Πανεπιστήμιο Πειραιώς

Τμήμα Ασφάλειας Ψηφιακών Συστημάτων

Διπλωματική Εργασία

"Εξομοίωση Υπολογιστικού Διαδικτυακού Πλέγματος και καθορισμός πολιτικών"

Πετρέας Φαίδων

Απρίλιος 2012

Πίνακας περιεχομένων

Πίνακας εικόνων

Εισαγωγή

Τα τελευταία χρόνια έχει έρθει στο προσκήνιο μία νέα τεχνολογία η οποία είναι το αποτέλεσμα της συνένωσης ενός συνόλου γνωστών τεχνολογιών. Στην παγκόσμια ορολογία ονομάζεται ως *"Cloud Computing*", και στην παρούσα εργασία προτιμήθηκε να χρησιμοποιηθεί ο όρος *"διαδικτυακό υπολογιστικό πλέγμα*", επιχειρώντας την προσέγγιση με βάση το τι ακριβώς αποτελεί αυτή η τεχνολογία, και όχι με απευθείας μετάφραση του αγγλικού όρου.

Αναμφίβολα το διαδικτυακό υπολογιστικό πλέγμα έχει γίνει η νέα "μόδα" της εποχής στον κόσμο της πληροφορικής. Αφορά τους πάντες. Είτε είναι επιχειρήσεις που ψάχνουν να βρούν τρόπους για μείωση των εξόδων είτε απλοί καταναλωτές. Ακόμα και σε διαφημίσεις κινητών, προβάλλεται η δυνατότητα χρήσης της υπηρεσίας του διαδικτυακού πλέγματος με την συγκεκριμένη συσκευή, προβάλλοντας αυτό το χαρακτηριστικό, και δείχνοντας την άποψη από την πλευρά της κατασκευάστριας εταιρείας, ότι αυτό το χαρακτηριστικό είναι καθοριστικό για την εμπορική επιτυχία του προιόντος.

Η βάση που στηρίζεται αυτός ο νεωτερισμός όμως, είναι η υποδομή του διαδικτύου. Αυτό, σε συνδυασμό με το ότι είναι μία τεχνολογία στα πρώτα της βήματα, έχει διχάσει τον κόσμο σε δύο πλευρές. Η μία πλευρά που είναι υπέρμαχος και βλέπει τα ωφέλη που αποκομίζει, και η πιο σκεπτική πλευρά που αναγνωρίζει κάποιες αδυναμίες που υποβόσκουν στα θέματα ασφάλειας και την απορρίπτουν. Το μόνο σίγουρο είναι ότι η αλήθεια βρίσκεται κάπου στην μέση: αδυναμίες υπάρχουν, όπως και σε κάθε νέα τεχνολογία. Το ζητούμενο όμως, είναι να ανιχνεύσουμε όλα τα προβλήματα με αναλυτικό τρόπο, ώστε να προβούμε σε κατάλληλα διορθωτικά μέτρα και να έξασφαλίσουμε ένα επίπεδο λειτουργικότητας το οποίο να είναι αποδεκτό από άποψη ασφάλειας. Για να γίνει αυτό, αναγκαίο είναι να υπάρχει γνώση της αρχιτεκτονικής του συστήματος, καταγραφή και μελέτη προβλημάτων που έχουν παρατηρηθεί στην πλατφόρμα, και το πιο ουσιαστικό ίσως απο όλα είναι η πλήρης εξοικοίωση με τις τεχνολογίες ασφάλειας. Αν και είναι μία νέα τεχνολογία, σε ένα εκπληκτικό ποσοστό, η ασφάλεια επιτυγχάνεται με την εφαρμογή παραδοσιακών τεχνικών, που εφαρμόζονται άρδην στα παραδοσιακά συστήματα. Βεβαίως υπάρχει και μία λίστα από νέου τύπου αδυναμίες, οι οποίες θα αναφερθούν σε σχετικό εδάφιο της εργασίας.

Στην παρούσα διπλωματική, θα αναλύσουμε την αρχιτεκτονική και τον τρόπο λειτουργίας του διαδικτυακού υπολογιστικού πλέγματος, ώστε στην συνέχεια να διερευνηθούν τα όποια ζητήματα ασφάλειας καθώς και οι προτεινόμενες λύσεις που πρέπει να υιοθετηθούν, τόσο από τον πάροχο όσο και από τον ίδιο πελάτη - οργανισμό - χρήστη της υπηρεσίας του διαδικτυακού υπολογιστικού πλέγματος. Στο

δεύτερο μέρος, θα αναλυθεί η state of the art τεχνολογία εξουσιοδότησης πρόσβασης XACML και η αρχιτεκτονική της.

Στο τελευταίο μέρος της εργασίας, θα παρουσιαστεί η υλοποίηση μίας εφαρμογής ιστού κάνοντας χρήση τεχνολογίας Java/Java Server Faces και η οποία εκτελείται από ένα JBOSS Application Server. Η εφαρμογή αυτή εφαρμόζει το νέο πρότυπο XACML προκειμένου να παρέχει εξουσιοδότηση πρόσβασης σε χρήστες που δινουν τα διαπιστευτήρια τους. Η όλη πλατφόρμα παραδίδεται σε ένα DVD και περιέχει ένα εικονικό λειτουργικό σύστημα Windows XP, το οποίο έχει εγκατεστημένα τα εξής:

- JBOSS Application Server με τις βιβλιοθήκες XACML.
- Την διαδικτυακή εφαρμογή που αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας, σε περιβάλλον Eclipse και με χρήση της Java/Java Server Faces.
- Το γραφικό περιβάλλον ανάπτυξης λογισμικού Eclipse Indigo.
- Ο πηγαίος κώδικας της διαδικτυακής εφαρμογής.

Λέξεις κλειδιά: *έλεγχος πρόσβασης με ρόλους (RBAC), έλεγχος πρόσβασης με χαρακτηριστικά (ABAC), εξουσιοδότηση (Authorization), Αυθεντικοποίηση (Authentication) διαδικτυακό υπολογιστικό πλέγμα, ιδιωτικότητα (Cloud Computing), XACML, SAML, SaaS, IaaS, PaaS, JBoss Application Server, Java, Διαχειριστής Εικονικών Μηχανών (Hypervisor), Κέντρο Απόφασης Πολιτικής (Policy Decision Point), Κέντρο Επιβολής Πολιτικής (Policy Enforcement Point), Κέντρο Διαχείρισης Πολιτικής (Policy Administration Point), Κ-Ανωνυμία, Single Sign On, Τείχος Προστασίας, Εικονικές Μηχανές, Εικονικό Δίκτυο, Υπηρεσίες Ιστού.*

Κεφάλαιο 1

Εισαγωγή στο Διαδικτυακό υπολογιστικό πλέγμα

[1]

Ο όρος Cloud Computing (διαδικτυακό υπολογιστικό πλέγμα), ορίζει ένα ένα νέο λειτουργικό μοντέλο το οποίο χρησιμοποιείται για να προσφέρουμε υπολογιστικούς πόρους και υπηρεσίες δια μέσω του διαδικτύου. Συγκροτείται από ένα αριθμό εξυπηρετητών οι οποίοι είναι δυνατό να είναι διασκορπισμένοι σε όλο τον κόσμο και διασυνδέονται μέσω του διαδικτύου. Το μοντέλο αυτό αποτελείται από τους Cloud Providers (παρόχους υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος), οι οποίοι προσφέρουν στους πελάτες τους εφαρμογές, εκτελούμενες από έναν περιηγητη ιστού (Web Browser). Ένα τυπικό σενάριο, ορίζει ότι το λογισμικό και το υλικό ευρίσκονται στον χώρο του παρόχου υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος. Το νέο αυτό μοντέλο, αποτελεί μία καινοτομία στον χώρο της πληροφορικής, προσφέροντας μία εναλλακτική λύση σε σχέση με το καθιερωμένο μοντέλο χρήσης υπολογιστικών μηχανημάτων εντός της έδρας ενός οργανισμού. Το κλασσικό μοντέλο απαιτεί από την πλευρά του οργανισμού την συνεχή αναβάθμιση των υπολογιστικών μηχανημάτων και αγορά αδειών χρήσης λογισμικού καθώς ο οργανισμός επεκτείνεται. Το διαδικτυακό υπολογιστικό πλέγμα έρχεται να απαλλάξει τον οργανισμό από αυτήν την αναγκαιότητα, μετατρέποντας το κόστος κεφαλαίου (υλικό) σε κόστος λειτουργίας το οποίο είναι σημαντικά μειωμένο.

Το διαδικτυακό υπολογιστικό πλέγμα δεν είναι μία νέα τεχνολογική εξέλιξη, παρά θα λέγαμε ότι είναι η σύγκλιση ενός συνόλου υπαρχόντων τενολογιών του Grid και Cluster computing, Υπηρεσίες Ιστού (Web Services), Αρχιτεκτονικές προσανατολισμένες σε υπηρεσίες (Service Oriented Architectures).

Σύμφωνα με το μοντέλο του διαδικτυακού υπολογιστικού πλέγματος, υπηρεσίες, επεξεργαστική ισχύς και αποθηκευτικός χώρος παρέχονται στους πελάτες με μία σύμβαση πληρωμής ανάλογα με την χρήση. Ανάγκες για αυξημένη ή μειωμένη χρήση ενός ή περισσότερων από τις προαναφερθείσες παροχές, καλύπτεται με ένα δυναμικό τρόπο ο οποίος είναι εντελώς διαφανής στον τελικό χρήστη. Οι δυνατότητες για βάθμωση που προσφέρει το διαδικτυακό υπολογιστικό πλέγμα είναι εμφανείς όταν παρατηρούμε το τελικό κόστος για την χρήση των πόρων. Οι

πελάτες πληρώνουν μόνο την υπηρεσία στον πάροχο, και αποφεύγουν το κόστος σε επένδυση αγοράς πανάκριβου υλικού (εξυπηρετητές) οι οποίοι χάνουν την αξία τους με το πέρασμα του χρόνου, την εκπαίδευση εξειδικευμένου προσωπικού για την διαχείριση των εξυπηρετητών καθώς και την αγορά πολλαπλών αδειών εγκατάστασης και χρήσης λογισμικού.

Το ώφελος που προκύπτει από την αποφυγή αγοράς υλικού είναι τεράστιο. Η επένδυση σε υλικό είναι στατική, δηλαδή το υλικό που έχει αγοραστεί επαρκεί για συγκεκριμένες απαιτήσεις. Οι απαιτήσεις όμως είναι πάντα δυναμικές, με αποτέλεσμα ως επί το πλείστον είτε το υλικό έχει μεγαλύτερες δυνατότητες από την απαιτούμενη υπολογιστική ισχύ, πράγμα που υποδηλώνει σπατάλη όσον αφορά την εκτίμηση της αρχικής επένδυσης, είτε το υλικό είναι λιγότερων δυνατοτήτων με αποτέλεσμα η επιχείρηση να υπολειτουργεί. Ακόμα και με την ακριβή εκτίμηση των προδιαγραφών του υλικού, αυτή επιτελείται σύμφωνα με σενάρια μέσης χρήσης και δεν καλύπτουν τις περιπτώσεις όπου απαιτούνται αυξημένες απαιτήσεις σε επεξεργαστική ισχύ. Το πλεονέκτημα του διαδικτυακού υπολογιστικού πλέγματος είναι εμφανές: προσφέρει ευελιξία όσον αφορά την παροχή των πόρων, και οποτεδήποτε απαιτηθούν περισσότεροι αυτοί προσφέρονται. Αν διαπιστωθεί μειωμένη χρήση πόρων, τότε αποδεσμεύεται μέρος της επεξεργαστικής ισχύς για εξοικονόμηση. Η όλη διαχείριση δέσμευσης και αποδέσμευσης των πόρων επιτελείται στο παρασκήνιο χωρίς να αντιλαμβάνεται ο πελάτης κάποια διαφορά. Το πιο συνταρακτικό είναι, ότι ο πελάτης μπορει να δεσμεύσει οποιοδήποτε ποσό ισχύος οποιαδήποτε χρονική στιγμή και για οποιοδήποτε χρονικό διάστημα.

Βάσει των παραπάνω, το διαδικτυακό υπολογιστικό πλέγμα έχει γίνει η νέα μόδα στον χώρο των υπολογιστών και έχει κερδίσει ένθερμους υποστηρικτές. Κοντά στους υποστηρικτές αυτούς όμως υπάρχουν και οι πολέμιοι αυτής της τάσης, οι οποίοι υποστηρίζουν ότι η επένδυση σε διαδικτυακό υπολογιστικό πλέγμα φαντάζει αχρείαστη από την στιγμή που το κόστος αγοράς για υλικό έχει πέσει δραματικά τα τελευταία χρόνια. Επίσης το κόστος εκπαίδευσης προσωπικού δεν είναι τόσο μεγάλο. Εν μέρει είναι λογική η άποψη της αντίθετης πλευράς. Όμως, η εξοικονόμηση χρημάτων που επιτελείται με την επένδυση σε υπηρεσία διαδικτυακού υπολογιστικού πλέγματος είναι μεγάλη σε βάθος χρόνου. Επιπλέον, το κέρδος σε πρόσβαση υπολογιστικής ισχύος η οποία είναι ασύλληπτη σε μέγεθος, την οποίαν δεν μπορεί να την ισοσκελίσει ούτε και η πιο φιλόδοξη από άποψη ποσού επένδυσης για αγορά υλικού. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση των New York Times. Η εφημερίδα νοίκιασε το διαδικτυακό υπολογιστικό πλέγμα της Amazon προκειμένουν να δημιουργήσει μία βάση από PDFs άρθρων της εφημερίδος αρκετών δεκαετιών. Η εκτίμηση για τον χρόνο της αποπεράτωσης αυτού του έργου στην περίπτωση που θα χρησιμοποιούνταν οι εξυπηρετητές των New York Times ήταν 14 χρόνια (!). Η Amazon ολοκλήρωσε το έργο σε μία μέρα με κόστος $240 [2].

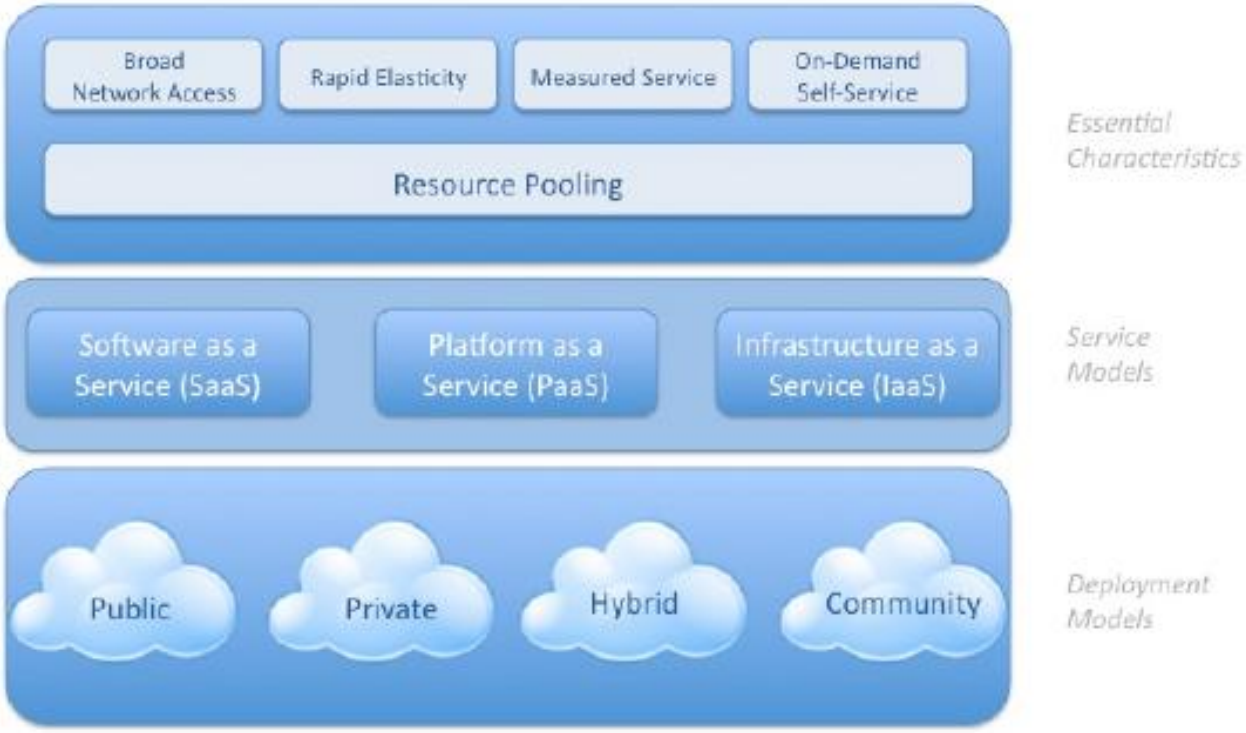
Η εμφάνιση του διαδικτυακού υπολογιστικού πλέγματος ως μία εναλλακτική λύση για την επεξεργασία και αποθήκευση δεδομένων των οργανισμών ειδικά σε μία δύσκολη εποχή όπως η σημερινή, που μαστίζεται από την οικονομική κρίση, δεν θα μπορούσε να αποτελεί παρά μία κατάλληλη λύση, προσφερόμενη την κατάλληλη χρονική στιγμή, και η οποία είναι κρίσιμη για την βιωσιμότητα των εταιρειών που αναγκάζονται εκ των δεινών συνθηκών να βρουν λύσεις για να συμπτύξουν τα έξοδα τους. Παρόλα αυτά, η ένταξη στο διαδικτυακό υπολογιστικό πλέγμα δεν είναι πανάκεια, καθώς υπεισέρχονται ένα σωρό από κινδύνους, για την ίδια την εταίρεία στο τομέα της ασφάλειας. Και ενώ από άποψη οικονομικού κόστους, το διαδικτυακό υπολογιστικό πλέγμα δύναται να βοηθήσει έναν οργανισμό από την άλλη, η όποια παραβίαση της ασφάλειας των δεδομένων του στον τομέα της ιδιωτικότητας, ακεραιότητας εμπιστευτικότητας και διαθεσιμότητας είναι δυνατόν να καταστρέψει την ίδια την εταιρεία.

Μοντέλο διαδικτυακού υπολογιστικού πλέγματος κατά NIST

[4] [5]

Στο παρόν εδάφιο θα περιγραφεί το μοντέλο του διαδικτυακού υπολογιστικού πλέγματος όπως έχει καθοριστεί από το U.S. National Institute of Standards and Technology (NIST) [5]. Το παρακάτω σχήμα απεικονίζει το γραφικό μοντέλο του NIST, το οποίο θα πρέπει να σημειώσουμε ότι τυγχάνει ευρείας αποδοχής.Ο οργανισμός NIST προσδιορίζει τον όρο του διαδικτυακού υπολογιστικού πλέγματος περιγράφοντας:

- πέντε βασικές ιδιότητες
- τρία μοντέλα υπηρεσιών
- τέσσερα μοντέλα αξιοποίησης



Εικόνα 1: Μοντέλο Διαδικτυακού υπολογιστικού πλέγματος κατά NIST

Μία από τις πιο σημαντικές έννοιες στο διαδικτυακό υπολογιστικό πλέγμα είναι η υποστήριξη του Multi Tenancy. Επιχειρώντας μία μετάφραση του ορισμού, ένα Multi Tenant περιβάλλον είναι αυτό στο οποίο εδρεύουν πολλοί διαφορετικοί χρήστες. Πιο συγκεκριμένα ένα περιβάλλον τύπου Multi Tenant σε ένα διαδικτυακό υπολογιστικό πλέγμα, επιτρέπει την κοινή χρήση των εφαρμογών, υλικού (επεξεργαστική ισχύς και αποθήκευτικός χώρος) από πολλούς χρήστες/πελάτες. Ο διαχωρισμός του περιβάλλοντος του κάθε πελάτη επιτελείται στο επίπεδο της εφαρμογής, με τέτοιο τρόπο ώστε κανένας άλλος πελάτης δεν είναι σε θέση να παρακολουθήσει τα δεδομένα οποιουδήποτε άλλου. Το γεγονός αυτό προσφέρει μεγάλες οικονομικές διευκολύνσεις στις επιχειρήσεις καθώς μία μόνο άδεια είναι επαρκής για την εκτέλεση ενός προγράμματος από πολλαπλούς χρήστες. Ωστόσο, γεννούνται ερωτηματικά σχετικά με το παρεχόμενο επίπεδο ασφαλείας καθώς η εμπιστευτικότητα και η ακεραιότητα των δεδομένων του πελάτη επαφίεται στις ενέργειες του παρόχου υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος. Και ενώ μπορούμε να πούμε ότι είναι θεμιτό να συγκεντρώνουμε τα δεδομένα όλων των πελατών σε μία κοινή βάση δεδομένων προκειμένου να ασκήσουμε νόμιμη εξόρυξη δεδομένων (παραδείγματος χάρην σύγκριση τιμών από διαφόρους παρόχους προιόντων και υπηρεσιών και επαναπροσδιορισμός της τιμής του προιόντος), από την άλλη πλευρά, δημιουργούνται βάσιμες ανησυχίες για το

ενδεχόμενο της μη εξουσιοδοτημένης πρόσβασης της βάσης δεδομένων από εξωτερικούς χρήστες.

