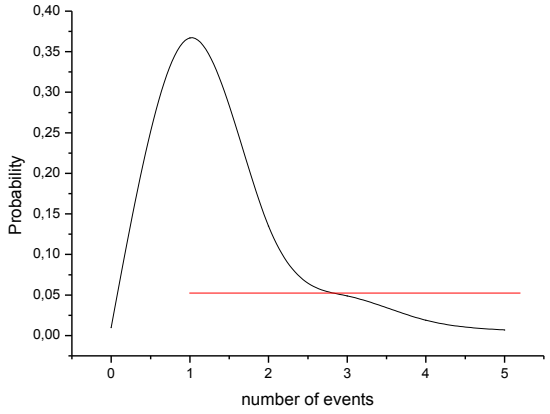
Παρατηρήσαμε και ένα ενδιαφέρον παράπλευρο φαινόμενο το οποίο δεν ήταν στο αντικείμενο της έρευνάς μας ωστόσο αξίζει να αναφερθεί. Υπήρχε σημαντική διαφοροποίηση ανάμεσα στις απαντήσεις που λάβαμε από το ιατρικό προσωπικό και στις απαντήσεις που λάβαμε από το προσωπικό που διαχειρίζεται τα πληροφοριακά συστήματα. Σύμφωνα με το τμήμα της πληροφορικής, καταγράφονται σημαντικά λιγότερες περιπτώσεις (της τάξης του 30%) κατ' εξαίρεση πρόσβασης σε σχέση με τις πληροφορίες που μας δόθηκαν από το ιατρικό προσωπικό. Στο πλαίσιο της μελέτης μας θα λάβουμε υπόψη τα αποτελέσματα που λάβαμε από το ιατρικό προσωπικό, καθώς η διαφορά αυτή μπορεί να αποδοθεί στο γεγονός ότι το ιατρικό προσωπικό απέκτησε την πρόσβαση που επιθυμούσε (ή τουλάχιστον προσπάθησε) παρακάμπτοντας τη συνήθη διαδικασία και το προσωπικό της πληροφορικής δεν έλαβε γνώση για σημαντικό αριθμό κατ' εξαίρεση προσβάσεων που αποκτήθηκαν.

Οι πληροφορίες που λάβαμε από το ιατρικό προσωπικό χρησιμοποιήθηκαν έτσι ώστε να καθορίσουμε τις παραμέτρους μιας κατανομής Poisson στην οποία θα βασιστούμε για να αξιολογήσουμε την επίδοση και την αποτελεσματικότητα της υλοποίησης του DSTEM-RBAC. Σύμφωνα λοιπόν με τις απαντήσεις που λάβαμε, κατά μέσο όρο σε μια εβδομάδα υπάρχει ανάγκη για κατ εξαίρεση πρόσβαση οχτώ φορές την εβδομάδα στην κλινική Β, δηλαδή 1,14 την ημέρα.

Η χρήση των πειραματικών δεδομένων στην κατανομή Poisson μας δίνει μια γενική επισκόπηση της αναμενόμενης συμπεριφοράς της υλοποίησης του προτεινόμενου μοντέλου στην συγκεκριμένη περίπτωση. Η πιθανότητα να υπάρχει κάποιο αίτημα για κατ' εξαίρεση πρόσβαση υπολογίζεται σύμφωνα με την παρακάτω εξίσωση:

$$P_a(x) = \frac{e^{-a} a^x}{x!} \quad (5)$$

Στην κατανομή Poisson ο αριθμός των συμβάντων (στην περίπτωσή μας τα αιτήματα πρόσβασης) δεν μπορεί παρά να είναι ακέραιοι αριθμοί. Στην συγκεκριμένη περίπτωση μελέτης λαμβάνουμε υπόψη τον μέσο όρο συμβάντων σε μια ημέρα.



	α=1	α=2
P(0)	0.3679	0.1353
P(1)	0.3679	0.2707
P(2)	0.1839	0.2707
P(3)	0.0613	0.1804
P(4)	0.0153	0.0902
P(5)	0.0031	0.0361
P(6)	0.0005	0.0120
P(7)	0.0001	0.0008

Εικόνα 21 Πιθανότητα πραγματοποίησης συμβάντων και κατανομή Poisson για α=1 και α=2

Η παραπάνω προσέγγιση μπορεί να χρησιμοποιηθεί και για τον εντοπισμό αφύσικης συμπεριφοράς κάποιου χρήστη. Ορίζουμε ένα κατώφλι ΠΠ τέτοιο ώστε εάν η συνθήκη $P(x) \leq p_t$ είναι αληθής έχει εντοπιστεί κάποια μη φυσιολογική συμπεριφορά χρήστη. Το κατώφλι ουσιαστικά είναι η αποδεκτή πιθανότητα του αριθμού των εξαιρέσεων που θα παρουσιαστούν σε μια ημέρα, το οποίο απεικονίζεται στην Εικόνα 21 με την κόκκινη γραμμή (παράλληλα στον άξονα Χ). Στην μελέτη περίπτωσης που εξετάζουμε ορίζουμε το κατώφλι: p_t=0.05. Έτσι λοιπόν εφόσον $P(3) = 0.0613 \succ 0.05$ ο αποδεκτός αριθμός κατ εξαίρεση προσβάσεων είναι τρεις σε μια ημέρα. Εάν πραγματοποιηθεί τέταρτη πρόσβαση BTG έχουμε: $P(4) = 0.0153 \prec 0.05$ και θα πρέπει να ενεργοποιηθεί μια διαδικασία ενημέρωσης του διαχειριστή του συστήματος για να ληφθούν περαιτέρω ενέργειες.

Ένας πιο κομψός τρόπος ώστε να λαμβάνουμε υπόψη τις κατ' εξαίρεση προσβάσεις που έχει γίνει σε μία ημέρα είναι να συμπεριλάβουμε αυτή την πληροφορία στο $DDoF_p$.

$$DDoF_p = DDoF - {k_j}/{cP(x)}, \quad (6)$$

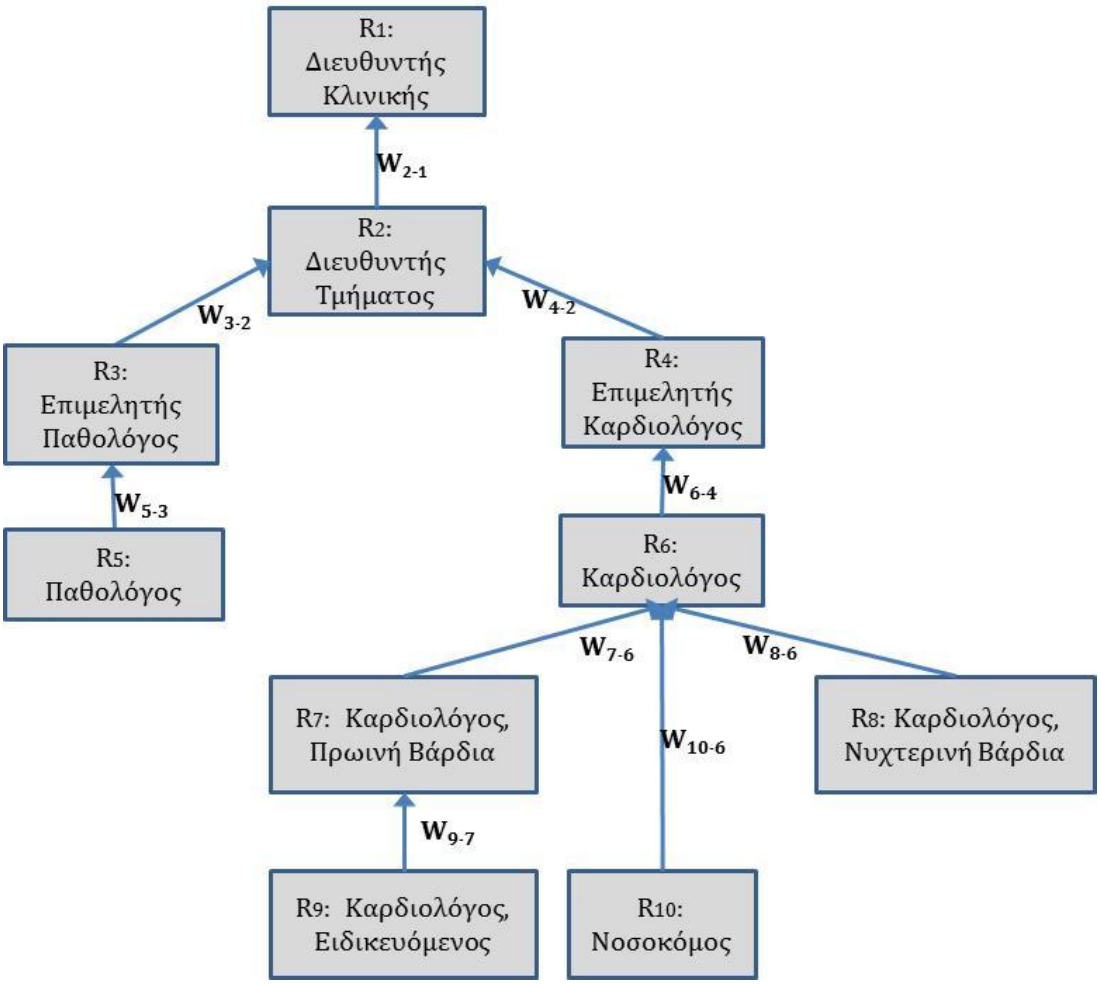
όπου $k_j = \begin{cases} 0, if \;\; j \leq a \\ 1, if \;\; j \succ a \end{cases}$, και

c είναι μια σταθερά που έχει το ρόλο του διορθωτικού παράγοντα ώστε να ρυθμίζεται το όριο και η ανεκτικότητα στον αναμενόμενο αριθμό συμβάντων (παραβιάσεων).

3.6. Περίπτωση Μελέτης

Κατόπιν της ολοκλήρωσης της παρουσίασης όλων των δυνατοτήτων του DSTEM-RBAC και τις παραμέτρους που τις υποστηρίζουν, κρίνουμε σκόπιμο να παρουσιάσουμε και μία περίπτωση μελέτης η οποία θα αναδεικνύει την χρησιμότητα και την λειτουργικότητα του μοντέλου. Θα εστιάσουμε περισσότερο στην λειτουργία του μηχανισμού της κατ' εξαίρεση πρόσβασης και λιγότερο στις υπόλοιπες παραμέτρους του μοντέλου, όπως την παράμετρο *Παράκαμψης Χωρικών Περιορισμών*.

Στο παράδειγμα μας θα βασιστούμε στην ιεραρχία που παρουσιάστηκε στην ενότητα «Ιεραρχίες Ρόλων ως Γράφοι» αλλά θα την επεκτείνουμε και θα την διαφοροποιήσουμε ώστε να μπορέσουμε να αποδώσουμε ορισμένα πιο σύνθετα σενάρια χρήσης. Οι ρόλοι και η ιεραρχία παρουσιάζονται στην Εικόνα 22.



Εικόνα 22. Ιεραρχία και ρόλοι - περίπτωσης μελέτης

Οι Ρόλοι R_1, R_2, . . R_n καθώς και τα βάρη που αποδίδονται στην ακμή που συνδέει κάθε ρόλο με τον πρεσβύτερο του στην ιεραρχία περιγράφονται στον Πίνακα 4. Ο πιο προνομιούχος ρόλος δεν διαθέτει ακμή που να τον συνδέει με άλλο ρόλο και, συνεπώς, δεν του αποδίδεται και κάποιο βάρος.

Πίνακας 4: Ρόλοι, Δικαιώματα και Βάρη Ακμών

Ρόλος	Περιγραφή Ρόλου	Δικαιώματα	Βάρος	Τιμή
R_1	Διευθυντής Κλινικής	P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}		
R_2	ΔιευθυντήςΤμήματος	P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9	$W_{2\text{-}1}$	10
R_3	Επιμελητής Γιατρός Παθολόγος	P_1, P_2, P_3, P_4, P_7, P_8,	$W_{3\text{-}2}$	8
R_4	Επιμελητής Γιατρός Καρδιολόγος	P_1, P_2, P_3, P_4, P_5, P_6	$W_{4\text{-}2}$	7
R_5	Γιατρός Παθολόγος	P_1, P_2, P_3, P_4, P_7	$W_{5\text{-}3}$	5
R_6	Γιατρός Καρδιολόγος	P_1, P_2, P_3, P_4, P_5	$W_{6\text{-}4}$	6
R_7	Γιατρός Καρδιολόγος, Πρωινή Βάρδια	P_2, P_3, P_4, P_7	$W_{7\text{-}6}$	4
R_8	Γιατρός Καρδιολόγος, Νυχτερινή Βάρδια	P_2, P_3, P_4, P_7	$W_{8\text{-}6}$	4
R_9	Γιατρός Καρδιολόγος, Ειδικευόμενος	P_2, P_3, P_4	$W_{9\text{-}7}$	6
R_{10}	Νοσοκόμος	P_1, P_2	$W_{10\text{-}6}$	6

ΧρονικοίΠεριορισμοί

Ορίζουμε τα ακόλουθα ημερολόγια:

- PE_1 = all.months+{1, 2, 3, 4, 5}.weeks+{8.00}.hours $\triangleright$ 8.hours
- PE_2 = all.months+{1, 2, 3, 4, 5}.weeks+{16.00}.hours $\triangleright$ 6.hours
- PE_3 = all.months+{1, 2, 3, 4, 5}.weeks+{8.00}.hours $\triangleright$ 14.hours
- PE_4 = all.days+{8.00}.hours $\triangleright$ 14.hours

Ο «ΓιατρόςΚαρδιολόγος, Πρωινή Βάρδια» δύναται να χρησιμοποιηθεί κατά τις πρωινές εργάσιμες ώρες, τις εργάσιμες ημέρες τις εβδομάδας, και του ανατίθεται το ημερολόγιο PE_1. Αντίστοιχα, στον«ΓιατρόςΚαρδιολόγος, Νυχτερινή Βάρδια» ανατίθεται το ημερολόγιο PE_2. Οι «Γιατρός Παθολόγος» και «Γιατρός Καρδιολόγος» υπόκεινται σε λιγότερο αυστηρούς περιορισμούς καθώς τους ανατίθεται το ημερολόγιο PE_3.

Στον «Γιατρός Καρδιολόγος, Ειδικευόμενος» δεν θα αναθέσουμε κάποιο χρονικό περιορισμό απ' ευθείας, ωστόσο θα τον ορίσουμε ως εξαρτημένο από τον ρόλο «Γιατρός Καρδιολόγος» ή «Γιατρός Καρδιολόγος, Πρωινή Βάρδια» οπότε ο ρόλος του ειδικευόμενου ενδέχεται να είναι ενεργός μόνο όταν είναι ενεργός κάποιος από αυτούς τους ρόλους και έτσι ουσιαστικά υπόκεινται στους χρονικούς περιορισμούς που καθορίζονται από τα ημερολόγιο PE_1 ή PE_3.

Χωρικοί Περιορισμοί

Για να ορίσουμε χωρικούς περιορισμούς θα χρησιμοποιήσουμε τις ακόλουθες φυσικές τοποθεσίες:

- L_1: Κλινική
- L_2: Εξωτερικά Ιατρεία
- L_3: Τομέας Καρδιολογίας
- L_4: Τομέας Παθολογικού
- L_5: Έκτακτα Περιστατικά.

και τις ακόλουθες Λογικές Τοποθεσίες:

- LL_1: $\{L_1\}$
- LL_2: $\{ L_2,L_3,L_5\}$
- LL_3: $\{ L_2,L_4,L_5\}$.

Παράμετροι κατ' εξαίρεση πρόσβασης

Ορίζουμε την παράμετρο *Ταυτόχρονων Παραβιάσεων (SimultaneousViolations - SV),* μια αριθμητική –ακέραια- τιμή ή οποία δρα ως το ανώτερο όριο ταυτόχρονων παραβιάσεων της πολιτικής ασφαλείας. Οι περιορισμοί που εισάγονται από το SV εφαρμόζονται σε κάθε σύνοδο που εκκινείται.

Ο διαχειριστής του συστήματος θα πρέπει να ορίσει και το εύρος των τιμών που δύνανται να εκχωρηθούν στις παραμέτρους οι οποίες αθροίζουν στο DDoF:

- LLT [0,3], OTL [0,4], IRL [0,2], OES [0, 4].

Επιπλέον, στους ρόλους αποδίδεται και η στατική τιμή του DoF όπως φαίνεται στον Πίνακα 5.

Για μην υπάρχει κατάχρηση της κατ' εξαίρεσης πρόσβασης ορίζουμε την παράμετρο «*Ταυτόχρονων Παραβιάσεων» SV=3* για όλους τους ρόλους.

Πίνακας 5 Απόδοση τιμών DoF στους Ρόλους

Ρόλος	**Περιγραφή**	**DoF**
R_1	Διευθυντής Κλινικής	-
R_2	Διευθυντής Τμήματος	7
R_3	Επιμελητής Γιατρός Παθολόγος	5
R_4	Επιμελητής Γιατρός Καρδιολόγος	5
R_5	Γιατρός Παθολόγος	4
R_6	Γιατρός Καρδιολόγος	4
R_7	Γιατρός Καρδιολόγος, Πρωινή Βάρδια	3
R_8	Γιατρός Καρδιολόγος, Νυχτερινή Βάρδια	4
R_9	Γιατρός Καρδιολόγος, Ειδικευόμενος	2
R_{10}	Νοσοκόμος	6

Ας υποθέσουμε ότι ένας χρήστης εφόσον καλύπτει τους χρονικούς και χωρικούς περιορισμούς που απαιτούνται έχει εκκινήσει μια σύνοδο με τον ρόλο R_4 «Επιμελητής Γιατρός Παθολόγος» και επιθυμεί να αποκτήσει πρόσβαση σε μια πληροφορία η οποία απαιτεί το δικαίωμα πρόσβασης P_9. Συνεπώς, για να αποκτήσει πρόσβαση θα ενεργοποιήσει την διαδικασία της κατ' εξαίρεση πρόσβασης.

Ο πιο κοντινός ρόλος που διαθέτει τις κατάλληλες προσβάσεις είναι ο R_2 «Διευθυντής Τμήματος». Συνεπώς θα πρέπει να ελεγχθεί κατά πόσο η απόσταση του R_4 από το R_2 είναι μικρότερη από το DDoF.

Ο χρήστης βρίσκεται εντός της κλινικής που είναι έμπιστη τοποθεσία, συνεπώς το LLT λαμβάνει την μέγιστη δυνατή τιμή,

- LLT=3.

Επιπλέον, ας υποθέσουμε ότι πρόσφατα ανακαλύφθηκαν σειρά από επικίνδυνες ευπάθειες και αναπτύχθηκε κακόβουλο λογισμικό το οποίο αυτοματοποιημένο μπορεί να εκμεταλλευτεί τις ευπάθειες αυτές. Το επίπεδο ασφαλείας που λαμβάνεται καθορίζεται ως "medium" από τους οργανισμούς που λαμβάνουμε υπόψη. Συνεπώς:

- *IRL=1.*

Οι συνθήκες λειτουργίες της κλινικής είναι οι συνήθεις. Συνεπώς, θα ορίσουμε τις τιμές των *OTL* και *OES* ως μηδενικές.

Με βάση τις συνθήκες που περιγράψαμε παραπάνω έχουμε ότι:

DDoF = DoF + LLT + OES - OTL – IRL =9

Στην απλή αυτή περίπτωση η απόσταση $d(R_3, R_2)$ ισούται με το W_{3-2} όπου τελικά έχουμε ότι $DDoF>d(R_3, R_2)$ και θα δοθούν οι προσβάσεις P_9. Εάν ο ίδιος χρήστης αιτηθεί πρόσβαση στο P_{10} τότε θα πρέπει το DDoF να συγκριθεί με την απόσταση του R_3 με το R_1. Σημειώνεται ότι έχει αποδοθεί μεγάλη τιμή στο βάρος W_{2-1} ώστε οι συνθήκες που θα επιτρέψουν την πλήρη πρόσβαση σε πληροφορίες και πόρους που κανονικά έχουν αποδοθεί στον Διευθυντή Κλινικής να είναι εξαιρετικά σπάνιες.

Εάν κάποιος χρήστης έχει εκκινήσει μια συνεδρία με το ρόλο «Νοσοκόμος» με τις συνθήκες που ισχύουν όπως παραπάνω θα έχει:
DDoF=8 + 3 +0 -0 - 1= 10.

Ιεραρχικά ο ρόλος «Νοσοκόμος» έχει περιορισμένα δικαιώματα. Ωστόσο, λόγω της ενδεχόμενης άμεσης εμπλοκής σε επείγουσες καταστάσεις για την περιποίηση ασθενών του έχει αποδοθεί υψηλή τιμή στο DoF για να μπορεί εν δυνάμει να χρησιμοποιεί τον μηχανισμό της κατ' εξαίρεση πρόσβασης για να αποκτήσει ισχυρά δικαιώματα.

Έτσι, λοιπόν, για να αποκτήσει πρόσβαση στο P_3 θα πρέπει η απόσταση $d(R_{10}, R_6)$ να είναι μικρότερη από το DDoF, κάτι που πράγματι ισχύει, καθώς η απόσταση αυτή ισούται με το $W_{10-6}=8$. Για να αποκτήσει πρόσβαση στο P_6 θα πρέπει όμως η απόσταση $d(R_{10}, R_6)$να είναι μικρότερη από το DDoF. Η απόσταση ισούται με:
$d(R_{10}, R_6)= W_{10-6} + W_{6-4} = 12$

και οπότε σε αυτή την περίπτωση δεν θα του επιτραπεί η πρόσβαση.

Υπό άλλες συνθήκες, ωστόσο, ενδέχεται η ίδια προσπάθεια κατ' εξαίρεση πρόσβασης να μην καρποφορήσει. Εάν υποθέσουμε ότι δεν υπάρχουν σημαντικές τεχνικές αδυναμίες που έχουν αποκαλυφθεί σε επίπεδο λογισμικού, τότε το IRL λαμβάνει την τιμή 0. Επιπλέον, στην κλινική λόγω πολλών έκτακτων περιστατικών που οφείλονται σε κάποιο ατύχημα το επίπεδο του οργανισμού έχει περιέλθει σε κρίσιμη κατάσταση και έτσι το OES λαμβάνει την τιμή 3. Πλέον, το DdoF διαμορφώνεται ως εξής:
DDoF=8 + 3 +3 -0 - 0= 14.

Επανερχόμενοι τώρα στο αίτημα ενός χρήστη με το ρόλο «Νοσοκόμος» για πρόσβαση στο P_6 έχουμε $DDoF>d(r_{10}, r_6)$ και συνεπώς θα του επιτραπεί η πρόσβαση.

Συνεχίζοντας, εάν ο ίδιος χρήστης αιτηθεί πρόσβαση στο P_6 το συντομότερο μονοπάτι είναι προς τον ρόλο «Επιμελητής Γιατρός Καρδιολόγος» όπου η απόσταση είναι:
$d(R_{10}, R_6) = W_{10-6} + W_{6-4} + W_{4-2} = 19$

και συνεπώς το σύστημα θα του αρνηθεί την πρόσβαση.

Αξίζει να σημειωθεί ότι ανεξάρτητα από τις συνθήκες που μπορεί να επικρατούν, ο ρόλος «Νοσοκόμος» δεν θα μπορέσει σε καμία περίπτωση να αποκτήσει πρόσβαση στο P_6 καθώς η μέγιστη τιμή που μπορεί να λάβει το DDoF είναι ίση με 15, η οποία είναι μικρότερη από την απόσταση $d(R_{10}, R_6) = 19$. Εάν κρίνεται ότι υπάρχει χρησιμότητα να πρέπει να υπάρχει τέτοιου είδους πρόσβαση θα πρέπει ο διαχειριστής του συστήματος να

προβεί στην κατάλληλη τροποποίηση των παραμέτρων που εμπλέκονται στην κατ' εξαίρεση πρόσβαση, π.χ. να αυξήσει την στατική τιμή του DoF του ρόλου «Νοσοκόμος» ή να μειώσει την τιμή στο βάρος κάποιου από τα $W_{10\text{-}6}$, $W_{6\text{-}4}$, $W_{4\text{-}2}$.

4. Αυθεντικοποίηση Χρηστών σε Πληροφοριακά Συστήματα

4.1. Εισαγωγή

Η αυθεντικοποίηση είναι η διαδικασία κατά την οποία καθορίζεται κατά πόσο κάποιος ή κάτι είναι αυτός ή αυτό που δηλώνει ότι είναι. Οι χειρόγραφες υπογραφές είναι από τις αρχαιότερες και πιο διαδεδομένες μεθόδους κάποιος να δηλώσει υπεύθυνα την θέλησή του και να δώσει την συγκατάθεσή του σε μια ενέργεια, όπως σε ένα συμβόλαιο. Η χρήση σφραγίδων (αρχικά από πηλό και αργότερα από κερί) αποτελεί μια μέθοδο αυθεντικοποίησης της καταγωγής ενός εγγράφου από τις απαρχές των ανθρώπινων κοινωνιών είτε πρόκειται για ερωτικό γράμμα είτε για μια βασιλική διαταγή. Με την ραγδαία εξέλιξη των πληροφοριακών και των τηλεπικοινωνιακών συστημάτων στις σύγχρονες κοινωνίες οι άνθρωποι γίνονται ολοένα και περισσότερο εξαρτώμενοι από τα πληροφοριακά συστήματα για τις καθημερινές τους εργασίες και η ανάγκη για αυθεντικοποίηση σε ηλεκτρονικές υπηρεσίες έχει πλέον αναχθεί σε ένα πολύ σοβαρό ζητούμενο. Για να επιτύχει την αυθεντικοποίησή του ένας χρήστης (ή ένα υποκείμενο γενικότερα) θα πρέπει να παρουσιάσει κάποια πληροφορία στο πληροφοριακό σύστημα προκειμένου αυτό να επιβεβαιώσει ότι είναι αυτός που ισχυρίζεται ότι είναι. Η πληροφορία αυτή μπορεί να προέρχεται από μια από τις παρακάτω πηγές ή από κάποιο συνδυασμό αυτών:

- Κάτι που ο χρήστης γνωρίζει, όπως ένας κωδικός ασφαλείας
- Κάτι που ο χρήστης κατέχει, π.χ. μια ηλεκτρονική κάρτα
- Κάτι που ο χρήστης είναι ή κάνει, π.χ. δακτυλικά αποτυπώματα ή ρυθμός πληκτρολόγησης
- Πού βρίσκεται ο χρήστης, π.χ. μπροστά από ένα συγκεκριμένο τερματικό.

Ο πιο διαδεδομένος τρόπος αυθεντικοποίησης είναι αυτός που γίνεται με βάση κάτι που ο χρήστης γνωρίζει. Η ευρεία διάδοση και αποδοχή του οφείλεται αφενός στην ευκολία υλοποίησής του με χαμηλό κόστος και αφετέρου στην ευκολία χρήσης που παρέχει.

Η αυθεντικοποίηση με κάτι που ο χρήστης κατέχει παρέχει υψηλό επίπεδο ασφαλείας αλλά επιφέρει σημαντικό οικονομικό κόστος για την υλοποίησή του και πάντοτε υπάρχει ο κίνδυνος να χαθεί ή να κλαπεί μια ηλεκτρονική κάρτα ή ένα token.

Τα βιομετρικά συστήματα που αυθεντικοποιηθούν με βάση κάτι που ο χρήστης είναι ή κάνει είναι κάτι το οποίο δεν μπορεί να ξεχαστεί και η αντιγραφή του είναι δύσκολη και επίπονη χωρίς να είναι και αδύνατη. Ένα από τα ζητήματα που υπάρχουν με τα βιομετρικά συστήματα είναι η απόρριψη ενός χρήστη με κατάλληλα διαπιστευτήρια καθώς και η αποδοχή ενός χρήστη με εσφαλμένα διαπιστευτήρια. Τα ποσοστά των παραπάνω περιπτώσεων είναι σημαντικά για τα σύγχρονα βιομετρικά σύστημα. Τα

βιομετρικά συστήματα επίσης παρουσιάζουν προβλήματα αποδοχής από τους χρήστες που μπορεί να αισθάνονται ότι παραβιάζεται η ιδιωτικότητά τους. Τέλος, η υλοποίηση ενός βιομετρικού συστήματος απαιτεί ειδικό εξοπλισμό και επιφέρει σημαντικό οικονομικό κόστος.

4.2. Αυθεντικοποίηση με Κωδικούς Πρόσβασης

Οι αλφαριθμητικοί κωδικοί ασφαλείας οι οποίοι είναι και το κυρίαρχο μέσο αυθεντικοποίησης βασίζονται σε κάτι το οποίο ο χρήστης γνωρίζει. Η εγγενής αδυναμία των κωδικών ασφαλείας είναι αρκετά προφανής: ο άνθρωπος διαθέτει περιορισμένη δυνατότητα να απομνημονεύει μια σειρά από ένα μεγάλο πλήθος τυχαίων χαρακτήρων, οι οποίοι και θα αποτελούσαν έναν ασφαλή κωδικό ασφαλείας. Σύντομοι ή απλοϊκοί κωδικοί ασφαλείας που είναι εύκολο να τους θυμόμαστε είναι εύκολο να τους μαντέψει και ένας κακόβουλος χρήστης, ενώ μια σειρά από τυχαίους χαρακτήρες μεγάλου μήκους δεν είναι εύκολο να τους μαντέψει κάποιος. Ωστόσο τέτοιους κωδικούς ασφαλείας οι χρήστες τείνουν είτε να μην τους θυμούνται ή να αναγκάζονται να τους σημειώνουν π.χ. σε σημειώματα κάτω από το πληκτρολόγιο τους, προκειμένου να μην τους ξεχάσουν.

4.3. Αυθεντικοποίηση με Γραφικούς κωδικούς Πρόσβασης

Τα τελευταία χρόνια έχουν αναδειχθεί και προταθεί πολλοί μηχανισμοί αυθεντικοποίησης οι οποίοι είναι βασισμένοι σε οπτική πληροφορία ως εναλλακτική πρόταση για τους κωδικούς πρόσβασης. Η βασική έννοια η οποία έχει αποτελέσει το έναυσμα για αυτές τις προσπάθειες είναι το γεγονός ότι οι άνθρωποι τείνουν να θυμούνται ή να ανακαλούν οπτική πληροφορία πιο εύκολα συγκριτικά με την γραπτή πληροφορία (όπως είναι οι παραδοσιακοί κωδικοί πρόσβασης). Εκτεταμένη μελέτη και έρευνα έχει πραγματοποιηθεί για τα βασισμένα στους παραδοσιακούς κωδικούς πρόσβασης μοντέλα αυθεντικοποίησης. Παρόλα τα εγνωσμένα μειονεκτήματα και τις αδυναμίες τους, παραμένουν μακράν το δημοφιλέστερο μέσο αυθεντικοποίησης σε πληροφοριακά συστήματα λόγω του χαμηλού κόστους υλοποίησής τους και της ευκολίας χρήσης τους.

Οι Κωδικοί Γραφικών περιλαμβάνουν τα συστήματα κωδικών τα οποία προκειμένου να αυθεντικοποιήσουν τους χρήστες βασίζονται σε οπτική πληροφορία, συμπεριλαμβανομένου του να επιλέξουν ένα υποσύνολο εικόνων, να σχεδιάσουν κάτι, ή να επιλέξουν σημεία σε μια φωτογραφία.

Οι Κωδικοί Γραφικών προτάθηκαν αρχικά από τον G. Blonder το 1996 [B96]. Έκτοτε, έχει προταθεί μια πληθώρα συστημάτων Κωδικών Γραφικών και η έρευνα στο αντικείμενο αυτό έχει προσελκύσει μεγάλο ενδιαφέρον από την επιστημονική κοινότητα, και όχι μόνο, καθώς έχουν προταθεί και πολλά εμπορικά προϊόντα.

Οι Κωδικοί Γραφικών μπορεί να κατηγοριοποιηθούν ως ακολούθως:

- Βασισμένοι στην Αναγνώριση (Recognition Based): παρουσιάζεται στον χρήστη ένα σύνολο εικόνων/φωτογραφιών και αυτός καλείται να αναγνωρίσει το υποσύνολο των φωτογραφιών που είχε διαλέξει κατά το στάδιο της αρχικής του εγγραφής στο σύστημα
- Βασισμένοι στην Ανάκληση (Recall Based): στον χρήστη παρουσιάζεται μια εικόνα, και αυτός καλείται να επιλέξει/σχεδιάσει/ζωγραφίσει σε ένα ή περισσότερα σημεία στην εικόνα που του εμφανίζεται κατά το στάδιο της εγγραφής. Κατά την είσοδό του στο σύστημα ο χρήστης θα πρέπει να αναπαραγάγει με επιτυχία τις ενέργειες αυτές.

4.3.1. Γραφικοί Κωδικοί Βασισμένοι στην Αναγνώριση

Το σύστημα αυθεντικοποίησης Passfaces™ [PASS] είναι ένα εμπορικό προϊόν στο οποίο ο χρήστης θα πρέπει να διαλέξει από ένα σύνολο εννέα προσώπων που θα του παρουσιαστούν εκείνο το οποίο είχε επιλέξει και κατά την εγγραφή του και την αρχικοποίηση του Γραφικού κωδικού του (βλέπε Εικόνα 23). Η διαδικασία επαναλαμβάνεται μέχρις ότου όλα τα «γνωστά» πρόσωπα έχουν επιτυχώς αναγνωριστεί από τον χρήστη (ο αριθμός των προσώπων κυμαίνεται συνήθως από τρία έως επτά).

Εικόνα 23. Επίδειξη του Passfaces

Το S-Passface [TMM13] αποτελεί μια παραλλαγή του Passface που στοχεύει στην αντιμετώπιση επιθέσεων σερφαρίσματος ώμου. Ο χρήστης θα πρέπει να διαλέξει από ένα σύνολο προσώπων που του παρουσιάζονται αλλά αντί να χρησιμοποιήσει το ποντίκι και να κάνει κλικ πάνω σε εικόνες για να διαμορφώσει τον Γραφικό Κωδικό του,

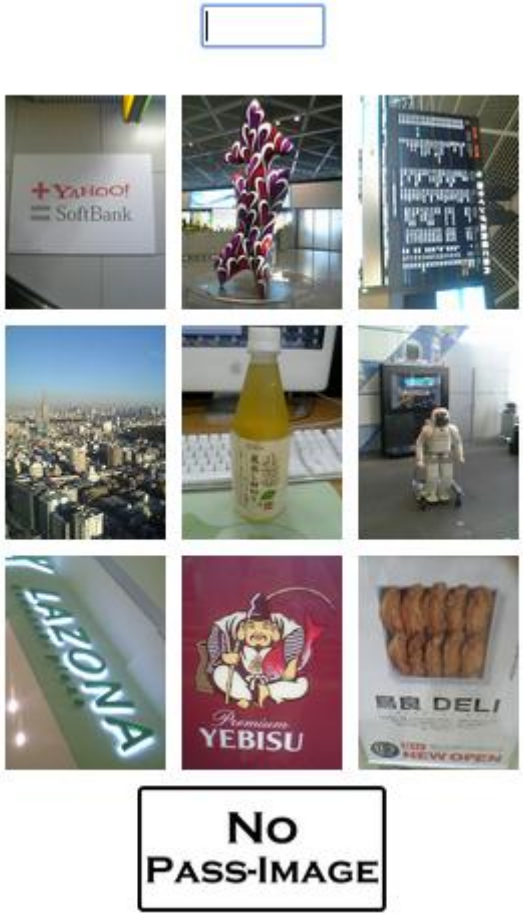
πληκτρολογεί στο πεδίο “password” αλφαριθμητικούς χαρακτήρες οι οποίοι έχουν αντιστοιχηθεί σε κάθε μια εικόνα (βλέπε Εικόνα 24).

Εικόνα 24. Επίδειξη του S-Passface

Παρόμοια λύση είναι το σχήμα “Story” [DMR04], όπου ο Γραφικός Κωδικός αποτελείται από μια ακολουθία k εικόνων που έχουν επιλεγεί από τον χρήστη και αποτελούν μια ιστορία (Story). Οι εικόνες επιλέγονται από ένα σύνολο n εικόνων (n>k) όπου η κάθε μια από αυτές ανήκει σε μια διαφορετική κατηγορία / θέμα. Σε ένα σύνολο εννέα εικόνων κάθε μια θα ανήκει σε από τις ακόλουθες διαφορετικές κατηγορίες: αντικείμενα, φαγητό, ζώα, παιδιά, αθλήματα, αυτοκίνητα, τοποθεσία/αξιοθέατα, άντρες και γυναίκες. Ένα παράδειγμα εικόνων (με n=9) από τις οποίες μπορεί να επιλέξει ο χρήστης παρουσιάζεται στην Εικόνα 25.

Εικόνα 25. Επίδειξη του Story

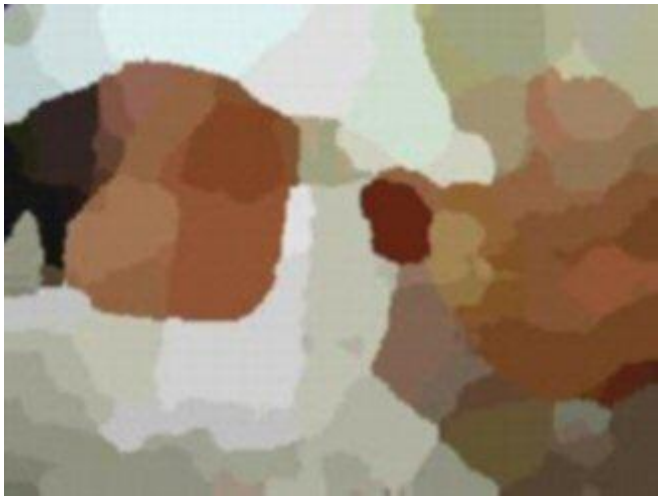
Στο Awase [TK03], [TOK06], ο χρήστης κατά την εγγραφή του μεταφορτώνει μια εικόνα της επιλογής του. Κατά την διαδικασία της αυθεντικοποίησης του παρουσιάζεται η εικόνα αυτή ανάμεσα σε μια σειρά από τυχαίες εικόνες και θα πρέπει να την αναγνωρίσει επιτυχώς. Εάν η εικόνα δεν είναι ανάμεσα σε αυτές που του παρουσιάζονται ο χρήστης θα πρέπει να επιλέξει το πλήκτρο “NoPass-Image” και οι εικόνες θα ανανεωθούν, εάν η εικόνα που έχει επιλέξει είναι ανάμεσα σε αυτές την διαλέγει για να αυθεντικοποιηθεί, αλλιώς επιλέγει πάλι το “NoPass-Image” και η διαδικασία επαναλαμβάνεται.



Εικόνα 26. Επίδειξη του Awase

Το Use your Illusion [HDCP08] έχει παρόμοια προσέγγιση αλλά λαμβάνει υπόψη του και τις δυσκολίες που μπορεί να υπάρχουν λόγω περιορισμών της συσκευής που χρησιμοποιείται, πχ. τη χαμηλή ανάλυση της οθόνης, και οι εικόνες έχουν αλλοιωθεί με ελεγχόμενο τρόπο.

Βασίζεται στην ικανότητα που έχουν οι άνθρωποι να μπορούν να αναγνωρίσουν επιτυχώς μια υποβαθμισμένη σε ποιότητα και χαρακτηριστικά εικόνα (Εικόνα 27) που έχουν παλαιότερα δει (Εικόνα 28). Βλέποντας μια εικόνα με υποβαθμισμένα χαρακτηριστικά είναι δύσκολο να μπορέσει ένας κακόβουλος να αντιστρέψει πλήρως την διαδικασία μετασχηματισμού της στην αρχική εικόνα παρέχοντας έτσι έναν μηχανισμό απέναντι σε επιθέσεις κοινωνικής μηχανικής και απ' ευθείας παρατήρησης.

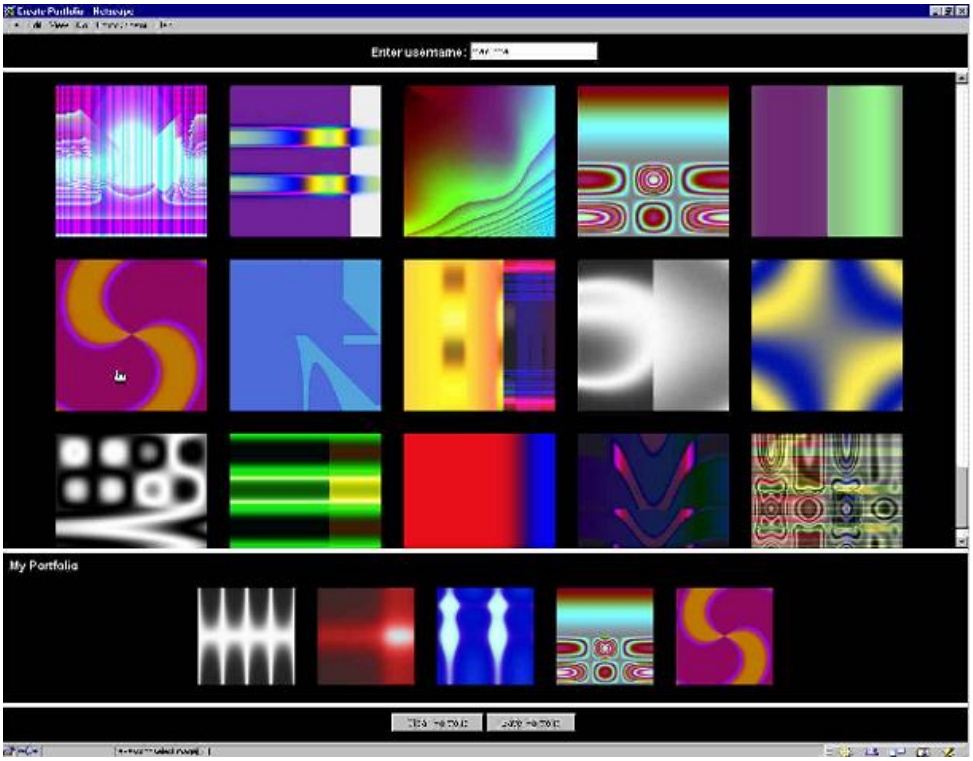


Εικόνα 27. Use your Illusion - εικόνα αλλοιωμένη με ελεγχόμενο τρόπο

Εικόνα 27. UseyourIllusion – αρχική εικόνα

Η Εικόνα 26 είναι η εικόνα που θα παρουσιαστεί στον χρήστη να αναγνωρίσει προκειμένου να αυθεντικοποιηθεί, ενώ η Εικόνα 27 είναι η εικόνα που είχε αρχικά επιλεγεί ως το μυστικό διαπιστευτήριο του χρήστη.

Στο Déjà vu [DP00] στους χρήστες παρουσιάζεται ένα σύνολο εικοσιπέντε φωτογραφιών και αυτοί καλούνται να επιλέξουν ένα υποσύνολο πέντε φωτογραφιών που είχαν επιλέξει κατά την εγγραφή τους στο σύστημα. Προκειμένου να αποθαρρυνθούν οι χρήστες από την επιλογή φωτογραφιών που είναι εύκολο να περιγραφούν και, συνεπώς, να διαμοιραστούν με τρίτους αλλά και φωτογραφίες που ενδεχομένως να είναι προβλέψιμες και εύκολο να τις μαντέψει ένας επιτιθέμενος στο Déjà vu το σύνολο των φωτογραφιών επιλέγονται από την Τυχαία Τέχνη του Andrej Bauer [AB98].



Εικόνα 28. Επίδειξη Déjà vu

Οι Sobrado and Birget [SB02], [WWSB06] έκαναν ορισμένες προτάσεις για Κωδικούς Γραφικών οι οποίοι θα μπορούν να αντιμετωπίσουν επιθέσεις τύπου «περιήγησης ώμου» (shoulder surfing). Ο χρήστης παρουσιάζεται με ένα μεγάλο σύνολο εικόνων και επιλέγει τρεις. Κατά την αυθεντικοποίησή του θα πρέπει να επιλέξει ένα σημείο εντός του τριγώνου που ορίζεται από τις τρεις εικόνες που είχε αρχικά επιλέξει. Οι Asghar et al. [APW13], όμως, παρουσίασαν μια επίθεση κρυπτανάλυσης που υπονομεύει σημαντικά την ασφάλεια των προτεινόμενων μοντέλων.

4.3.2. Γραφικοί Κωδικοί Βασισμένοι στην Ανάκληση

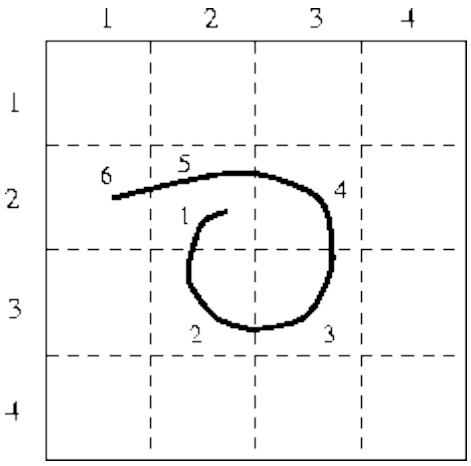
Στο Passpoints [BBMWM05], [WWBBM05a], [WWBBM05b] τα διαπιστευτήρια του χρήστη αποτελούνται από τα διαδοχικά κλικ σε συγκεκριμένα σημεία σε εικόνες που παρουσιάζονται στους χρήστες. Στον χρήστη παρουσιάζεται μια προεπιλεγμένη εικόνα (βλέπε Εικόνα 29) και αυτός επιλέγει τον Γραφικό Κωδικό επιλέγοντας λ.χ. επτά διαδοχικά σημεία όπως φαίνεται στην Εικόνα 30.