Βασικές ιδιότητες διαδικτυακού υπολογιστικού πλέγματος

Με την εισαγωγή του μοντέλου του διαδικτυακού υπολογιστικού πλέγματος, είναι γεγονός ότι η χρήση του όρου αυτού έχει καταχραστεί από πολλούς παρόχους υπηρεσιών ιστού, προκειμένου να προσελκύσουν πελάτες. Το αποτέλεσμα είναι να δημιουργείται μία σύγχιση από την πλευρά των πελατών, οι οποίοι σε πολλές περιπτώσεις εσφαλμένα θεωρούν ότι χρησιμοποούν υπηρεσίες διαδικτυακού υπολογιστικού πλέγματος, χωρίς αυτό να ισχύει. Για παράδειγμα, η παροχή εφαρμογών ως υπηρεσία (SaaS) δεν είναι απόλυτα συνδεδεμένη με την χρήση πόρων διαδικτυακού υπολογιστικού πλέγματος. Ενώ σε ένα μοντέλο διαδικτυακού υπολογιστικού πλέγματος, οι απαιτούμενη ισχύς θα κατανέμεται σε ένα δίκτυο υπολογιστών διεσπαρμένων σε όλο τον κόσμο, ακολουθώντας κανόνες βαθμομέτρησης του φόρτου και δυναμική δεσμευση και αποδέσμευση υπολογιστικών μηχανημάτων για την εκτέλεση. Στο παραδοσιακό μοντέλο πελάτη εξυπηρετητή όμως, η εφαρμογή εκτελείται σε ένα συγκεκριμένο εξυπηρετητή πράγμα που διαφέρει ριζικά σε σχέση με την προηγούμενη περίπτωση. Προκειμένου λοιπόν να θεωρούμε ότι ένας πάροχος ακολουθεί το μοντέλο του διαδικτυακού υπολογιστικού πλέγματος, είναι απαραίτητο να διαθέτει τα ακόλουθα πέντα χαρακτηριστικά που έχει ορίσει το NIST:

1. **Αυτο-εξυπηρέτηση κατ' απαίτηση(On-demand self service).** Οι χρήστες ενός διαδικτυακού υπολογιστικού πλέγματος θα πρέπει να έχουν την δυνατότητα να απαιτούν και να λαμβάνουν υπολογιστικούς πόρους με ένα τρόπο δυναμικό χωρίς να μεσολαβεί ανθρώπινος παράγοντας προκειμένου να αποδωθούν οι πόροι αυτοί. Οι απαιτούμενοι πόροι μπορεί να είναι: επεξεργαστική ισχύς, επιπλέον αποθηκευτικός χώρος ή και μεγαλύτερο εύρος ζώνης επικοινωνίας.

2. **Ευρείας κλίμακας δικτυακή πρόσβαση (Broad network access).** Οι πάροχοι θα πρέπει να προσφέρουν υπηρεσίες διαδικτυακού υπολογιστικού πλέγματος σε μία ευρεία γκάμα συσκευών ετερογενών μεταξύ τους δυνατοτήτων. Θα πρέπει συνεπώς να έχουν προσβαση τόσο τα υπολογιστικά συστήματα πλήρων δυνατοτήτων, όσο και αυτά των πιο περιορισμένων δυνατοτήτων όπως λόγου χάρη τα PDAs, οι ταμπλέτες αλλά ακόμα και τα κινητά τηλέφωνα.

3. **Συνδιασμός πόρων (Resource pooling).** Οι πάροχοι υπηρεσιών θα πρέπει να αξιοποιούν την πολυχρηστική (multi tenant) αρχιτεκτονική προκειμένου να προσφέρουν στους πελάτες πόρους κατ' απαίτηση οποιαδήποτε χρονική στιγμή. Οι πελάτες δεν είναι απαραίτητο να γνωρίζουν τη τοποθεσία των υλικών πόρων αλλά και των δεδομένων τους. Σε ορισμένες περιπτώσεις όμως και για λόγους που θα αναλυθούν σε επόμενη ενότητα, είναι αναγκαίο όχι μόνο να γνωρίζουν αλλά και να οριοθετούν την περιοχή τοποθεσίας των δεδομένων τους επιλέγοντας κάποια συγκεκριμένη γεωγραφική ζώνη.

4. **Ελαστικότητα και αμεσότητα προσφοράς πόρων(Rapid elasticity)** Ο όρος αυτός καθορίζει τον τρόπο που οι πόροι δεσμεύονται ή αποδεσμεύονται σε ένα χρήστη. Θα πρέπει να επιτελείται με τρόπο πλήρως αυτοματοποιημένο και ακαριαία χωρίς να επιβάλλεται κάποιο περιοριστικό κατώφλι όσον αφορά το μέγεθος των διαθέσιμων προσφερόμενων πόρων. Έχοντας ως βάση το ότι ο πελάτης πληρώνει, ο πάροχος υποχρεούται να παρέχει οποιοδήποτε πόρο σε οποιοδήποτε απαιτούμενο μέγεθος οποιαδήποτε χρονική στιγμή ζητηθεί και ακαριαία.

5. **Βαθμονομημένη υπηρεσία (Measured Service)** Οι πάροχοι χρησιμοποιούν προγράμματα τα οποία μετρούν την χρήση των πόρων και εκτελούν επί μέρους βελτιστοποιήσεις όσον αφορά την κατανομή των πόρων στα απαιτούμενα σημεία. Για παράδειγμα, ρυθμίζουν το ποσό της διαθέσιμης επεξεργαστικής ισχύος, στις περιπτώσεις που παρατηρείται αυξημένη ζήτηση. Οι βελιστοποιήσεις αυτές, λαμβάνουν χώρα σε όλα τα επίπεδα υπηρεσιών (αποθηκευτικός χώρος, επεξεργασία, εύρος ζώνης, ή αριθμός ενεργών χρηστών).

Μοντέλα υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος

Οι πάροχοι υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος προσφέρουν τρία διαφορετικά μοντέλα υπηρεσιών, ανάλογα με τις ανάγκες των πελατών:

- **Λογισμικό ως υπηρεσία (Cloud Software as a Service - SaaS).** Ο πελάτης χρησιμοποιεί εφαρμογές που έχουν δημιουργηθεί απ΄οτον πάροχο και εκτελούνται στην περιοχή του. Η εκτέλεση πραγματοποιείται από συσκευές μειωμένων επεξεργαστικών δυνατοτήτων (thin clients) μέσω περιηγητή ιστού.

- **Πλατφόρμα ως υπηρεσία (Cloud Platform as a Service - PaaS).** Ο πάροχος προσφέρει στον πελάτη όλα τα απαραίτητα εργαλεία ούτως ώστε ο τελευταίος να δημιουργήσει τις δικές του εφαρμογές που θα εκτελεστούν στο περιβάλλον του διαδικτυακού υπολογιστικού πλέγματος. Ο πελάτης δεν έχει πρόσβαση στον καθορισμό των παραμέτρων της δικτυακής υποδομής αλλά έχει την ελευθερία να δημιουργήσει τις δικές του εφαρμογές σύμφωνα με τις ανάγκες του.

- **Υποδομή ως υπηρεσία (Cloud infrastructure as a Service - IaaS).** Η υπηρεσία αυτή προσφέρει την δυνατότητα στον πελάτη να καθορίσει ο ίδιος την δικτυακή υποδομή, όπως για παράδειγμα τον αποθηκευτικό χώρο, το δίκτυο, την επεξεργαστική ισχύ ανάλογα με τις ανάγκες του. Επιπρόσθετα, ο πελάτης είναι σε θέση να εκτελεί τις δικές του εφαρμογές στην πλατφόρμα. Στερείται της δυνατότητος να διαχειριστεί πλήρως την υποδομή, αλλά έχει την ελευθερία να καθορίσει τα χαρακτηριστικά του δικού του δικτύου, διαθέτοντας την δυνατότητα επιλογής λειτουργικού συστήματος, δικτυακών μονάδων όπως τείχη προστασίας και τερματικοί σταθμοί.

Μοντέλα αξιοποίησης διαδικτυακού υπολογιστικού πλέγματος

Υπάρχουν τέσσερα μοντέλα αξιοποίησης υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος, όπου κάθε ένα από αυτά καλύπτει συγκεκριμένες ανάγκες πελατών:

- Δημόσιο υπολογιστικό πλέγμα (Public Cloud). Μεγάλοι οργανισμοί όπως για παράδειγμα το διαδικτυακό υπολογιστικό πλέγμα παροχής υπηρεσιών διαδικτύου της Amazon (Amazon Web Services Cloud) προσφέρει υπηρεσίες και την υποδομή της για χρήση από το κοινό.
- Ιδιωτικό υπολογιστικό πλέγμα (Private Cloud). Σε αυτήν την περίπτωση, η υποδομή του διαδικτυακού υπολογιστικού πλέγματος χρησιμοποιείται εξ'ολοκλήρου από έναν οργανισμό ή από ένα third party οργανισμό που είναι συμβεβλημένος με τον πρώτο. Η υποδομή είναι δυνατό να ευρίσκεται εντός ή εκτός από την περιοχή του οργανισμού.
- Κοινοτικό υπολογιστικό πλέγμα (Community Cloud). Σε αυτήν την περίπτωση, ένα γκρούπ από οργανισμούς οι οποίοι έχουν κοινούς στόχους ανάγκες και επιδιώξεις, αξιοποιούν ένα νέφος από κοινού ένα διαδικτυακό υπολογιστικό πλέγμα, εξού και ο προσδιορισμός: "κοινοτικό". Το πλέγμα το διαχειρίζεται ή το γκρούπ των οργανισμών ή ενας third party οργανισμός

συμβεβλημένος με το γκρουπ. Όπως και στην περίπτωση του ιδιωτικού πλέγματος, η υποδομή ευρίσκεται εντός ή εκτός τοπολογικών ορίων του γκρουπ.

- Υβριδικό νέφος (Hybrid Cloud). Η υποδομή ενός υβριδικού νέφους, συγκροτείται από δύο ή περισσότερες κατηγορίες πλεγμάτων, τα οποία παραμένουν ως διακριτές οντότητες, αλλά είναι εφαρμόζουν καθορισμένες τεχνολογίες από κοινού, υπολοιώντας με αυτόν τον τρόπο αντίμετρα ως προς τους κινδύνους ασφαλείας και ιδιωτικότητας δεδομένων και εφαρμογών.

Βιβλιογραφία Κεφαλαίου

[1] G. G. Eric Knorr, «What cloud computing really means,» InfoWorld.

[2] N. Weinberg, «Cloudy picture for cloud computing,» Network World.

[3] M. Spinola, «An essential guide to possibilities and risks of cloud computing,» 2009.

[4] «Clous Security Alliance,» [Ηλεκτρονικό]. Available: http://cloudsecurityalliance.org/ .

[5] «NIST,» [Ηλεκτρονικό]. Available: http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html.

Κεφάλαιο 2

Ζητήματα ασφάλειας και ιδιωτικότητας σχετιζόμενα με το διαδικτυακό πλέγμα

[1], [2], [3], [4] , [5], [6]

Η όλη φιλοσοφία της λειτουργίας του διαδικτυακού υπολογιστικού πλέγματος, στηρίζεται στην χρήση των πόρων δια μέσω του διαδικτύου. Το γεγονός ότι ο πελάτης απο την μία πλευρά και τα δεδομένα και η υποδομή του δικτύου από την άλλη είναι πλήρως διαχωρισμένα, φέρει σοβαρά ζητήματα από άποψη διατήρησης της ασφάλειας και της ιδιωτικότητας των δεδομένων σε αυτό το επιχειρησιακό μοντέλο.

Στο κεφάλαιο αυτό θα αναφερθούμε στα προβλήματα ασφάλειας, ιδιωτικότητας και λειτουργικότητας που υπάρχουν στο διαδικτυακό υπολογιστικό πλέγμα. Θα αναφερθούν προτεινόμενες λύσεις και τεχνικές από την βιβλιογραφία, και θα κλείσουμε αναλύοντας το αρχιτεκτονικό μοντέλο ασφαλείας ενός από τους πιο γνωστούς πάροχους υπηρεσιών διαδικτυακού πλέγματος, της Amazon.

Πρόσβαση κατ'εξαίρεση (Privileged user access)

Ο πάροχος υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος έχει γενικά αυξημένα επίπεδα δικαιωμάτων πρόσβασης στην όλη υποδομή. Αυτό τον καθιστά ικανό να υπέρβει όποιους ελέγχους που έχουν θεσπιστεί για την προστασία των δεδομένων από τρίτους, και να προσπελάσει τα δεδομένα. Για αυτήν την περίπτωση απαραίτητη είναι η επικοινωνία μεταξύ πελάτη και πάροχου ώστε ο πελάτης να ενημερωθεί πλήρως για το επίπεδο πρόσβασης που έχει ο πάροχος στα δεδομένα του. Θα πρέπει να θεσπιστεί ένα Συμφωνητικό για το Επίπεδο Υπηρεσιών (Service Level Agreement) μεταξύ τους ώστε να καθορίσουν τί ειναι επιτρεπτό.

Συμμόρφωση στους κανονισμούς (Regulatory Compliance)

Τόσο ο πάροχος όσο και ο πελάτης μοιράζονται ευθύνες όσον αφορά την διαχείριση των δεδομένων. Ο πελάτης θα πρέπει να είναι υπεύθυνος για την εμπιστευτικότητα και την ακεραιότητα των δεδομένων του και να λάβει όλα τα απαραίτητα μέτρα. Αντίστοιχα ο πάροχος θα πρέπει να υπόκειται σε όλους τους απαραίτητους ελέγχους πιστοποίησης ασφαλείας που προσφέρει. Είναι μείζονος σημασίας, η εφαρμογή διαδικτυακών υπηρεσιών που υποστηρίζουν τεχνολογίες ασφάλειας και ιδιωτικότητας των δεδομένων. Αυτά τα στάνταρντς θα πρέπει να ακολουθούνται από όλους τους παρόχους προκειμένου να προσφέρουν οι τελευταίοι το απαιτούμενο επίπεδο ποιότητας υπηρεσιών. Τα ISO27001 και ISO27002 προσφέρουν οδηγίες για την διαχείριση ασφάλειας με σκοπό να βελτιστοποιήσουν την διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα της πληροφορίας. Τα παραπάνω στάνταρντς σε συνδιασμό με το ευρέως χρησιμοποιούμενο SAS70, προσφέρουν την βάση για μία αξιολόγηση ασφαλείας από τρίτο ελεγκτικό φορέα [7]. Τυχόν αδυναμία ενός πάροχου να συμμορφωθεί με τους άνω κανονισμούς, υποδηλώνει ότι το επίπεδο προσφερόμενων υπηρεσιών είναι επαρκές μόνο για περιπτώσεις διαφύλαξης και επεξεργασίας δεδομένων που δεν χρήζουν ανάγκης για εξασφάλιση της ιδιωτικότητας. Πολύ συχνά παρατηρείται το γεγονός πως ο ίδιοκτήτης των δεδομένων δεν έχει την πλήρη μορφή εξουσίας πάνω στα δεδομένα του στον κόσμο του διαδικτυακού υπολογιστικού πλέγματος. Και αυτό γιατί ο πάροχος συχνά υποβάλλει περιορισμούς μέσα στα επιτρεπτά πλαίσια των Όρων Χρήσης, να μην ασκούν για παράδειγμα οποιαδήποτε μορφής ελέγχους διείσδυσης (penetration testing). Αυτό είναι πολύ περιοριστικό και δείχνει αδυναμία στην ασφάλεια, και παρόλο που οι πάροχοι χρησιμοποιούν υπηρεσίες τρίτων για την εξασφάλιση των δεδομένων, κανένας δεν μπορεί να είναι σίγουρος ότι οι τελευταίοι ακολουθούν κατα γράμμα τις επιταγές του νόμου καθώς και τις απαραίτητες ή τις πιο αποτελεσματικές πρακτικές. Η αδυναμία διαφύλαξης των δεδομένων ενέχει κινδύνους για την βιωσιμότητα του οργανισμού που εξαρτά την λειτουργία του σε αυτόν τον πάροχο. [8]

Τοποθεσία των δεδομένων (Data Location)

Ο πάροχος είναι δυνατόν να έχει εκατοντάδες εξυπηρετητές στην κατοχή του και διεσπαρμένους σε όλον τον κόσμο. Αυτό έχει ως αποτέλεσμα ο πελάτης να μην γνωρίζει που ευρίσκονται τα δεδομένα του, πράγμα που φέρνει στην επιφάνεια νομικά ζητήματα. Δεδομένα που θεωρούνται ασφαλή σε μία χώρα, σε κάποια άλλη χώρα δεν ισχύει το ίδιο απαραίτητα. Παραδείγματος χάρην οι ευρωπαικοί νόμοι καθορίζουν αυστηρές πολιτικές σχετικά με το θέμα της ιδιωτικότητας ενώ οι

Αμερικάνικοι νόμοι δια μέσου του Patriot Act, προσφέρουν την ελευθερία σε υπηρεσίες και στην κυβέρνηση να έχουν απεριόριστη πρόσβαση στα δεδομένα των οργανισμών. Η ανησυχία απο την Ευρώπη για αυτη την ασυμφωνία πολιτικών μεταξύ των δύο ηπείρων, έχουν οδηγήσει στην δημιουργία των αρχών ιδιωτικότητας κατά US Safe Harbor. Σύμφωνα με αυτές, οι Ευρωπαικοί οργανισμοί αποκτούν κατά ένα βαθμό εξαίρεση από τους Αμερικάνικους νόμους. Ωστόσο, ακόμα και με αυτές τις ρυθμίσεις, κανείς δεν μπορεί να είναι βέβαιος ότι οι νόμοι αυτοί δεν θα παραβιαστούν. Δεν είναι λίγες οι περιπτώσεις όπου χρησιμοποιείται σαν βάση η αντι τρομοκρατική νομοθεσία - πολλές φορές καταχρηστικά - με σκοπό να αποκτηθεί πρόσβαση σε ιδιωτικά δεδομένα. Προφανώς η αντιτρομοκρατική νομοθεσία είναι μία δικαιολογία για αυτές τις περιπτώσεις. Σε κάθε περίπτωση, ο πελάτης θα πρέπει να διασφαλίσει κατόπιν συννενόησης με τον πάροχο ότι τα δεδομένα του θα ευρίσκονται σε συγκεκριμένες γεωγραφικές ζώνες όπου τηρείται πιστά η νομοθεσία περί ιδιωτικότητας των δεδομένων. Επιπλέον, κρίνεται απαραίτητο να έχει την δυνατότητα να κρυπτογραφεί και να αποκρυπτογραφεί τα δεδομένα του ο ίδιος ο πελάτης, ανεξάρτητα από τον πάροχο, αφαιρώντας την ιδιότητα του γνώστη των δεδομένων από τον πάροχο και υποβιβάζοντας τον στον ρόλο της κράτησης/αποθήκευσης των δεδομένων. Ο πάροχος θα πρέπει να παρέχει την δυνατότητα στον πελάτη να αποθηκεύει τα δεδομένα σε ζώνες συγκεκριμένες, και για τις οποίες υπάρχει πλήρη ενημέρωση για την ισχύουσα νομοθεσία σε κάθε μία από αυτές. [5]

Απομόνωση των δεδομένων (Data segregation)

Το γεγονός ότι τα δεδομένα πελατών ευρίσκονται σε ένα κοινό περιβάλλον, επιβάλλει την ανάγκη για εφαρμογή τεχνικών κρυπτογράφησης. Είναι καθοριστικής σημασίας η εφαρμογή των πιο σύγχρονων και αποτελεσματικών τεχνικών από πλήρως εξειδικευμένο προσωπικό, των οποίων η αποτελεσματικότητα θα έχει ελεγχθεί εκτενώς. Παράλειψη της εφαρμογής των παραπάνω θα έχει ως αποτέλεσμα όχι μόνο την απώλεια της εμπιστευτικότητας αλλά και την απώλεια της διαθεσιμότητας λόγω της καταστροφής των δεδομένων. Ένα παράδειγμα πρόσφατο αποτελεί το σύτημα των ψηφιακών υπογραφών του διαδικτυακού υπολογιστικού πλέγματος της Amazon, το οποίο στην αρχική του έκδοση παρουσίαζε την αυξημένη πιθανότητα να αποτυπώσει την ίδια ψηφιακή υπογραφή σε δύο διαφορετικά μηνύματα δεδομένων. Αυτό είχε σαν αποτέλεσμα την πρόκληση της σύγκρουσης των δεδομένων αυτών και επιτρέπει στον επιτιθέμενο να εφαρμόσει την ίδια υπογραφή στο δικό του μήνυμα και να παρακάμψει τους ελέγχους του συστήματος. Παρόλο που τα λάθη σε ένα σύστημα είναι αναμενόμενα, εν τούτοις ένα σύστημα θα πρέπει να υπόκειται σε εξονυχιστικό έλεγχο προκειμένου να βρεθούν οι όποιες

αδυναμίες του συστήματος ασφαλείας προτού χρησιμοποιηθεί αυτό στην παραγωγή [4]. Ο πελάτης δικαιούται να γνωρίζει ποιός έχει πρόσβαση στα κλειδιά αποκρυπτογράφησης. Σε ένα ιδανικό σενάριο ο πελάτης θα δύναται να εφαρμόσει ο ίδιος τις πολιτικές ασφαλείας, ανεξάρτητα από τον πάροχο. Είναι μία πρόκληση ή όλη εφαρμογή μίας ασφαλούς συνύπαρξης των δεδομένων πολλών πελατών. Θα πρέπει να σημειωθεί βέβαια ότι η επίθεση στον Hypervisor, το στρώμα που φιλοξενεί τα λειτουργικά συστήματα, είναι πιο δύσκολη σε σχέση με μία παραδοσιακή επίθεση σε ένα σύστημα υπολογιστή [8].

Μη ασφαλής ή μη ολοκληρωμένη διαγραφή δεδομένων

Το πρόβλημα με την διαγραφή δεδομένων είναι πολυδιάστατο. Καταρχάς όταν ο πελάτης απαιτεί την διαγραφή δεδομένων του, ο πάροχος δεν μπορει να εξασφαλίσει ότι έχουν διαγραφεί ολοκληρωτικά αυτά. Μπορεί μεν τα δεδομένα να μην είναι προσβάσιμα αλλά με ειδικά εργαλεία, επιτιθέμενοι είναι δυνατόν να αποκτήσουν πρόσβαση. Δεύτερον, αντίγραφα από τα δεδομένα του πελάτη είναι δυνατόν να ευρίσκονται σε πολλές τοποθεσίες προκειμένου να προσφέρεται υψηλό επίπεδο διαθεσιμότητας αλλά και αξιοπιστίας στην περίπτωση που ένας εξυπηρετητής τεθεί εκτός λειτουργίας. Το μειονέκτημα όμως είναι ότι τα αντίγραφα δεδομένων δεν είναι πάντοτε προσβάσιμα, επομένως η διαγραφή δεδομένων δεν εξασφαλίζει ότι έχει ως αποτέλεσμα την διαγραφή όλων των αντιγράφων [8].