Εικόνα 29. Passpoints – προεπιλεγμένη εικόνα

Εικόνα 30. Passpoints – σημεία επιλεγμενα από τον χρήστη

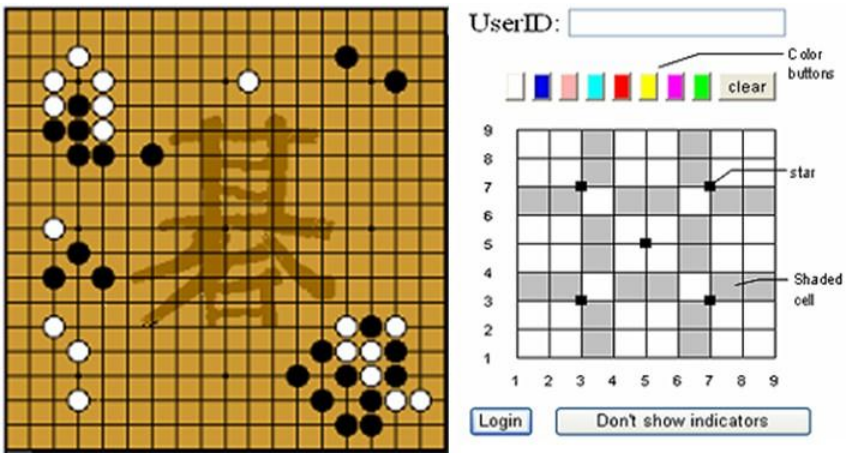
Χρησιμοποιώντας τεχνικές επεξεργασίας εικόνας, την μεροληπτική επιλογή από χρήστες καθώς και με άλλες μεθόδους αποδεικνύεται ότι η ασφάλεια ενός τέτοιου συστήματος είναι ιδιαίτερα ευάλωτη και ουσιαστικά καθιστά το σύστημα ανοιχτό σε κακόβουλες επιθέσεις [DMB07], [TO07], [G07].

Στο Draw A Secret (DAS), από τους Jermyn et al. [JMRR99], ο χρήστης καλείται να ζωγραφίσει κάτι της επιλογής του σε έναν διδιάστατο πλέγμα, όπως φαίνεται και στην Εικόνα 31. Οι συντεταγμένες των πλεγμάτων απ' όπου «περνά» η ζωγραφιά του χρήστη αποτελούν των κωδικό ασφαλείας. Το DAS προσφέρει κωδικούς με ικανοποιητικό μέγεθος. Όπως φαίνεται και στην Εικόνα 31 ο χρήστης καλείται να ζωγραφίσει σε ένα πλέγμα 4x4, και το σχήμα που επιλέγει αντιστοιχεί σε ένα Γραφικό Κωδικό ανάλογα με την σειρά επιλογής στα σημεία του πλέγματος που περνά.



Εικόνα 31. Επίδειξη DrawASecret

Το Pass-Go είναι βασισμένο σε ένα παλιό κινέζικο παιχνίδι το Go. Ο χρήστης επιλέγει τις διασταυρώσεις ενός πλέγματος, αντί τα ίδια τα κελιά του πλέγματος, ως μέθοδο εισαγωγής του κωδικού πρόσβασης (βλέπε Εικόνα 32).



Εικόνα 32. Επίδειξη Pass-Go

4.4. Μέθοδοι Επιθέσεων σε Κωδικούς Ασφαλείας

Οι κωδικοί ασφαλείας έχουν αποτελέσει το αντικείμενο εκτεταμένης έρευνας αλλά και επιθέσεων λόγω της ευρείας χρήσης τους. Κατά αντιστοιχία αλλά σε μικρότερο βαθμό έχουν διερευνηθεί οι αδυναμίες σε συστήματα Γραφικών Κωδικών και έχουν επιδειχτεί και οι προσπάθειες να «σπάσουν» γραφικοί κωδικοί. Η έρευνες που έχουν πραγματοποιηθεί έχουν αναδείξει ότι παρά την διαφορετική φύση τους οι Γραφικοί Κωδικοί αντιμετωπίζουν αδυναμίες παρεμφερείς με αυτές των παραδοσιακών κωδικών ασφαλείας όπως είναι οι επιθέσεις λεξικού.

Προκειμένου να αξιολογήσουμε την ασφάλεια που παρέχουν οι διαφορετικές μέθοδοι κωδικών ασφαλείας θα τους εξετάσουμε σε σχέση με τις ακόλουθες δυνατές επιθέσεις:

- Επιθέσεις δια της Βίας (Brute force attacks)
- Επιθέσεις Λεξικού και Εικασίας (Dictionary & Guessing attacks)
- Λογισμικά Υποκλοπής και Καταγραφής Πληκτρολογίου (Spyware & keyloggers)
- Επιθέσεις Κοινωνικής Μηχανικής (Social engineering)
- Επιθέσεις Περιήγησης Ώμου (Shoulder surfing).

4.4.1. Επιθέσεις δια της Βίας

Οι Επιθέσεις δια της Βίας αναφέρονται στις επιθέσεις όπου δοκιμάζονται εξαντλητικά όλοι οι πιθανοί κωδικοί ασφαλείας που μπορεί να περιέχονται στο χώρο των κωδικών.

Οι Επιθέσεις δια της Βίας και οι Επιθέσεις Λεξικού σχετίζονται άμεσα με την εντροπία ενός κωδικού. Ο Claude Shannon [S48] εισήγαγε την έννοια της εντροπίας ως το μέτρο της αβεβαιότητας των επιλογών, η οποία συχνά αναφέρεται και ως Εντροπία Shannon. Η εντροπία ενός κωδικού ασφαλείας αποτελεί το μέτρο της αβεβαιότητας που έχει ένας επιτιθέμενος για τους χαρακτήρες που αποτελούν έναν κωδικό και είναι ένας τρόπος να μετρήσουμε πόσο δύσκολο είναι να τον μαντέψει ένας επιτιθέμενος.

Ας υποθέσουμε ότι έχουμε στη διάθεσή μας μια συσκευή η οποία παράγει χαρακτήρες, τον έναν μετά τον άλλο, επιλεγμένους από ένα αλφάβητο $A(\alpha_1, \alpha_2, \ldots, \alpha_N)$. Η συσκευή δεν ακολουθεί κάποιο μοτίβο και κάθε χαρακτήρας που παράγεται δεν εξαρτάται από τους προηγούμενους.

Ο *Χώρος Κωδικών (Keyspace)* ορίζεται ως το σύνολο των διαφορετικών τιμών που μπορεί να λάβει ένας κωδικός. Ένας κωδικός ασφαλείας αποτελούμενος από l χαρακτήρες, στους οποίους μπορεί να αποδοθούν N διαφορετικές τιμές, θα έχει *χώρο κωδικών* $k = N^l$. Εφόσον δεν υπάρχει μεροληψία τα γεγονότα είναι ισοπίθανα και άρα κάθε γράμμα της αλφαβήτου θα έχει πιθανότητα 1/N να παραχθεί. Η εντροπία των l χαρακτήρων θα ισούται με:

$$H \quad = \sum_{L=0}^{l} P_l log(P_l).$$

4.4.2. Επιθέσεις Λεξικού & Εικασίας

Εάν αντί για μια τυχαία σειρά χαρακτήρων ένας χρήστης επιλέγει ελεύθερα τον κωδικό ασφαλείας του είναι σαφές ότι θα επιλέξει μια σειρά χαρακτήρων που θα μπορεί να απομνημονεύσει παρά τυχαίους χαρακτήρες. Στο σενάριο όπου ένας επιτιθέμενος έχει περαιτέρω πληροφορίες για τον χρήστη π.χ. ημερομηνία γενεθλίων, όνομα, όνομα κατοικίδιων, αριθμό πινακίδων αυτοκινήτου, χόμπι κτλ. θα είναι σε θέση να κάνει μια στοχευμένη *επίθεση εικασίας*. Οι επιθέσεις εικασίας αποτελούν κατά κάποιο τρόπο ένα υποσύνολο τον επιθέσεων λεξικού, όπου το λεξικό αποτελείται από στοχευμένες και ενδεχομένως αποτελεσματικότερες επιλογές. Το να μπορέσει ο χρήστης να αμυνθεί αποτελεσματικά, και να μπορεί να το αποδείξει, απέναντι σε τέτοιου είδους επιθέσεις είναι εξαιρετικά δύσκολο αφού η τελική επιλογή ενός κωδικού είναι πάντοτε στην διακριτική ευχέρεια του χρήστη. Οι προσπάθειες να αναγκαστούν οι χρήστες μέσω κανόνων να επιλέγουν ισχυρούς κωδικούς έχει αμφίβολα αποτελέσματα. Ο κωδικός SuperM@n!1234 έχει μήκος 14 χαρακτήρων και αποτελείται από μικρά και κεφαλαία γράμματα, αριθμούς και ειδικούς χαρακτήρες, μια πολιτική ασφαλείας που θεωρείται ικανοποιητική εφόσον εφαρμόζεται από τους χρήστες, αλλά είναι τελικά ασφαλής ένας τέτοιος κωδικός ασφαλείας;

Οι *επιθέσεις λεξικού* βρίσκουν εφαρμογή και σε Γραφικούς Κωδικούς, δεδομένου ότι υπάρχει ένα υποσύνολο γραφικών κωδικών το οποίο είναι πιο πιθανό να επιλέξει ένας χρήστης. Γενικότερα, οι *επιθέσεις Λεξικού* βρίσκουν εφαρμογή σε οποιοδήποτε μοντέλο Κωδικών Ασφαλείας το οποίο είναι βασισμένο σε κάτι το οποίο ο χρήστης γνωρίζει. Το υποσύνολο που προαναφέραμε αποτελεί το Λεξικό.

4.4.3. Κοινωνική Μηχανική

Σε επιθέσεις κοινωνικής μηχανικής (Social engineering) στόχος είναι ο επιτιθέμενος να καταφέρει να εκμαιεύσει από τους χρήστες τα μυστικά διαπιστευτήριά τους με την θέλησή τους, για παράδειγμα, τηλεφωνώντας και προσποιούμενοι ότι είναι από το τμήμα υποστήριξης χρηστών ή στέλνοντας κάποιο ηλεκτρονικό μήνυμα ταχυδρομείου ψαρέματος. Τέτοιου είδους επιθέσεις μπορεί να απαιτούν να γίνει κάποια συλλογή πληροφοριών για τον χρήστη-στόχο αλλά συχνά είναι ένας πολύ πιο εύκολος τρόπος να παραβιαστεί ένα σύστημα από το να το προσπαθήσει κάποιος να το κάνει με τεχνικά μέσα [MS02].

Οι επιθέσεις κοινωνικής μηχανικής απαιτούν λίγο ή και καθόλου τεχνικά μέσα και όπως και στις επιθέσεις Λεξικού η άμυνα απέναντί τους επαφίεται στον τελικό χρήστη. Έτσι λοιπόν το να αμυνθείς σε επιθέσεις κοινωνικής μηχανικής με τεχνικά μέσα είναι εξαιρετικά δύσκολο, εάν όχι αδύνατο. Η εκπαίδευση των χρηστών και η ενημέρωσή τους

για τους κινδύνους και τις μεθόδους επίθεσεων κοινωνικής μηχανικής φαίρεται να είναι το πιο αποτελεσματικό μέτρο που μπορεί να ληφθεί.

4.4.4. Σερφάρισμα Ώμου

Η διαδικασία κατά την οποία ένας κακόβουλος χρήστης κάνει απ' ευθείας παρατήρηση π.χ. κοιτώντας πίσω από τον ώμο κάποιου, για να υποκλέψει τον κωδικό του αναφέρεται ως σερφάρισμα ώμου (Shoulder surfing). Το σερφάρισμα ώμου είναι ένας ιδιαίτερα αποτελεσματικός τρόπος να ανακτήσει κάποιος πληροφορίες σε ένα δημόσιο χώρο ή γενικότερα σε ένα συνωστισμένο χώρο. Είναι σχετικά εύκολο να παρατηρηθεί κάποιος όταν πληκτρολογεί τον κωδικό ασφαλείας του ή το PIN (Personal Identification Number) του σε ένα ATM (Automated Teller Machine). Η περιήγηση ώμου μπορεί να πραγματοποιηθεί και από απόσταση π.χ. με κυάλια ή με άλλο εξοπλισμό βελτίωσης του οπτικού πεδίου. Μια ιδιαίτερα αποτελεσματική παραλλαγή είναι η χρήση κάμερας (οι οποίες πλέον έχουν μικρό κόστος και μικρό μέγεθος) η οποία μπορεί εύκολα να αποκρυφθεί και να παρέχει στον επιτιθέμενο μια συνεχή πηγή πληροφόρησης.

5. NAVI

5.1. Περιγραφή NAVI

Το NAVI είναι ένα καινοτόμο σύστημα Γραφικών Κωδικών στο οποίο οι χρήστες προκειμένου να αυθεντικοποιηθούν επιτυχώς θα πρέπει να είναι σε θέση να αναπαραγάγουν σε έναν προκαθορισμένο χάρτη την διαδρομή που είχαν δημιουργήσει κατά το στάδιο της αρχικής εγγραφής τους.

Οι χρήστες κατά την έγγραφή τους επιλέγουν , κατ' ελάχιστο, το αρχικό και το τελικό σημείο της διαδρομής καθώς και έναν όνομα χρήστη. Οι χρήστες έχουν την δυνατότητα να ορίσουν και ενδιάμεσα σημεία από τα οποία θα πρέπει να περνά η διαδρομή. Περαιτέρω παραμετροποίηση της διαδρομής μπορεί να επιτευχθεί εάν οι χρήστες καθορίσουν παραμέτρους όπως εάν η διαδρομή θα υπολογιστεί για αυτοκίνητο, για ποδήλατο ή για πεζό, όπως και το εάν η διαδρομή θα αποφύγει διόδια ή κεντρικές λεωφόρους. Ορίζοντας όποιες παραμέτρους επιθυμεί ο χρήστης εντέλει δημιουργεί την διαδρομή του η οποία θα είναι και το μυστικό συνθηματικό του για να αυθεντικοποιείται, το οποίο θα ονομάσουμε «Κωδικός Διαδρομής» (Route Password).

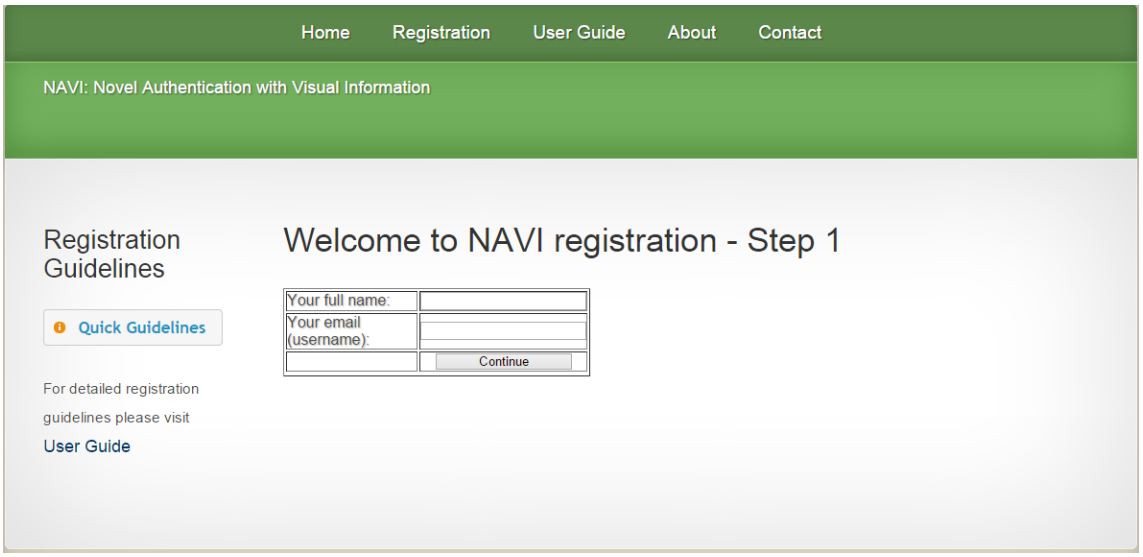
Το προτεινόμενο σύστημα αυθεντικοποίησης βασισμένο σε οπτική πληροφορία, Novel Authentication with Visual Information (NAVI), χρησιμοποιεί ως διαπιστευτήρια την διαδρομή που επιλέγει ένας χρήστης σε έναν προκαθορισμένο χάρτη. Προκειμένου να αξιολογήσουμε την ευκολία χρήσης, την δυνατότητα απομνημόνευσης του μυστικού, την προσφερόμενη ασφάλεια και την συνολική εμπειρία χρήσης του NAVI πραγματοποιήσαμε και μία έρευνα σε τελικούς χρήστες. Επιπλέον, ζητήθηκε από τους χρήστες που συμμετείχαν στην έρευνα να απαντήσουν σε ένα ερωτηματολόγιο αξιολόγησης προκειμένου να λάβουμε υπόψη μας την γνώμη τους σε μια σειρά από ζητήματα που αφορούν την υλοποίηση του NAVI. Σύμφωνα με τα αποτελέσματα που λάβαμε από την χρήση του NAVI και τις απαντήσεις του ερωτηματολόγιου καταλήξαμε στο συμπέρασμα ότι οι κωδικοί πρόσβασης που παράγονται από τη χρήση του NAVI είναι μεγάλης εντροπίας, οι χρήστες με την πάροδο του χρόνου εξοικειώνονται με το σύστημα και επιτυγχάνουν την αυθεντικοποίησή τους επιτυχώς με υψηλότερα ποσοστά επιτυχίας και ότι οι οπτικοί κωδικοί αυθεντικοποίησης είναι εύκολοι στην απομνημόνευσή τους.

Όταν ο χρήστης επιχειρεί να συνδεθεί θα πρέπει να μπορέσει να δημιουργήσει επιτυχώς την διαδρομή που έχει επιλέξει ως τον Κωδικό Διαδρομής του. Το αρχικό και τελικό σημείο της διαδρομής δεν είναι αναγκαίο να είναι απολύτως ίδια με αυτά που είχαν επιλεχθεί κατά την εγγραφή καθώς αφενός είναι δύσκολο να θυμάται ένας χρήστης με μεγάλη λεπτομέρεια τα σημεία αλλά ακόμα και να τα θυμάται ακριβώς είναι αμφίβολο εάν θα μπορέσει να επιλέξει ακριβώς το ίδιο σημεία. Το παραπάνω ζήτημα δεν είναι σημαντικό πρόβλημα για το NAVI καθώς το σημαντικό είναι ο χρήστης να θυμάται την διαδρομή και να μπορέσει να την αναπαραγάγει.

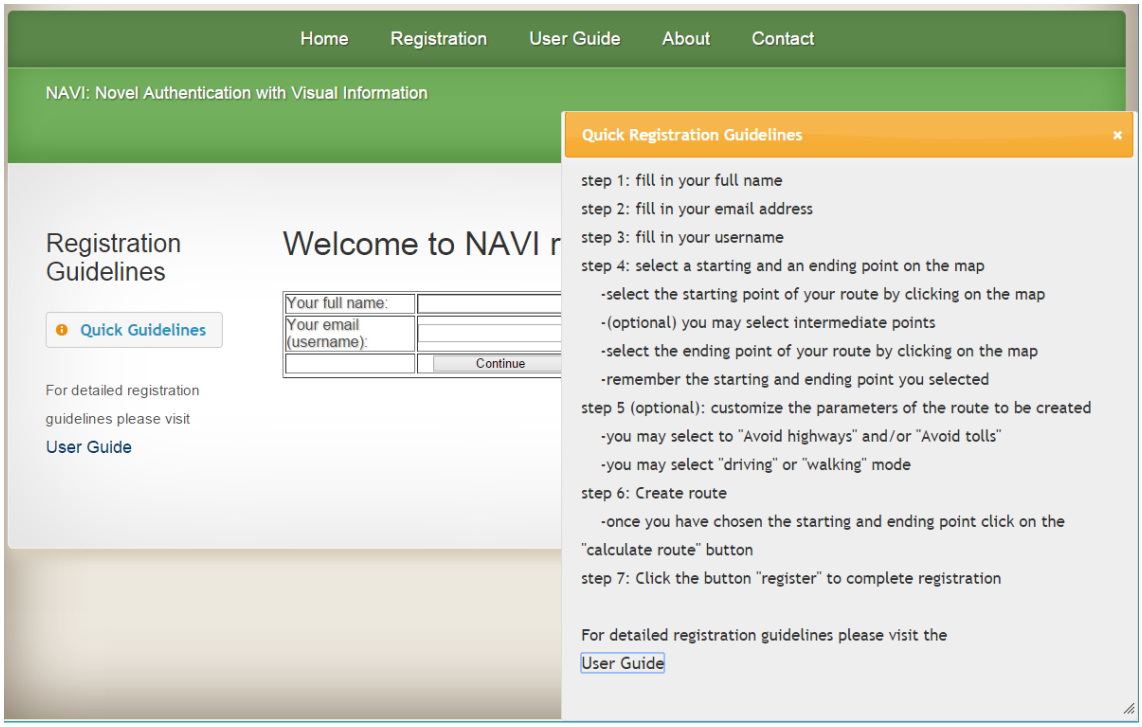
5.2. Υλοποίηση NAVI

Μια πρότυπη υλοποίηση του NAVI πραγματοποιήθηκε βασισμένη στην υπηρεσία χαρτών της Google (Google maps™). Σημειώνεται ότι επί της αρχής θα μπορούσαμε να χρησιμοποιήσουμε οποιαδήποτε υπηρεσία ή πλατφόρμα η οποία δίνει την δυνατότητα υπολογισμών διαδρομής όπως τα bing maps, ploigos κτλ. Προτιμήσαμε την χρήση των Google maps καθώς κρίναμε ότι θα βοηθήσει στην αποδοχή του συστήματος από τους τελικούς χρήστες λόγω της υψηλής διείσδυσης που έχει η υπηρεσία στο ευρύ κοινό καθώς και λόγω της δυνατότητας χρήστης του Google maps API για την υλοποίηση. Πέραν από την χρήση του Google Maps API χρησιμοποιήσαμε και τις τεχνολογίες php, javascript, JSON, apache web server και μια βάση δεδομένων mysql. Ο ιστότοπος είναι διαθέσιμος στο http://navi.cs.unipi.gr/ και αποτελεί και την πλατφόρμα την οποία δώσαμε και προς χρήση για την αξιολόγηση του NAVI.

Για να εγγραφεί ο χρήστης παρέχει το όνομά του και μια έγκυρη διεύθυνση ταχυδρομείου, η οποία θα αποτελεί και το όνομα χρήστη (username) για την εφαρμογή (Εικόνα 33). Επιπλέον, παρέχονται και σύντομες οδηγίες για τα βήματα που θα πρέπει να ακολουθηθούν για την εγγραφή (Εικόνα 34) ως αναδυόμενο παράθυρο εάν δεν επιθυμεί ο χρήστης να μεταβεί στις λεπτομερείς οδηγίες του ιστότοπου.



Εικόνα 33. NAVI – αρχική οθόνη εγγραφής χρήστη



Εικόνα 34. Οδηγίες εγγραφής χρήστη στο NAVI

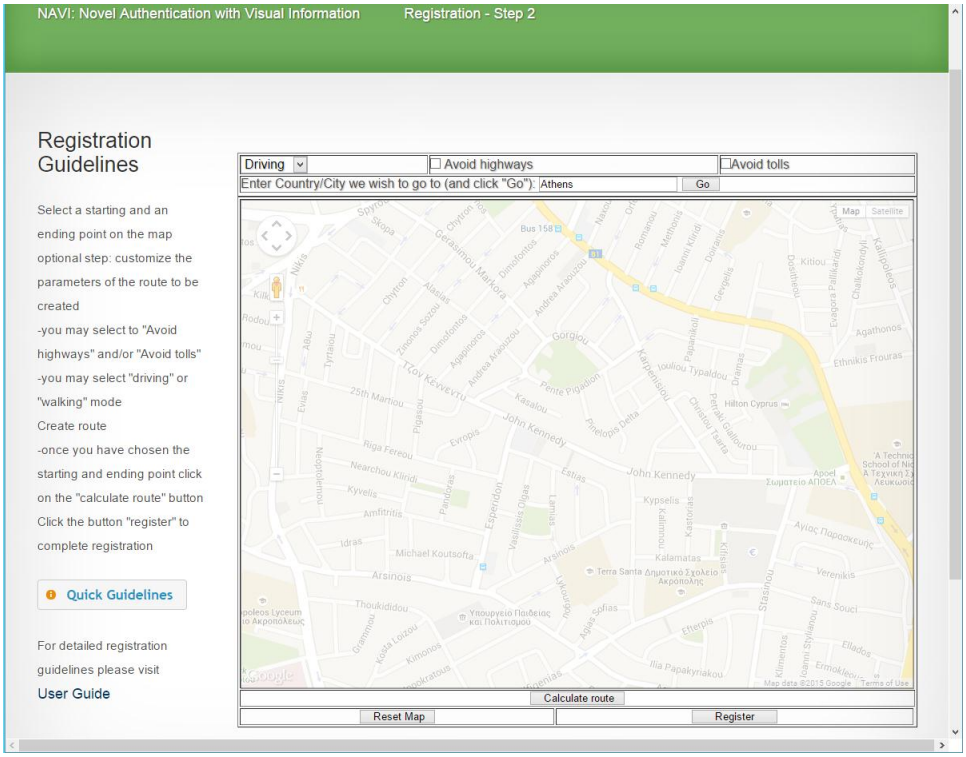
Στο δεύτερο στάδιο της εγγραφής ο χρήστης θα πρέπει να επιλέξει τον Κωδικό Διαδρομής του. Του δίνονται οι δυνατότητες να επιλέξει εάν η διαδρομή θα υπολογιστεί για πεζούς ή για αυτοκίνητο, εάν επιθυμεί η διαδρομή να αποφύγει κεντρικές οδούς και εάν επιθυμεί να αποφύγει οδούς με διόδια.

Επιπρόσθετα, για να διευκολυνθεί ο χρήστης στην επιλογή της περιοχής μπορεί να μεταβεί σε μια χώρα / πόλη / διεύθυνση που επιθυμεί πληκτρολογώντας στο πεδίο “Enter Country / City you want to go” τις λεπτομέρειες τις τοποθεσίας που τον ενδιαφέρει και κατόπιν κάνοντας κλικ στο κουμπί ”Go” για να μεταβεί στο χάρτη και να επιλέξει από εκεί την διαδρομή του.

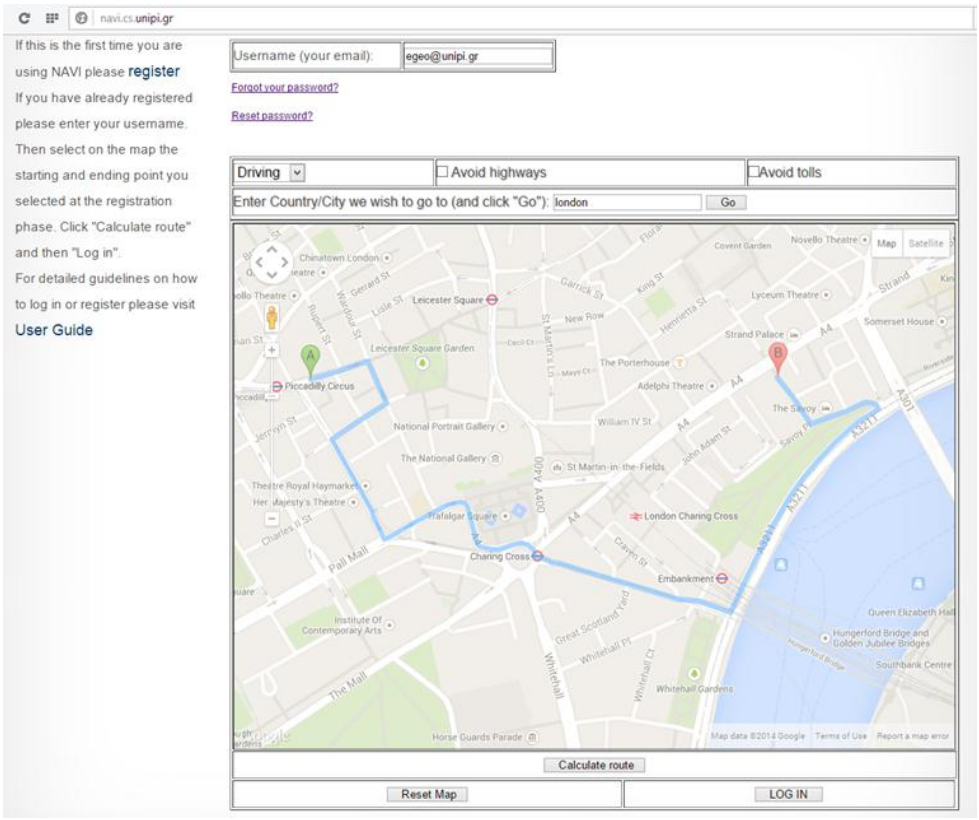
Επιλέγοντας το αρχικό και το τελικό σημείο της διαδρομής και, προαιρετικά, κάποιο ενδιάμεσο σημείο κάνοντας κλικ στο κουμπί «υπολογισμός διαδρομής» (“calculate route”) γίνεται ο υπολογισμός σύμφωνα με τα σημεία που έχουν επιλεγεί και τις παραμέτρους που έχει επιλέξει ο χρήστης.

Για διευκόλυνση του τελικού χρήστη εμφανίζεται και ένα κουμπί για να γίνει επανεκκίνηση του χάρτη (“reset”) εάν για οποιοδήποτε λόγο η διαδρομή που υπολογίστηκε δεν είναι η επιθυμητή.

Το τελικό βήμα είναι η επιλογή του πλήκτρου «εγγραφή» (“Register”) για να ολοκληρωθεί η εγγραφή του χρήστη. Τα παραπάνω φαίνονται στις Εικόνες 35 και 36.



Εικόνα 35. NAVI - εγγραφή χρήστη



Εικόνα 36. NAVI - εγγραφή χρήστη – υπολογισμός διαδρομής

Εφόσον έχει πραγματοποιηθεί επιτυχώς η εγγραφή, ο χρήστης για να συνδεθεί επιτυχώς θα πρέπει να δώσει το όνομα χρήστη (username) και να επιλέξει την διαδρομή που έχει επιλέξει ως Κωδικό Διαδρομής. Για να το επιτύχει αυτό θα πρέπει οι παράμετροι που θα επιλέξει να είναι ίδιοι καθώς και ίδια να είναι και τα σημεία πάνω στον χάρτη. Το περιβάλλον είναι παρόμοιο με αυτό της εγγραφής και υπάρχουν οι επιλογές παραμετροποίησης της διαδρομής (πεζός / αυτοκίνητο, αποφυγή διοδίων, αποφυγή κεντρικών οδών) καθώς και το πεδίο για εισαγωγή χώρας / πόλης για την μετάβαση του χάρτη. Όπως και κατά το στάδιο της εγγραφής, υπάρχουν διαθέσιμα τα κουμπιά “Calculate route” και “Reset map” αλλά και το κουμπί «Σύνδεση» (“login”).

Σε περίπτωση που ένας χρήστης δεν μπορεί να συνδεθεί επειδή δεν θυμάται τον Κωδικό Διαδρομής του δίνονται δύο επιλογές:

- Να ορίσει νέο κωδικό (σύνδεσμος “Reset password?”)
- Να του αποσταλεί υπενθύμιση (σύνδεσμος “Forgot your password”).

Εάν ο χρήστης επιθυμεί να ορίσει καινούριο κωδικό θα πρέπει να καταχωρίσει τη διεύθυνση ηλεκτρονικού ταχυδρομείου με την οποία έχει εγγραφεί και θα του αποσταλεί στη διεύθυνση αυτή ένας μοναδικός σύνδεσμος (ενεργός για 24 ώρες) στον οποίο θα παραπέμπεται σε περιβάλλον όπως αυτό της διαδικασίας εγγραφής για να ορίσει τον καινούριο του κωδικό.

Εάν ο χρήστης επιλέξει να του αποσταλεί κάποια υπενθύμιση, τότε και πάλι καταχωρεί την διεύθυνση του ηλεκτρονικού ταχυδρομείου με την οποία έχει εγγραφεί και κατόπιν του αποστέλλεται στη διεύθυνση αυτή το αρχικό και το τελικό σημείο που επέλεξε κατά την εγγραφή του (εάν είχε επιλεγεί και ενδιάμεσο σημείο αυτό δεν θα αποσταλεί, καθώς ούτε και οι υπόλοιπες παράμετροι λ.χ. αποφυγή διοδίων)

Στην πλευρά του διακομιστή χρησιμοποιήσαμε την γλώσσα διαδικτύου php και τη βάση δεδομένων mysql, ενώ στην πλευρά του πελάτη χρησιμοποιήσαμε το Google Maps JavaScript API v3 σε συνδυασμό με html, JavaScript, και CSSγια την διαμόρφωση της ιστοσελίδας.

Εφόσον η διαδρομή είναι κάτι το οποίο ο χρήστης γνωρίζει, ενδέχεται το NAVI να υπόκειται σε επιθέσεις παρόμοιες με αυτές που αντιμετωπίζουν και άλλα συστήματα αυθεντικοποίησης Βασισμένα στην Ανάκληση. Προτείνουμε μια σειρά από κριτήρια και παραμέτρους οι οποίες θα οδηγούν στην επιλογή ενός ασφαλούς Κωδικού Διαδρομής, σε αντιστοιχία με τους κανόνες δημιουργίας κωδικών ασφαλείας λ.χ. πολυπλοκότητα, ελάχιστο μήκος κτλ. Έτσι, λοιπόν, η διαδρομή θα πρέπει να μην είναι εύκολα προβλέψιμη, τόσο το σημείο εκκίνησης όσο και το τελικό σημείο καθώς και τα τυχόν ενδιάμεσα σημεία από τα οποία περνά η διαδρομή. Η διαδρομή θα πρέπει να έχει επαρκές μήκος ώστε να περιλαμβάνει μεγάλο αριθμό στροφών ώστε να παρέχει ικανοποιητική πολυπλοκότητα στον κωδικό που θα δημιουργηθεί. Επιπλέον, είναι σημαντικό ο χρήστης να μην

χρησιμοποιεί ως κωδικό την διαδρομή που του προτείνεται εξ ορισμού από το Google maps αλλά να εισάγει τουλάχιστον μια ακόμα παράμετρο που να την διαφοροποιεί. Πιο συγκεκριμένα, οι παρακάτω οδηγίες χρήσης θα πρέπει να δίνονται στους τελικούς χρήστες:

- Το αρχικό και το τελικό σημείο θα πρέπει να είναι απρόβλεπτα, λ.χ. δε θα πρέπει να συμπεριλαμβάνουν την διεύθυνση της οικίας ή της εργασίας, και άλλες προβλέψιμες τοποθεσίες όπως το γυμναστήριο του χρήστη ή την κοντινότερη σε αυτόν στάση του μετρό.
- Η διαδρομή που θα παραχθεί θα πρέπει να αποτελείται από τουλάχιστον τέσσερις στροφές (χωρίς να λαμβάνονται υπόψη τα σημεία εκκίνησης και τερματισμού της διαδρομής).
- Θα πρέπει να εισάγεται τουλάχιστον μια παρέκκλιση από την διαδρομή που υπολογίζεται εξ ορισμού.

Σε κάθε περίπτωση θα πρέπει να λάβουμε υπόψη ότι η πρώτη απαίτηση δεν μπορεί να επιβληθεί, καθώς εξαρτάται από τις επιλογές του χρήστη και δεν υπάρχει κάποιος τρόπος να επιβεβαιώσουμε κατά πόσο μια τοποθεσία που επιλέγεται σχετίζεται άμεσα με τον χρήστη λ.χ. ότι το σημείο εκκίνησης είναι η οικία του χρήστη, όπως κατ' αντιστοιχία δεν είναι εφικτό να απαγορευτεί σε ένα χρήστη να συμπεριλάβει στον κωδικό ασφαλείας του τον αριθμό πινακίδας του αυτοκινήτου του. Ωστόσο, οι υπόλοιπες απαιτήσεις μπορεί να επιβληθούν από το σύστημα αυθεντικοποίησης και εφόσον κρίνεται απαραίτητο να παραμετροποιηθούν από τον διαχειριστή του συστήματος ανάλογα με την πολιτική που θέλει να ακολουθήσει π.χ. οι στροφές να είναι τουλάχιστον έξι για ακόμα μεγαλύτερη ασφάλεια.

5.3. Αξιολόγηση NAVI

5.3.1. Ερωτηματολόγιο

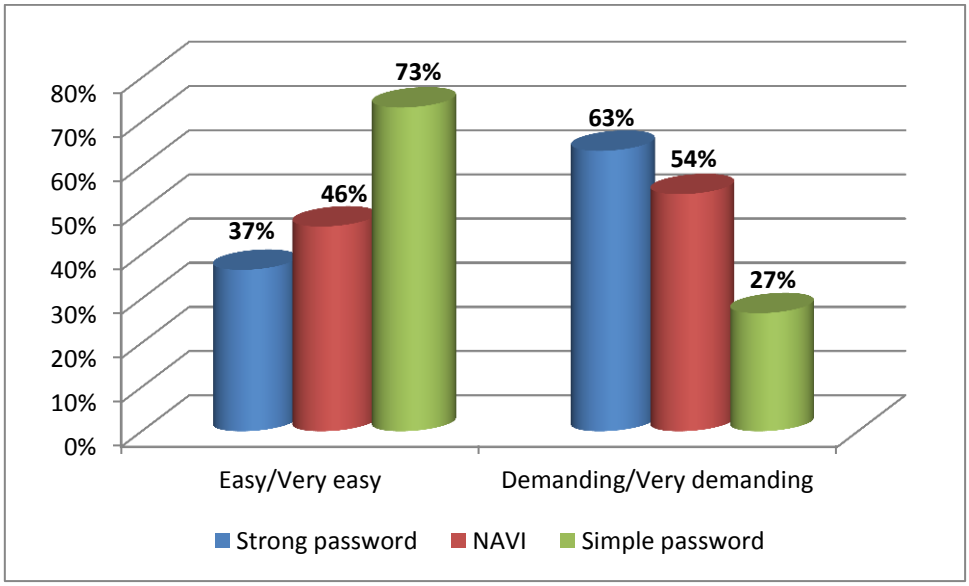
Προκειμένου να αξιολογήσουμε το NAVI όσον αφορά την χρηστικότητα και έτσι ώστε να συλλέξουμε πληροφορίες σχετικά με την εμπειρία των χρηστών, κατόπιν επιτυχούς αυθεντικοποίησης ζητήσαμε από τους χρήστες να συμπληρώσουν ένα ερωτηματολόγιο (βλέπε Παράρτημα Β - Ερωτηματολόγιο Αξιολόγησης NAVI).

Η βασική μας επιδίωξη ήταν να συλλέξουμε πληροφορίες για τις ακόλουθες περιοχές:

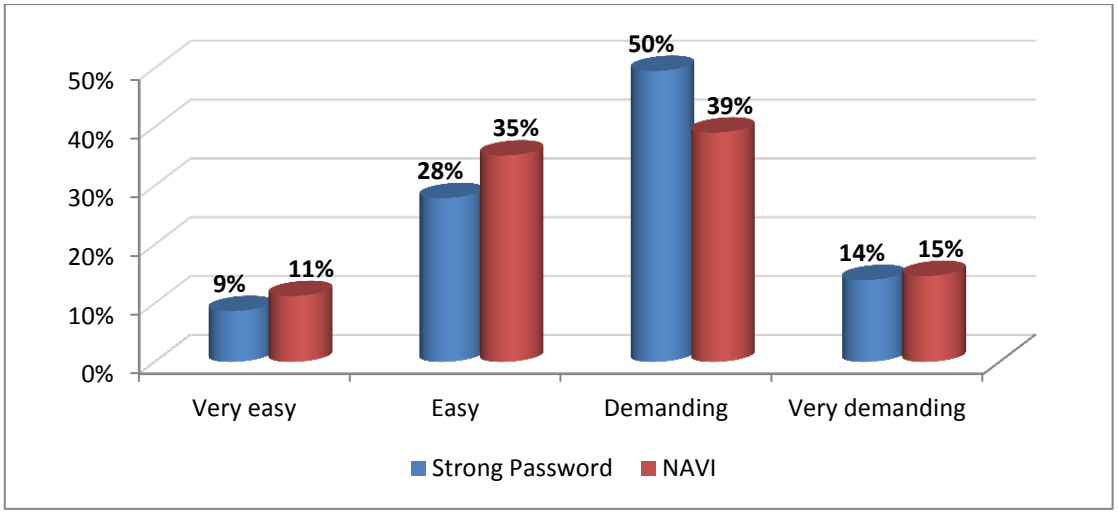
- Αξιολόγηση ευκολίας χρήσης
- Σύγκριση NAVI και Κωδικών Ασφαλείας Κειμένου
- Αξιολόγηση της διαδικασίας εγγραφής και σύνδεσης
- Εκτίμηση για το πόσο ισχυροί Κωδικοί Διαδρομής επιλέχθηκαν
- Αξιολόγηση της εξοικείωσης και μάθησης του συστήματος αυθεντικοποίησης
- Αξιολόγηση της αξιοπιστίας και της συνολικής αποδοχής για το NAVI.

Η απάντηση του ερωτηματολογίου ήταν προαιρετική, και, επίσης, δεν ήταν υποχρεωτικό να απαντήσει κάποιος σε όλες τις ερωτήσεις. Οι χρήστες είχαν τη δυνατότητα να απαντήσουν το ερωτηματολόγιο κάθε φορά που συνδέονταν επιτυχώς. Την παραπάνω δυνατότητα την επιτρέψαμε καθώς θεωρούμε σημαντικό να μπορέσουμε να παρατηρήσουμε και να αξιολογήσουμε τις απαντήσεις των χρηστών στην πάροδο του χρόνου και καθώς αποκτούν μεγαλύτερη εξοικείωση με το NAVI. Στο Παράρτημα Β - Ερωτηματολόγιο Αξιολόγησης NAVI καταγράφονται οι απαντήσεις που λάβαμε σε όλες τις ερωτήσεις με μορφή γραφημάτων.
Δεδομένου ότι η χρήση του NAVI απαιτεί από τους χρήστες να επιδείξουν μια κάποια εξοικείωση με πληροφοριακά συστήματα συλλέξαμε πληροφορίες σχετικά με την εμπειρία των χρηστών σε σχέση με τη χρήση υπολογιστών γενικότερα αλλά και με τη χρήση του Google Maps ειδικότερα. Το 41% των χρηστών δήλωσε ότι είναι άπειροι ή σχετικά άπειροι ενώ το 59% ότι είναι έμπειροι ή πολύ έμπειροι.

Ζητήθηκε από τους συμμετέχοντες στο πείραμα να αξιολογήσουν τη δυσκολία του να απομνημονεύσουν ένα απλό κωδικό ασφαλείας, έναν σύνθετο κωδικό ασφαλείας (δηλαδή έναν κωδικό μεγάλου μήκους που περιέχει τυχαίους χαρακτήρες, γράμματα αριθμούς και ειδικούς χαρακτήρες) και, επιπλέον, να αξιολογήσουν τη δυσκολία να απομνημονεύσουν έναν Κωδικό Διαδρομής. Τα αποτελέσματα παρουσιάζονται στις Εικόνες 37 και 38.



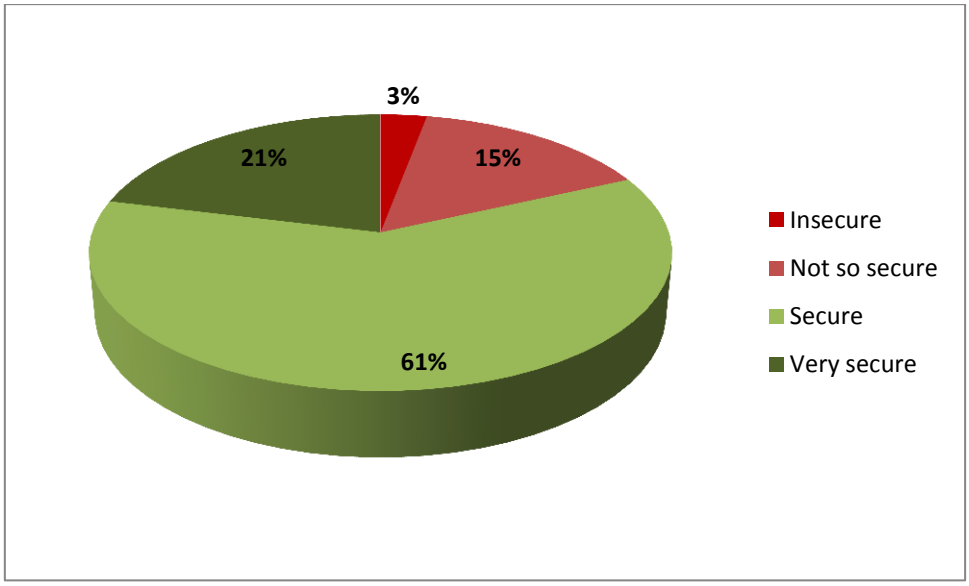
Εικόνα 37. Αξιολόγηση δυσκολίας απομνημόνευσης διαπιστευτηρίων σε διαφορετικά μοντέλα αυθεντικοποίησης



Εικόνα 38. Σύγκριση αξιολόγησης χρηστών για την απομνημόνευση διαπιστευτηρίων για το NAVIκαι ισχυρού κωδικού ασφαλείας

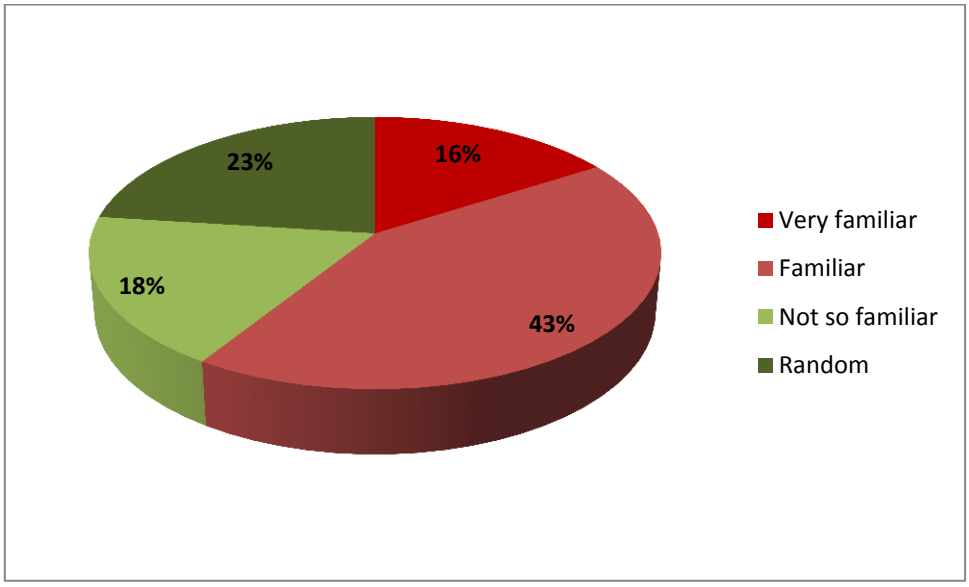
Σύμφωνα με τα αποτελέσματα που λάβαμε το επίπεδο δυσκολίας απομνημόνευσης ενός Κωδικού Διαδρομής είναι συγκρίσιμο με το επίπεδο δυσκολίας απομνημόνευσης ενός ισχυρού κωδικού ασφαλείας ωστόσο είναι σαφές ότι το να θυμηθεί κάποιος μια διαδρομή της επιλογής του θεωρήθηκε πιο εύκολο από το να θυμάται έναν πολύπλοκο κωδικό.