Ανάκτηση δεδομένων

Είναι αναγκαίο ένας πάροχος να εξασφαλίζει οπωσδήποτε την επανάκτηση δεδομένων που έχουν καταστραφεί υπο οποιεσδήποτε συνθήκες. Για αυτόν τον λόγο ο πάροχος θα πρέπει να κρατάει πολλαπλά αντίγραφα δεδομένων διασκορπισμένα σε διάφορες γεωγραφικές τοποθεσίες. Μη τήρηση αυτής της τακτικής μπορεί να οδηγήσει σε μη διαθεσιμότητα των δεδομένων. Επίσης θα πρέπει να καθορίσει εκ των προτέρων και να γνωστοποιήσει στον πελάτη το μέγιστο απαιτούμενο χρονικό διάστημα που απαιτείται για να ανακτηθούν τα δεδομένα.

Έρευνα αρχείων καταγραφής και υποστήριξη

Το γεγονός ότι τα δεδομένα είναι διεσπαρμένα σε ποικίλλες γεωγραφικές τοποθεσίες και μαζί με δεδομένα διαφορετικών πελατών, κάνει την εργασία της καταγραφής ενεργειών και αναφοράς για συγκεκριμένο πελάτη, δύσκολη. Για αυτόν τον λόγο δεν παρέχουν όλοι οι πάροχοι υπηρεσίες καταγραφής και αναφοράς. Ο πελάτης θα πρέπει να διασφαλίσει ότι ο πάροχος που θα συνεργαστεί, υποστηρίζει μηχανισμούς έρευνας και καταγραφής συμβάντων, πράγμα που θα οδηγήσει στην διελεύκανση παράνομων ενεργειών από εξωτερικούς παράγοντες, αλλά και στην απόδοση ευθυνών προς παν υπαίτιο. Εξάλλου, ο μηχανισμός αυτός βοηθάει να ανιχνευτούν οι αδυναμίες του συστήματος και να προταθούν και να εφαρμοστούν βελτιωμένα μέτρα ασφάλειας για την ενίσχυση της ιδιωτικότητας και ασφάλειας στο μέλλον.

Βιωσιμότητα σε βάθος χρόνου

Σε ένα ιδανικό σενάριο ο πάροχος θα είναι πάντα δραστήριος και θα υποστηρίζει τους πελάτες του. Ωστόσο κανείς δεν μπορει να προβλέψει το ενδεχόμενο μίας χρεωκοπίας του παρόχου καθώς και το πως θα αντιμετωπίσει τους πελάτες του απο κει και πέρα. Είναι δυνατόν ο πάροχος να εξαγοραστεί από εταιρείες αντίπαλες του πελάτη με αποτέλεσμα να καταλήξουν τα δεδομένα του πελάτη σε αυτές για βιομηχανική κατασκοπεία. Σε ένα τέτοιο ενδεχόμενο οι πελάτες θα πρέπει να έχουν την δυνατότητα να εξάγουν τα δεδομένα τους από την βάση του παρόχου, και μάλιστα σε ένα γενικώς αποδεκτό και αναγνωρίσιμο φορμά, και να διαγράψουν πλήρως την βάση τους που ευρίσκεται στον πάροχο.

Αλυσσίδα παρόχων

Η εξέλιξη του διαδικτυακού υπολογιστικού πλέγματος, δημιούργησε την ανάγκη για την σύναψη συνεργασίας ομάδας από παρόχους υπηρεσιών, ώστε να ανταπεξέλθουν στις απαιτήσεις των πελατών. Το γεγονός αυτό περιπλέκει τις Συμφωνίες Επιπέδου Υπηρεσιών (Service Level Agreements) μεταξύ του πελάτη και του παρόχου. Ακόμα και αν υπάρχει πλήρης συμφωνία μεταξύ του παρόχου και του

πελάτη, ουδείς μπορεί να εγγυηθεί για την τήρηση των κανόνων ασφάλειας και ιδιωτικότητας από τους τρίτους που συνεργάζονται με τον βασικό πάροχο υπηρεσίας διαδικτυακού υπολογιστικού πλέγματος [5]. Χαρακτηριστικό παράδειγμα όπου είχαμε την παραβίαση της ιδιωτικότητας πελάτη, από ένα τρίτο εξωτερικό συνεργάτη, ήταν η περίπτωση της υπηρεσίας Beacon στο Facebook. Οι χρήστες είνια δυνατό να εμπιστεύονται το Facebook, και το τελευταίο να εφαρμόζει τα πιο σύγχρονα μέτρα ασφάλειας, αλλά αυτή η συγκεκριμένη υπηρεσία έκανε ανάρμοστη χρήση των δεδομένων των πελατών. Συγκεκριμένα, έκανε συλλογή πληροφοριών των ιστοσελίδων που πήγαιναν οι πελάτες, και δημοσιοποιούσε αυτήν την δραστηριότητα στις επαφές του κάθε χρήστη δια μέσω των ροών RSS (!). Ακόμα χειρότερα, αυτό πραγματοποιούνταν χωρίς να ζητείται η συγκατάθεση από τον χρήστη, και χωρίς να γνωρίζει τίποτα για αυτό ο χρήστης. Στις 12 Αυγούστου 2008, ασκήθηκε νομική δίωξη ενάντια στους οργανισμούς: Facebook, Blockbuster Inc, Overstock.com, Fandago, Hotwire.com, Game Fly, Zappos.com καθώς και οποιαδήποτε άλλος οργανισμός ο οποίος έκανε χρήση της υπηρεσίας Beacon, και δημοσίευσαν προσωπικές πληροφορίες χρηστών στις κοινωνικές επαφές τους, μέσω της εφαρμογής Beacon στο Facebook. Σύμφωνα με την κατηγορητήρια αρχή, η δημοσιοποίηση της πληροφορίας αυτής παρά την θέληση των χρηστών, παραβίαζε τις παρακάτω πράξεις για την προστασία των πολιτών:

1. Video Privacy Protection Act
2. Electronic Communication Privacy Act
3. Computer Fraud and Abuse Act
4. California Consumer Legal Remedies Act
5. California Computer Crime Law

Η υπηρεσία Beacon, έκλεισε με σχετική απόφαση του δικαστηρίου τον Σεπτέμβριο του 2009 [6].

Ειδοποίηση για ευάλωτα σημεία

Ένας πάροχος διαδικτυακού υπολογιστικού πλέγματος, θα πρέπει να ενημερώνει τους πελάτες σχετικά με οποιαδήποτε προβλήματα που παρουσιάζονται και τους καθιστούν ευάλωτους. Είναι απαραίτητο να συνδράμουν με τέτοιο τρόπο ώστε να είναι σε θέση οι πελάτες να αντιληφθούν με ποιό τρόπο επηρεάζονται, και να τους παρέχουν λύσεις αν υπάρχουν όσο το δυνατόν πιο άμεσα. Ο αντίκτυπος οποιουδήποτε ζητήματος ασφαλείας είναι σημαντικός αν λάβουμε υπ'όψιν ότι σε συστήματα υψηλής πολυπλοκότητας όπως αυτά, οι διορθώσεις των προβλημάτων καθυστερούν να δωθούν, με αποτέλεσμα να

υπάρχουν μεγάλες πιθανότητες να εισέλθουν τα προβλήματα ασφαλείας στην πλατφόρμα των πελατών. Στην περίπτωση του διαδικτυακού υπολογιστικού πλέγματος της Amazon, η ψηφιακή υπογραφή που δημιουργούσε η συγκεκριμένη υλοποίησης hash, παρήγαγε δύο όμοια αποτελέσματα για δύο διαφορετικές εισόδους. Το κόστος από άποψη ασφάλειας ήταν μεγάλο καθώς απαιτήθηκαν 7.5 μήνες από την πρώτη παρατήρηση προκειμένου να διορθωθεί [4].

Απώλεια κλειδιών κρυπτογράφησης/κωδικών πρόσβασης

Η ανάγκη για καθορισμό αποτελεσματικών κωδικών πρόσβασης είναι μεγαλύτερη από ποτέ. Αρκεί να σκεφτούμε ότι η απκάλυψη ενός κωδικού πρόσβασης προχωράει πολύ πέρα από την όποια αμηχανία που θα έχει ο παθών σχετικά με την αποκάλυψη προσωπικών του δεδομένων στο ευρύ κοινό. Στην περίπτωση του διαδικτυακού υπολογιστικού πλέγματος έχουμε το ρίσκο της αποκάλυψης των ευαίσθητων δεδομένων ενός οργανισμού σε τρίτους. Ένα χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση του Twitter, όπου εκατοντάδες άκρως απόρρητοι φάκελοι που περιείχαν οικονομικά δεδομένα, δημοσιοποιήθηκαν στο ευρύ κοινό από hacker. Το άκρως ανησυχητικό είναι ότι μία ζημιά ενός τέτοιου μεγάλου μεγέθους προκλήθηκε με την ελάχιστη δυνατή προσπάθεια, με τις ελάχιστες δυνατές τεχνικές γνώσεις: Ο επιτιθέμενος εκμεταλλεύτηκε τον ανασφαλή μηχανισμό των ρυθμίσεων του ηλεκτρονικού ταχυδρομείου: πραγματοποιήσε την διαδικασία επανακαθορισμού του κωδικού πρόσβασης του ηλεκτρονικού ταχυδρομείου GMail, ο οποίος είχε ρυθμιστεί έτσι ώστε να αποστέλλει τον κωδικό πρόσβασης σε ένα δεύτερο ηλεκτρονικό ταχυδρομείο. Το δεύτερο αυτό ηλεκτρονικό ταχυδρομείο ήταν τύπου hotmail το οποίο όμως είχε λήξει, και έτσι ο επιτιθέμενος εύκολα πήρε αυτό το ηλεκτρονικό ταχυδρομείο υπο την κατοχή του και συνεπώς τον κωδικό πρόσβασης του συγκεκριμένου εργαζόμενου του Twitter. Έχοντας υπο την κατοχή του τον κωδικό πρόσβασης του GMail, ο επιτιθέμενος απέκτησε πρόσβαση και στον λογαριασμό του Twitter και αυτό λόγω της μεγάλης ομοιότητας των δύο αυτών κωδικών. Με αυτόν τον τρόπο απέκτησε πρόσβαση και στον οργανισμό Twitter δια μέσω του λογαριασμού αυτού και αντέγραψε τα έγγραφα [5]. Ακόμα και στην περίπτωση που χρησιμοποιούσαμε τεχνικές κρυπτογράφησης, αναδύονται ζητήματα απόδοσης του συστήματος. Ο Bruce Schneier έχει τονίσει ότι για μια κρυπτογράφηση μόνο των κλειδιών μιας διαδικτυακής αναζήτησης ο απαιτούμενος χρόνος επεξεργασίας αυξάνεται κατά ένα τρίς σε σχέση με αυτόν που στερείται της κρυπτογράφησης [8].

Μη αποτελεσματική διαχείριση κλειδιών

Η δημοσιοποίηση των προγραμματιστικών διεπαφών διαχείρισης των κλειδιών στο διαδίκτυο, είναι μία πρακτική που θα οδηγήσει σε προβλήματα ασφάλειας. Είναι αναγκαίο να ληφθούν μέτρα τα οποία θα λαμβάνουν υπ'όψιν τους την αυστηρά κατανομημένη δομή του διαδικτυακού υπολογιστικού πλέγματος καθώς και την δυνατότητα πρόσβασης δια μέσω του διαδικτύου. Δυστυχώς δεν υπάρχουν παγιωμένες τεχνικές για την διαχείριση κλειδιών [8].

Εξάρτηση σε συγκεκριμένο πάροχο (Lock-In)

Η τεχνολογία του διαδικτυακού υπολογιστικού πλέγματος είναι πολύ νέα και οι προσφερόμενες λύσεις στους πελάτες είναι περιορισμένες. Οι πάροχοι προσφέρουν εξειδικευμένα εργαλεία, υπηρεσίες και φορμά αρχείων τα οποία στερούνται συμμόρφωσης σε κάποια στάνταρντς (είναι τόσο νέα η τεχνολογία που ως επι το πλείστον δεν έχουν θεσπιστεί στανταρντς για πολλές περιπτώσεις). Το γεγονός αυτό δεσμεύει τον πελάτη με τον συγκεκριμένο πάροχο, καθώς δεν υπάρχει εύκολος τρόπος για αλλαγή παρόχου και μετατροπή των αρχείων του συγκεκριμένου φορμά στο φορμά του νέου παρόχου. Το κυριότερο, όταν υπάρχει ο τρόπος, αυτός είναι κοστοβόρος. Το κόστος εκπαίδευσης στα νέα εργαλεία είναι μεγάλο, και σε πολλές φορές η μετατροπή των αρχείων στην μορφή που υποστηρίζει ο νέος πάροχος είναι αδύνατη. Ακόμα και αν επιτευχθεί αυτό, ο πελάτης έχει να αντιμετωπίσει μια νέα πρόκληση: την ασυμβατότητα των προγραμματιστικών διεπαφών (APIs) μεταξύ των δύο παρόχων, πράγμα που επιφέρει την επαναδημιουργία των εφαρμογών του πελάτη, χρησιμοποιώντας τις νέες διεπαφές. Η αδυναμίας της φορητότητας των δεδομένων των πελατών μεταξύ διαφορετικών παρόχων, είναι εις βάρος του πελάτη, καθώς δεν είναι σε θέση να επιλέξει τον πάροχο που καλύπτει με τον καύτερο τρόπο τις ανάγκες του. Επιπλέον, ορισμένο πάροχοι βασιζόμενοι σε αυτήν την δέσμευση των πελατών, είναι δυνατό να εκμεταλευτούν τις συνθήκες αυτές και να αυξήσουν το κόστος χρήσης των εργαλείων τους [8].

Εξάντληση των πόρων

Το κύριο πλεονέκτημα της υποδομής του διαδικτυακού υπολογιστικού πλέγματος είναι η δυνατότητα να παρέχει στους πελάτες πρόσθετους πόρους κατ' απαίτηση. Από την άλλη πλευρά αυτή η ευελιξία μπορεί να αναδείξει την

πιθανότητα της μη δυνατότητας εξυπηρέτησης. Αυξημένες απαιτήσεις από πολλούς πελάτες για επεξεργαστική ισχύ, μνήμη, αποθηκευτικό χώρο μπορεί να προκαλέσει σοβαρή μείωση στην προσφερόμενη απόδοση και επίπεδο ποιότητας υπηρεσιών με τελικό ενδεχόμενο την άρνηση εξυπηρέτησης των πελατών. Αυτό θα μπορούσε να επιφέρει σοβαρές οικονομικές ζημιές τόσο στους πελάτες, αλλά και στους παρόχους [8].

Αδυναμίες της διαχείρισης της υποδομής

Το γεγονός ότι οι πάροχοι προσφέρουν πόρους δια μέσω του διαδικτύου, εισάγει το ρίσκο της μη εξουσιοδοτημένης διαχείρισης δεδομένων πελατών αξιοποιώντας αδυναμίες των προγραμμάτων περιήγησης. Επιπλέον, ή όλη υποδομή στηρίζεται στην συνεχή μεταφορά δεδομένων μεταξύ των πελατών και παρόχων, πράγμα που αυξάνει την πιθανότητα να εμφανιστεί ένας επιτιθέμενος στο επικοινωνιακό κανάλι και να ασκήσει κάθε μορφή επίθεσης. Η συνδέση VPN προσφέρει υψηλά επίπεδα ασφάλειας, αλλά πολλοί πάροχοι δεν την ενστερνίζονται στις υλοποιήσεις τους. Ο Hypervisor, το υπόστρωμα λογισμικού το οποίο "φιλοξενεί" τα λειτουργικά συστήματα των πελατών είναι στόχος επίθεσης, όπου οι επιτιθέμενοι ασκούν επίθεση δια μέσω των εφαρμογών λογισμικού που προσφέρει ο πάροχος (SaaS) μέσα από εικονικές μηχανές (IaaS) αλλά και από το περιβάλλον εκτέλεσης και ανάπτυξης εφαρμογών (PaaS). Επιτυχημένη επίθεση στον Hypervisor, έχει ως αποτέλεσμα την δυνατότητα πρόσβασης στα δεδομένα πελατών και την ακύρωση της εμπιστευτικότητας και της ακεραιότητας. Οι επιτιθέμενοι είναι δυνατό να επηρεάσουν σε τέτοιο βαθμό την προσφερόμενη ποιότητα υπηρεσιών, προκαλώντας τεχνητά το φαινόμενο της άρνησης εξυπηρέτησης (denial of service) και κατά συνέπεια ακόμα και την οικονομική καταστροφή της εταιρείας που στηρίζεται εξ ολοκλήρου στον πάροχο για την επεξεργασία των δεδομένων της. Είναι αξιοσημείωτο, ότι οι hypervisors έχουν εγγενείς αδυναμίες οι οποίες δεν έχουν εξιχνιαστεί όλες, και οι οποίες είναι δυνατόν να προσφέρουν σε απλούς χρήστες δικαιώματα διαχειριστή του δικτύου, και συνεπώς αυτοί να έχουν καθολική πρόσβαση στον υπόστρωμα του Hypervisor και σε όλες τις εικονικές μηχανές των πελατών [8].

Κατάχρηση της υπηρεσίας του Διαδικτυακού Πλέγματος

Οι πάροχοι διαδικτυακού πλέγματος ακολουθούν την τακτική της "διαφήμισης" της υποδομής τους, προσφέροντας την δυνατότητα να την χρησιμοποιήσει οποιοσδήποτε κατέχει πιστωτική κάρτα. Πολλοί από αυτούς μάλιστα προσφέρουν και δωρεάν περιόδους δοκιμαστικής χρήσεως. Η ανωνυμία που προσφέρει αυτή η πολιτική των παρόχων, δίνει πεδίο δράσης σε κακόβουλους οι οποίοι δύνανται να ασκήσουν οποιαδήποτε μορφή επίθεσης μετά την εγγραφή τους στο σύστημα. Επιθέσεις περιλαμβάνουν: άρνηση εξυπηρέτησης, εγκατάσταση κακόβουλου λογισμικού, spamming, botnets, εύρεση κωδικών πρόσβασης.

Για την αντιμετώπιση αυτών των προβλημάτων, προτείνεται μία πιο αυστηρή διαδικασία εγγραφής στο πλέγμα, η οποία θα περιλαμβάνει αρκετές πληροφορίες για τον αιτούντα. Επίσης θα πρέπει να επιτελείται λεπτομερής έλεγχος στην δηλωμένη πιστωτική κάρτα με σκοπό την ανίχνευση πιθανής απάτης. Τέλος συστήνεται η λειτουργία συστήματος καταγραφής διαδικτυακής κίνησης από τον κάθε πελάτη και μελέτη των ενεργειών του. [9]

Μη ασφαλείς διεπαφές επικοινωνίας

Οι πάροχοι, προσφέρουν διεπαφές για χρήση από τους πελάτες ούτως ώστε να εκτελούν τμήματα της υπηρεσίας που προσφέρουν για χρήση. Η όλη ασφάλεια του παρόχου στηρίζεται στο πόσο ασφαλή είναι όλες οι δημοσιευμένες διεπαφές. Θα πρέπει να είναι υλοποιημένες με τέτοιο τρόπο ώστε ο επιτιθέμενος να μην μπορεί να παρακάμψει πολιτικές ασφαλείας και να λάβει πρόσβαση σε τομείς που δεν είναι εξουσιοδοτημένος.

Ως παραδείγματα μπορούμε να αναφέρουμε την δυνατότητα για ανώνυμη πρόσβαση, επαναχρησιμοποίηση κωδικών πρόσβασης, κακογραμμένων πολιτικών πρόσβασης. Οι πολιτικές πρόσβασης αποτελούν ένα κομβικό σημείο για την ασφάλεια του συστήματος, καθώς πρέπει να είναι καλώς ορισμένες προκειμένου να μην έχουμε φαινόμενα εξουσιοδότησης σε τρίτους. Σε αυτό το σημείο είναι που παίζει ρόλο η υιοθέτηση πρότυπων μηχανισμών αυθεντικοποίησης/εξουσιοδότησης που συντηρούνται και εξελίσσονται από ομάδες εταιρειών και πανεπιστημιακών. Αυτά τα πρότυπα προσφέρουν μία λειτουργικότητα η οποία σε σχέση με ένα εξειδικευμένο σύστημα ενός παρόχου προσφέρει:

- λιγότερες αδυναμίες
- άμεσες διορθώσεις στις εκάστοτε παρατηρούμενες αδυναμίες
- εκτενής έλεγχος της λειτουργικότητας εξ αιτίας της ευρείας χρήσης τους με συνέπεια την παραγωγή ασφαλέστερης υλοποίησης

Για την αντιμετώπιση αυτών των προβλημάτων απαιτείται εντατική μελέτη της αρχιτεκτονικής ασφαλείας που υλοποιούν οι διεπαφές και επιβεβαίωση ότι χρησιμοποιείται επαρκώς η κρυπτογράφηση, ισχυρή αυθεντικοποίηση, καθώς και καταγραφή των ενεργειών.

Η ασφάλεια στον Διαχειριστή Εικονικών Μηχανών (Hypervisor)

Ο διαχειριστής εικονικών μηχανών, ή εν συντομία ΔΕΜ στην παρούσα εργασία, επιτρέπει την ταυτόχρονη εκτέλεση και λειτουργία εικονικών λειτουργικών συστημάτων σε κοινούς υλικούς πόρους. Για παράδειγμα αν υποθέσουμε ότι ένας πάροχος, έχει πελάτες με αντικρουόμενα συμφέροντα στην υποδομή του, οι τελευταίοι θα έχουν εικονικές μηχανές που θα λειτουργούν πάνω στην ίδια πλατφόρμα υλικού. Οι επιθέσεις πραγματοποιούνται σε επίπεδο εικονικής μηχανής, όπου μία εικονική μηχανή επιτίθεται σε μία άλλη εκμεταλλευόμενη τις τυχόν αδυναμίες του ΔΕΜ και αποσπά κρίσιμες πληροφορίες των οποίων η διατήρηση της ιδιωτικότητας κρίνεται απαραίτητη για την βιωσιμότητα της επιχείρησης.