Είναι σημαντικό, ειδικά για ένα καινούριο σύστημα αυθεντικοποίησης, προκειμένου να αποκτήσει την αποδοχή των χρηστών οι τελικοί χρήστες να το εμπιστεύονται υπό την έννοια ότι τους παρέχει υψηλό βαθμό ασφάλειας. Στους τελικούς χρήστες δεν έγινε κάποια ειδική εκπαίδευση ή επεξήγηση για τον μηχανισμό που υλοποιείται για τον υπολογισμό και τη χρήση του Κωδικού Διαδρομής ούτε ανάλυση της εντροπίας ή άλλων χαρακτηριστικών του NAVI. Ωστόσο τους ζητήθηκε να δώσουν την εκτίμησή του πόσο ασφαλής τους φαίνεται η χρήση Κωδικών Διαδρομής ως μέσο αυθεντικοποίησης. Η συντριπτική πλειοψηφία (82%) αποκρίθηκε ότι εκτιμούν ότι το επίπεδο ασφάλειας που παρέχει το NAVI είναι υψηλό ή πολύ υψηλό, βλέπε Εικόνα 39 για περαιτέρω λεπτομέρειες. Τονίζουμε ότι η απάντηση αυτή έχει να κάνει με την αίσθηση που δημιουργήθηκε στους τελικούς χρήστες και δεν σχετίζεται με την ασφάλεια των Κωδικών Διαδρομής και την εντροπία που προσφέρουν, τα ζητήματα αυτά θα τα αναλύσουμε εκτενώς σε παρακάτω ενότητα.



Εικόνα 39. Εκτίμηση τελικών χρηστών για το παρεχόμενο επίπεδο ασφαλείας από το NAVI

Επιπλέον, οι χρήστες ρωτήθηκαν για τις επιλογές του σημείου εκκίνησης και τερματισμού της διαδρομής και κατά πόσο αποτελούν οικεία σημεία. Το 41% αποκρίθηκε ότι επέλεξε σημεία τα οποία δεν είναι οικεία, στην Εικόνα 40 φαίνονται αναλυτικότερα τα αποτελέσματα των απαντήσεων.

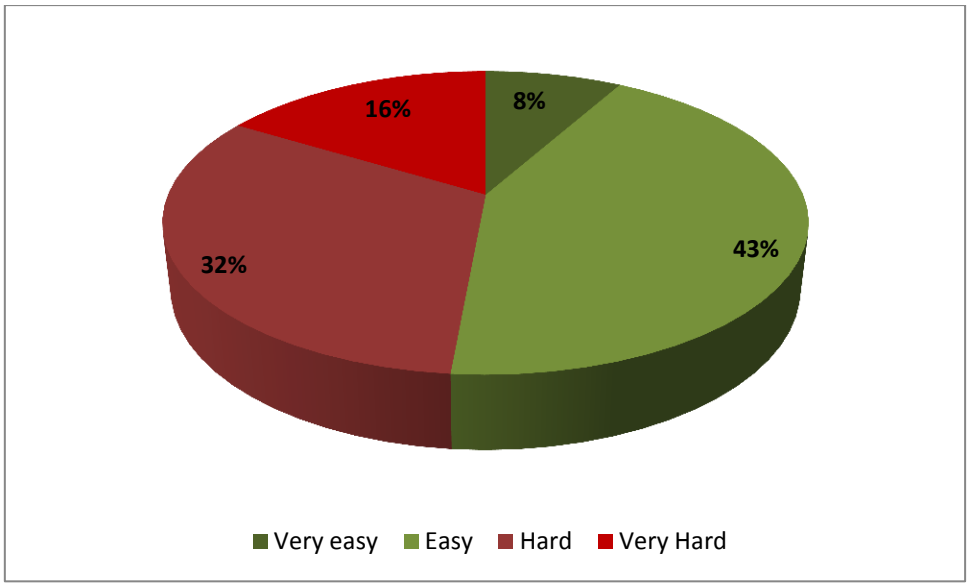


Εικόνα 40. Επιλογή αρχικού και τελικού σημείου διαδρομής

Παρόλο που οι απαντήσεις σε σχέση με την εκτιμώμενη ασφάλεια του NAVI και την ευκολία απομνημόνευσης του Κωδικού Διαδρομές ήταν ενθαρρυντικές, το 30% των συμμετεχόντων δήλωσαν ότι μάλλον δεν θα επέλεγαν να χρησιμοποιήσουν το NAVI για αυθεντικοποίηση σε υπηρεσίες που χρησιμοποιούν τακτικά όπως το ηλεκτρονικό ταχυδρομείο. Ένα 10% ισχυρίστηκε ότι σίγουρα θα επέλεγε να χρησιμοποιήσει το NAVI και το υπόλοιπο 60% ότι θα χρησιμοποιούσαν ή ίσως να χρησιμοποιούσαν το NAVI.

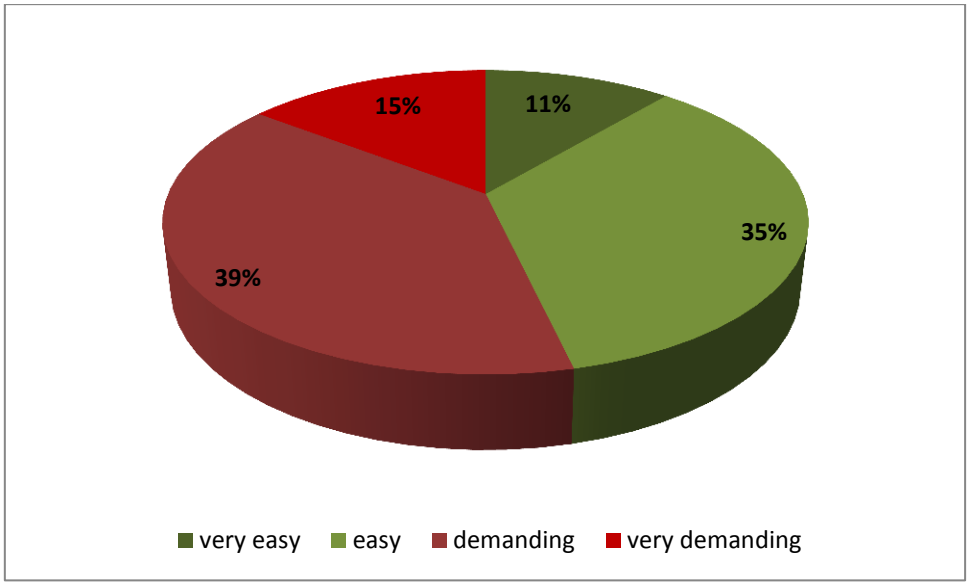
Ο λόγος για τον οποίο ένα μερίδιο των χρηστών φαίνεται να είναι επιφυλακτικοί στην χρήση του NAVI πιθανότατα μας αποκαλύπτεται από τις απαντήσεις που λάβαμε στο ερώτημα «Πόσο δύσκολο σας ήταν να εγγραφείτε και να συνδεθείτε χρησιμοποιώντας το NAVI;» όπου το 48% των χρηστών θεωρεί την διαδικασία εγγραφής και σύνδεσης δύσκολη ή πολύ δύσκολη (βλέπε Εικόνες 41 και 42).

Στην παραπάνω ερώτηση εάν δούμε τις απαντήσεις από το υποσύνολο των χρηστών οι οποίοι δηλώνουν ότι είναι έμπειροι χρήστες πληροφοριακών συστημάτων τότε το ποσοστό αυτών που δήλωσαν ότι δεν θα χρησιμοποιούσαν το NAVI περιορίζεται στο 18%.



Εικόνα 41. Αξιολόγηση επιπέδου δυσκολίας για την σύνδεση στο NAVI

Από τα παραπάνω αποτελέσματα θεωρούμε ότι θα πρέπει να διερευνηθεί περαιτέρω το ενδεχόμενο το NAVI να είναι καταλληλότερο προς χρήση σε περιβάλλοντα ή υπηρεσίες που είτε παρουσιάζουν υψηλές απαιτήσεις ασφαλείας ή σε περιπτώσεις που δεν χρειάζεται να γίνονται συχνά συνδέσεις (login) των χρηστων (λ.χ. υπάρχει λύση SingleSignOn) όπου ο επιπλέον φόρτος που εισάγεται με τη χρήση του NAVI να αναπληρώνεται από την ανάγκη για ισχυρή αυθεντικοποίηση.



Εικόνα 42. Αξιολόγηση επιπέδου προσπάθειας για την σύνδεση στο NAVI

5.3.2. Ανάλυση Χρήσης

Το NAVI ως ένα νέο μοντέλο αυθεντικοποίησης είναι κατά βάση άγνωστο στους χρήστες. Συνεπώς θεωρήσαμε σημαντικό να αξιολογήσουμε κατά πόσο οι χρήστες με την πάροδο του χρόνου και με επανάληψη της χρήσης του αποκτούν μεγαλύτερη εξοικείωση και άνεση στη χρήση του.

Στο πείραμα συμμετείχαν πενήντα άτομα. Οι χρήστες (ένα μέρος των αρχικών χρηστών) χρησιμοποίησαν το NAVI σε εβδομαδιαία βάση για συνολική διάρκεια 5 εβδομάδων. Την πρώτη εβδομάδα πραγματοποιήθηκε η εγγραφή και στις υπόλοιπες τέσσερεις πραγματοποιήσαμε την μελέτη μας σε σχέση με τα ποσοστά επιτυχίας για τις συνδέσεις χρηστών.

Ο στόχος της περίπτωσης μελέτης είχε δύο βασικούς άξονες:

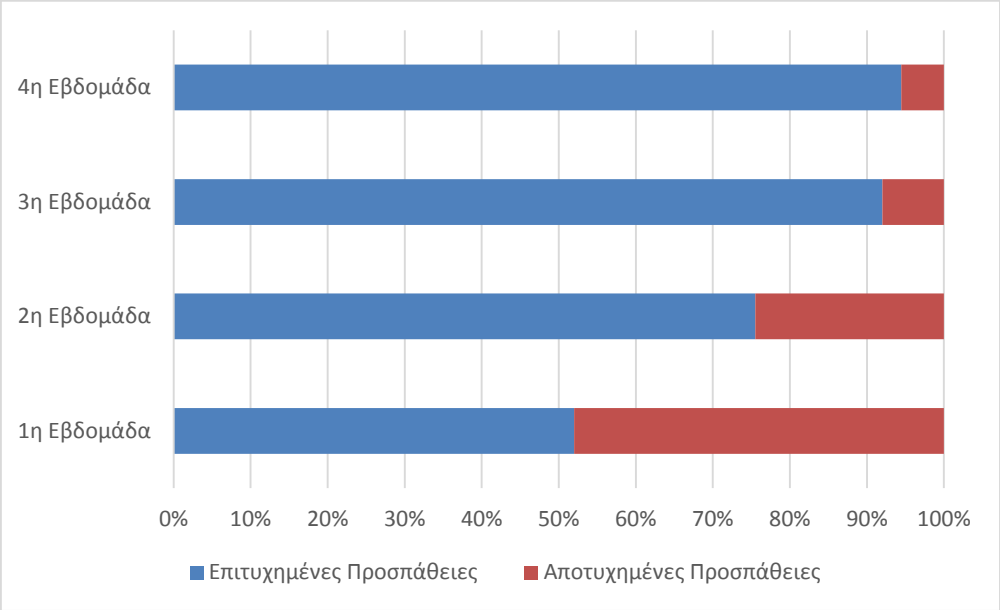
- Να αξιολογήσουμε κατά πόσο η εξοικείωση με το NAVI οδηγεί σε υψηλότερα ποσοστά επιτυχίας σύνδεσης, και
- Να αξιολογήσουμε την δυνατότητα απομνημόνευσης του Κωδικού διαδρομής από τους χρήστες σε βάθος χρόνου.

Στην πρώτη περίπτωση, λαμβάνουμε υπόψη μας το σύνολο των επιτυχημένων και των αποτυχημένων προσπαθειών σύνδεσης. Στην δεύτερη περίπτωση, θα πραγματοποιήσουμε σύγκριση του ποσοστού επιτυχημένων συνδέσεων στην πάροδο των τεσσάρων εβδομάδων.

Τα αποτελέσματα ήταν ιδιαίτερα ενθαρρυντικά, και παρουσιάζονται στον Πίνακα 6 και με γραφική απεικόνιση στην Εικόνα 43:

Πίνακας 6: Αποτυχημένες και επιτυχημένες προσπάθειες σύνδεσης στο NAVI

	Επιτυχημένες Προσπάθειες	Αποτυχημένες Προσπάθειες	Ποσοστό Επιτυχίας
1η Εβδομάδα	26	24	52%
2η Εβδομάδα	37	12	76%
3η Εβδομάδα	23	2	92%
4η Εβδομάδα	17	1	94%



Εικόνα 43. Αποτυχημένες και επιτυχημένες προσπάθειες σύνδεσης στο NAVI

Πιο λεπτομερή αποτελέσματα παρουσιάζονται στον Πίνακα 7. Όταν ένας χρήστης απέτυχε να συνδεθεί με την πρώτη προσπάθεια και κατόπιν δεν ξαναπροσπάθησε το συμβολίζουμε ως «1 αποτυχία», όταν ένας χρήστης απέτυχε να συνδεθεί σε δυο διαδοχικές προσπάθειες και κατόπιν δεν ξαναπροσπάθησε το συμβολίζουμε με «2 αποτυχίες» και ούτω καθεξής για τα «3 αποτυχίες». «4 αποτυχίες », «5 αποτυχίες » και «6 αποτυχίες». Όταν ένας χρήστης συνδέθηκε με την πρώτη του προσπάθεια το συμβολίζουμε με «1 προσπάθεια», όταν συνδέθηκε με την δεύτερη προσπάθεια με «2 προσπάθειες» και ούτω καθεξής για τα «3 προσπάθειες», «4 προσπάθειες», «5

προσπάθειες» και «6 προσπάθειες». Οι χρήστες που πραγματοποίησαν επαναφορά του κωδικού τους δεν ελήφθησαν υπόψη στα αποτελέσματα μέχρι και την επόμενη εβδομάδα.

Πίνακας 7: Αποτυχημένες και επιτυχημένες προσπάθειες σύνδεσης στο NAVI σε βάθος χρόνου

	1 αποτυχία	2 αποτυχίες	3 αποτυχίες	4 αποτυχίες	5 αποτυχίες	6 αποτυχίες	1προσπάθεια	2 προσπάθειες	3 προσπάθειες	4 προσπάθειες	5 προσπάθειες	6 προσπάθειες
1η Εβδομάδα	9	2	4	1	0	8	15	6	2	1	0	2
2η Εβδομάδα	2	4	3	0	0	3	30	5	1	1	0	0
3η Εβδομάδα	1	0	0	0	1	0	19	2	1	0	1	0
4η Εβδομάδα	0	1	0	0	0	0	8	0	0	0	0	0
Συνολικά	12	7	7	1	1	11	72	13	4	2	1	2

Μια ενδιαφέρουσα παρατήρηση είναι ότι οι χρήστες που συνδέθηκαν επιτυχώς στην συντριπτική τους πλειοψηφία το πέτυχαν στην πρώτη προσπάθεια και αρκετοί στην δεύτερη προσπάθεια. Μετά από δύο αποτυχημένες προσπάθειες ελάχιστοι χρήστες κατάφεραν τελικά να συνδεθούν επιτυχώς. Στην Εικόνα 44, παρουσιάζονται οι προσπάθειες που έκαναν οι χρήστες για να συνδεθούν επιτυχώς στο σύνολο των τεσσάρων εβδομάδων.

Εικόνα 44. Επιτυχείς προσπάθειες σύνδεσης

Επιπλέον παρατηρούμε ότι όσο περνούν οι εβδομάδες το ποσοστό των χρηστών που συνδέθηκαν επιτυχώς αυξάνεται. Προκειμένου να επικυρώσουμε τα συμπεράσματα που αναφέραμε πραγματοποιήσαμε δοκιμή Ανάλυσης Διακύμανσης (ANOVA – Analysis of Variance) ώστε να εξετάσουμε εάν η διακύμανση που παρατηρούμε στην αύξηση του ποσοστού των επιτυχημένων συνδέσεων μπορεί να εμπίπτει στα όρια του στατιστικού σφάλματος και της διακύμανσης. Η δοκιμή που πραγματοποιήσαμε είναι μια μονόδρομη Ανάλυση Διακύμανσης (one-way ANOVA) με διάστημα εμπιστοσύνης 95%. Η μηδενική υπόθεση (null hypothesis) δηλώνει ότι δεν υπάρχουν διαφορές στους μέσους των δειγμάτων ή με άλλα λόγια ότι δεν υπάρχει διαφορά στα ποσοστά επιτυχία στις διαφορετικές εβδομάδες που πραγματοποιήσαμε το πείραμα. Τα αποτελέσματα της δοκιμής παρουσιάζονται στους Πίνακες 8 και 9.

Πίνακας 8: Αποτελέσματα μονόδρομης Ανάλυσης Διακύμανσης – μέρος πρώτο

Ομάδες (Groups)	**Μέτρηση (Count)**	**Άθροισμα (Sum)**	**Μέσος (Average)**	**Διακύμανση (Variance)**
1η Εβδομάδα	50	26	0,520	0,2547
2η Εβδομάδα	49	37	0,755	0,1888
3η Εβδομάδα	25	23	0,920	0,0767
4η Εβδομάδα	18	17	0,944	0,0556

Πίνακας 9: Αποτελέσματα μονόδρομης Ανάλυσης Διακύμανσης – μέρος δεύτερο

Πηγή της διακύμανσης (Source of Variation)	*Άθροισμα Τετραγώνων (Sums of Squares)*	*Βαθμοί Ελευθερίας (Degrees of freedom)*	*Μέσο Τετράγωνο (Mean Square)*	*F*	*Τιμή P (P-value)*	*Κριτήριο F (F criteria)*
Μεταξύ Εβδομάδων	3,963	3	1,321	7,494	0,00011	2,670
Εντός εβδομάδων	24,326	138	0,176			
Σύνολο	28,289	141				

Το P-value αποτελεί το μέτρο του πόσο ισχυρές είναι οι ενδείξεις έναντι της μηδενικής υπόθεσης. Τα αποτελέσματα που λάβαμε υποδεικνύουν ότι μπορούμε να απορρίψουμε την μηδενική υπόθεση καθώς P<0.05. Συνεπώς, συμπεραίνουμε ότι η βελτίωση που παρατηρήθηκε στο ποσοστό επιτυχών συνδέσεων οφείλεται στο ότι οι χρήστες καθώς απόκτησαν εξοικείωση με το NAVI τους ήταν πιο εύκολο να συνδεθούν.

Ωστόσο η δοκιμή ANOVA έχει τον εγγενή περιορισμό ότι δεν μας δίνει στοιχεία για το ποιοι μέσοι είναι που διαφοροποιούνται από το σύνολο των δεδομένων που έχουμε για κάθε μια από τις τέσσερις εβδομάδες. Για να έχουμε πιο ξεκάθαρη εικόνα για την εξέλιξη της εξοικείωσης των χρηστών, πραγματοποιήσαμε δοκιμές t-test στα ακόλουθα ζεύγη: Εβδομάδα-1 & Εβδομάδα -2, Εβδομάδα -2 & Εβδομάδα -3, Εβδομάδα -3 & Εβδομάδα -4, Εβδομάδα -2 & Εβδομάδα -4 και Εβδομάδα -1 & Εβδομάδα -4. Στον Πίνακα 10 φαίνονται τα αποτελέσματα των t-tests.

Πίνακας 10: Αποτελέσματα t-tests

	*Τιμή P (***P-value**)	**Μηδενική Υπόθεση**
Εβδομάδα - 1 & Εβδομάδα -2	0,0147	Απόρριψη
Εβδομάδα -2 & Εβδομάδα -3	0,0515	Αποδοχή
Εβδομάδα -3 & Εβδομάδα -4	0,7569	Αποδοχή
Εβδομάδα -2 & Εβδομάδα -4	0,0270	Απόρριψη
Εβδομάδα -1 &Εβδομάδα -4	0,0000157	Απόρριψη

Παρατηρούμε ότι η μηδενική υπόθεση είναι αποδεκτή για τα ζεύγη «Εβδομάδα - 2 & Εβδομάδα - 3» και «Εβδομάδα -3 & Εβδομάδα - 4». Συνεπώς, η βελτίωση που παρατηρήθηκε από την δεύτερη προς την τρίτη και από την τρίτη προς την τέταρτη εβδομάδα δεν μπορεί με ασφάλεια να αποδοθεί στο ότι οι χρήστες εξοικειώθηκαν με το NAVI. Ωστόσο, είναι σαφές ότι ήδη από την δεύτερη χρήση του NAVI (Εβδομάδα - 2) υπάρχει εξοικείωση των χρηστών, οι οποίοι επιτυγχάνουν να αυθεντικοποιηθούν με μεγαλύτερη ευκολία. Τέλος, η βελτίωση των ποσοστών σύνδεσης που παρατηρήθηκαν την Εβδομάδα -3 και την Εβδομάδα – 4 σε σχέση με την Εβδομάδα – 1 αναδεικνύουν ότι με την συνεχή χρήση του NAVI επέρχεται εξοικείωση και μεγαλύτερη ευκολία των χρηστών στο να συνδεθούν επιτυχώς.

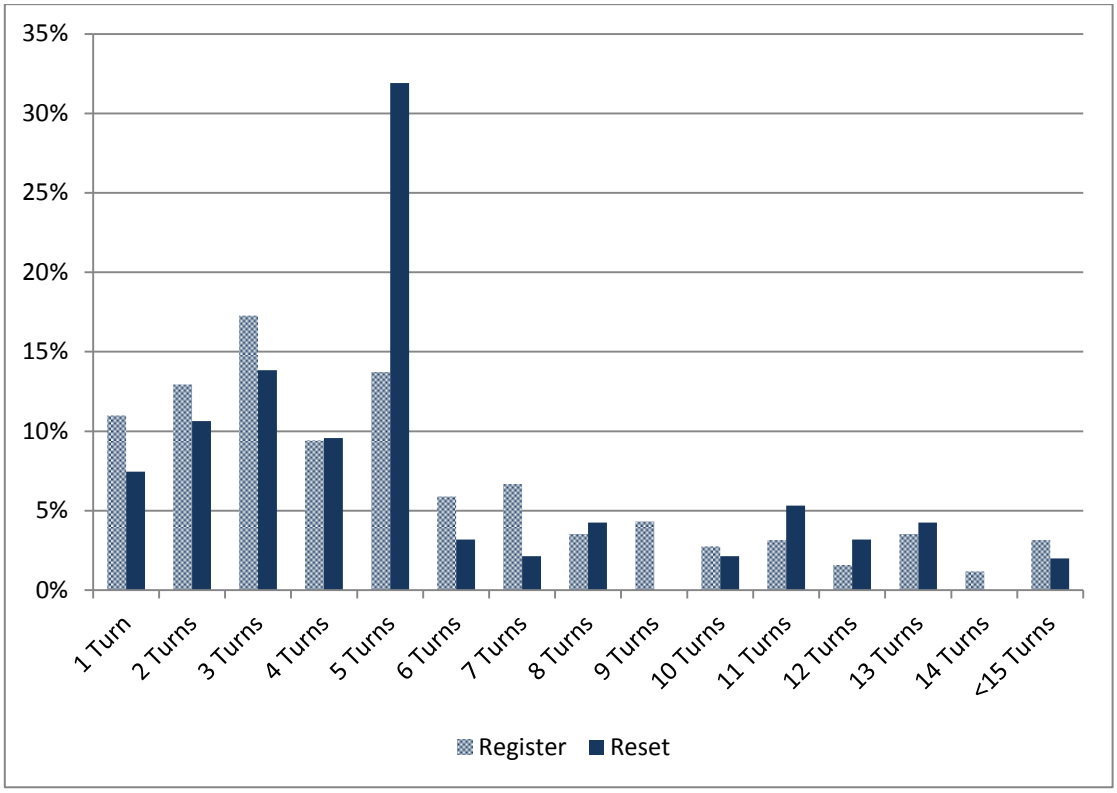
Ανάλυση της επιλογής διαδρομών από τους χρήστες

Προκειμένου να μπορούμε να μελετήσουμε και να αξιολογήσουμε την συμπεριφορά των χρηστών όσον αφορά τις επιλογές που θα έκαναν. η υλοποίηση του NAVI που διαθέσαμε στους χρήστες δεν επέβαλε περιορισμούς στους χρήστες προκειμένου να αναγκαστούν να επιλέξουν μεγάλες διαδρομές κτλ.

Κατά την αρχική εγγραφή τους, οι χρήστες επέλεξαν Κωδικούς Διαδρομής που αποτελούνται από τρεις ή και περισσότερες στροφές και περίπου οι μισοί χρήστες επέλεξαν διαδρομές με πέντε ή παραπάνω στροφές. Ένα ακόμα αξιοσημείωτο αποτέλεσμα είναι ότι όταν κάποιος χρήστης ξέχναγε τον Κωδικό και δημιουργούσε έναν καινούριο δεν επέλεγε να δημιουργήσει μια «εύκολη» διαδρομή με λίγες στροφές. Μόλις 18% από αυτούς που άλλαξαν κωδικό επέλεξαν διαδρομή με λιγότερες από τρεις στροφές.

Συνολικά, οι επιλογές των χρηστών ήταν ιδιαίτερα ικανοποιητικές καθώς ήταν κατά βάση μεγάλου μήκους διαδρομές.

Ένας Κωδικός Διαδρομής παρέχει περίπου ισοδύναμη εντροπία με έναν «δυνατό» Κωδικό Ασφαλείας Κειμένου οχτώ χαρακτήρων. Συνολικά, μόλις το 22% των χρηστών επέλεξαν διαδρομές με μία ή δύο στροφές (λαμβάνοντας υπόψη την αρχική εγγραφή αλλά και τις επαναφορές κωδικού διαδρομής. Στην Εικόνα 45, φαίνεται η κατανομή των επιλογών κωδικών διαδρομής σε σχέση με τον αριθμό των στροφών που περιέχουν.



Εικόνα 45. Κατανομή των επιλογών κωδικών διαδρομής σε σχέση με τον αριθμό των στροφών που περιέχουν

5.4. Συγκριτική Ανάλυση Ασφάλειας

Προκειμένου να αξιολογήσουμε την ασφάλεια που παρέχουν οι διαφορετικές μέθοδοι κωδικών ασφαλείας για αυθεντικοποίηση, και, πιο συγκεκριμένα, οι ακόλουθοι μηχανισμοί:

- Κωδικοί Ασφαλείας Κειμένου
- Κωδικοί Γραφικών - Βασισμένοι στην Αναγνώριση
- Κωδικοί Γραφικών - Βασισμένοι στην Ανάκληση
- NAVI.

θα πραγματοποιήσουμε μια σύγκριση της ανθεκτικότητάς τους σε σχέση με τις δυνατές επιθέσεις που παρουσιάσαμε σε προηγούμενη ενότητα:

- Επιθέσεις δια της Βίας
- Επιθέσεις Λεξικού & Εικασίας
- Λογισμικά Υποκλοπής & Καταγραφής Πληκτρολογίου
- Επιθέσεις Κοινωνικής Μηχανικής
- Επιθέσεις Περιήγησης Ώμου.

5.4.1. Επιθέσεις δια της Βίας

Κωδικοί Ασφαλείας Κειμένου

Ας υποθέσουμε ότι έχουμε έναν κωδικό ασφαλείας ο οποίος συμμορφώνεται και με τους ακόλουθους κανόνες: έχει μήκος οχτώ χαρακτήρων, αποτελείται από τουλάχιστον μικρά γράμματα, κεφαλαία γράμματα, αριθμούς και ειδικούς χαρακτήρες. Στην περίπτωση αυτή, η αλφάβητος αποτελείται από 94 γράμματα (πενήντα δύο γράμματα, δέκα αριθμούς και τριάντα δύο ειδικούς χαρακτήρες). Ο κωδικός μήκους L επιλεγμένος από το σύνολο των 94 γραμμάτων λαμβάνει 94xL πιθανές τιμές και έχει 6,55xL bit εντροπίας. Ο παραπάνω υπολογισμός υποθέτει ότι οι χαρακτήρες που αποτελούν τον κωδικό έχουν παραχθεί εντελώς τυχαία. Η εντροπία ορίζει το ανώτερο όριο της πολυπλοκότητας που μπορεί να έχει ένας κωδικός ασφαλείας, ενώ στην πράξη η πολυπλοκότητα που έχει ένας κωδικός ασφαλείας επιλεγμένος από χρήστες έχει σημαντικά μικρότερη πολυπλοκότητα.

Κωδικοί Γραφικών - Βασισμένοι στην Αναγνώριση

Στο Passfaces κατά την αυθεντικοποίηση οι χρήστες θα πρέπει να αναγνωρίσουν και να διαλέξουν τις εικόνες όπως και στην εγγραφή τους. Ο χώρος κωδικών είναι N^K, όπου N είναι ο αριθμός των φωτογραφιών που παρουσιάζονται σε κάθε γύρο στον χρήστη και K είναι ο αριθμός των γύρων που περνάει ο χρήστης για να αυθεντικοποιηθεί. Για ένα πλέγμα 5x5 (N=25) και τρείς γύρους αυθεντικοποίησης ο *χώρος κωδικών* ισούται με $25^3=15625 \approx 2^{14}$ και άρα με 14 bit εντροπίας.

Ο *χώρος κωδικών* που παρέχουν τα Βασισμένα στην Αναγνώριση σχήματα είναι αρκετά περιορισμένος, γεγονός το οποίο τα καθιστά ευάλωτα σε επιθέσεις βίας. Προκειμένου να μεγαλώσουμε το keyspace μπορούμε να αυξήσουμε τον αριθμό των φωτογραφιών ή/και να αυξήσουμε τον αριθμό των γύρων δηλαδή τις φορές που καλείται ο χρήστης να επιλέξει τις σωστές εικόνες. Ωστόσο, μια τέτοια προσέγγιση ενδέχεται να προκαλέσει δυσλειτουργίες καθώς θα αυξηθεί ο χρόνος που απαιτείται για την αυθεντικοποίηση, θα είναι πιο κουραστικό για τον τελικό χρήστη και θα είναι και πιο δύσκολο να θυμάται κάποιος τα διαπιστευτήρια του.

Στο Déjà vu ο *χώρος κωδικών* είναι $\binom{N}{M}$ δυνατοί κωδικοί ασφαλείας για N σύνολα εικόνων και M οι εικόνες σε κάθε σετ που δείχνονται στο χρήστη. Για παράδειγμα, εάν ορίσουμε N=2 και M=55 έχουμε, $\binom{2}{55} = 53{,}130 \approx 2^{16}$.

Κωδικοί Γραφικών - Βασισμένοι στην Ανάκληση

Η βιβλιογραφία και η σχετική έρευνα που αφορά γραφικούς κωδικούς βασισμένους στην Ανάκληση κυριαρχείται από το Passpoints και τις παρεμφερείς παραλλαγές του. Για μια

εικόνα μεγέθους 640x480 pixel και ανοχή σφάλματος 10 pixels έχουμε 264 τετράγωνα στο πλέγμα. Ένας κωδικός των πέντε κλικ μας δίνει *χώρο κωδικών* $264^5 \approx 2^{35}$. Για να μεγαλώσουμε τον *χώρο κωδικών* μπορούμε να αυξήσουμε τον αριθμό των κλικς που χρειάζονται ή/και να μειώσουμε την ανοχή σφάλματος, ωστόσο έτσι εγείρονται ζητήματα χρηστικότητας και φιλικότητας προς τον χρήστη.

Στο DAS για ένα πλέγμα 5x5 και μέγιστο μέγεθος 12, ο θεωρητικός *χώρος κωδικών* είναι 2^{58} [JMMRR99]. Ωστόσο, οι επιλογές των κωδικών δεν είναι ισοπίθανες και η εντροπία των κωδικών που επιλέγουν οι χρήστες είναι σημαντικό μικρότερη από την θεωρητική μέγιστη τιμή της.

NAVI

Στο GoogleMaps κάθε στροφή, που είναι ισοδύναμη με ένα σημείο, αναπαρίσταται από είναι ζεύγος τιμών ή συντεταγμένων π.χ. (51.50364050493053, -0.135955810546875). Από τα 16 ψηφία που αποτελούν τη κάθε συντεταγμένη θα χρησιμοποιήσουμε μόνο τις δεκαδικές τιμές και θα αγνοήσουμε τις ακέραιες τιμές. Οι ακέραιες τιμές μπορεί εύκολα να γίνουν αντικείμενο επιθέσεων καθώς οι πιθανές τιμές τους είναι αρκετά περιορισμένες εάν σκεφτεί κανείς ότι οι διαδρομές που θα επιλέγουν οι χρήστες προφανώς δεν θα περιλαμβάνουν σημεία τα οποία βρίσκονται στους ωκεανούς, σε βουνά και άλλες ακατοίκητες περιοχές όπου δεν υπάρχει οδικό δίκτυο.
Επιπλέον, δεν θα χρησιμοποιήσουμε ούτε τα δυο πρώτα δεκαδικά ψηφία καθώς μας δίνουν χαμηλή εντροπία. Αυτό συμβαίνει διότι οι αναμενόμενες διαδρομές των χρηστών θα είναι σε περιορισμένο γεωγραφικό εύρος από την εκκίνηση μέχρι τον τερματισμό, και συνεπώς οι τιμές των δύο αυτών δεκαδικών θα παραμένουν σταθερές ή ακόμα και εάν αλλάζουν η τιμή τους θα αλλάζει κατά μια μονάδα. Τα υπολειπόμενα 12 ψηφία είναι αυτά που θα χρησιμοποιήσουμε για την δημιουργία του Γραφικού κωδικού για το NAVI.

Για κάθε στροφή στην διαδρομή παράγονται 24 ψηφία «μυστικού». Θα εφαρμόσουμε ένα ακόμα μέτρο ενάντια σε επιθέσεις. Θα εφαρμόσουμε μια μη αναστρέψιμη διαδικασία π.χ. εφαρμογή της XOR (λογικό AND) ανάμεσα στις δυο συντεταγμένες που ορίζουν κάθε σημείο. Έτσι, λοιπόν, έχουμε 12 ψηφία για κάθε στροφή αλλά έχουμε ισχυροποίηση του κωδικού που θα παραχθεί έναντι σε επιθέσεις. Εάν υποθέσουμε, λοιπόν, ότι ο η διαδρομή αποτελείται από 4 στροφές ο παραγόμενος κωδικός ασφαλείας θα αποτελείται από 4x12=48 ψηφία. Ο *χώρος κωδικών* θα είναι: $10^{48} \approx 2^{160}$. Υπενθυμίζουμε ότι το σημείο εκκίνησης και το σημείο τερματισμού δεν λαμβάνονται υπόψη καθώς υπόκεινται σε περιορισμούς ακρίβειας κατά την επιλογή από τον χρήστη. Το NAVI μας επιτρέπει την δημιουργία κωδικών ασφαλείας με μεγάλο *χώρο κωδικών* και συνεπώς και υψηλή εντροπία.

5.4.2. Επιθέσεις Λεξικού & Εικασίας

Κωδικοί Ασφαλείας Κειμένου

Το πώς μπορούν να αντιμετωπιστούν οι επιθέσεις λεξικού δεν είναι εύκολο ζήτημα ούτε υπάρχει μια ξεκάθαρη τακτική που θα πρέπει να ακολουθηθεί μιας και επαφίεται στις επιλογές του τελικού χρήστη. Οι επιθέσεις λεξικού είναι αποδεδειγμένα εξαιρετικά αποτελεσματικές και υπάρχει διαθέσιμο πλήθος εργαλείων που αυτοματοποιούν τέτοιες επιθέσεις όπως τα brutus [BRU], και John the Ripper [JOHN].

Κωδικοί Γραφικών – Βασισμένοι στην Αναγνώριση

Το Face, μια ελαφριά παραλλαγή του passfaces, αναλύθηκε από τους D. Davisetal. [DMR04] και έδειξε ότι οι χρήστες τείνουν να επιλέγουν πρόσωπα ελκυστικά, της ιδίας φυλής και εντέλει επιλέγουν προβλέψιμα σύνολα εικόνων τέτοια ώστε εάν ο επιτιθέμενος γνωρίζει την πρώτη εικόνα που επιλέχθηκε μπορεί να μαντέψει με υψηλό ποσοστό επιτυχίας και την επόμενη εικόνα. Επιπλέον, το φύλο του χρήστη φάνηκε να επηρεάζει τις επιλογές των εικόνων. Στο πείραμα που διεξήγαγαν, το 25% από τους πιο αδύναμους κωδικούς βρέθηκε επιτυχώς μετά από 13 προσπάθειες ενώ ο χώρος κωδικών είναι 9^4 = 6,561. Ένα 10% των κωδικών βρέθηκε μετά από μόλις 2 προσπάθειες. Η μελέτη αυτή ανέδειξε τις αδυναμίες των κωδικών γραφικών και τα ζητήματα που προκύπτουν όταν οι χρήστες επιλέγουν τον κωδικό τους χωρίς περιορισμούς.

Στο [EBFK09] παρουσιάστηκε μια μελέτη στο Passfaces όπου εφαρμόστηκαν περιορισμοί στους γραφικούς κωδικούς που μπορεί να επιλέξει ο χρήστης προκειμένου να αντιμετωπιστούν ζητήματα όπως αυτά που αναφέραμε παραπάνω. Ωστόσο οι περιορισμοί είχαν επιπτώσεις στην απομνημόνευση των κωδικών από τους χρήστες. Εάν οι χρήστες χρησιμοποιήσουν δικές τους εικόνες βελτιώνεται η απομνημόνευση αυτών, από την άλλη μια τέτοια προσέγγιση ενδέχεται καθιστά ευάλωτους τους κωδικούς ασφαλείας σε στοχευμένες επιθέσεις.

Σε μια πρόσφατη μελέτη [AP13], έγινε χρήση πληροφοριών που είναι διαθέσιμες στα κοινωνικά δίκτυα. Οι επιθέσεις που πραγματοποιήθηκαν λαμβάνοντας υπόψη τις πληροφορίες που συλλέχθηκαν ήταν αποτελεσματικές.

Κωδικοί Γραφικών – Βασισμένοι στην Ανάκληση

Σε σειρά από μελέτες έχει αποδειχθεί ότι είναι εφικτές και αποτελεσματικές αυτοματοποιημένες επιθέσεις ενάντια στο PassPoints

Η ανάκτηση γραφικών κωδικών για τα Pass-Go και DAS με χρήση επίθεσης Λεξικών είχε ως αποτέλεσμα την εύρεση των κωδικών με σημαντικά λιγότερες προσπάθειες από όσες θα περίμενε κανείς με βάση το διαθέσιμο *χώρο κωδικών* [T08],

[OT08]. Χρησιμοποιώντας μια μέθοδο πρόβλεψης με βάση την συμμετρία αντικατοπτρισμού και χαρακτηριστικά μέτρησης των χτυπημάτων (κλικ) των κωδικών του DAS ταυτοποιήθηκαν αδύναμοι υποχώροι κωδικών.

Το 40% των επιλεγμένων κωδικών από τους χρήστες εμπίπτουν στους υποχώρους κωδικών που ορίζονται από την συμμετρία του κάθετου και του οριζόντιου άξονα (χωρίς περιορισμούς στον αριθμό των κλικ) και 72% εμπίπτουν σε υποχώρο που χαρακτηρίζεται από 4 ή και λιγότερα κλικ.

Η επιτυχία των επιθέσεων λεξικού καθίσταται δυνατή από δύο σημαντικές αδυναμίες που σχετίζονται με τις επιλογές των χρηστών: σημεία ή περιοχές σε μια εικόνα έχουν μεγαλύτερη πιθανότητα να επιλεγούν από τους χρήστες. και γεωμετρικά μοτίβα, τα οποία μπορεί να είναι γραμμές ή γεωμετρικά σχήματα που σχηματίζονται από τις επιλογές των χρηστών και είναι εύκολα προβλέψιμα.

Οι παραπάνω γενικές αρχές μπορεί να εφαρμοστούν σε επιθέσεις στο PassPoints.

Η κυριαρχία σε απλές σειρές επιλογών σημείων (με κλικ) στο PassPoint κατέστησαν δυνατή την δημιουργία Λεξικών για επίθεση στο PassPoints και σε αντίθεση με ότι θα περίμενε κανείς τα Λεξικά δεν εξαρτώνται από τις εικόνες καθώς τα μοτίβα που περιέχει το Λεξικό εμφανίζονται σε πολλές εικόνες. Οι Salehi-Abari et al. [STO08] και οι van Oorschot et al. [OST10] πραγματοποιήσαν και αυτοματοποιημένες επιθέσεις χωρίς να χρειάζεται καμία ανθρώπινη παρέμβαση.

Το DejaVu φέρεται να είναι αρκετά ανθεκτικό απέναντι σε επιθέσεις Λεξικού καθώς στη μελέτη που παρουσιάστηκε από τους Dhamija και Perrig [DP00] λίγες ήταν οι εικόνες που επιλέχθηκαν από πολλαπλούς χρήστες.

5.4.3. Λογισμικό Υποκλοπής και Καταγραφείς Πληκτρολογίου

Κωδικοί Ασφαλείας Κειμένου

Οι Κωδικοί Ασφαλείας Κειμένου είναι ιδιαίτερα ευάλωτοι σε λογισμικό υποκλοπής και σε καταγραφείς πληκτρολογίου λόγω της ίδιας της φύσης τους, καθώς η απλή καταγραφή των πληκτρολογήσεων είναι επαρκής ώστε να υποκλαπούν τα διαπιστευτήρια αυθεντικοποίησης ενός χρήστη. Έχουν γίνουν αρκετές προσπάθειες προκείμενου να μετριαστεί η αδυναμία αυτή [FH06], [ZO12]. Σε κάθε περίπτωση το γεγονός παραμένει ότι οι Κωδικοί πρόσβασης είναι ιδιαίτερα ευάλωτοι σε λογισμικά υποκλοπής και σε καταγραφείς πληκτρολογίου.

Κωδικοί Γραφικών – Βασισμένοι στην Αναγνώριση & Βασισμένοι στην Ανάκληση & NAVI

Στην περίπτωση των κωδικών κειμένου, ως μόνη ουσιαστική λύση για να αντιμετωπιστεί ο κίνδυνος υποκλοπής είναι η χρήση λύσεων εντοπισμού και περιορισμού του κακόβουλου λογισμικού. Από την άλλη, παρόλο που τέτοιες επιθέσεις δύναται να

υλοποιηθούν απέναντι σε Κωδικούς Γραφικών από την φύση τους είναι σαφώς πιο δύσκολο να πραγματοποιηθούν επιτυχημένες επιθέσεις

Επιπρόσθετα, η πλειοψηφία του κακόβολου λογισμικού και των κ*αταγραφέων πληκτρολογίου* επικεντρώνεται στην καταγραφή των πληκτρολογήσεων του χρήστη παρόλο που υπάρχουν διαθέσιμα και λογισμικά που έχουν τη δυνατότητα να λαμβάνουν και στιγμιότυπα οθόνης. Ενώ όσο οι Κωδικοί Γραφικών κερδίζουν έδαφος ως μέθοδος αυθεντικοποίησης είναι αναμενόμενο οι ωτακουστές και οι κακόβουλοι χρήστες να αναπτύξουν κακόβουλο λογισμικό το οποίο θα είναι ειδικά παραμετροποιημένο και προσαρμοσμένο ώστε να μπορούν να υποκλέπτουν και τους Κωδικούς Γραφικών.

5.4.4. Κοινωνική Μηχανική

Κωδικοί Ασφαλείας Κειμένου

Οι επιθέσεις κοινωνικής μηχανικής απέναντι σε Κωδικούς Γραφικών Κειμένου είναι ιδιαίτερα διαδεδομένες καθώς είναι εύκολο να μεταδωθεί προφορικά ή μέσω ηλεκτρονικού ταχυδρομείου το μυστικό αυθεντικοποίησης το οποίο αποτελείται από γράμματα, αριθμούς κτλ.