Ο ΔΕΜ αποτελεί ένα περίπλοκο σύστημα τεράστιας υποδομής σε όγκο λογισμικού, καθιστώντας το έτσι ευάλωτο προς επιθέσεις. Αρκεί να αναλογιστούμε ότι η πλατφόρμα του Xen ΔΕΜ συγκροτείται από 200.000 γραμμές κώδικα, 600.000 γραμμές ο προσομοιωτής και 1.000.000 γραμμές το μητρικό λειτουργικό σύστημα. Αν σκεφτεί κανείς ότι τα σημερινά εργαλεία πιστοποίησης κώδικα διαχειρίζονται όγκο κώδικα της τάξης των 10.000 γραμμών, συμπεραίνουμε ότι η ποιότητα λογισμικού ενός ΔΕΜ δεν είναι και δεν δύναται να ελεγθεί επαρκώς. [10] Η παραβίαση ασφαλείας ενός ΔΕΜ ισοδυναμεί με παραβίαση όλων των εικονικών μηχανών που εξυπηρετεί, πράγμα που επιβάλλει την άμεση λήψη βέλτιστων μέτρων ασφαλείας για ένα ΔΕΜ. Αναφορικά, τα εικονικά συστήματα έχουν εισάγει 259 νέα κενά ασφαλείας τα τελευταία 5 χρόνια. Επίσης έχουν υλοποιηθεί και δημοσιευτεί επίσημα, 36 εργαλεία επίθεσης σε τέτοια συστήματα [11].

Χαρακτηριστικό παράδειγμα εφαρμογής της παραβίασης ενός ΔΕΜ είναι η περίπτωση του ερευνητή Jon Oberheide του πανεπιστημίου του Michiegan. Ο κ. Oberheide ανάπτυξε ένα εργαλείο με το όνομα Xensploit, το οποίο επιτρέπει στον επιτιθέμενο να πάρει τον έλεγχο του Xen ΔΕΜ, και στην συνέχεια να υποκλέψει ευαίσθητες πληροφορίες από όλα τα εικονικά μηχανήματα που ευρίσκονται σε λειτουργία. Το εργαλείο εκμεταλεύεται την διαδικασία του Live Migration των

εικονικών μηχανών. Σύμφωνα με αυτήν την διαδικασία, μία εικονική μηχανή μεταφέρεται από ένα εξυπηρετητή σε κάποιον άλλον για λόγους ισόνομης κατανομής φορτίου στους εξυπηρετητές του παρόχου. Η μεταφορά των δεδομένων που συγκροτούν την εικονική μηχανή μεταφέρονται σε μη κρυπτογραφημένη μορφή (clear text). Κατά συνέπεια αυτό δίνει βήμα σε επιτιθέμενο που έχει εισβάλλει στην γραμμή επικοινωνίας να υποκλέψει δεδομένα. Το Xensploit πραγματοποιεί μία επίθεση στον μηχανισμό αυθεντικοποίησης του SSH μεταβάλλοντας την μνήμη της διεργασίας SSH (SSH Daemon) κατά την εκτέλεση του Live Migration μίας εικονικής μηχανής. Η μεταβολή αυτή επιτρέπει στην απόδοση πλήρους πρόσβασης στον επιτιθέμενο [12].

Λύσεις για αυτές τις αδυναμίες είναι η επιβολή ενός πιο αυστηρού μοντέλου αυθεντικοποίησης, αναγκάζοντας τον χρήστη να αυθεντικοποιηθεί προτού λειτουργήσει η εικονική μηχανή στον νέο εξυπηρετητή. Άλλη λύση είναι να εφαρμοστεί κρυπτογράφηση στα δεδομένα, ή και χρήση ξεχωριστού φυσικού ή εικονικού (VPN) δικτύου για την διαδικασία του Live Migration.

Για τον περιορισμό αυτών των κενών ασφαλείας που ευρίσκονται στον ΔΕΜ, υπάρχουν διάφορες προτάσεις στην βιβλιογραφία. Έχουν διατυπωθεί ιδέες όπως λογισμικό που φροντίζει τον έλεγχο ασφάλειας του ΔΕΜ, περιορισμός της λειτουργικότητας του ΔΕΜ ώστε να ελαττωθεί το εύρος των διαθέσιμων ανοιγμάτων για επίθεση ή και ακόμα και νέες αρχιτεκτονικές επεξεργαστή. Η πιο χαρακτηριστική και πιο πολλά υποσχόμενη θεωρούμε ότι είναι η αρχιτεκτονική NoHype [13], με την οποία καθορίζεται μία μεθοδολογία για λειτουργία των εικονικών μηχανών απευθείας στο υλικό καταργώντας την αναγκαιότητα της ύπαρξης του ΔΕΜ για ένα σύνολο ενεργειών των οποίων η δράση αφήνει περιθώρια για επίθεση. Ενέργειες όπως η κατανομή μνήμης και πυρήνων επεξεργαστών επιτελείται από το ΔΕΜ σε ένα τυπικό σύστημα εικονικού συστήματος. Με την αρχιτεκτονική NoHype η κατανομή αυτή γίνεται εκ των προτέρων, απαλλάσσοντας το ΔΕΜ από αυτά τα καθήκοντα. Το αποτέλεσμα είναι η δραστική μείωση του εύρους της απειλής καθώς η επικοινωνία μεταξύ του εικονικού μηχανήματος και του ΔΕΜ περιορίζεται στο ελάχιστο. Η επικοινωνία των δύο είναι σημαντικός παράγοντας κινδύνου, αφού μετά την διακοπή λειτουργίας του εικονικού μηχανήματος, παραδίδεται ο έλεγχος στο ΔΕΜ μέσα από μία κλασσική επικοινωνία αίτησης-απόκρισης μεταξύ ΔΕΜ και εικονικής μηχανής. Η επικοινωνία αυτή, προσφέρει δυνατότητα για επίθεση από ενδιάμεσο χρήστη.

Επιπλέον αποφεύγεται η χρήση εικονικών πόρων εισόδου-εξόδου, αλλά προτιμάται η επιλογή αντίστοιχων φυσικών πόρων για κάθε εικονική μηχανή. Με αυτόν τον τρόπο οι εικονικές μηχανές περιορίζονται στο να προσπελαύνουν μόνο τους πόρους εισόδου-εξόδου με τους οποίου είναι άμεσα συνδεδεμένοι, και όχι με αντίστοιχους άλλων εικονικών μηχανών. Ένας επιπρόσθετος παράγοντας που οδηγεί στην

επικοινωνία ΔΕΜ και εικονικής μηχανής, και ο οποίος μπορεί να εξαλειφθεί, είναι η αίτηση μίας εικονικής μηχανής για αποστολή πληροφοριών υλικού. Αν αυτές οι πληροφορίες αποθηκευτούν σε προσωρινή μνήμη, τότε καταργείται η αναγκαιότητα επικοινωνίας ΔΕΜ και εικονικής μηχανής.

Ένα άλλο σημείο που χρήζει προσοχής, είναι η ίδια η φύση του δικτύου. Σε ένα φυσικό δίκτυο, οι πιο ευάλωτοι σταθμοί εργασίας μπορούν να ανιχνευτούν εύκολα και να εγκαταστήσουμε διορθώσεις. Σε ένα δίκτυο εικονικών μηχανών όμως, οι ευάλωτες εικονικές μηχανές είναι δυνατόν να παύσουν προτού ανιχνευτεί η όποια δυσλειτουργία από τον διαχειριστή του συστήματος. Εν τω μεταξύ θα έχουν μολύνει άλλες εικονικές μηχανές, και αν λάβουμε υπ'όψιν ότι το μέγεθος της βάσης των εικονικών μηχανών είναι εξαιρετικά μεγάλο, λόγω της μεγάλης ευκολίας της δημιουργίας αυτών, οι διαστάσεις του προβλήματος μεγενθύνονται σημαντικά. Ο αριθμός των εικονικών μηχανών, αλλά και η ποικιλία των λειτουργικών συστημάτων καθώς και των εκδόσεων του. Το γεγονός αυτό, καθιστά δύσκολη την επίβλεψη και την επιτέλεση της συντήρησης σε επίπεδο λογισμικού από τους διαχειριστές του δικτύου. Αυτό που παρατηρείται είναι είτε να αμελείται η συντήρηση των εικονικών μηχανών - εως και το 60% των εικονικών μηχανών είναι λιγότερο ασφαλή από τα φυσικά μηχανήματα [14], είτε να περιορίζεται δραστικά ο αριθμός των διαθέσιμων εικονικών μηχανών ούτως ώστε να είναι πιο εφικτή η διαχείριση τους. Όμως στην τελευταία περίπτωση καταργούμε ένα βασικό πλεονέκτημα του εικονικού περιβάλλοντος σε σχέση με το φυσικό.

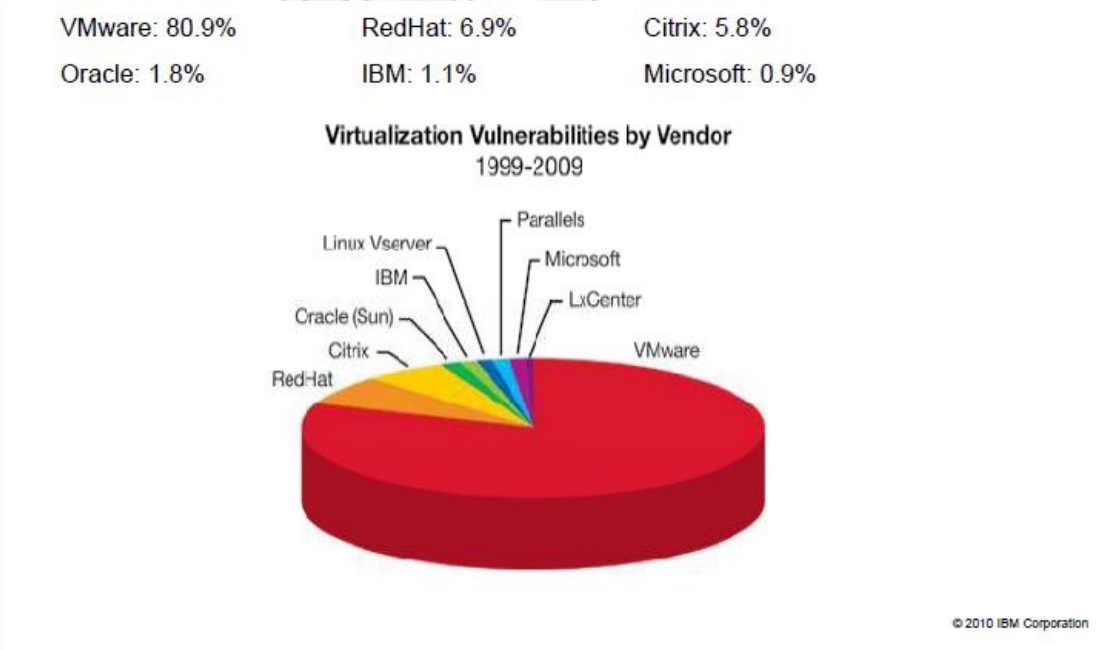
Πρόβλημα ασφαλείας παρουσιάζεται και με την δυνατότητα να επαναφέρουμε έκαστο εικονικό μηχάνημα σε πρότερη κατάσταση με σκοπό να απαλείψουμε λάθη στην διαμόρφωση του συστήματος. Η επαναφορά αυτή σε μία προηγούμενη κατάσταση, φέρνει στο προσκήνιο μία έκδοση του λειτουργικού συστήματος χωρίς τις διορθώσεις ασφαλείας, και πιθανόν την επαναφορά κακόβουλου λογισμικού. Ο επιτιθέμενος μπορεί να εκμεταλευτεί την παρουσία της πρότερης κατάστασης, ώστε να εισέλθει στο σύστημα χρησιμοποιώντας κωδικούς πρόσβασης που είχε υποκλέψει και ισχύαν για το συγκεκριμένο αποτύπωμα της εικονικής μηχανής.

Η δυναμικότητα των εικονικών μηχανών, η οποία εκφράζεται με την διαδικασία της συνεχούς μετακίνησης τους σε διαφορετικούς εξυπηρετητές, δυσκολεύει τους διαχειριστές στο έργο της ανίχνευσης των μηχανών που έχουν κενά ασφαλείας. Στην βιβλιογραφία προτείνεται η δημιουργία ενός υποστρώματος μεταξύ της εικονικής μηχανής και του ΔΕΜ, το οποίο θα επιτελεί λειτουργίες διαχείρισης ασφάλειας. Η κεντρικοποίηση αυτών των λειτουργιών με την απεμπλοκή τους από τις εικονικές μηχανές διευκολύνει τους διαχειριστές στην συντήρηση των. Δεν υπάρχει εξάρτηση από το συγκεκριμένο λογισμικό και λειτουργικό σύστημα που χρησιμοποιεί η κάθε εικονική μηχανή. Επιπλέον είναι δυνατόν να αποθηκεύουμε κρίσιμους μηχανισμούς ασφάλειας, όπως αυθεντικοποίηση, ή αποθήκευση

καταστάσεων συστήματος, όπως βάσεις δεδομένων των χρηστών, κανόνες τείχους προστασίας, στο εξωτερικό υπόστρωμα. Αυτό το υπόστρωμα θα αποτελείται από ένα σύνολο εξυπηρετητών το οποίο θα διαχωρίζεται από το υπόλοιπο δίκτυο μέσω τείχων προστασίας ή με την χρήση ενός δρομολογητή. Η όποια επικοινωνία θα επιτελείται με την χρήση της κρυπτογράφησης, και η πρόσβαση θα είναι περιορισμένη στους απολύτως απαραίτητους διαχειριστές. Οποιαδήποτε επαναφορά της εικονικής μηχανής του υπολοίπου δικτύου σε πρότερη κατάσταση, δεν θα επηρεάσει τα μέτρα ασφαλείας του συστήματος. Χρήση συγκεκριμένων εικονικών μηχανών για την εγκατάσταση λογισμικού τρίτων κατασκευαστών είναι μία λύση για την αποφυγή του κενού ασφαλείας με τυχούσα εγκατάσταση προβληματικού κώδικα.

Τα εικονικά μηχανήματα, θα πρέπει να είναι συμβατά με κάποιο εξελιγμένο και πρότυπο μηχανισμό ελέγχου πρόσβασης, να έχουν ενεργοποιημένο τείχος προστασίας, και να εφαρμόζεται κρυπτογράφηση, όπου είναι δυνατόν. Οι απολύτως απαραίτητες εργασίες θα πρέπει να είναι ενεργοποιημένες, και οπωσδήποτε θα πρέπει να είναι ενεργοποιημένος ο καταγραφέας ενεργειών για την ενημέρωση των διαχειριστών, σχετικά με τις ενέργειες του χειριστή της εικονικής μηχανής [15].

Ως σημείο αναφοράς για τα επίπεδα ασφάλειας των ΔΕΜ, η παρακάτω εικόνα απεικονίζει τις αδυναμίες διαφόρων προιόντων εταιρειών. Αξιοσημείωτα είναι τα χαμηλά ποσοστά για Oracle, IBM και Microsoft [11].



Εικόνα 2: Αδυναμίες ασφάλειας στα ΔΕΜ

Εξόρυξη δεδομένων

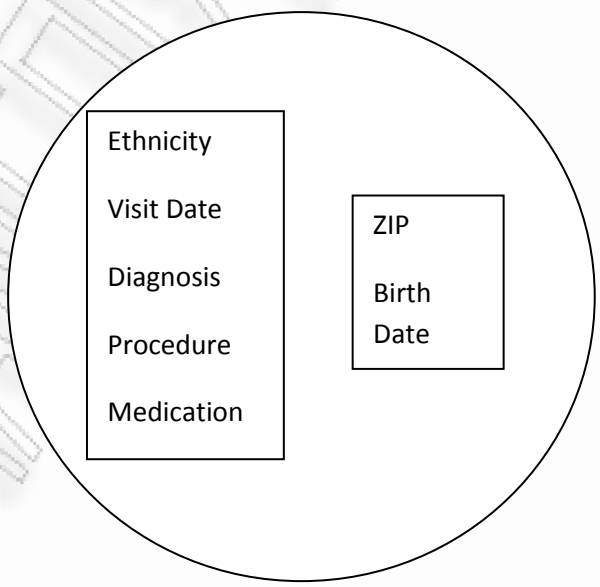
Η ανάπτυξη του διαδικτυακού υπολογιστικού πλέγματος έχει σαν φιλοσοφία την συνεύρεση δεδομένα διαφορετικών πελατών στις εγκαταστάσεις του παρόχου της υπηρεσίας. Το απότελεσμα είναι η δημιουργία μίας βάσης δεδομένων τεραστίου μεγέθους. Τέτοιες βάσεις δεδομένων, αποτελούν την ιδιαίτερη αδυναμία φορέων που αποσκοπούν στην εξόρυξη δεδομένων και ανάλυση τους, με σκοπούς είτε για να προβάλλουν τις κατάλληλες διαφημίσεις που ταιριάζουν στο προφίλ του ιδιοκτήτη των δεδομένων είτε για βιομηχανική κατασκοπεία. Η πιο γνωστή εταιρεία που προβάλλει διαφημίσεις στηριζόμενη σε αυτό το μοντέλο είναι η Google. Η τελευταία μάλιστα χρησιμοποιεί το ίδιο το εργαλείο διαδικτυακής αναζήτησης για να προβάλλει διαφημίσεις που ταιριάζουν με το περιεχόμενο των αναζητήσεων του χρήστη. Η «εξόρυξη δεδομένων» και η αποκόμιση πληροφοριών που συνεπάγεται με την χρήση αυτής της πρακτικής είναι αποτέλεσμα της τεχνολογικής εξέλιξης των τελευταίων χρόνων. Οι αυξημένες δυνατότητες των υπολογιστικών συστημάτων όσον αφορά την επεξεργασία της πληροφορίας, τον αποθηκευτικό τους χώρο, την δικτύωση τους η οποία επιτρέπει την πρόσβαση σε βάσεις δεδομένων διεσπαρμένες σε όλα τα πλάτη και μήκη της γης, συνδράμουν στην εξόρυξη δεδομένων και διεξαγωγή συμπερασμάτων. Ενώ στο παρελθόν η δομή της πληροφορίας ήταν σε στατιστική μορφή επονομαζόμενη και ως «μακροπληροφορία» σήμερα σε πολλές περιπτώσεις αναφερόμαστε στην λεγόμενη «μικροπληροφορία», δηλαδή αναλυτική πληροφορία η οποία μπορούμε να την επεξεργαστούμε περαιτέρω με τον τρόπο που επιθυμεί ο χρήστης και να εξάγει τα ανάλογα επιθυμητά αποτελέσματα που στοχεύει η έρευνα του. Συμπερασματικά έχουμε περάσει από την εποχή της προεπεξεργασμένης πληροφορίας, στην αναλυτική πληροφορία όπου μπορούν οι ιδιώτες να την επεξεργαστούν. Αυτό που πρέπει να σημειωθεί είναι ότι η εξόρυξη δεδομένων δεν αποτελεί ενα αναγκαίο κακό, απόρροια της εξέλιξης της τεχνολογίας και της κοινωνικής δικτύωσης. Είναι μία χρήσιμη διαδικασία η οποία στα χέρια των οικονομολόγων και ερευνητών προσφέρει στην καινωνική οικονομική και τεχνολογική πρόοδο. Η δομή της μικροπληροφορίας είναι τόσο αναλυτική η οποία αποκαλύπτει ανθρώπινα προσωπικά δεδομένα. Για αυτόν τον λόγο κρίνεται επιτακτική η ανάγκη για απόκρυψη της ταυτότητας των ανθρώπων που χαρακτηρίζονται από τις πληροφορίες.

Η εξόρυξη δεδομένων είναι μία δυνατότητα η οποία πρέπει να παρέχεται – είναι δύσκολο να φανταστούμε το έργο των σημερινών ερευνητών φαρμακοβιομηχανίας αν δεν έχουν στα χέρια τους αναλυτικές φόρμες με την αντίδραση των ασθενών στην χορήγηση φαρμάκων, επιπλοκές, παρενέργειες κλπ. Για αυτό τον λόγο αυτό

που επιβάλλεται να κάνει κάθε φορέας που δημοσιεύει βάσεις δεδομένων, είναι να αφαιρεί την πληροφορία που ταυτοποιεί μία ανθρώπινη οντότητα από τις επιμέρους πληροφορίες.

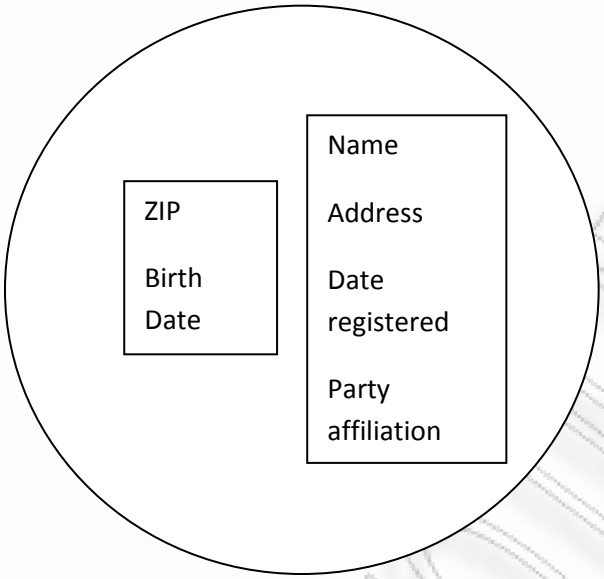
Δυστυχώς οι φορείς όσο και καλή θέληση να έχουν, πολλές φορές παρερμηνεύουν το θέμα της εξασφάλισης της ανωνυμίας. Ως επι το πλείστον το θεωρούν κάτι απλό και προφανές, με αποτέλεσμα στην πλειονότητα των περιπτώσεων να υποστηρίζουν ότι μία απλή διαγραφή του ονοματεπώνυμου του ασθενούς από τον ιατρικό φάκελο εξασφαλίζει την απόλυτη ανωνυμία. Το πρόβλημα είναι ότι κοινοποιούν πληροφορία η οποία μοιάζει ανώνυμη. Και φυσικά επειδή θεωρείται ανώνυμη, είναι και νόμιμο να δημοσιευτεί. Χαρακτηριστικό παράδειγμα αποτελεί η νομοθετική ρύθμιση σε 37 πολιτείες της Αμερικής όπου επιτρέπει την δημοσίευση ανώνυμων ιατρικών δεδομένων. Ο φορέας, βασιζόμενος στην *υπόθεση* ότι τα δεδομένα που στερούνται ονοματεπώνυμου, διεύθυνσης και τηλεφώνου είναι ανώνυμα, τα δημοσιεύει. Η υπόθεση αυτή είναι εσφαλμένη γιατί μελέτες έχουν αποκαλύψει ότι έμμεσοι προσδιοριστές όπως ο *ταχυδρομικός κώδικας*, το *φύλο* και η *ημερομηνία γέννησης* μπορούν να προσδιορίσουν μοναδικά το 87% του πληθυσμού των Η.Π.Α. Είναι σύνηθες να περιέχονται αυτοί οι προσδιοριστές σε δημοσιευμένους ιατρικούς φακελους.

Άπαξ και δημοσιευτούν τα δεδομένα σε αυτήν την μορφή, η επαναταυτοποίηση των δεδομένων είναι εύκολη υπόθεση. Αυτό έχει πραγματοποιηθεί στα πλαίσια μίας έρευνας στην Μασαχουσέτη. Η Group Insurance Commission πούλησε ιατρικούς φακέλους στην βιομηχανία και προσέφερε μία κόπια τους ερευνητές. Τα δεδομένα είχαν τα εξήςπροσδιοριστικά:



Εικόνα 3: "Ανώνυμα" Δεδομένα Ιατρικού Φακέλου

Ο ερευνητής στην συνέχεια αγόρασε με το ποσο των $20 την λίστα των δημοτών που ψηφίσαν:

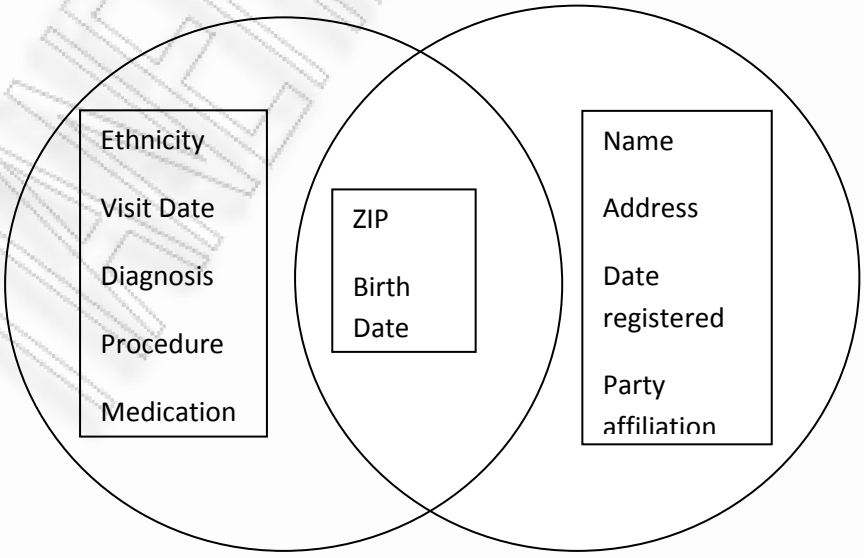


Εικόνα 4:Λίστα δημοτών που ψηφισαν

Παρατηρούμε ότι και οι δύο πίνακες μοιράζονται τα εξής προσδιοριστικά:

- Ταχυδρομικός κώδικας
- Ημερομηνία γέννησης
- Φύλο

Πραγματοποιώντας μία σύνδεση των πινάκων χρησιμοποιώντας αυτήν την τριάδα η οποία προσδιορίζει το 87% του πληθυσμού των Η.Π.Α μπορούμε να επαναταυτοποιήσουμε τους ασθενείς:



Εικόνα 5: Διασύνδεση πινάκων και επαναταυτοποίηση

Χαρακτηριστικό παράδειγμα απο τελεί ο William Weld πρωην κυβερνήτης της Μασαχουσέτης. Συμφωνα με το δημοτολόγιο 6 άνθρωποι με αυτό το όνομα είχαν γεννηθεί την ίδια ημερομηνία από τους οποίους οι 3 ήταν άντρες και ο ένας – ο ίδιος – ζούσε στην περιοχήμε τον συγκεκριμένο ταχυδρομικό κώδικα. Ο ιατρικός φάκελος του πρωην κυβερνήτη ήταν γνωστός πλέον στον ερευνητή.

Κλασσικά ζητήματα ασφάλειας και ιδιωτικότητας που συναντώνται στο διαδικτυακό πλέγμα

Αυθεντικοποίηση

Με την αυθεντικοποίηση, διαχειριζόμαστε τα διαπιστευτήρια των χρηστών και επαληθεύουμε την ύπαρξη του χρήστη στο σύστημα. Χρήζει προσοχής, η διαφύλαξη των κωδικών πρόσβασης, ψηφιακών πιστοποιητικών και γενικότερα των δυναμικά δημιουργούμενων διαπιστευτηρίων. Η απώλεια του κωδικού πρόσβασης έχει ιδιαίτερα μεγάλες επιπτώσεις, καθώς είναι δυνατό να είναι κοινό για ένα σύνολο υπηρεσιών σε όλο το πλέγμα. Κλασσικές τακτικές υποκλοπής, μέσω της παραπομπής σε κακόβουλες ιστοσελίδες που είτε ζητούν τα διαπιστευτήρια, είτε εγκαθιστούν κακόβουλο λογισμικό υποκλοπών, βρίσκουν πεδίο εφαρμογής και στο διαδικτυακό πλέγμα.

Προτεινόμενα μέτρα για την ασφαλή Αυθεντικοποίηση

Εφαρμογές που χρήζουν αυξημένων μέτρων προστασίας θα πρέπει να χειρίζονται κωδικούς πρόσβασης που αλλάζουν σε κάθε συνέδρια σύνδεσης με τον διακομιστή. Εναλλακτικά, προτείνεται η χρήση ψηφιακών πιστοποιητικών. Μία άλλη λύση είναι η χρήση αυστηρής αυθεντικοποίησης πολλαπλών κριτηρίων (για παράδειγμα απαίτηση κωδικού και εξαψήφιου αριθμού παραγόμενου από εξειδικευμένη συσκευή).

SaaS/PaaS

Για την περίπτωση του οργανισμού, οι χρήστες προτείνεται να αυθεντικοποιούνται μέσω ενός διαχειριστή ταυτοτήτων και να εδραιώνουν σχέση εμπιστοσύνης με το πάροχο λογισμικού εφαρμογής ως υπηρεσία (SaaS).

Ο χρήστης θα πρέπει να δύναται να αυθεντικοποιείται σε πολλαπλές τοποθεσίες με την χρήση ενός μοναδικού διαπιστευτηρίου.

Iaas

Στην υποδομή ως υπηρεσία έχουμε δύο ομάδες χρηστών: το προσωπικό που διαχειρίζεται την υποδομή του δικτύου και το προσωπικό που χρησιμοποιεί τις εφαρμογές. Για την αυθεντικοποίηση των χρηστών, το λόγο έχει ο ίδιος ο οργανισμός και η πιο συνηθισμένη λυση είναι η χρήση ενός εικονικού δικτύου. Αυτή σε συνδιασμό ενός μηχανισμού Μοναδικής Εισόδου (Single Sign On) ή LDAP τύπου αυθεντικοποίησης ισχυροποιούν την ασφάλεια του συστήματος. Στην περίπτωση που δεν μπορεί να εφαρμοστεί ένα εικονικό δίκτυο, τότε εναλλακτικά μπορεί να χρησιμοποιηθεί κρυπτογράφηση με SSL και χρήση SAML για επικοινωνία αιτημάτων αυθεντικοποίησης. Με αυτήν την λύση, ο οργανισμός μπορεί να εξασφαλίσει διαλειτουργικότητα με υπηρεσίες που ευρίσκονται εκτός του οργανισμού. Το OpenID αποτελεί μία εναλλακτική λύση, αλλά απαιτεί την αποθήκευση των διαπιστευτηρίων εκτός του οργανισμού. Για αυτόν τον λόγο, συστήνεται να δίνεται περιορισμένη πρόσβαση σε εξωτερικούς χρήστες που αυθεντικοποιούνται.

Για την περίπτωση που επιλεγεί να εμπεριέχεται ο μηχανισμός αυθεντικοποίησης των χρηστών εντός της εφαρμογής, θα πρέπει να ακολουθηθεί ένα ανοιχτό πρότυπο όπως το OATH.Με αυτόν τον τρόπο θα αποφευχθεί ο κίνδυνος εξάρτησης του οργανισμού από τον συγκεκριμένο πάροχο υπηρεσιών πλέγματος.

Ιδιωτικά Πλέγματα

Στα ιδιωτικά πλέγματα, προτείνεται να διαχωρίζεται ο μηχανισμός αυθεντικοποίησης από τις εφαρμογές, αλλά να ευρίσκεται εντός του οργανισμού. Η χρήση ενός συστήματος Μοναδικής Εισόδου(Single Sing On) και Πρόσβασης μέσω Ιστού (Web Access Management) προσφέρουν, πέρα από την λειτουργικότητα της αυθεντικοποίησης, την δυνατότητα διαχείρισης των κωδικών πρόσβασης αλλά και μηχανισμούς για την διαχείριση του συστήματος.

Ισχυρή Αυθεντικοποίηση

Η ισχυρή αυθεντικοποίηση είναι η αυθεντικοποίηση που επιτελείται με την χρήση πολλαπλών παραμέτρων ή χρησιμοποιείται η κρυπτογράφηση. Συστήματα Έξυπνων Καρτών, και Κέρβερου είναι τα πιο αντιπροσωπευτικά παραδείγματα που αξιοποιούν πολυπαραμετρική αυθεντικοποίηση. Αυτά χρησιμοποιούνται σε

εσωτερικά δίκτυα οργανισμών, και προτείνεται η χρήση τους και σε πλατφόρμα τύπου Υποδομής ως Υπηρεσία (IaaS) για την πιο ασφαλή διαχείριση των πόρων .

Οι πάροχοι υπηρεσιών διαδικτυακού πλέγματος, θα πρέπει να υποστηρίζουν μηχανισμούς ισχυρής αυθεντικοποίησης όπως μεταβαλλόμενους κωδικούς σε κάθε συνεδρία, βιομετρικούς ελέγχους, ψηφιακά πιστοποιητικά και Κέρβερο.

Προτείνεται η απεμπλοκή του μηχανισμού αυθεντικοποίησης από την εφαρμογή, και ανάθεση αυτής σε μία συγκεκριμένη αυτόνομη υπηρεσία εντός του οργανισμού που ευρίσκεται η εφαρμογή. Ο διαχωρισμός του συστήματος αυθεντικοποίησης και της εφαρμογής θα πρέπει να συνοδεύεται με χρήση κοινών προτύπων επικοινωνίας όπως για παράδειγμα επικοινωνία μέσω κουπονιών συμβατά με SAML, πράγμα που διευκολύνει την μετάβαση της όλης λειτουργικότητας, σε εξωτερικό πάροχο διαδικτυακού πλέγματος αν αυτό κριθεί αναγκαίο.

Ενοποίηση Ταυτοτήτων

Η ενοποίηση ταυτοτήτων επιτρέπει την συνεργασία πολλαπλών οργανισμών και την διαμοιρασμό των υπηρεσιών τους, προσφέροντας δυνατότητα για μοναδική είσοδο. Το μοντέλο αποτελείται από ένα πάροχο ταυτοτήτων και ένα πάροχο υπηρεσιών οι οποίοι ανταλάσσουν μεταξύ τους στοιχεία ταυτοποιήσης.

Μοναδική Είσοδος (Single Sign On)

Με την συμμετοχή του σε ένα διαδικτυακό πλέγμα, ένας οργανισμός θα πρέπει να λάβει υπ'όψιν του την επέκταση της χρήσης του μηχανισμού μοναδικής εισόδου σε εφαρμογές εκτός των ορίων του.

Μεμονωμένοι Χρήστες

Για τους μεμονωμένους χρήστες, η ταυτοποίηση μέσω ενός λογαριασμού Google ή Yahoo είναι επαρκής, αν και μπορεί να χρησιμοποιηθεί και το OpenID, με το οποίο χρησιμοποιεί ο χρήστης ένα και μοναδικό κωδικό πρόσβασης που συνδέεται με την ταυτότητα του, και όλοι οι υπόλοιποι ιστότοποι, χρησιμοποιούν την OpenID ταυτότητα του, καταργώντας την αναγκαιότητα για επιπλέον κωδικούς πρόσβασης.

Το OpenID είναι ένα αρκετά δημοφιλές πρωτόκολλο, διαθέτωντας άνω του ενός εκκατομμυρίου λογαριασμούς χρηστών, και άνω των 50.000 ιστότοπων συμβατών

με αυτό, όπως για παράδειγμα Google, Facebook, Yahoo!, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, Telecom Italia [16].

Για την περίπτωση όπου δεν δύναται να αξιοποιηθεί το OpenID, τοπικός μηχανισμός αυθεντικοποίησης ή χρήση τρίτων υπηρεσιών συνδεδεμένων με σχέση εμπιστοσύνης, είναι απαραίτητο για την υποστήριξη ελέγχου πρόσβασης.

Οι οργανισμοί έχουν είτε την δυνατότητα να βασιστούν σε πρότυπα SAML WS-Federation για υποστήριξη εφαρμογών πλέγματος ***(Ενοποιημένο Δημόσιο SSO)*** είτε να επεκτείνουν την λειτουργικότητα Μοναδικής Εισόδου με την χρήση Εικονικού Δικτύου στο Πλέγμα ***(Ενοποιημένο Ιδιωτικό SSO).***

Στην παρούσα κατάσταση, υπάρχει μία τάση για απεδέσμευση εξειδικευμένων μηχανισμών που χρησιμοποιούνταν ως τώρα και οι οργανισμοί που επιθυμούν να αξιοποιήσουν τις υπηρεσίες ενός διαδικτυακού πλέγματος, προσανατολίζονται στις προτάσεις που ενσωματώνουν τα τελευταία πρότυπα, όπως η SAML ή το WS-Federation. Η SAML θα αναλυθεί στο επόμενο κεφάλαιο, και αποτελεί ένας ευρέως διαδεδομένο πρότυπο, το οποίο υποστηρίζουν οι σοβαροί πάροχοι υπηρεσιών διαδικτυακού πλέγματος. Το τελικό ζητούμενο είναι, να βρεθούν στην κατάσταση όπου θα υποστηρίζουν πολλαπλά πρότυπα. Προς το παρόν υποστηρίζεται SAML είτε η 1.1 είτε η 2.0.

Για την περίπτωση όπου ένας οργανισμός θα χρησιμοποιήσει υπηρεσίες πολλών παρόχων, θα πρέπει ο διαχειριστής ταυτοτήτων του οργανισμού, να δύναται να υποστηρίζει κουπόνια αυθεντικοποίησης σε πολλαπλά φορμά συμβατά με το πρότυπο που υποστηρίζει ο κάθε πάροχος. Για την μετατροπή των κουπονιών στις διαφορετικές μορφές που υπαγορεύει το κάθε πρότυπο, υπάρχουν οι πύλες ενοποίησης (Federation Gateways). Οι πύλες αυτές είναι δυνατόν να είναι υλοποιημένες εντός του οργανισμού είτε εκτός, στο πλέγμα όπου και αναφερόμαστε στην παροχή ταυτοτήτων ως υπηρεσία (Identity as a Service) σε αυτήν την περίπτωση.

Έλεγχος Πρόσβασης

Μετά την διαδικασία της αυθεντικοποίησης, ακολουθεί η διαδικασία της απόδοσης εξουσιοδότησης για πρόσβαση σε πόρους του συστήματος. Ένα προφίλ χρήστη διατηρείται στο σύστημα, το οποίο προσπελαύνεται από το σύστημα ελέγχου πρόσβασης και αποφασίζει το τελευταίο αν δικαιούται ή οχι να χρησιμοποιήσει μία υπηρεσία και αν ναι ποιά τμήματα της υπηρεσίας. Τα στοιχεία του προφίλ του κάθε χρήστη καθορίζονται από τον ίδιο τον πάροχο για

μεμονωμένους χρήστες, ενώ για εταιρικούς χρήστες, η ίδια η εταιρεία αναλαμβάνει το έργο καθορισμού του προφίλ των εργαζομένων της.

Ο πάροχος υπηρεσιών πλέγματος θα πρέπει να έχει καλώς καθορισμένες πολιτικές πρόσβασης για κάθε χρήστη, και να διασφαλίζει ότι τα δεδομένα χρηστών δεν είναι προσπελάσιμα από άλλους πελάτες του πλέγματος. Θα πρέπει να παρέχει αναλυτικά αρχεία καταγραφών για τις ενέργειες έκαστου χρήστη. Οι υποχρεώσεις του παρόχου συμπίπτουν με τις υποχρεώσεις ενός κλασσικού διαχειριστή εταιρικού δικτύου, με την διαφορά ότι στο πλέγμα:

- έχουμε την συμβίωση πολλών διαφορετικών πελατών στους ίδιους πόρους
- τα προφίλ χρήστη και οι πολιτικές πρόσβασης είναι δυνατόν να ευρίσκονται σε απομακρυσμένες πηγές, πράγμα που επιβάλλει τον περιοδικό έλεγχο τωνπολιτικών αυτών,
- ο πάροχος θα πρέπει να λάβει υπ'όψιν του αν ο χρήστης είναι μεμονωμένος ή εταιρικός, αν πρέπει να υλοποιηθεί ο μηχανισμός Μοναδικής Εισόδου, και να επιλέξει τον κατάλληλο σύστημα διαχείρισης ταυτοτήτων.

Προτεινόμενα μέτρα για τον ασφαλή Έλεγχο Πρόσβασης

Μοντέλο Ελέγχου Πρόσβασης. Ένα μοντέλο που εξυπηρετεί ικανποιητικά τις συναλλαγές πελατών και εξυπηρετητών είναι το Σύστημα Ελέγχου Πρόσβασης Βασισμένο σε Ρόλους (Role Based Access Control - RBAC). Για την περίπτωση μη δομημένου περιεχομένου, τότε η πιο κατάλληλη επιλογή είναι η Λίστες Ελέγχου Πρόσβασης (Access Control Lists - ACL) σε συνδιασμό με MAC/MLS μοντέλο για τον καθορισμό αποφάσεων.

Η XACML αποτελεί ένα μοντέλο ελέγχου πρόσβασης βασισμένο σε χαρακτηριστικά (Attribute Based Access Control - ABAC). Σύμφωνα με αυτό το μοντέλο, ένα σύνολο από χαρακτηριστικά είναι συσχετισμένο με ένα χρήστη ή με μία ενέργεια ή με έναν πόρο. Τα παραπάνω αποτελούν είσοδο στο σύστημα ώστε να καθοριστεί απόφαση για το αν θα δωθεί πρόσβαση σε ένα συγκεκριμένο πόρο, και για την συγκεκριμένη ενέργεια που ζητείται. Η XACML θα λέγαμε ότι αποτελεί ένα υπερσύνολο ενός συστήματος βασισμένο σε ρόλους, και δύναται να διαμορφωθεί με τέτοιο τρόπο ώστε να ενσωματώνει και έλεγχο με ρόλους εκτός από χαρακτηριστικά.

Η XACML επιτρέπει την αποδέσμευση των πολιτικών πρόσβασης από τον πηγαίο κώδικα των εφαρμογών, διευκολύνοντας το έργο της συντήρησης του συστήματος ελέγχου πρόσβασης [17], [18].

Το γεγονός ότι η διαμόρφωση της απόφασης εξουσιοδότησης καθορίζεται από χαρακτηριστικά των αιτούντων ή του συστήματος, από τους ίδιους τους πόρους, και από το ειδος των ενεργειών, καθιστά το είδος του ελέγχου αυτού ώς πιο ευέλικτο και με πολυ πιο αποδοτική βάθμωση για συστήματα ευρέως μεγέθους σε σχέση με ένα σύστημα ελέγχου με ρόλους [19].

Πολιτική Ιδιωτικότητας. Για την παροχή ιδιωτικότητας σε εταιρικούς πελάτες, η XACML υποστηρίζει το XSPA προφίλ το οποίο ενσωματώνει εξουσιοδότηση ασφάλειας και ιδιωτικότητας και καθορίζει τις απαιτήσεις σε ιδιωτικότητα. Για τους μεμονωμένους χρήστες, η υλοποίηση της ιδιωτικότητας επαφίεται στον πάροχο του πλέγματος.

Η μορφή της πολιτικής πρόσβασης.Το γεγονός ότι η πολιτική πρόσβασης μπορεί να ευρίσκεται αφενός εντός του οργανισμού, και αφετέρου να διακοινώνεται στον πάροχο, επιβάλλει την προτυποποίηση της μορφής στην οποία περιγράφεται μία πολιτική ώστε να αποφευχθεί το φαινόμενο της ασυμφωνίας της μορφής που ακολουθούν ο πάροχος και ο πελάτης. Το συστηνόμενο πρότυπο ευραίας αποδοχής είναι η XACML με εναλλακτικό το WS-Policy για τις περιπτώσεις που χρησιμοποιείται το WS-Federation. Ακόμα και με την τήρηση του προτύπου, όσο ο πελάτης όσο και ο πάροχος θα πρέπει να συμφωνήσουν σε κοινές ονομασίες/σημασιολογίες δεδομένων εντός των αιτημάτων πρόσβασης.

Μετάδοση Πολιτικής. Όπως και στην προηγούμενη περίπτωση, θα πρέπει να υπάρχει συμφωνία μεταξύ του παρόχου και του πελάτη για το είδος της κρυπτογράφησης που θα ακολουθηθεί ή τον τρόπο μετάδοσης. Για την περίπτωση που μεταδίδονται οι πολιτικές στον πάροχο ανεξάρτητα από τα αιτήματ, προτείνεται η χ΄ρηση του SPML προτύπου. Για την περίπτωση που χρησιμοποιείται η SAML για την μετάδοση των πληροφοριών πολιτικής, συστήνεται η χρήση της ψηφιακής υπογραφής στους SAML ισχυρισμούς (προφίλ SAML 2.0).