Κωδικοί Γραφικών - Βασισμένοι στην Αναγνώριση και Βασισμένοι στην Ανάκληση

Στην περίπτωση των Γραφικών Κωδικών, πριν πραγματοποιηθεί μια επίθεση θα πρέπει να υπάρχει ένα πλαίσιο αναφοράς στο οποίο θα δοθούν τα διαπιστευτήρια (credentials). Το πλεονέκτημα αυτό, από την μεριά της ασφάλειας, έχει κόστος στην ευκολία χρήσης. Για παράδειγμα, καθίσταται πολύπλοκο να γίνει επαναφορά του κωδικού μέσω τηλεφώνου με την υπηρεσία υποστήριξης χρηστών. Παρόλες τις δυσκολίες που αναφέραμε, οι Dunphy et al. [DNO08] έδωσαν ενδείξεις ότι οι χρήστες του PassPoints μπορούν να μεταφέρουν επαρκώς τον Κωδικό τους προφορικά σε τρίτους. Άλλα μέσα για τον διαμοιρασμό Κωδικού Γραφικών περιλαμβάνουν το να λάβει ο χρήστης κάποια φωτογραφία,ή screenshot και να το ζωγραφίσει.

5.4.5. Σερφάρισμα Ώμου

Κωδικοί Ασφαλείας Κειμένου

Οι Κωδικοί Ασφαλείας Κειμένου είναι ευάλωτοι σε σερφάρισμα ώμου, και για το λόγο αυτό έχουν γίνει και αρκετές προσπάθειες να προταθούν παραλλαγές που θα είναι πιο ανθεκτικές [CM14], [LM14], [SAS11].

Κωδικοί Γραφικών – Βασισμένοι στην Αναγνώριση και Βασισμένοι στην Ανάκληση

Το σερφάρισμα ώμου γίνεται πιο εύκολο για τους Κωδικούς Γραφικών εάν λάβουμε υπόψη ότι υπάρχει και η οπτική πλευρά στην αυθεντικοποίηση [TOH06], [RVF04], [BDU08], [LWS08], [ZGBY11], [LHZMSH14]. Όταν ο χρήστης εισαγάγει τα πιστοποιητικά αυθεντικοποίησής του ένας επιτιθέμενος μπορεί να παρατηρήσει απ' ευθείας ή να χρησιμοποιήσει κάποια συσκευή καταγραφής π.χ. κάμερες υψηλής ανάλυσης και εξοπλισμό παρακολούθησης καθιστώντας το σερφάρισμα ώμου σημαντική απειλή ειδικά εάν στοχοποιηθεί ένας συγκεκριμένος χρήστης.

Όπως θα περίμενε κανείς έχουν προταθεί συστήματα αυθεντικοποίησης Γραφικών Κωδικών τα οποία είναι ανθεκτικά απέναντι σε επιθέσεις σερφαρίσματος ώμου, αλλά έχουν σημαντικό κόστος στην ευκολία χρήσης, κυρίως στην προσπάθεια και στο χρόνο που απαιτείται για να συνδεθεί κάποιος [KH08], [WWSB0606].

NAVI

Τα μοντέλα Γραφικών Κωδικών είναι ευάλωτα στις επιθέσεις σερφαρίσματος ώμου, και το NAVI δεν αποτελεί εξαίρεση. Προκειμένου να μετριάσουμε την έκθεση του NAVI στο σερφάρισμα ώμου ο χάρτης εμφανίζεται στον τελικό χρήστη με αδιαφάνεια (opacity) 30%, μειώνοντας έτσι τον ορίζοντα στον οποίο είναι ορατή η διαδρομή – κωδικός χωρίς να δημιουργεί ζητήματα ευχρηστίας.

Στον Πίνακα 11, συνοψίζουμε την επίδοση των Κωδικών Ασφαλείας Κειμένου, των Γραφικών Κωδικών (recognitionandrecall-based) και του NAVI σε σχέση με τις επιθέσεις βίας, επιθέσεις λεξικού, κακόβουλο λογισμικό, σερφάρισμα ώμου και κοινωνική μηχανική.

Πίνακας 11: Σύγκριση επίδοσης μεθόδων αυθεντικοποίησης σε επιθέσεις

Μέθοδος Επίθεσης	NAVI	Γραφικοί Κωδικοί Αναγνώρισης	Γραφικοί Κωδικοί Ανάκλησης	Κωδικοί Ασφαλείας
Επιθέσεις βίας	■■■■■	■□□□□	■■■■□	■■■□□
Επιθέσεις λεξικού	■■■■□	■□□□□	■■■■□	■■□□□
Κακόβουλο λογισμικό	■■■■□	■■■■□	■■■■□	■■□□□
Σερφάρισμα ώμου	■■□□□	■■□□□	■■□□□	■■■■□
Κοινωνική μηχανική	■■■□□	■■■□□	■■■□□	■■□□□

Σύμφωνα με την ανάλυση που πραγματοποιήσαμε, στο κεφάλαιο αυτό αναδείξαμε ότι το NAVI παρέχει Κωδικούς Ασφαλείας με υψηλή εντροπία και συνεπώς με μεγάλη ανθεκτικότητα έναντι σε επιθέσεις βίας. Στον αντίποδα, οι Γραφικοί Κωδικοί

αναγνώρισης παρέχουν Κωδικούς χαμηλής πολυπλοκότητας και είναι ευάλωτοι σε επιθέσεις βίας. Ενώ οι Γραφικοί Κωδικοί Ανάκλησης αλλά και οι παραδοσιακοί Κωδικοί Ασφάλειας μπορούν εν δυνάμει να μας δώσουν αρκετά ισχυρούς κωδικούς.

Στο NAVI και στα μοντέλα Γραφικών Κωδικών Ανάκλησης είναι δύσκολο να επιτευχθούν επιθέσεις λεξικού καθώς η δημιουργία κατάλληλου λεξικού για να χρησιμοποιηθεί σε κάποια επίθεση είναι εξαιρετικά σύνθετη και αμφιβόλου αποτελέσματος., σε αντιδιαστολή με τους Κωδικούς Ασφαλείας κειμένου αλλά και με τους Γραφικούς Κωδικούς Αναγνώρισης όπου οι επιθέσεις λεξικού είναι αποδεδειγμένα εξαιρετικά επιτυχημένες απέναντι τους.

Όλα τα μοντέλα που βασίζονται σε οπτική πληροφορία (NAVI, Γραφικοί Κωδικοί Αναγνώρισης και Γραφικοί Κωδικοί Ανάκλησης) δεν είναι ιδιαίτερα ευάλωτα σε κακόβουλο λογισμικό καθώς προκειμένου να υποκλαπεί η οπτική πληροφορία που χρησιμοποιείται ως μυστικό απαιτείται εξειδικευμένο κακόβουλο λογισμικό το οποίο θα πρέπει να έχει ιδιαίτερα προχωρημένες δυνατότητες καταγραφής λ.χ. print screens, καταγραφή κινήσεων του ποντικιού του χρήστη. Οι κωδικοί ασφαλείας κειμένου είναι ιδιαίτερα ευάλωτοι σε κακόβουλο λογισμικό της κατηγορίας key logger όπου καταγράφεται οτιδήποτε πληκτρολογεί ο χρήστες, συμπεριλαμβανομένων και των κωδικών ασφαλείας.

Ωστόσο, οι κωδικοί ασφάλειας κειμένου έχουν την μεγαλύτερη αντοχή έναντι σε επιθέσεις σερφαρίσματος ώμου, καθώς τα μοντέλα στα οποία ο κωδικός ασφαλείας είναι βασισμένος σε οπτική πληροφορία είναι ευκολότερο να υποκλαπεί δεδομένου ότι η εν λόγω πληροφορία απεικονίζεται στην οθόνη του χρήστη.

Στα μοντέλα τα οποία βασίζονται σε οπτική πληροφορία (NAVI, Γραφικοί Κωδικοί Αναγνώρισης και Γραφικοί Κωδικοί Ανάκλησης) είναι δύσκολο να επιτύχει μια επίθεση κοινωνικής μηχανικής καθώς για να περιγραφτεί η οπτική πληροφορία θα πρέπει είτε να δοθεί εκτεταμένη προφορική διήγηση ή να δοθεί στον επιτιθέμενο με κάποιο τρόπο αυτούσια η ζητούμενη οπτική πληροφορία. Αντιθέτως, η αναπαραγωγή ενός Κωδικού Ασφαλείας κειμένου είναι τετριμένη και οι επιθέσεις κοινωνικής μηχανικής έχουν αποδειχθεί ιδιαίτερα αποτελεσματικές για την απόκτηση κωδικών ασφαλείας από κακόβουλους χρήστες.

6. Συμπεράσματα και Μελλοντικές Κατευθύνσεις

Η διείσδυση της τεχνολογίας σε όλο και μεγαλύτερο φάσμα των καθημερινών δραστηριοτήτων μας, η αυξανόμενη εξάρτησή μας από τα πληροφοριακά συστήματα για την εκτέλεση εργασιών καθώς και ο εμπλουτισμός των τελικών χρηστών από ανθρώπους διαφορετικών ηλικιών και επαγγελμάτων θέτουν συνεχώς νέες προκλήσεις που θα πρέπει να αντιμετωπιστούν. Αντικείμενο έρευνας της παρούσας διατριβής αποτέλεσαν η αυθεντικοποίηση και η διαχείριση πρόσβασης χρηστών, ο καθορισμός δηλαδή του ποιος είσαι (αυθεντικοποίηση) και του τι μπορείς να κάνεις (διαχείριση πρόσβασης), δύο εννοιών αναγκαίων για την διασφάλιση της ομαλής και ασφαλούς χρήσης πληροφοριακών συστημάτων.

Στον τομέα της αυθεντικοποίησης προτάθηκε το NAVI, ένα καινοτόμο σύστημα Γραφικών Κωδικών στο οποίο οι χρήστες προκειμένου να αυθεντικοποιηθούν επιτυχώς θα πρέπει να είναι σε θέση να αναπαράγουν σε έναν προκαθορισμένο χάρτη την διαδρομή που είχαν δημιουργήσει κατά το στάδιο της αρχικής εγγραφής τους. Για την υλοποίηση βασιστήκαμε στο Google Maps API καθώς και στις τεχνολογίες php, javascript, JSON, apache web server και mysql.

Στο πλαίσιο της έρευνάς μας υλοποιήσαμε το NAVI ως μια εφαρμογή διαδικτύου και κατόπιν διεξαγάγαμε μια μελέτη εφικτότητας δίδοντάς το προς πειραματική χρήση σε χρήστες. Η ανάλυσή μας βασίστηκε στα ίχνη (logs) που παρήχθησαν από την χρήση του NAVI και από τις απαντήσεις που μας δόθηκαν από τους χρήστες σε ερωτηματολόγιο που τους παρείχαμε.

Τα συνολικά αποτελέσματα που λάβαμε είναι ιδιαίτερα ενθαρρυντικά όσον αφορά την αποδοχή από τους χρήστες, και την ευκολία χρήσης και εξοικείωσης με το προτεινόμενο μοντέλο αυθεντικοποίησης. Σύμφωνα με τα αποτελέσματα της έρευνάς μας οι κωδικοί διαδρομής παρέχουν υψηλό επίπεδο ασφαλείας σε σύγκριση με τους κωδικούς κειμένου αλλά και σε σχέση με άλλα σχήματα γραφικών κωδικών. Επιπλέον, η απομνημόνευση του κωδικού διαδρομής αξιολογήθηκε θετικά. Ωστόσο, σχεδόν οι μισοί χρήστες που συμμετείχαν στο πείραμα δήλωσαν ότι θεωρούν ότι η προσπάθεια που απαιτείται για να αυθεντικοποιηθούν χρησιμοποιώντας το NAVI είναι υψηλή.

Στο πλαίσιο της βελτιστοποίησης της εμπειρίας χρήσης ο βασικός άξονας της περαιτέρω έρευνας αποτελείται από την πρόκληση να παραμετροποιηθεί το NAVI ώστε να καθιστάται ευκολότερη και γρηγορότερη η αυθεντικοποίηση του τελικού χρήστη. Δεδομένου ότι το NAVI παρέχει κωδικούς ασφαλείας υψηλής πολυπλοκότητας αξίζει να διερευνηθεί το ενδεχόμενο να δοθεί στους χρήστες ένα περιθώριο λάθους ακρίβειας όταν εισάγουν τον κωδικό διαδρομής προκειμένου να είναι πιο φιλική προς το χρήστη η διαδικασία σύνδεσης. Ωστόσο, θα πρέπει να αξιολογηθούν οι επιπτώσεις που θα έχει μια τέτοια προσέγγιση στην ασφάλεια του NAVI.

Παρά τις όποιες αλλαγές και βελτιστοποιήσεις που μπορεί να επιτευχθούν, η αυθεντικοποίηση με το NAVI σε σύγκριση με την χρήση κωδικών κειμένου θα παραμένει πιο χρονοβόρα. Συνεπώς θα πρέπει να διερευνηθεί το επιθυμητό πλαίσιο χρήσης του NAVI. Για να καθοριστεί το πλαίσιο αυτό θα πρέπει να καθοριστούν με επιτυχία οι ακόλουθοι παράμετροι:

- Η συχνότητα με την οποία ο χρήστης είναι διατεθειμένος να κάνει χρήση μιας μεθόδου η οποία παρέχει μεγαλύτερη ασφάλεια και μεγαλύτερη ευκολία στην απομνημόνευση αλλά και μεγαλύτερο χρόνο για την αυθεντικοποίησή του.
- Οι εφαρμογές για τις οποίες ο χρήστης είναι πρόθυμος να εγκαταλείψει την ευκολία χρήσης των κωδικών κειμένου.
- Οι συνθήκες εκείνες που ελαχιστοποιούν την έκθεση σε επιθέσεις σερφαρίσματος ώμου.

Επιπλέον, για την αντιμετώπιση μιας σημαντικής αδυναμίας που είναι εγγενής σε όλα τα σχήματα γραφικών κωδικών, της περιήγησης ώμου, ήδη εφαρμόσαμε αδιαφάνεια (opacity) για να μειώσουμε την έκθεση σε τέτοιου είδους επιθέσεις. Σε αυτήν την κατεύθυνση θα μπορούσαν να εφαρμοστούν περαιτέρω αντίμετρα, όπως το να εφαρμοστεί ένα επίπεδο αδιαφάνειας στην γραμμή που απεικονίζει την διαδρομή ώστε να μην είναι ορατή από μεγάλη απόσταση. Επιπλέον, για να δυσχερανθεί το έργο του επιτιθέμενου θα μπορούσαμε να εφαρμόσουμε παραλλαγές στο πώς εμφανίζεται ο χάρτης, λ.χ. με τη να χρησιμοποιηθεί διαφορετικό χρώμα ή τρόπος απεικόνισης του χάρτη. Σε κάθε περίπτωση, οποιοδήποτε αλλαγή υλοποιηθεί θα πρέπει να αξιολογηθεί λαμβάνοντας υπόψη τα πλεονεκτήματα που παρέχει σε σχέση με τις επιπτώσεις στην εμπειρία των τελικών χρηστών. Μια ακόμα πιο αποτελεσματική αντιμετώπιση των επιθέσεων περιήγησης ώμου αποτελεί μια σημαντική πρόκληση η οποία θα πρέπει να διερευνηθεί περαιτέρω σε εξάρτηση και με τον καθορισμό του πλαισίου χρήσης του NAVI.

Μια ακόμα κατεύθυνση η οποία θα έχει ενδιαφέρον να διερευνηθεί είναι η προσαρμογή και χρήση του NAVI σε έξυπνα κινητά (Smartphones) τα οποία είναι πλέον εξαιρετικά διαδεδομένα. Η χρήση του NAVI σε έξυπνα κινητά απαιτεί, πέραν από την ανάπτυξη της αντίστοιχης εφαρμογής για κινητά (σε περιβάλλον iOS, android και windows mobile), και τροποποιήσεις στην λειτουργικότητα του NAVI ώστε να ανταπεξέλθει στις ειδικές απαιτήσεις που καθορίζονται από τους περιορισμούς που θέτουν οι έξυπνες συσκευές και ειδικότερα το περιορισμένο μέγεθος της οθόνης καθώς και η χρήση οθόνης αφής.

Έπειτα από βιβλιογραφική έρευνα στα υπάρχοντα μοντέλα διαχείρισης πρόσβασης, με έμφαση στα μοντέλα βασισμένα σε ρόλους αλλά και στα μοντέλα που αφορούν την κατ' εξαίρεση πρόσβαση εντοπίσαμε τις ελλείψεις των υπαρχόντων μοντέλων διαχείρισης πρόσβασης σε περίπτωσης έκτακτης ανάγκης. Συνεπώς, όσον αφορά τη διαχείριση πρόσβασης η έρευνα που πραγματοποιήθηκε επικεντρώθηκε στην ανάπτυξη ενός καινοτόμου μοντέλου το οποίο εμπεριέχει χωρικούς και χρονικούς

περιορισμούς και λαμβάνει υπόψη του δυναμικές παραμέτρους. Οι χρονικοί ή / και χωρικοί περιορισμοί επιβάλλονται στους ρόλους και σύμφωνα με τις παραμέτρους αυτές και τα δικαιώματα πρόσβασης που έχουν αποδοθεί σε ένα συγκεκριμένο ρόλο οι χρήστες λαμβάνουν εξουσιοδότηση να προσπελάσουν και να επεξεργαστούν ένα αντικείμενο. Σε περίπτωση που ένας χρήστης αιτηθεί να αποκτήσει πρόσβαση σε πόρους για τους οποίους ο ρόλος που έχει ενεργοποίησει δεν έχει πρόσβαση ενεργοποιείται ο μηχανισμός της κατ' εξαίρεση πρόσβασης. Η απόφαση για την απόδοση της κατ' εξαίρεση πρόσβασης σχετίζεται με στατικές παραμέτρους, τον ρόλο με τον οποίο έχει εκκινήσει συνεδρία ο χρήστης και τα βάρη που έχουν καθοριστεί ότι έχουν οι γράφοι οι οποίοι αναπαριστούν τους ρόλους στο ιεραρχικό RBAC αλλά και με δυναμικές παραμέτρους. Οι δυναμικές παράμετροι που λαμβάνονται υπόψη αποτελούνται από την τοποθεσία του χρήστη και το επίπεδο εμπιστοσύνης που έχει ανατεθεί στην τοποθεσία αυτή, το επίπεδο ασφάλειας του οργανισμού, το επίπεδο έκτακτης ανάγκης του οργανισμού και τέλος, το επίπεδο των απειλών προερχόμενων από το διαδίκτυο. Παρουσιάστηκε μια πρότυπη υλοποίηση που εμπεριέχει τα παραπάνω χαρακτηριστικά η αρχιτεκτονική της οποίας είναι βασισμένη στην XACML. Σημειώνεται ότι οι τεχνολογίες που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής διαδικτύου αποτελούνται από τις php, JavaScript, JSON, apache web server και mysql. Οι τεχνολογίες που χρησιμοποιήσαμε είναι ευρέως διαδεδομένες και είναι διαθέσιμες χωρίς οικονομικό κόστος.

Το προτεινόμενο μοντέλο επιφέρει μικρό διαχειριστικό κόστος κατά την υλοποίησή του, δεδομένου ότι η διαχείριση πρόσβασης πραγματοποιείται με ρόλους και αυτό που θα πρέπει να καθοριστεί επιπλέον είναι τα στατικά, βάρη στους γράφους. Επιπρόσθετα, προτάθηκε και ένα πλαίσιο αξιολόγησης της χρήσης του DSTEM-RBAC προκειμένου να διευκολυνθεί ο καθορισμός των παραμέτρων της κατ' εξαίρεσης πρόσβασης αλλά και παράλληλα να εντοπίζονται τυχόν καταχρήσεις των δυνατοτήτων πρόσβασης που παρέχονται.

Σημαντικός τομέας επέκτασης αυτής της ερευνητικής προσπάθειας αφορά τη χρήση περιγραφικής λογικής (description logic) καθώς τη χρήση σημασιολογίας (semantics) η οποία ενδέχεται να παράσχει σημαντικά πλεονεκτήματα στην περιγραφή των στατικών και, κυρίως, των δυναμικών παραμέτρων που καθορίζουν την απόδοση ή μη πρόσβασης.

Εάν οι παραπάνω προσθήκες στο DSTEM-RBAC αποδειχθούν αποτελεσματικές δίνεται η δυνατότητα της μετατροπής του DSTEM-RBAC από ένα μοντέλο κατ' εξαίρεση πρόσβασης σε ένα μοντέλο καθολικής εφαρμογής, όπου οι προσβάσεις των χρηστών θα καθορίζονται δυναμικά και όχι μόνο σε έκτακτες καταστάσεις. Σε αυτή την προσέγγιση, θα χρειαστεί να εμπλουτιστούν περαιτέρω και οι παράμετροι που θα καθορίζουν τους δυναμικούς βαθμούς ελευθερίας, όπως για παράδειγμα να εμπεριέχεται και μια παράμετρος που θα σχετίζεται με ένα σχήμα στο οποίο θα υπολογίζεται η φήμη (reputation) των χρηστών. Μια τέτοια επέκταση ωστόσο αυξάνει σημαντικά την πολυπλοκότητα των περιορισμών που θα πρέπει να εφαρμόσουμε ώστε να διασφαλίσουμε την ασφάλεια των δεδομένων και θα πρέπει να πραγματοποιηθούν εκτεταμένες δοκιμές και υλοποιήσεις περιπτώσεων μελέτης.

Όσον αφορά το πλαίσιο αξιολόγησης της χρήσης του μηχανισμού κατ' εξαίρεση πρόσβασης χρήζει διερεύνησης, εάν πέραν από την κατανομή Poisson στην οποία βασιστήκαμε, θα μπορούσαμε να χρησιμοποιήσουμε και άλλες μεθόδους / κατανομές προκειμένου να βελτιστοποιήσουμε τον εντοπισμό ενδεχόμενης κατάχρησης του μηχανισμού BTG. Προς την ίδια κατεύθυνση, θα έχει αξία να εξετάσουμε το πώς μπορούμε να διαχειριστούμε περιπτώσεις όπου λαμβάνονται, ενδεχομένως δικαιολογημένα, μαζικά αιτήματα κατ' εξαίρεση πρόσβασης και πώς λαμβάνοντας υπόψη την χρονική κατανομή των αιτημάτων να ενσωματώσουμε στο πλαίσιο αξιολόγησης χρήσης του DSTEM-RBAC τέτοιου είδους συμπεριφορές των χρηστών.

Καταλήγοντας, οι προτεινόμενες λύσεις που παρουσιάστηκαν στην παρούσα διατριβή στοχεύουν στην αποτελεσματικότερη και αποδοτικότερη αυθεντικοποίηση και κατόπιν στη διαχείριση της πρόσβασης των τελικών χρηστών. Λαμβάνοντας υπόψη την πολυπλοκότητα των σύγχρονων πληροφοριακών συστημάτων αλλά και την εξέλιξη στις ανάγκες των χρηστών αλλά και των οργανισμών που βασίζονται σε πληροφοριακά συστήματα προτείναμε καινοτόμες μεθόδους αυθεντικοποίησης και διαχείρισης πρόσβασης που χαρακτηρίζονται από την εφικτότητα της υλοποίησης τους, αφενός λόγω των διαδεδομένων και χωρίς κόστος τεχνολογιών που χρησιμοποιήσαμε και αφετέρου στο ελάχιστο διαχειριστικό κόστος και τον περιορισμένο φόρτο που επιφέρουν στον τελικό χρήστη.

Βιβλιογραφία

[AB98] Bauer, A. (1998). Gallery of random art. WWW at http://andrej. com/art.

[ANSI00] Glossary, A. T. (2000). American National Standards Institute, Inc. Also available: http://www.atis.org/tg2k/t1g2k.html.

[ANSI04] INCITS, A. (2004). INCITS 359-2004, American national standard for information technology, role based access control. American National Standards Institute.

[AP13] Aljahdali, H. M., & Poet, R. (2013). The affect of familiarity on the usability of recognition-based graphical passwords: Cross Cultural Study between Saudi Arabia and the United Kingdom. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on (pp. 1528-1534). IEEE.

[APW13] Asghar, H. J, Pieprzyk J., Li, S. & Wang, H. (2013) Cryptanalysis of the convex hull click human identification protocol. In International Journal of Information Security, Springer-Verlag, April 2013, Volume 12, Issue 2, (pp 83-96).

[AS08] Alsulaiman, F. A., & El Saddik, A. (2008). Three-dimensional password for more secure authentication. Instrumentation and Measurement, IEEE Transactions on, 57(9), (pp. 1929-1938).

[AW05] Atluri, V., & Warner, J. (2005). Supporting conditional delegation in secure workflow management systems. In Proceedings of the tenth ACM symposium on Access control models and technologies (pp. 49-58).

[B77] Biba, K. J. (1977). Integrity considerations for secure computer systems (No. MTR-3153-REV-1). MITRE CORP BEDFORD MA.

[B96] Blonder, G. E. (1996). U.S. Patent No. 5,559,961. Washington, DC: U.S. Patent and Trademark Office.

[B05] Bell, D. E. (2005). Looking back at the Bell-La Padula model. In Computer Security Applications Conference, 21st Annual (pp. 337-351).

[B12] Bishop, M. (2012). Computer security: art and science (Vol. 200). Addison-Wesley.

[BBF01] Bertino, E., Bonatti, P. A., & Ferrari, E. (2001). TRBAC: A temporal role-based access control model. ACM Transactions on Information and System Security (TISSEC), 4(3), (pp. 191-233).

[BBMWM05] Birget, J., Brodskiy, A., Memon, N., Waters, J., & Wiedenbeck, S. (2005). Authentication using graphical passwords: basic results. In ACM International Conference Proceeding Series (Vol. 93).

[BCDP05] Bertino, E., Catania, B., Damiani, M. L., & Perlasca, P. (2005). GEO-RBAC: a spatially aware RBAC. In Proceedings of the tenth ACM symposium on Access control models and technologies (pp. 29-37).

[BDU08] Backes, M., Durmuth, M., & Unruh, D. (2008). Compromising reflections-or-how to read LCD monitors around the corner. In Security and Privacy, 2008. SP 2008. IEEE Symposium on (pp. 158-169).

[BE77] Belnap, N. D. (1977). Modern Uses of Multiple-Valued Logics. Reidel, Dordrecht, (pp 30-56).

[BN89] Brewer, D. F., & Nash, M. J. (1989). The chinese wall security policy. In Security and Privacy, 1989. Proceedings. 1989 IEEE Symposium on (pp. 206-214).

[BP76] Bell, D. E., & La Padula, L. J. (1976). Secure computer system: Unified exposition and multics interpretation (No. MTR-2997-REV-1). MITRE CORP BEDFORD MA.

[BRU] Brutus the remote password cracker http://www.hoobie.net/brutus/

[BSA00] Barka, E., & Sandhu, R. (2000, December). Framework for role-based delegation models. In Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference (pp. 168-176).

[BS00] Barka, E., & Sandhu, R. (2000, October). A role-based delegation model and some extensions. In 23rd National Information Systems Security Conference (pp. 396-404).

[BS04] Barka, E., & Sandhu, R. (2004, December). Role-based delegation model/hierarchical roles (RBDM1). In Computer Security Applications Conference, 2004. 20th Annual (pp. 396-404).

[CJ05] Chandran, S. M., & Joshi, J. B. (2005). LoT-RBAC: a location and time-based RBAC model. In Web Information Systems Engineering–WISE 2005 (pp. 361-375). Springer Berlin Heidelberg.

[CK06] Crampton, J., & Khambhammettu, H. (2006). Delegation in role-based access control. In Computer Security–ESORICS 2006 (pp. 174-191). Springer Berlin Heidelberg.

[CM14] Chakraborty, N., & Mondal, S. (2014). SLASS: Secure login against shoulder surfing. In Recent Trends in Computer Networks and Distributed Systems Security (pp. 346-357). Springer Berlin Heidelberg.

[CO06] Chadwick, D. W., & Otenko, A. (2003). The PERMIS X. 509 role based privilege management infrastructure. Future Generation Computer Systems, 19(2), (pp. 277-289).

[DMB07] Dirik, A. E., Memon, N., & Birget, J. C. (2007). Modeling user choice in the PassPoints graphical password scheme. In Proceedings of the 3rd symposium on Usable privacy and security (pp. 20-28). ACM.

[DMR04] Davis, D., Monrose, F., & Reiter, M. K. (2004, August). On user choice in graphical password schemes. In USENIX Security Symposium (Vol. 13, pp. 11-11).

[DNO08] Dunphy, P., Nicholson, J., & Olivier, P. (2008). Securing passfaces for description. In Proceedings of the 4th symposium on Usable privacy and security (pp. 24-35). ACM.

[DS07] Douligeris, C., & Serpanos, D. N. (2007). Network security: current status and future directions. John Wiley & Sons.

[DW87] D Clark, D. D., & Wilson, D. R. (1987, April). A comparison of commercial and military computer security policies. In Security and Privacy, 1987 IEEE Symposium on (pp. 184-184). IEEE.

[EBFK09] Everitt, K. M., Bragin, T., Fogarty, J., & Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 889-898). ACM.

[FCK95] Ferraiolo, D., Cugini, J., & Kuhn, D. R. (1995). Role-based access control (RBAC): Features and motivations. In Proceedings of 11th annual Computer Security Applications Conference (pp. 241-48).

[FH06] Florêncio, D., & Herley, C. (2006). Klassp: Entering passwords on a spyware infected machine using a shared-secret proxy. In Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual (pp. 67-76).

[FK92] Ferraiolo, D. F., & Kuhn, R. (1992). Role based access controls [15th National Computer Security Conference paper]. Retrieved from NIST Computer security resource center: http://csrc. nist. gov/rbac/rbacSTD-ACM. pdf.

[FKC07] Ferraiolo, D., Kuhn, D., & Chandramouli, R. (2003). Role-based access control, Artech House computer security series. Artech House.

[G07] Gołofit, K. (2007). Click passwords under investigation. In Computer Security–ESORICS 2007 (pp. 343-358). Springer Berlin Heidelberg.

[GD72] Graham, G. S., & Denning, P. J. (1972). Protection: principles and practice. In Proceedings of the May 16-18, 1972, spring joint computer conference (pp. 417-429). ACM.

[HDCP08] Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use Your Illusion: secure authentication usable anywhere. In Proceedings of the 4th symposium on Usable privacy and security (pp. 35-45). ACM.

[HFK06] Hu, V. C., Ferraiolo, D., & Kuhn, D. R. (2006). Assessment of access control systems. US Department of Commerce, National Institute of Standards and Technology.

[HR76] Harrison, M. A., Ruzzo, W. L., & Ullman, J. D. (1976). Protection in operating systems. Communications of the ACM, 19(8), (pp. 461-471).

[JBLG01] Joshi J. B. D., Bertino E., Latif U., & Ghafoor A. (2001). Generalized Temporal Role Based Access Control Model (GTRBAC) (Part I)- Specification and Modeling. CERIAS TR 2001-47, Purdue University, USA.

[JMMRR99] Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The Design and Analysis of Graphical Passwords. In Usenix Security.

[JOHN] John the Ripper password cracker http://www.openwall.com/john/

[K03] Kang, K. D. (2003). QoS-aware real-time data management (Doctoral dissertation, University of Virginia).

[KH08] Komanduri, S., & Hutchings, D. R. (2008). Order and entropy in picture passwords. In Proceedings of Graphics Interface 2008 (pp. 115-122). Canadian Information Processing Society.

[MS11] Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. John Wiley & Sons.

[NCSC87] National Computer Security Center (NCSC), Jordan, C. S. (1987). Guide to Understanding Discretionary Access Control in Trusted Systems. DIANE Publishing.

[NIST15] NIST. WWW at http://csrc.nist.gov/groups/SNS/rbac/faq.html

[NS92] Niezette, M., & Stevenne, J. (1992). An efficient symbolic representation of periodic time. In Proceedings of the International Conference on Information and Knowledge Management (CIKM) (pp. 161-168).

[L74] Lampson, B. W. (1974). Protection. ACM SIGOPS Operating Systems Review, 8(1), (pp. 18-24).

[LHZMSH14] De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M. E., Slawik, B. E., Hussmann, H., & Smith, M. (2014). Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2937-2946). ACM.

[LM14] Chakraborty, N., & Mondal, S. (2014). SLASS: Secure login against shoulder surfing. In Recent Trends in Computer Networks and Distributed Systems Security (pp. 346-357). Springer Berlin Heidelberg.

[LWS08] Laxton, B., Wang, K., & Savage, S. (2008). Reconsidering physical key secrecy: Teleduplication via optical decoding. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 469-478). ACM.

[MDP10] Mhaske-Dhamdhere, V., & Patil, G. A. (2010). Three diamentional object used for data security. In Computational Intelligence and Communication Networks (CICN), 2010 International Conference on (pp. 403-408). IEEE.

[O97] Osborn, S. (1997). Mandatory access control and role-based access control revisited. In Proceedings of the second ACM workshop on Role-based access control (pp. 31-40). ACM.

[OST10] Van Oorschot, P. C., Salehi-Abari, A., & Thorpe, J. (2010). Purely automated attacks on passpoints-style graphical passwords. In Information Forensics and Security, IEEE Transactions on, 5(3), (pp. 393-405).

[OT08] van Oorschot, P. C., & Thorpe, J. (2008). On predictive models and user-drawn graphical passwords. In ACM Transactions on Information and system Security (TISSEC), 10(4), 5.

[PASS] Passfaces Corporation: WWW at http://www.passfaces.com

[DP00] Dhamija, R., & Perrig, A. (2000). Deja Vu-A user study: Using images for authentication. In USENIX Security Symposium (Vol. 9, pp. 4-4).

[QZWKM85] Qiu, L., Zhang, Y., Wang, F., Kyung, M., & Mahajan, H. R. (1985). Trusted computer system evaluation criteria. In National Computer Security Center.

[RVF04] Roth, V., Richter, K., & Freidinger, R. (2004). A PIN-entry method resilient against shoulder surfing. In Proceedings of the 11th ACM conference on Computer and communications security (pp. 236-245). ACM.

[S48] Shannon, C. E. (2001). Originally published: 1948. A mathematical theory of communication. ACM SIGMOBILE Mobile Computing and Communications Review, 5(1), (pp. 3-55).

[SAS11] Srinadhu, C., Addanki, S. K., & Acharyulu, B. R. (2011). MIRAGE 1.0: A key entry scheme resilient to shoulder surfing. International Journal of Computer Applications, 29(1), (pp. 47-53).

[SB02] Sobrado, L., & Birget, J. C. (2002). Graphical passwords. The Rutgers Scholar, an electronic Bulletin for undergraduate research, 4, 2002.

[SCFY96] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. Computer, (2), (pp. 38-47).

[SDA05] Sohr, K., Drouineaud, M., & Ahn, G. J. (2005). Formal specification of role-based security policies for clinical information systems. In Proceedings of the 2005 ACM symposium on Applied computing (pp. 332-339). ACM.

[SFK00] Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST model for role-based access control: towards a unified standard. In ACM workshop on Role-based access control (Vol. 2000).

[SGB07] Samuel, A., Ghafoor, A., & Bertino, E. (2007). A framework for specification and verification of generalized spatio-temporal role based access control model.

[SS94] Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. Communications Magazine, IEEE, 32(9), (pp. 40-48).

[SSNDS07] Zhao, G., Chadwick, D., & Otenko, S. (2007). Obligations for role based access control. In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on (Vol. 1, pp. 424-431). IEEE.

[STO08] Salehi-Abari, A., Thorpe, J., & van Oorschot, P. C. (2008). On purely automated attacks and click-based graphical passwords. In Computer Security Applications Conference. ACSAC 2008. Annual (pp. 111-120). IEEE.

[TA08] Tao, H., and Carlisle A. (2008). Pass-Go: A proposal to improve the usability of graphical passwords. In IJ Network Security 7.2 (pp. 273-292).

[T08] Thorpe, J. (2008). On the predictability and security of user choice in passwords (Doctoral dissertation, CARLETON UNIVERSITY Ottawa).

[TK03] Takada, T., & Koike, H. (2003). Awase-E: Image-based authentication for mobile phones using user's favorite images. In Human-computer interaction with mobile devices and services (pp. 347-351). Springer Berlin Heidelberg.

[TMM13] Towhidi, F., Masrom, M., & Abdul Manaf, A. (2013). An enhancement on passface graphical password authentication. Journal of Basic and Applied Scientific Research, 3(2), (pp 135-141).

[TN13] Tripunitara, M. V., & Li, N. (2013). The foundational work of Harrison-Ruzzo-Ullman revisited. Dependable and Secure Computing, IEEE Transactions on, 10(1), (pp. 28-39).

[TO07] Thorpe, J., & van Oorschot, P. C. (2007). Human-seeded attacks and exploiting hot-spots in graphical passwords. In USENIX Security (Vol. 7).

[TOH06] Tari, F., Ozok, A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In Proceedings of the second symposium on Usable privacy and security (pp. 56-66). ACM.

[TOK06] Takada, T., Onuki, T., & Koike, H. (2006, November). Awase-e: Recognition-based image authentication scheme using users' personal photographs. In Innovations in Information Technology, 2006 (pp. 1-5). IEEE.

[TP97] Tidswell, J., & Potter, J. (1997). An approach to dynamic domain and type enforcement. In Information Security and Privacy (pp. 26-37). Springer Berlin Heidelberg.

[W03] Weber, H. A. (2003). Role-based access control: the NIST solution. Sans Institute.

[WK05] Wainer, J., & Kumar, A. (2005). A fine-grained, controllable, user-to-user delegation method in RBAC. In Proceedings of the tenth ACM symposium on Access control models and technologies (pp. 59-66). ACM.

[WWBBM05a] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63(1), (pp. 102-127).

[WWBBM05b] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12). ACM.

[WWSB06] Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces (pp. 177-184). ACM.

[ZAC01] Zhang, L., Ahn, G. J., & Chu, B. T. (2001). A rule-based framework for role based delegation. In Proceedings of the sixth ACM symposium on Access control models and technologies (pp. 153-162). ACM.

[ZAC02] Zhang, L., Ahn, G. J., & Chu, B. T. (2002). A role-based delegation framework for healthcare information systems. In Proceedings of the seventh ACM symposium on Access control models and technologies (pp. 125-134). ACM.

[ZGBY11] Zakaria, N. H., Griffiths, D., Brostoff, S., & Yan, J. (2011). Shoulder surfing defence for recall-based graphical passwords. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 6). ACM.

[ZOS03] Zhang, X., Oh, S., & Sandhu, R. (2003). PBDM: a flexible delegation model in RBAC. In Proceedings of the eighth ACM symposium on Access control models and technologies (pp. 149-157). ACM.

[ZO12] Zaitsev, O. V. (2012). U.S. Patent No. 8,145,913. Washington, DC: U.S. Patent and Trademark Office.

[ZP03] Zhang, G., & Parashar, M. (2003). Dynamic context-aware access control for grid applications. In Grid Computing, 2003. Proceedings. Fourth International Workshop on (pp. 101-108). IEEE.

[ZP04] Zhang, G., & Parashar, M. (2004, January). Context-aware dynamic access control for pervasive applications. In Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (pp. 21-30).

[ZS03] Zhang, X., Oh, S., & Sandhu, R. (2003, June). PBDM: a flexible delegation model in RBAC. In Proceedings of the eighth ACM symposium on Access control models and technologies (pp. 149-157). ACM.

Παράρτημα Α – Ερωτηματολόγιο προς κλινικές

Ερωτήσεις προς τμήμα πληροφοριακών συστημάτων (IT)

1. Έχουν όλοι οι γιατροί όλα τα δικαιώματα πρόσβασης σε δεδομένα;
    a. Ναι
    b. Όχι, παρακαλώ διευκρινίστε πχ Διαφοροποιούνται ανά ειδικότητα; ανάλογα με την ιεραρχική θέση; (πχ ειδικευόμενος γιατρός, καθηγητής):
    ……
    ……..
2. Προϊστάμενοι τμημάτων έχουν πρόσβαση σε όλα τα δεδομένα που έχουν οι υφιστάμενοι τους;
    a. Ναι
    b. Όχι
    c. Άλλο, παρακαλώ διευκρινίστε: ……
    ……..
3. Πόσο συχνά χρήστες (Γιατροί) σας έχουν ζητήσει πρόσβαση σε δεδομένα που κανονικά δεν θα έπρεπε να έχουν;
    a. Πολύ συχνά (σε καθημερινή βάση)
    b. Συχνά (Περισσότερο από 3 φορές τη βδομάδα)
    c. Σπάνια (1 φορά την εβδομάδα)
    d. Πολύ σπάνια (λιγότερο από μια φορά το μήνα)
    e. Άλλο, παρακαλώ διευκρινίστε: ……
    ……..
4. Πόσοι γιατροί απασχολούνται στην κλινική: …..

5. Πόσο συχνά χρήστες (Νοσηλευτικό προσωπικό) σας έχουν ζητήσει πρόσβαση σε δεδομένα που κανονικά δεν θα έπρεπε να έχουν;
    a. Πολύ συχνά (σε καθημερινή βάση)
    b. Συχνά (Περισσότερο από 3 φορές τη βδομάδα)
    c. Σπάνια (1 φορά την εβδομάδα)
    d. Πολύ σπάνια (λιγότερο από μια φορά το μήνα)
    e. Άλλο, παρακαλώ διευκρινίστε: ……
    ……..
6. Πόσα άτομα απασχολούνται στην κλινική ως νοσηλευτικό προσωπικό: …..

7. Πόσο συχνά χρήστες (άλλο προσωπικό) σας έχουν ζητήσει πρόσβαση σε δεδομένα που κανονικά δεν θα έπρεπε να έχουν;
    a. Πολύ συχνά (σε καθημερινή βάση)
    b. Συχνά (Περισσότερο από 3 φορές τη βδομάδα)
    c. Σπάνια (1 φορά την εβδομάδα)
    d. Πολύ σπάνια (λιγότερο από μια φορά το μήνα)
    e. Άλλο, παρακαλώ διευκρινίστε: ……
    ……..
8. Πόσα άτομα απασχολούνται στην κλινική ως «άλλο προσωπικό»: …..

9. Ποιοι χρήστες σας έχουν ζητήσει πρόσβαση σε δεδομένα που κανονικά δεν θα έπρεπε να έχουν
    a. Ειδικευόμενοι Γιατροί
    b. Γιατροί
    c. Καθηγητές Γιατροί
    d. Νοσοκόμες
    e. Προϊσταμένη Νοσοκόμα
    f. Ειδικευόμενη Νοσοκόμα
    g. Άλλο ιατρικό προσωπικό (πχ ακτινολόγοι, ραδιολόγοι)
    h. Άλλο, παρακαλώ διευκρινίστε: ……..
    ……
10. Τι γίνεται σε αυτή τι περίπτωση;
    a. Ζητάνε Πρόσβαση από κάποιον έχει ήδη
    b. Απευθύνονται στο IT για αποκτήσουν πρόσβαση
    c. Άλλο, παρακαλώ διευκρινίστε: ……..
    ……

Ερωτήσεις προς το προσωπικό του νοσοκομείου

Δημογραφικά στοιχεία του ιατρικού προσωπικού
Ειδικότητα / Βαθμός
Ηλικία

Ερωτήσεις

1. Έχει τύχει να χρειάζεστε πρόσβαση σε δεδομένα ασθενούς και να σας αρνείται η πρόσβαση;
    a. Ναι
    b. Όχι

2. Εάν ναι πόσο συχνά;
    d. Πολύ συχνά (σε καθημερινή βάση)
    e. Αρκετά Συχνά (Περισσότερο από 3 φορές τη βδομάδα)
    f. Συχνά (1 φορά την εβδομάδα)
    g. Λιγότερο συχνά (1 φορά τις δύο βδομάδες)
    h. Σπάνια (μια φορά το μήνα)
    i. Πολύ σπάνια (Μια φορά το τρίμηνο)
    j. Άλλο, παρακαλώ διευκρινίστε: ……
    ……..

3. Υπάρχει τρόπος να αποκτείστε πρόσβαση;
    a. Ναι
    b. Όχι

4. Επιτύχατε γρήγορα την πρόσβαση στα δεδομένα που χρειαζόσασταν;
    a. Ναι
    b. Όχι

5. Θεωρείται εύκολο να αποκτήσετε την επιθυμητή πρόσβαση;
    a. Ναι
    b. Όχι

Παράρτημα Β – Ερωτηματολόγιο αξιολόγησης NAVI

1. Age
   - <20
   - 20-28
   - 28-35
   - 35-40
   - >40

2. Gender
   - Male
   - Female

3. Profession

4. Do you consider your self an experienced user of information systems e.g. personal computers, smartphones etc.
   - Inexperienced
   - Nearly experienced
   - Experienced
   - Very experienced

5. Were you experient in the use of google maps service before using NAVI?
   - Inexperienced
   - Nearly experienced
   - Experienced
   - Very experienced

6. How demanding do you find it to remember a strong password (a long password that consists of random letters, numbers and special characters like !, #, &, * etc.)
   - Very easy
   - Easy
   - Demanding
   - Very demanding

7. How demanding do you find it to remember a simple password?
   - Very easy
   - Easy

- Demanding
- Very demanding

8. How hard did you find it to register and log in into NAVI?
   - Very easy
   - Easy
   - Hard
   - Very Hard

9. How demanding do you find it to remember your credentials for NAVI system?
   - Very easy
   - Easy
   - Hard
   - Very Hard

10. How secure do you consider NAVI is?
    - Insecure
    - Not so secure
    - Secure
    - Very secure

11. The starting and ending point you selected is something you are familiar with e.g. home, workplace, gym
    - Very familiar
    - Familiar
    - Not so familiar
    - Random

12. Would you consider using NAVI instead of traditional passwords in order to login to a web service e.g. email, social network, forum
    - No
    - Maybe
    - Yes
    - Definitely

13. Please provide us with any other comments regarding NAVI authentication scheme