Η λιγότερο διαδεδομένη λύση του WS-Federation επιβάλλει την χρήση του προτύπου WS-Policy, WS-Policy Attachment, WS-Trust.

Για τους μεμονωμένους χρήστες ή όταν οι πολιτικές ευρίσκονται στον ίδιο τον πάροχο, δεν απαιτείται η εφαρμογή κάποιου μηχανισμού μετάδοσης πολιτικής.

Μετάδοση προφίλ χρήστη. Για μεμονωμένους χρήστες, οι ίδιοι δύνανται να παραθέτουν τις πληροφορίες που χρειάζεται ο πάροχος κατόπιν ενός ερωτηματολογίου. Υπάρχει η επιλογή χρήσης του OpenID, Google, Yahoo κλπ, όπου ο πάροχος αναλαμβάνει να αντλήσει τις απαραίτητες πληροφορίες για κάθε χρήστη στους παρόχους αυτούς.Αν χρειαστεί, ο χρήστης εισάγει συμπληρωματικά κάποια στοιχεία.

Στην περίπτωση εταιρικών χρηστών, ο μηχανισμός της παροχής στοιχείων από τον ίδιο τον χρήστη δεν είναι αποδεκτός. Οι πληροφορίες χρηστών αντλούνται από κάποια έμπιστη πηγή η οποία χαίρει σχέση εμπιστοσύνης με τον πάροχο του πλέγματος. Η μετάδοση ακολουθεί το ίδιο μοτίβο με πριν: SPML , SAML ή WS-Policy, αναλόγως του προτύπου που ακολουθείται.

Αίτημα Απόφασης Πολιτικής. Για την διαχείριση της απόφασης εξουσιοδότησης, η οποία ευρίσκεται εκτός του παρόχου, η XACML αποτελεί το προτεινόμενο πρότυπο. Εναλλακτικά, και με μικρότερη δημοφιλία ακολουθεί τα WS-* πρότυπα. Η επιβολή της απόφασης επιτελείται εντός των εφαρμογών.

Καταγραφή Ενεργειών. Για την καταγραφή, η οποία θα πρέπει να την αναλαμβάνει το σύστημα ελέγχου πρόσβασης δεν υπάρχει κάποιο πρότυπο ως τώρα. Πάροχοι και πελάτες θα πρέπει να συνεργαστούν για να συμφωνηθεί μία κοινή φόρμα πληροφορίας που θα αποθηκεύεται ώστε να μπορεί ο πάροχος να ελέγχει τις χρεώσεις ή την αιτία διαφόρων προβλημάτων. Επιπλέον πληροφορίες όπως το ποιός παραχώρησε δικαίωμα πρόσβασης σε ποιόν, καθώς και τα πλήρη στοιχεία κάθε χρήστη θα πρεπει να καταγράφονται προς χρήση από τον οργανισμό που θέλει να ελέγχει τις ενέργειες των εργαζόμενων του.

Είναι σχετικά πολύπλοκη διεργασία καθώς έχουμε ροές πληροφοριών διεσπαρμένες σε πολλούς εξυπηρετητές και οι οποίες πρέπει να συγκεντρωθούν. [20]

Ιδιωτικότητα

Σημαντικό ζήτημα σε ένα περιβάλλον διαδικτυακού υπολογιστικού πλέγματος, αποτελεί η διασφάλιση της ιδιωτικότητας. Η επίτευξη της ασφάλειας των δεδομένων στηρίζεται σε κλασσικές τεχνικές που προυπήρχαν. Αυτές προσφέρουν ένα συγκεκριμένο και αναμενόμενο επίπεδο λειτουργίας. Τι θα συμβεί όμως όταν ο επιτιθέμενος βρεί τρόπο να καταστρατηγήσει όλες τις δικλείδες ασφαλείας που έχει θέσει ο πάροχος και ο πελάτης; Η απάντηση δεν είναι άλλη από ότι είναι σε θέση να επεξεργαστεί την βάση του πελάτη, να εξάγει συμπεράσματα και πληροφορίες για μεμονωμένα πρόσωπα, να επιτελέσει εν ολίγοις μία ανάλυση σε βάθος, πέρα από απλές στατιστικές πληροφορίες, και να επικεντρωθεί σε ατομικό επίπεδο.

Την στιγμή που τα μέτρα ασφάλειας αποδειχτούν ανεπαρκή, τότε η μόνη λύση για την διασφάλιση της πληροφορίας είναι να την αλλοιώσουμε σε τέτοιο βαθμό, όπου δεν θα μπορεί ο επιτιθέμενος να εξάγει συμπεράσματα.

Το πιό σημαντικό είναι, ότι ο ίδιος ο πελάτης, σε πολλές περιπτώσεις είναι υποχρεωμένος να δημοσιεύει την βάση του προκειμένου να γίνουν στατιστικές μελέτες. Το γεγονός αυτό συντελεί στην απόδοση ιδιαίτερης προτεραιότητας στην ιδιωτικότητα των πελατειακών δεδομένων.

Ένας τρόπος για να περιορίσουμε την διαρροή προσωπικών πληροφοριών είναι η εφαρμογή «θορύβου» στα δεδομένα, δηλαδή η πράξη με κάποιους τυχαίους αριθμούς με τέτοιο τρόπο ώστε να διατηρούνται αναλλοίωτες οι στατιστικές τιμές της βάσης. Αυτή η τεχνική μπορεί να εφαρμοστεί σε συνδιασμό με την εναλλαγή δεδομένων μεταξύ των γραμμών (εγγραφών). Ωστόσο αυτή η μέθοδος καταστρέφει την ακεραιότητα των δεδομένων των μεμονωμένων εγγραφών. Για αυτόν τον λόγο κρίνονται ως μη συνιστώμενες μέθοδοι προστασίας της ιδιωτικότητας. Γιατί μπορεί μεν να επιτυγχάνουν την ανωνυμία με την «σύγχιση» στα δεδομένα, αλλά αλλοιώνουν τα δεδομένα δε ώστε να καθίστανται μη ικανά για νόμιμη εξόρυξη δεδομένων.

Στηριζόμενοι στο χειρότερο σενάριο, δηλάδη το ότι η εξόρυξη των συγκεκριμένων δεδομένων κρίνεται ως νόμιμη, θα αναλύσουμε μία προτεινόμενη τεχνική ή οποία συνδιάζει με τον καλύτερο τρόπο την ανωνυμοποίηση των δεδομένων σε μία βάση δεδομένων. Η τεχνική αυτή διατηρεί αναλλοίωτες τις στατιστικές τιμές της επιτρέποντας την επιτέλεση της νόμιμης εξόρυξης δεδομένων για στατιστικούς λόγους.

Μία λύση που έχει προταθεί στην βιβλιογραφία είναι η αξιοποίηση βάσεων «πολλαπλών επιπέδων». Πρόκειται για βάσεις δεδομένων που εφαρμόζουν σύστημα ελέγχου προσπέλασης, ουτως ώστε διαφορετικοί χρήστες να έχουν πρόσβαση σε διαφορετικές πληροφορίες, ανάλογα με το επίπεδο εξουσιοδότησης που τους έχει αποδωθεί. Οι πληροφορίες υψηλού επιπέδου εξουσιοδότησης δεν είναι δυνατό να προσπελαστούν **άμεσα**. Επιπλέον Εφαρμόζεται αυστηρός περιορισμός στις πληροφορίες χαμηλού επιπέδου εξουσιοδότησης ώστε να μην αποκαλυφθούν και **έμμεσα** (με έμμεσα ερωτήματα στην βάση) οι πληροφορίες υψηλού επιπέδου εξουσιοδότησης. Μελέτες έχουν αποδείξει όμως ότι είναι σχεδον αδύνατο να εξαλειφτούν όλες οι πιθανές αλληλοσυσχετίσεις που μπορούν να βοηθήσουν στην εξαγωγή απόρρητων πληροφοριών. Ακόμα και η προσεκτική σχεδίαση μίας βάσης δεδομένων με εξουσιοδοτήσεις και έλεγχο πρόσβασης δεν εγγυάται την ιδιωτικότητα από την στιγμή που αντίγραφα των βάσεων είναι δυνατόν να βρίσκονται διεσπαρμένα στον κόσμο υπο την κατοχή διάφορων φορέων. Οι φορείς αυτοί υλοποιούν ο καθένας με τον δικό τους τρόπο, πολλές φορές λιγότερο αποτελεσματικό απο το σημειο αναφοράς. Το πιο σημαντικό χαρακτηριστικό μίας βάσης πολλαπλών επιπέδων είναι όμως και το μεγαλύτερο μειονέκτημα: η όλη φιλοσοφία στηρίζεται στην απόκρυψη πληροφοριών. Με την απόκρυψη έχουμε αλλοίωση της ποιότητας της πληροφορίας αλλά και των

στατιστικών της τιμών. Αυτό είναι αρκετο για να καταστήσει μία βάση ακατάλληλη για εξόρυξη δεδομένων.

Η εφαρμογή ελέγχου πρόσβασης θεωρείται ως μέσο ασφάλειας και όχι ως μέσο εξασφάλισης της ιδιωτικότητας. Ακόμα και αν αποκρύπτουμε πληροφορίες, αυτο δεν αποκλείει την εξαγωγή συμπερασμάτων ιδιωτικής φύσεως από συνδυασμό δεδομένων για τα οποία έχουμε πρόσβαση.

Η κρυπτογράφηση είναι μία λύση αλλά εισάγει την αναγκαιότητα για διατήρηση ενός συστήματος διαχείρισης κλειδιών και την μόνιμης ανησυχίας για το αν κάποια στιγμή σπάσουν τα κλειδιά και η ιδιωτική πληροφορία πέσει στους κακόβουλους χρήστες. Εκτός αυτού απαιτείται επιπλέον υπολογιστική ισχύς για την συνεχόμενη κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.

Ανάλυση Κ-ανωνυμίας

[21] [22] [23] [24]

Στην συνέχεια θα αναλυθεί μία άκρως αποτελεσματική τεχνική η οποία είναι σε θέση να διασφαλισει την ιδιωτικότητα της βάσης δεδομένων του πλέγματος, είτε ιδιωτικού είτε κοινόχρηστου. Ιδιαίτερα για την περίπτωση του ιδιωτικού πλέγματος, η τεχνική βοηθάει για την περίπτωση όπου ο οργανισμός είναι υποχρεωμένος από τον νόμο να δημοσιεύει τα δεδομένα της βάσης του προς μελέτη στατιστικολόγων, ερευνητών κλπ. Στην παρούσα ενότητα θα περιγραφεί η υλοποίηση μίας βάσης δεδομένων με γνώμονα την ιδιωτικότητα μέσα από την ανωνυμοποίηση των δεδομένων. Στην επόμενη ενότητα παίρνουμε μία βάση εγγραφών και δείχνουμε στην πράξη ένα ένα τα βήματα που περιγράφει η μελέτη της Κ-Ανωνυμίας.

Το πρώτο βήμα που πρέπει να κάνει ο σχεδιαστής της βάσης, είναι να καθορίσει ποιοι είναι οι προσδιοριστές οι οποίοι αν χρησιμοποιηθούν για να συνδέσουν βάσεις δεδομένων ανεξάρτητες μεταξύ τους, έχουν σαν αποτέλεσμα την εξαγωγή ιδιωτικής πληροφορίας. Στο παράδειγμα του ερευνητή της Μασαχουσέτης, οι προσδιοριστές ήταν ο ταχυδρομικός κώδικας, το φύλο και η ημερομηνία γέννησης. Πριν την εφαρμογή της τεχνικής της Κ-Ανωνυμίας, θεωρούμε ότι ο σχεδιαστής της βάσης είναι σε θέση να καθορίσει με σαφήνεια αυτούς τους προσδιοριστές στα δεδομένα του καθώς και να αναγνωρίσει ποιοί από αυτούς υπάρχουν και σε άλλες βάσεις. Οποιαδήποτε παράλειψη προσδιοριστή απο την εφαρμογή της τεχνικής έχει σαν αποτέλεσμα ένα σύστημα το οποίο είναι ευάλωτο σε επιθέσεις συνδιαστικών ερωτημάτων σε πολλαπλές βάσεις. Βάσει των παραπάνω ορίζουμε:

Ορισμός 1: Quasi-identifier (ημιπροσδιοριστής)

Έστω ότι έχουμε ένα πίνακα με n στοιχεία: T(A1,A2,…An). Ο quasi-identfier QT του Τ είναι ένα υποσύνολο προσδιοριστών από το σύνολο των προσδιοριστών που είναι κατανεμημένα σε δύο η περισσότερους πίνακες, τέτοιο ώστε ερωτήματα συνδιαστικά σε αυτούς τους πίνακες με βάση το υποσύνολο των προσδιοριστών, εξάγει απόρρητη πληροφορία.

Θεωρώντας γνωστή την ποσότητα Quasi Identifier, θα δώσουμε τον βασικό ορισμό της K-Ανωνυμίας:

Ορισμός 2: K-Ανωνυμία

Μία βάση υπακούει στην αρχή της K-Ανωνυμίας, αν και μόνο εαν για οποιοδήποτε ερώτημα στην βάση αυτή ή και σε συνδιασμό με περισσότερες εξωτερικές βάσεις, με είσοδο όλους τους δυνατούς συνδιασμούς και τιμές του Quasi Identifier, η βάση αποκρίνεται με τουλάχιστον K απαντήσεις.

Για την επίτευξη αυτού του αποτελέσματος, είναι αναγκαίο να μετασχηματίσουμε την βάση σε μία άλλη μορφή χρησιμοποιώντας δύο μεθόδους:

- Γενικοποίηση
- Καταστολή

Η εφαρμογή αυτών των μεθόδων αποτελεί και τον πυρήνα της τεχνικής καθότι καθιστά τα δεδομένα ανώνυμα και συγκεκριμένα ανώνυμα βαθμού K. Δηλαδή η ανωνυμία της οντότητας στηρίζεται στην ύπαρξη επιπλέον πλήθος K-1 αποκρίσεων από την βάση.

Στην συνέχεια αναλύουμε τις δύο βασικές μεθόδους της K-Ανωνυμίας και την λογική που στηρίζονται.

Γενικοποίηση

Η Γενικοποίηση έχει σαν στόχο την ελάχιστη επέμβαση στα δεδομένα με σκοπό να διατηρηθεί η πιστότητα της πληροφορίας. Ενώ ο θόρυβος και η εναλλαγη γραμμών αλλοιώνει ανεπανόρθωτα τα δεδομένα, με την γενικοποίηση θυσιάζουμε ένα μέρος από την πιστότητα τους. Η φιλοσοφία της γενικοποίησης εφαρμόζεται στις στήλες μίας βάσης οι οποίες καθορίζουν ένα χαρακτηριστικό του υποκειμένου, και αντικαθιστούμε το χαρακτηριστικό με μία πιο γενικευμένη ονομασία. Για παράδειγμα η ημερομηνία γέννησης η οποία συγκροτείται από την ημέρα, μήνα και χρονολογία μπορεί να γενικευτεί σε μία άλλη στήλη που θα αποτελείται από τον μήνα και την χρονιά γέννησης. Με αυτόν τον τρόπο επιτελούμε ομαδοποιήσεις

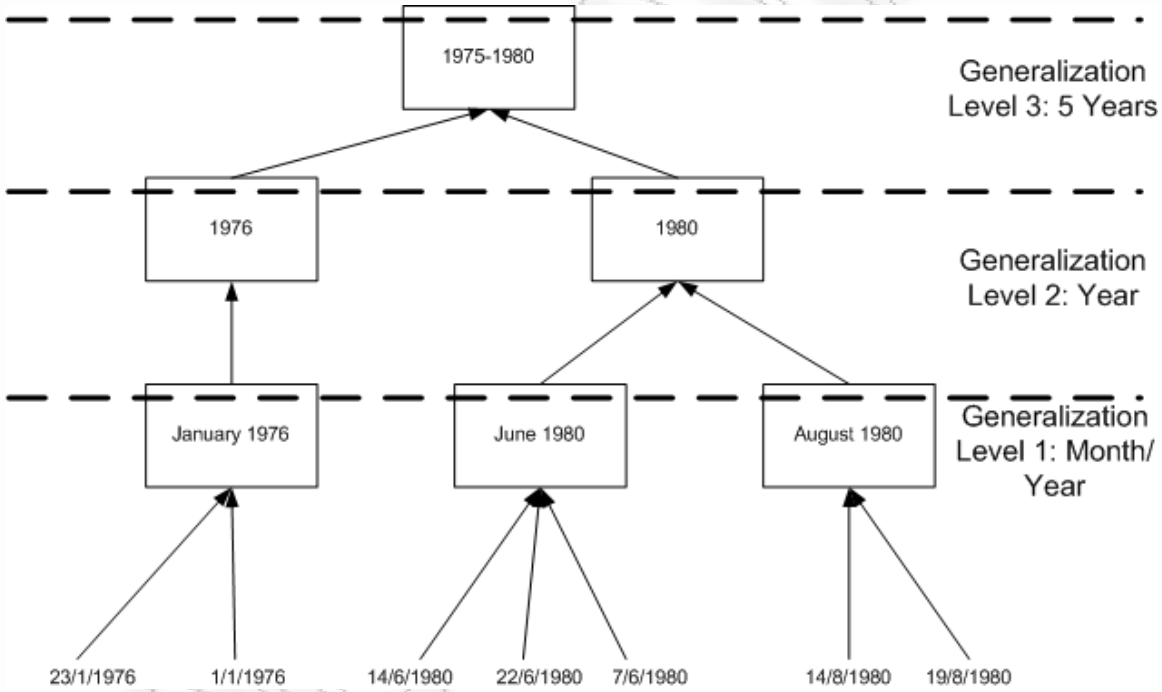
υποκειμένων, στην προκειμένη περίπτωση όλους όσους γεννήθηκαν τον συγκεκριμένο μήνα και αποφεύγουμε την απάντηση μία μοναδικής εγγραφής αν δωθεί ακριβής ημερομηνία γέννησης. Στην περίπτωση του ταχυδρομικού κώδικα η γενικοποίηση πραγματοποιείται αφαιρώντας ένα ψηφίο, ομαδοποιώντας έτσι κατα δεκάδες τους ταχυδρομικούς κώδικες.

Η γενικοποίηση που περιγράφηκε μπορεί να ονομαστεί ώς γενικοποίηση «πρώτου σταδίου». Είναι δυνατόν ακόμα και μετα από μία γενικοποίηση πρώτου σταδίου να μην εξασφαλίζεται η K-Ανωνυμία είτε επειδή η τιμή K είναι μεγάλη είτε επειδη τα δεδομένα δεν είναι ομοιόμορφα διεσπαρμένα: αν θέλουμε ανωνυμία με K=10 αλλά τυγχάνει στον μήνα Ιανουάριο οι εγγραφές να είναι μόλις 9 ενώ στους άλλους μήνες ξεπερνούν κατα πολύ τις 9 εγγραφές, τότε ακόμα και με την γενικοποίηση πρώτου σταδίου «μήνας-χρονολογία» η K=10 ανωνυμία δεν εεξασφαλίζεται. Σε αυτην την περίπτωση μπορούμε να εφαρμόσουμε περαιτέρω γενικοποίηση στην στήλη «ημερομηνία γέννησης». Το δεύτερο στάδιο γενικοποίησης είναι με βάση την χρονιά γέννησης. Σε αυτό το σημείο αναγκαίο είναι να διευκρινιστεί ότι ενας προσδιοριστής που ανήκει στο Quasi Identifier αντιστοιχεί στο πολύ μία γενικοποίηση είτε πρώτου είτε δευτέρου είτε του νιοστού σταδίου. Δεν είναι δυνατόν να υπάρχουν παρούσες δύο ή περισσότερες γενικοποιήσεις του ίδιου χαρακτηριστικού ταυτόχρονα. Η γενικοποίηση θα πρέπει να γίνεται βαθμωτά με αυξανόμενη τάση αποφεύγοντας την απώλεια πληροφορίας χωρίς να απαιτείται. Δηλαδή δεν θα γενικοποιήσουμε την ημερομηνία γέννησης σε χρονολογία γέννησης απευθείας στο πρώτο στάδιο. Μπορεί μεν να επιτυγχάνεται η K-Ανωνυμία με την χρονολογία αλλά το ζητούμενο είναι να επιτευχθεί με την μικρότερη απώλεια στην πληροφορία. Επομένως αν ο μήνας και η χρονιά γέννησης εξασφαλίζουν την επιθυμητή ανωνυμία τότε δεν υπάρχει λόγος να χρησιμοποιήσουμε την πιο ασαφή στήλη με την χρονολογία μόνο.

Επίσης η γενικοποίηση θα αντιστοιχεί σε ένα χαρακτηριστικό μοναδικό. Δηλαδή δεν θα είναι δυνατό να ερμηνευτεί και με διαφορετικό τρόπο, με αποτέλεσμα να μπορούμε να αντιστοιχίσουμε δύο ή περισσότερες διαφορετικές τιμές του χαρακτηριστικού.

Ένα θεωρητικό παράδειγμα το οποίο δεν εφαρμόζεται στην πράξη αλλά βοηθάει στην ερμηνεία της μη μοναδικής γενικοποίησης που περιγράφηκε πιο πάνω: αν έχουμε την Vmax στον δρόμο ενός οχήματος, αν την γενικοποιήσουμε σε Vmax, τότε αυτή θα μπορούσε να αντιστοιχεί για ένα τζιπ είτε στον χωματόδρομο είτε στην άσφαλτο με αποτέλεσμα να αντιστοιχεί σε δύο τιμές.

Στο σχήμα 4 απεικονίζεται ένα παράδειγμα γενικοποίησης της ημερομηνίας γέννησης τριών σταδίων. Παρατηρούμε ότι στο πρώτο στάδιο ομαδοποιώντας τις εγγραφές κατα μήνα και χρονολογία επιτυγχάνουμε ανωνυμία K=2. Ο ελάχιστος αριθμός εγγραφών είναι για τον ιανουάριο και τον αύγουστο άρα έχουμε K=2. Αν θέλουμε μεγαλύτερο K εφαρμόζουμε δεύτερο στάδιο γενικοποίησης με βάση την χρονιά γέννησης. Εδώ έχουμε ένα χαρακτηριστικό παράδειγμα που καταδεικνύει την περίπτωση που η γενικοποίηση δεν αυξάνει την ανωνυμία σε ιδιάζουσες περιπτώσεις (μικρές βάσεις με μη ομοιόμορφα διεσπαρμένες εγγραφές). Παρ'όλο που για το 1980 έχουμε 5 εγγραφές, εν τούτοις η ανωνυμία παραμένει K=2 λόγω του ότι για το 1976 οι εγγραφές είναι μόνο 2. Αν προχωρήσουμε στο τρίτο στάδιο της γενικοποίησης, το οποίο ομαδοποιεί κατα πενταετία, έχουμε 7 εγγραφές, άρα K=7.



Εικόνα 6: Δέντρο γενικοποίησης με τρία στάδια

Καταστολή

Σε αυτό το σημείο θα αναφερθούμε με την βοήθεια του παραδείγματος του σχήματος 5 στις αδυναμίες της γενικοποίησης. Παρατηρούμε κατ'αρχάς ότι η K ανωνυμία απαιτεί συνεχόμενη γενικοποίηση. Με ***G1, G2 G3*** στο παρακάτω σχήμα καλούμε τα στάδια της γενικοποίησης. Όσο περισσότερο γενικοποιούμε τόσο αυξάνουμε το K και αντίστροφα. Η δομή μίας βάσης όμως δεν είναι πάντα ομοιόμορφη. Άν έχουμε μία βάση 7 ασθενών, με ημερομηνία γέννησης από 1930 και μετά, και θέλουμε K=2 ανωνυμία αν γενικοποιήσουμε κατα μήνα και χρονιά

μπορεί μεν να έχουμε τουλαχιστον 2 ασθενείς σε κάθε μήνα/χρονιά αλλά αν στην βάση μας υπάρχει έστω και ένας ασθενής γεννημενος το 1929 τότε δεν εξασφαλίζεται η K=2 ανωνυμία. Μία λύση είναι η γενικοποίηση κατα πενταετίες ώστε να ομαδοποιήσουμε – να «κρύψουμε»- τον ασθενή γεννημενο το 1929 με τους ασθενείς που γεννηθηκαν το 1930 στην στήλη η οποία περιέχει τις χρονολογίες γέννησης από το 1925-1930. Αυτό όμως έχει σαν αποτέλεσμα την σοβαρή απώλεια της πληροφορίας και όλα αυτά εξ αιτίας μίας εγγραφής. Αρκεί να σημειωθεί ότι επιβάλλαμε γενικοποίηση δύο σταδίων εξ'αιτίας ενός ασθενούς, την στιγμή που αν δεν υπήρχε θα είχαμε ανωνυμία από το πρώτο μόλις στάδιο γενικοποίησης.

Εδώ έχουμε μία άλλη επιλογή η οποία επιτρέπει την αποφυγή της περαιτέρω απώλειας σε πιστότητα. Αυτή είναι η καταστολή μίας γραμμής (εγγραφή) από την βάση. Με αυτόν τον τρόπο επιτυγχάνουμε την επιθυμητη ανωνυμία με το ελάχιστο απαιτούμενο επίπεδο γενικοποίησης. Έτσι διατηρούμε όσο το δυνατόν περισσότερη πληροφορία για την πιο ακριβείας εξόρυξη δεδομένων. Στο παράδειγμα του σχήματος 5 αρκεί να αποκρύψουμε την γραμμή με τον ασθενή που γεννήθηκε το 1929.

Ελαχιστοποίηση της απαιτούμενης γενικοποίησης: Καταστολή

Η καταστολή προκαλεί απώλεια στην ***πληρότητα*** της πληροφορίας, ένα τίμημα που καλούμαστε να πληρώσουμε προκειμένου να διατηρήσουμε σε καλό επίπεδο την ***πιστότητα*** της πληροφορίας. Η ανοχή στην απώλεια πληρότητας εξαρτάται από το μέγεθος της βάσης. Αν για παράδειγμα έχουμε μία βάση με 1000 ασθενείς, μπορούμε να θεωρήσουμε ότι μέχρι 50 εγγραφές μπορούν να κατασταλλούν το πολύ προκειμένου να θεωρούμε την συνολική στατιστική πληροφορία πλήρη. Θέτοντας επομένως ένα ***κατώφλι καταστολής Ksup-thres*** η διαδικασία που ακολουθούμε λαμβάνοντας υπ'όψιν αυτήν την παράμετρο ονομάζεται ως η αρχή της ***K Ελάχιστης Γενικοποίησης με χρήση Καταστολής*** και έχει ώς εξής:

K Ελάχιστη Γενικοποίηση με χρήση Καταστολής

Έχοντας δεδομένο το Quasi Identifier στο τέλος κάθε βήματος γενικοποίησης υπολογίζουμε τον απαιτούμενο αριθμό γραμμών που πρέπει να κατασταλλούν ***Ksup*** προκειμένου να επιτευχθεί η K Ανωνυμία. Αν ***Ksup > Ksup-thres*** τότε εφαρμόζουμε περαιτέρω γενικοποίηση και επαναλαμβάνουμε τον προηγούμενο έλεγχο. Όταν το ***Ksup ≤ Ksup-thres*** τότε σταματάμε την διαδικασία της γενικοποίησης.

Name	Race	Gender	ZIP	DoB	Symptom	G1	G2	G3
Mr. Raymond Kiruki	african	m	911916	14/6/1930	short breath	Jun-30	1930	1925-1930
Mr. Richard Ives	caucasian	m	911908	22/6/1930	chest pain	Jun-30	1930	1925-1930
Mr. Cheikh A. Bamba Diop	asian	m	911909	19/8/1930	chest pain	Aug-30	1930	1925-1930
Mr. Shantha Kulathunge	african	m	911914	14/8/1930	HIV	Aug-30	1930	1925-1930
Mr John Delorean	caucasian	m	911914	17/6/1930	chest pain	Jun-30	1930	1925-1930
Ms. Jenny Carlsson	asian	f	911903	7/6/1930	short breath	Jun-30	1930	1925-1930
Mr. Duminda Edirisinghe	caucasian	m	911901	10/4/1929	short breath	Apr-29	1929	1925-1930

Εικόνα 7: Εκτεταμένη γενικοποίηση λόγω μοναδικής εγγραφής

Στρατηγική βέλτιστης γενικοποίησης

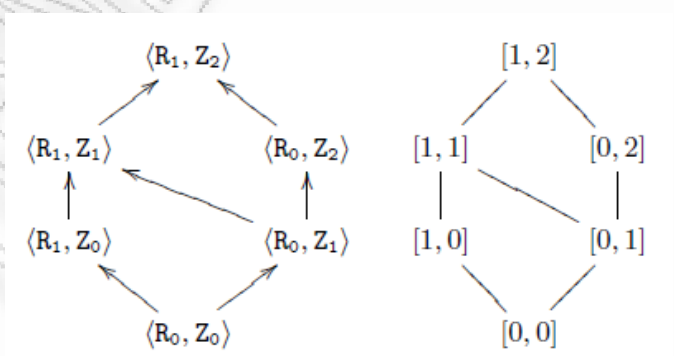
Στα παραπάνω παραδείγματα για λόγους απλότητας παρουσιάσαμε Quasi Identifiers οι οποίοι περιείχαν ένα χαρακτηριστικό (στήλη) προς γενικοποίηση. Στην πραγματικότητα ο Quasi Identifier συγκροτείται από πολλούς προσδιοριστές. Οι αρχή της γενικοποίησης εφαρμόζεται ομοιόμορφα σε όλα τα επιμέρους χαρακτηριστικά. Είναι δηλαδή το καρτεσιανό γινόμενο των γενκοποιήσεων όλων των επιμέρους χαρακτηριστικών.

$$DGH = DGH_{D1} \text{ X } \dots \text{ X } DGH_{Dn}$$

$$\text{If QI} = \{ZIP,Race\} \Rightarrow DGH = DGH_{ZIP} \text{ X } DGH_{Race}$$

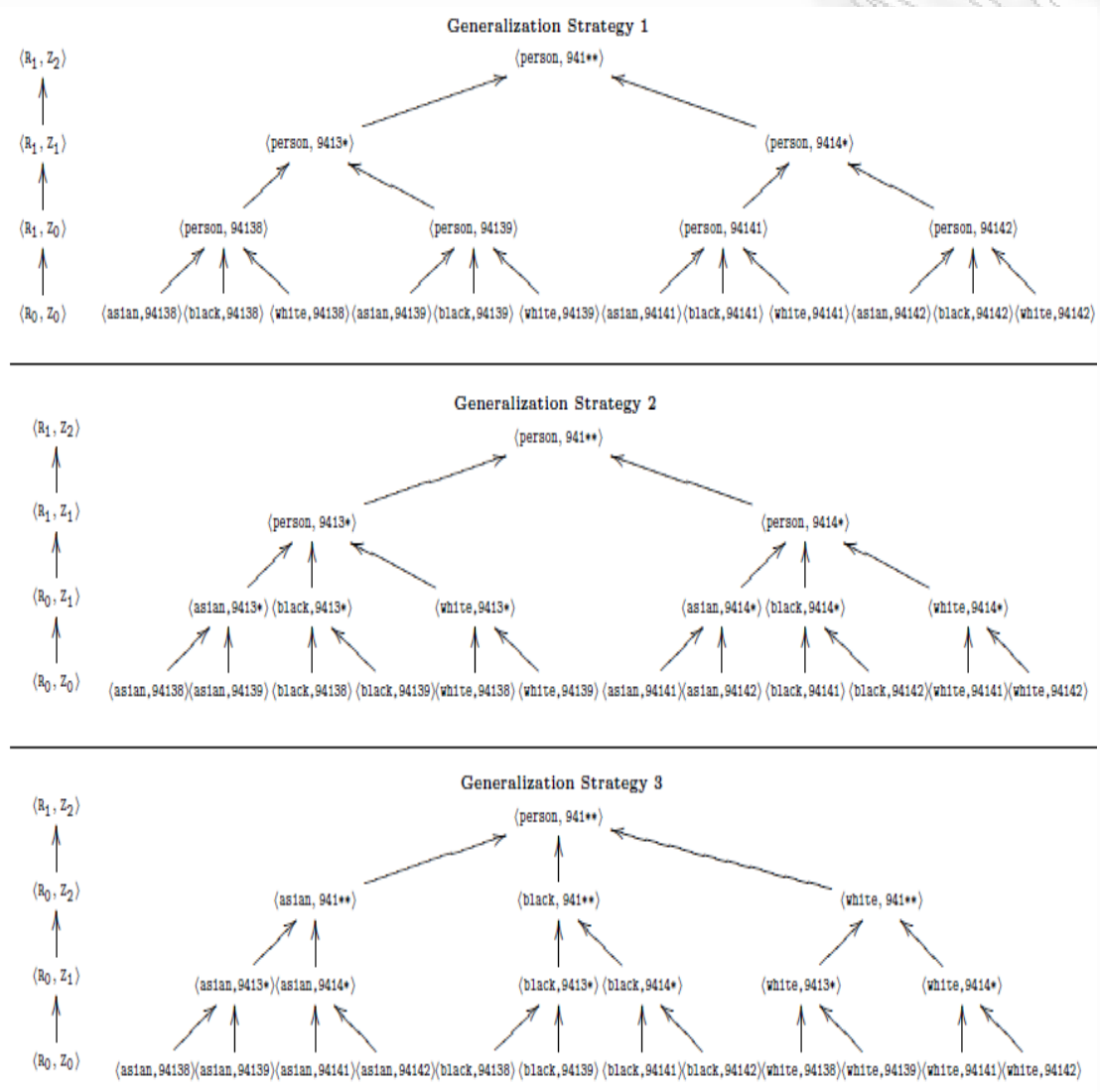
Το αποτέλεσμα είναι ένα δέντρο γενικοποιήσεων το οποίο αποτελείται από πολλά διαφορετικά μονοπάτια. Το κάθε μονοπάτι καθορίζει με ποιά σειρά γενικοποιούμε τα χαρακτηριστικά. Όσο πιο πολλά είναι τα χαρακτηριστικά τόσο πιο πολύπλοκο γίνεται το δέντρο με αποτέλεσμα να υπάρχουν πολλές δυνατές εναλλάκτικές γενικοποίησης οι οποίες πρέπει να δοκιμαστούν μία προς μία εως ότου επιτευχθεί η ανωνυμία.

Για το παράδειγμα Quasi Identifier που αποτελείται από το ZIP και το RACE έχουμε το εξής δέντρο:



Εικόνα 8: Δέντρο γενικοποίησης {ZIP,Race}

R0, Z0 συμβολίζει την αρχική κατάσταση στήλης της φυλής και ταχυδρομικού κώδικα και Rn, Zn το νιοστό στάδιο της γενικοποίησης. Για αυτό το απλό παράδειγμα στο επόμενο σχήμα απαριθμούμε όλα τα δυνατά μονοπάτια γενικοποίησης:



Εικόνα 9: Μονοπάτια γενικοποίησης

Η διαδικασία είναι να δοκιμάσουμε όλα τα πιθανά μονοπάτια και ένα προς ένα τα στάδια της γενικοποίησης μέχρι να πετύχουμε εκείνο που εξυπηρετεί την ανωνυμία με την ελάχιστη απώλεια της πληροφορίας. Αρκεί να φανταστούμε ένα Quasi Identifier και πως αυξάνονται εκθετικά το πλήθος των μονοπατιών. Είναι μία κουραστική και επίπονη εργασία για την οποία όμως έχει ευρεθεί τρόπος ελαχιστοποίησης της με την εφαρμογή του αλγορίθμου της δυαδικής αναζήτησης, ιδέα που εισήγαγε η Samarati.

Δυαδική αναζήτηση

Η δυαδική αναζήτηση βασίζεται στο ότι αν σε ένα στάδιο N γενικοποιήσεων επιτυγχάνεται η ανωνυμία με K = Ksup-thres, τότε όλες οι γενικοποιήσεις N-1 απαιτούν K' > K και επομένως κρίνονται ως απορριπτέες. Αντίστοιχα οι γενικοποιήσεις N+1 και πάνω απαιτούν K' < K. Βασιζόμενοι σε αυτήν την αρχή, αν έχουμε ένα δέντρο με N στάδια γενικοποίησης τότε επιλέγουμε το επίπεδο γενικοποιησης στο δέντρο που αντιστοιχεί στα N/2 στάδια και ελέγχουμε αν ικανοποιείται η K ανωνυμία με K καταστολή ίση με το κατώφλι.

- Αν ΔΕΝ ικανοποιείται τότε δοκιμάζουμε στα μισά του άνω άκρου [N/2 , N] δηλαδή στ ο 3N/4
- Αν ικανοποιείται και έχουμε K < Ksup-thres αυτό σημαίνει ότι υπάρχει περιθώριο να ακυρώσουμε κάποιες γενικοποιήσεις ώστε να αυξήσουμε την ακρίβεια των δεδομένων. Υπενθυμίζουμε ότι ο βαθμός της γενικοποίησης εξαρτάται από το Ksupthres. Επιθυμούμε να καταστείλουμε ***οχι λιγότερες*** από Ksupthres γραμμές. Επομένως δοκιμάζουμε στα μισά του κάτω άκρου [0, N/2] δηλαδή στο N/4.

Η διαδικασία επαναλαμβάνεται εώς ότου αντιληφθούμε ότι χρειαζόμαστε να αποκρύψουμε όχι λιγότερες απο Ksupthres γραμμές για να έχουμε την K Ανωνυμία.

Ελαχιστοποίηση απώλειας δεδομένων

Επιλογή κατάλληλης στήλης

Στην προηγούμενη ενότητα αναλύθηκε το δέντρο γενικοποιήσεων και παρατηρήσαμε ότι υπάρχουν πολλά δυνατά μονοπάτια επιλογής κατα την διαδικασία της γενικοποίησης. Για παράδειγμα, αν K Ανωνυμία επιτυγχάνται από το πρώτο στάδιο γενικοποίησης, τότε μπορούμε είτε να επιλέξουμε την γενικοποίηση στο πεδίο του ταχυδρομικού κώδικα είτε στην φυλή και να έχουμε το ίδιο αποτέλεσμα. Ωστόσο πολλές φορές θα πρέπει να συμπεριλάβουμε και ένα άλλο κριτήριο και αυτό είναι της διατήρησης της πιστότητας των δεδομένων. Οι γενικοποιήσεις αλλοιώνουν τα δεδομένα, αλλά επιπλέον οι γενικοποιήσεις σε ορισμένες στήλες καταστρέφουν περισσότερη πληροφορία από ότι σε κάποιες άλλες. Αναγκαίο είναι λοιπόν να εισάγουμε ένα ποιοτικό κριτήριο επιλογής στήλης για γενικοποίηση. Το κριτήριο αυτό είναι η διατήρηση της μικροπληροφορίας.

Η μικροπληροφορία είναι αυτή που προφέρει επιπλέον πληροφορίες για κάποιο υποκείμενο σε σχέση με την μακροπληροφορία. Η τελευταία είναι ένας στατιστικός μέσος όρος, ο οποίος δεν ενδιαφέρει τόσο στην εξόρυξη δεδομένων όσο

πληροφορία που αποκομίζουμε από την μεγάλη απόκλιση των τιμών. Επειδή οι αποκλίσεις μας ενδιαφέρουν, αυτό που πρέπει να μελετήσουμε είναι οι απόλυτες διαφορές των δύο άκρων σε μία στήλη. Αν αυτές είναι σημαντικές, τότε αποφεύγουμε την γενικοποίηση αυτής της στήλης. Αντίστοιχα αν μία άλλη στήλη παρουσιάζει τιμές στοιχείων με μικρές αποκλίσεις μεταξύ τους, τότε δίνουμε προτεραιότητα σε τέτοιες στήλες κατα την διαδικασία της γενικοποίησης.

Marital_status	*Sex*	*Hours*	*#tuples (Hyp. values)*
any_marital_status	any_sex	[1,100)	66 (32Y, 34N)

(a) Step 1: the most general table

Marital_status	*Sex*	*Hours*	*#tuples (Hyp. values)*
been_married	any_sex	[1,100)	40 (26Y, 14N)
never_married	any_sex	[1,100)	26 (6Y, 20N)

Εικόνα 10: Απόκλιση τιμών για την οικογενειακή κατάσταση

Στο παραπάνω σχήμα αναλύουμε την οικογενειακή κατάσταση σε

- Παντρεμένος
- Ανύπαντρος

Ελέγχοντας τις τιμές, 26 ναι, 14 οχι παντρεμένοι και 6 ναι και 20 όχι ανύπαντροι παρατηρούμε ότι τα ναι και τα όχι έχουν σημαντικές αποκλίσεις. Συνεπώς αυτή η top down προσέγγιση δείχνει ότι η οικογενειακή κατάσταση δεν πρέπει να γενικοποιηθεί. Θα χαθεί πολύτιμη πληροφορία.

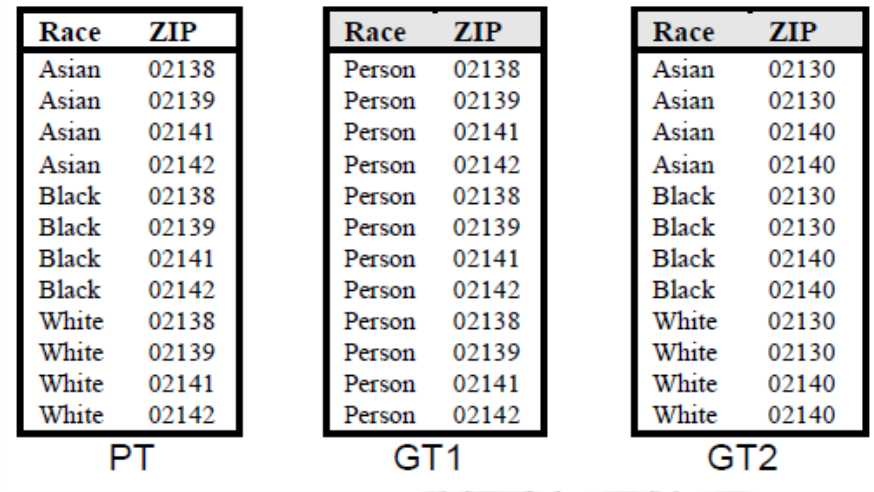
Περαιτέρω Βελτίωση ιδιωτικότητας με μελέτη επιθέσεων προσανατολισμένων στην κ-ανωνυμία

Για την βελτίωση της ιδιωτικότητας της βάσης, απαραίτητο είναι να μελετηθούν οι επιθέσεις που μπορεί να δεχτεί το μοντέλο της Κ-Ανωνυμίας. Στην συνέχεια θα παρουσιαστούν δύο σύνηθεις επιθέσεις όπου είναι σε θέση να εκμεταλευτούν τις αδυναμίες τις μεθόδου και να επαναταυτοποιήσουν τα δεδομένα.

Unsorted matching attack

Η επίθεση βασίζεται στην σειρά εμφάνισης των γραμμών. Ο επιτιθέμενος εκμεταλεύεται δύο ή περισσότερες βάσεις δεδομένων με τα ίδια στοιχεία ασθενων για παράδειγμα και όπου ο κάθε φορέας έχει εφαρμόσει διαφορετικές

γενικοποιήσεις και καταστολές δεδομένων. Ο επιτιθέμενος τότε συνδιάζοντας τα δεδομένα πολλών πινάκων δύναται να επανακατασκευάσει τον αρχικό μη γενικοποιημένο πίνακα όπως φαίνεται στο παρακάτω σχήμα.



Race	ZIP
Asian	02138
Asian	02139
Asian	02141
Asian	02142
Black	02138
Black	02139
Black	02141
Black	02142
White	02138
White	02139
White	02141
White	02142

PT

Race	ZIP
Person	02138
Person	02139
Person	02141
Person	02142
Person	02138
Person	02139
Person	02141
Person	02142
Person	02138
Person	02139
Person	02141
Person	02142

GT1

Race	ZIP
Asian	02130
Asian	02130
Asian	02140
Asian	02140
Black	02130
Black	02130
Black	02140
Black	02140
White	02130
White	02130
White	02140
White	02140

GT2

Εικόνα 11: Επαναπροσδιορισμός του PT από GT1, GT2

Οι δύο διαφορετικές γενικοποιήσεις του αρχικού PT είναι ο GT1 και GT2. Αν τους συνδιάσουμε τους πίνακες εκμεταλευόμενοι ότι οι γραμμές-εγγραφές διατηρούν την αυτή σειρά τότε για την πρώτη γραμμή επιλέγοντας την πιο σαφή πληροφορία από τους δύο πίνακες (Ασιάτης, ταχ. Κωδ. 02130) έχουμε την πλήρη εγγραφή. Η λύση για αυτού του είδους την επίθεση είναι σε κάθε ερώτημα στην βάση, η βάση να αποκρίνεται με τυχαία σειρά εγγραφών.

Temporal attack

Η επίθεση αυτή εκμεταλεύεται την ύπαρξη πολλών ανωνυμοποιημένων εκδόσεων μίας βάσης. Κάθε φορά που ανανεώνεται η βάση είναι δυνατό να απαιτηθεί η επαναδημιουργία μίας ανωνυμοποιημένης έκδοσης. Ο επιτιθέμενος συνδιάζοντας την αρχική ανωνυμοποιημένη έκδοση της βάσης καθώς και την νέα έκδοση μπορεί να εξάγει πληροφορίες. Λύση σε αυτό το πρόβλημα δίνεται με το να θεωρούμε ΟΛΑ τα χαρακτηριστικά της αρχικής βάσης σαν μέρος του Quasi Identifier.

Αρχιτεκτονική μοντέλου ασφαλείας της Amazon (AWS)

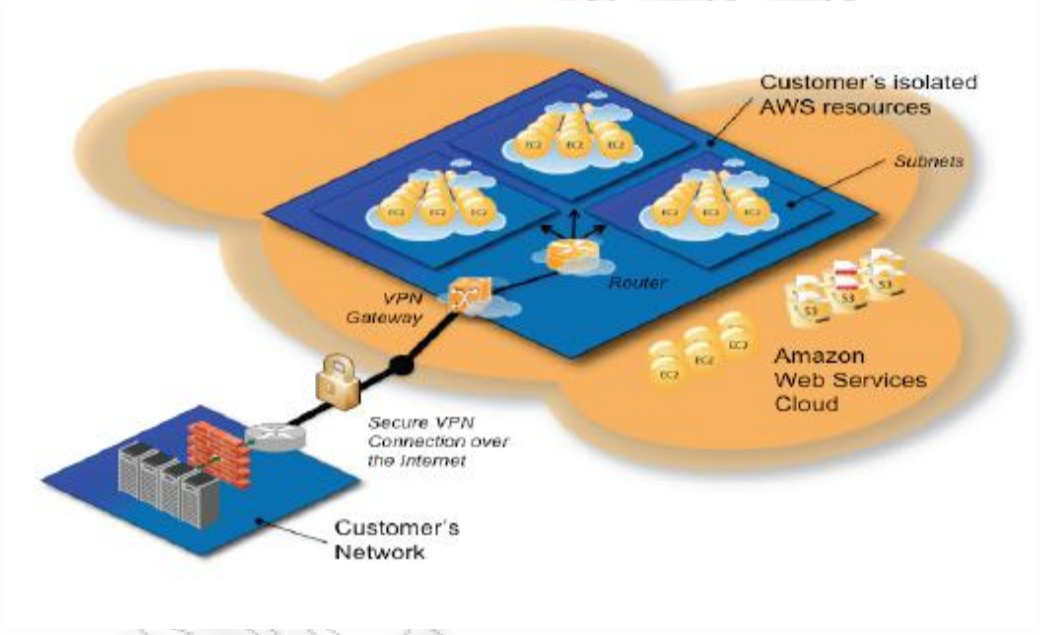
[25]

Σε αυτήν την ενότητα θα αναλύσουμε τεχνικά τους τρόπους με τους οποίους ο πάροχος υπηρεσίας διαδικτυακού υπολογιστικού πλέγματος επιτυγχάνει την

διατήρηση της ασφάλειας και της ιδιωτικότητας σε πολύ καλό επίπεδο. Για την παρουσίαση των τεχνικών αυτών θα χρησιμοποιήσουμε ένα πρακτικό παράδειγμα, το μοντέλο ασφαλείας των υπηρεσιών ιστού της Amazon.

Η επικοινωνία ενός πελάτη της Amazon με την δικτυακή της υποδομή της τελευταίας, επιτυγχάνεται με χρήση της τεχνολογίας εικονικού ιδιωτικού δικτύου (VPN). Το δοκιμασμένο πλέον IPSec πρωτόκολλο, χρησιμοποιείται προκειμένου να δρομολογηθούν τα πακέτα δεδομένων του πελάτη με ασφάλεια στους πόρους του διαδικτυακού υπολογιστικού πλέγματος.

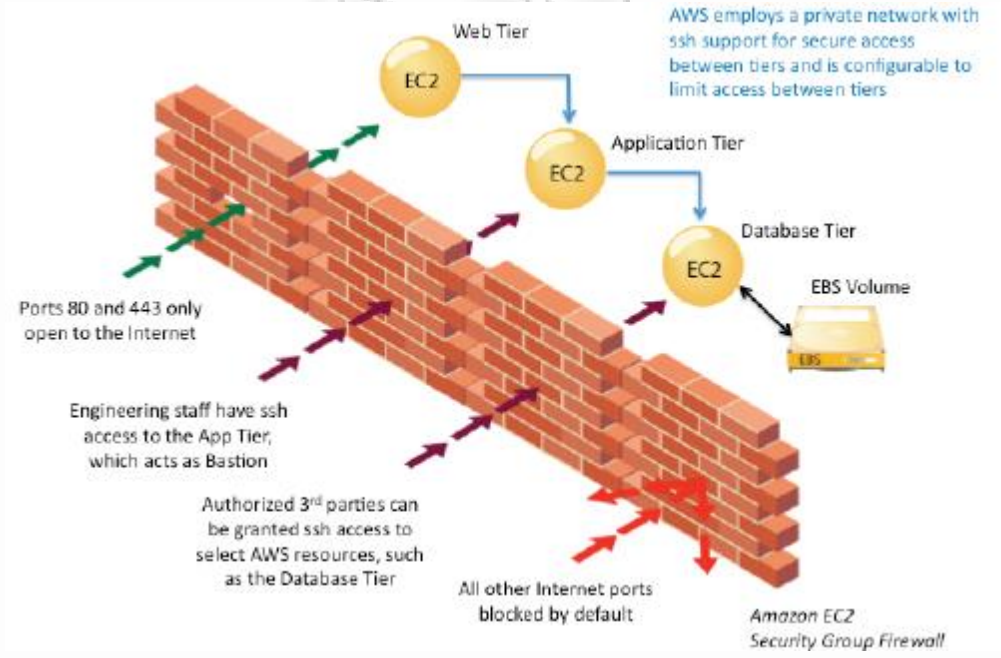
Μέριμνα για τον τομέα της ασφάλειας, λαμβάνεται σε πολλαπλά επίπεδα του διαδικτυακού υπολογιστικού πλέγματος. Αυτά περιλαμβάνουν το λειτουργικό σύστημα του πελάτη, το εικονικό λειτουργικό σύστημα, το τείχος προστασίας καθώς και τις κλήσεις Διεπαφών Εφαρμογών (APIs).



Εικόνα 12: Επικοινωνιακό κανάλι Πάροχου - Πελάτη

- Λειτουργικό Σύστημα Παρόχου. Η πρόσβαση στο λειτουργικό σύστημα του παρόχου πραγματοποιείται μέσω πολυεπίπεδης αυθεντικοποίησης ώστε να μειωθούν οι πιθανότητες εμφάνισης εισβολέα. Οποιαδήποτε ενέργεια καταγράφεται και ελέγχεται, και με τον τερματισμό των καθηκόντων τους, οι διαχειριστές του δικτύου χάνουν το δικαίωμα πρόσβασης στο σύστημα. Τέλος, η πρόσβαση στο λειτουργικό σύστημα δίδεται σε ορισμένο αριθμό ατόμων, και για συγκεκριμένες ενέργειες.

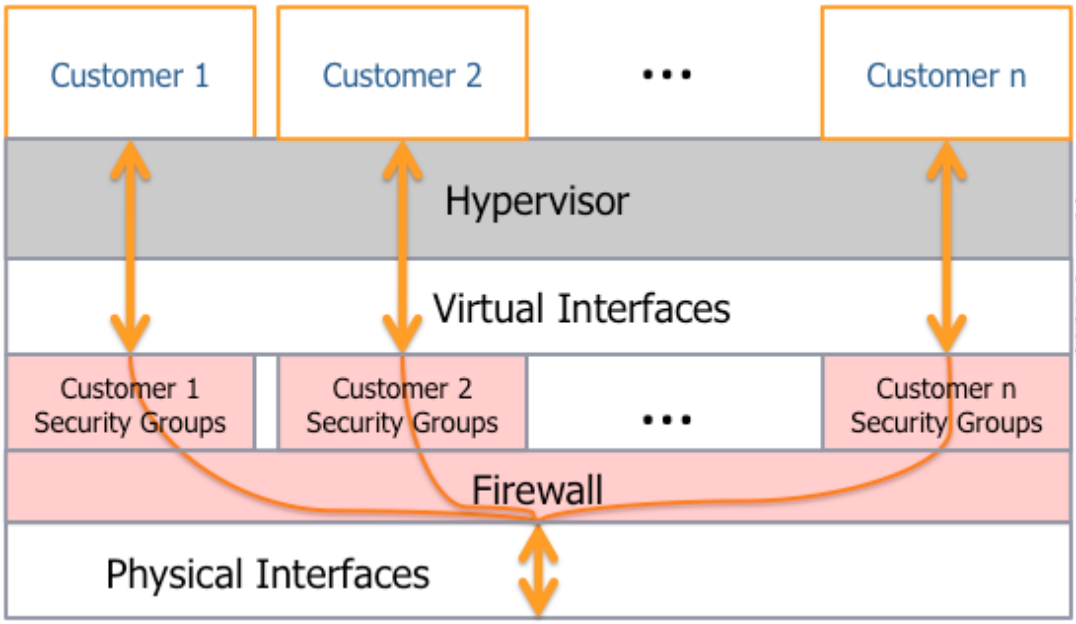
- Λειτουργικό Σύστημα Πελάτη. Η Amazon δηλώνε ότι δεν έχει πρόσβαση στα λειτουργικά συστήματα των πελατών της. Οι τελευταίοι, έχουν την επιλογή να αποφύγουν την απλή αυθεντικοποίηση με κωδικό πρόσβασης, και να επιλέξουν πιο εξελιγμένες τεχνικές, όπως η χρήση πιστοποιητικών, ή πολυεπίπεδη αυθεντικοποίηση. Περαιτέρω μέτρα για την ενίσχυση της ασφάλειας, περιλαμβάνουν την απενεργοποίηση της απομακρυσμένης σύνδεσης και την καταγραφή και ανάλυση όλως των ενεργειών των χρηστών. Οι πελάτες θα πρέπει να δημιουργούν τα δικά τους κλειδιά κρυπτογράφησης, προκειμένου να εξασφαλίσουν ότι είναι μοναδικά και δεν συμπίπτουν με κλειδιά άλλων πελατών.
- Τείχος προστασίας. Το τείχος προστασίας είναι ρυθμισμένο έτσι ώστε να απορρίπτει όλες τις συνδέσεις. Οι πελάτες ανοίγουν μόνο τις θύρες που χρειάζονται. Η ίδια η διαχείριση των παραμέτρων του τείχου προστασίας δεν επιτελείται δια μέσω του λειτουργικού συστήματος, αλλά απαιτείται ένα πιστοποιητικό τύπου X.509 και ένα κλειδί προκειμένου να δωθεί πρόσβαση στην κονσόλα ελέγχου των παραμέτρων. Σημαντική βελτίωση στην ασφάλεια προσφέρει η υιοθέτηση της πολιτικής να επιτρέπεται η πρόσβαση στις ρυθμίσεις του τείχους προστασίας σε συγκεκριμένους χρήστες/ομάδες σε καθορισμένες θύρες, για τους οποίους προσδίδεται το δικαίωμα να επιτελούν συγκεκριμένο και περιορισμένο σετ ενεργειών σε αυτές. Αυτό απεικονίζεται στο παρακάτω σχήμα:



Εικόνα 13: Το τείχος προστασίας της Amazon

Στην παραπάνω εικόνα παρατηρούμε ότι η πρόσβαση δια μέσω του τείχους προστασίας έχει χωριστεί σε ζώνες (Διαδικτυακή, Εφαρμογών, Βάσης Δεδομένων). Συγκεκριμένη ομάδα επιτρέπεται να διαχειριστεί μία συγκεκριμένη ζώνη. Για παράδειγμα μόνο το εξειδικευμένο προσωπικό έχουν πρόσβαση στην ζώνη ρύθμισης των εφαρμογών, και αποκλειστικά σε αυτήν. Εξουσιοδοτημένες τρίτες οντότητες έχουν προσβαση αντίστοιχα στην ζώνη της βάσης δεδομένων. Οι θύρες πρόσβασης των δύο ζωνών είναι διαφορετικές μεταξύ τους, ώστε να διαχωρίζουμε την πρόσβαση στις ζώνες ανάλογα με την ομάδα. Η πρόσβαση σε όλες τις ζώνες είναι περιορισμένης χρονικής διάρκειας.

- Προγραμματιστικές Διεπαφές Εφαρμογών. Όλες οι κλήσεις διεπαφών, απαιτούν την χρήση της υπογραφής με X.509 ψηφιακού πιστοποιητικού ή με το κρυφό κλειδί του πελάτη. Επιπλέον, οι κλήσεις είναι κωδικοποιημένες μέσω της χρήσης SSL.
- Hypervisor. Αυτή η μονάδα είναι υπεύθυνη για την ταυτόχρονη λειτουργία πολλαπλών λειτουργικών συστημάτων πελατών. Είναι Τύπου 2, δηλαδή όλα τα λειτουργικά συστήματα πελατών εκτελούνται πάνω στο λειτουργικό σύστημα του παρόχου. (Amazon) Αποτελεί ένα υπόστρωμα λογισμικού, το οποίο τοποθετείται μεταξύ του λειτουργικού συστήματος του παρόχου και του λειτουργικού συστήματος του πελάτη, προσφέροντας υπηρεσίες στους πελάτες. Η πρόσβαση στο λειτουργικό σύστημα του παρόχου είναι περιορισμένη και ρυθμίζεται μέσω ενός συστήματος απόδοσης προνομίων. Το λειτουργικό του παρόχου έχει το "προνόμιακό επίπεδο 0" δεικνύοντας το υψηλότερο προνομιακό επίπεδο, ενώ το λειτουργικό του πελάτη έχει επίπεδο 1. Η βαθμονόμηση αυτή διασφαλίζει ότι κανένας πελάτης δια μέσω του λειτουργικού του συστήματος δεν μπορεί να παρεισφρήσει στο λειτουργικό του παρόχου και να εκτελέση μη επιτρεπτές πράξεις. Το υπόστρωμα του Hypervisor σε συνδιασμό με το τείχος προστασίας, διαχωρίζει τα περιβάλλοντα των πελατών μεταξύ τους, περιορίζοντας δραστικά την πιθανότητα να επιτύχει κάποιος πελάτης να εισβάλλει στα δεδομένα άλλου πελάτη, ή διαφορετικά καθιστώντας την πιθανότητα αυτή ίδια με την πιθανότητα να εισβάλλει κάποιος εξωτερικός επιτιθέμενος στον διαδικτυακό υπολογιστικό πλέγμα δια μέσω του διαδικτύου. Ο δικτυακός διαχωρισμός των υποδομών των πελατών απεικονίζεται στην παρακάτω εικόνα:



Εικόνα 14: Διαχωρισμός της δικτυακής υποδομής των πελατών μέσω του Hypervisor

- Διαχωρισμός δεδομένων. Τα δεδομένα των πελατών τοποθετούνται σε πολλαπλές γεωγραφικές τοποθεσίες, ώστε να υπάρχει αυξημένη αξιοπιστία και διαθεσιμότητα δεδομένων σε περίπτωση απώλειας εξυπηρετητών. Επιλέγονται περιοχές χαμηλής σεισμικής δραστηριότητας, χρησιμοποιώντας αδιάλειπτη τροφοδοσία και πολλαπλούς εξυπηρετητές για αντίγραφα δεδομένων. Η Ευρώπη και η Αμερική θεωρούνται ως διαφορετικές-ανεξάρτητες ζώνες όπου ισχύουν διαφορετικοί κανόνες, και για αυτόν τον λόγο τα δεδομένα της μίας ζώνης αντιγράφονται στην άλλη εφόσον το επιθυμήσει ρητά ο πελάτης. Με αυτόν τον τρόπο αποφεύγουμε τις επιπλοκές από τις διαφορετικές ισχύουσες νομοθεσίες μεταξύ των δύο ζωνών.
- Πολυεπίπεδη αυθεντικοποίηση. Για την ενίσχυση της ασφάλειας, η Amazon προσφέρει στους πελάτες, μία συσκευή αυθεντικοποίησης, η οποία παράγει ένα εξαψήφιο κωδικό, τον οποίο τον εισάγει ο πελάτης στο σύστημα μαζί με τα υπόλοιπα στοιχεία αυθεντικοποίησης. Συγκεκριμένα εισάγουν την διεύθυνση ηλεκτρονικού ταχυδρομείου, ένα κωδικό πρόσβασης και τον κωδικό που παράγει η συσκευή.
- Εναλλαγή κλειδιών. Υπάρχει επιλογή να εναλλάσσονται τα κλειδιά και τα πιστοποιητικά ανα τακτά χρονικά διαστήματα, ούτως ώστε να περιορίζεται η πιθανότητα να έχουμε την αποκάλυψη τους απο επιτιθέμενους στο σύστημα.

Βιβλιογραφία κεφαλαίου

[1] Gartner, «Seven cloud-computing security risks,» [Ηλεκτρονικό]. Available: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[2] D. Binning, «Top five cloud computing security issues,» [Ηλεκτρονικό]. Available: http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm .

[3] J. Maguire, «The Many Dangers of Cloud Computing,» [Ηλεκτρονικό]. Available: http://www.itbusinessedge.com/topics/reader.aspx?oss=46132.

[4] C. Balding, «What's New in the Amazon Cloud?: Security Vulnerability in Amazon EC2 and SimpleDB Fixed (7.5 Months After Notification),» 2008. [Ηλεκτρονικό]. Available: http://cloudsecurity.org/blog/2008/12/18/whats-new-in-the-amazon-cloud-security-vulnerability-in-amazon-ec2-and-simpledb-fixed-75-months-after-notification.html.

[5] G. Trapani, «The Hidden Risks of Cloud Computing,» [Ηλεκτρονικό]. Available: http://lifehacker.com/5325169/the-hidden-risks-of-cloud-computing.

[6] B. Schneier, «Be Careful When You Come to Put Your Trust in the Clouds,» [Ηλεκτρονικό]. Available: http://www.schneier.com/essay-274.html.

[7] David Gregg, «Security Zone: Promoting accountability through ISO/IEC 27001 & 27002 (formerly ISO/IEC 17799),» [Ηλεκτρονικό]. Available: http://www.computerweekly.com/Articles/2009/01/06/233939/Security-Zone-Promoting-accountability-through-ISOIEC-27001-amp-27002-formerly-ISOIEC.htm.

[8] «Cloud Computing Security Risk Assessment,» European Network and Information Security Agency (ENISA) .

[9] C. S. Alliance, «Top Threats to Cloud Computing V1.0,» 2010.

[10] K. E. G. H. J. A. C. P. D. D. E. K. E. K. M. N. T. S. H. T. W. G. Klein, «Formal verification of an OS,» σε *Symposium on Operating Systems Principles*, 2009, pp. 207-220.

[11] T. C. Bryan Williams, «Virtualization System Security».

[12] E. C. F. J. Jon Oberheide, «Empirical Exploitation of Live Virtual Machine Migration».

[13] E. K. R. B. L. a. J. R. Jakub Szefer, «Eliminating the Hypervisor Attack Surface,» *ACM,* 2011.

[14] D. Hyde, «A Survey on the Security of Virtual Machines».

[15] T. G. M. Rosenblum, «When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments».

[16] [Ηλεκτρονικό]. Available: http://openid.net/get-an-openid/what-is-openid/ .

[17] Lucas, «eXtensible Access Control Markup Language (XACML) what is it and why is it important?,» [Ηλεκτρονικό]. Available: http://codingbliss.com/?p=161.

[18] F. Gaehtgens, «Finally: an open XACML API,» [Ηλεκτρονικό]. Available: http://blogs.kuppingercole.com/gaehtgens/2009/07/31/finally-an-open-xacml-api/.

[19] I. F. F. S. A. F. Bo Lang, «Attribute Based Access Control for Grid Computing».

[20] S. L. M. R. J. S. Y. W. Subra Kumaraswamy, «LINK:: Identity and Access Management Domain 12: Guidance for Identity and Access Management V2.1,» Cloud Security Alliancε, 2010.

[21] S. D. C. d. V. S. F. a. P. S. V. Ciriani, «k-Anonymity,» *Advances in Information Security ,* αρ. Springer US, 2007.

[22] D. R. J. Anderson, «Security in clinical information system,» Computer Laboratory University of Cambridge.

[23] L. Sweeney, «k-anonymity: a model for protecting privacy,» *International Journal on Uncertainty,,* 2002.

[24] S. D. C. d. V. S. F. a. P. S. V. Ciriani, «K-ANONYMOUS DATA MINING:A SURVEY,» *Advances in Database Systems.*

[25] «Amazon Web Services: Overview of Security Processes,» [Ηλεκτρονικό]. Available: http://aws.amazon.com/security.

Κεφάλαιο 3

Έλεγχος πρόσβασης και Διαχείριση Ταυτοτήτων σε Διαδικτυακό Υπολογιστικό Πλέγμα

Το διαδικτυακό υπολογιστικό πλέγμα στηρίζει την φιλοσοφία του στην παραχώρηση πόρων οι οποίοι μπορεί να είναι επεξεργαστική ισχύς, αποθηκευτικός χώρος, συνδέσεις δικτύου, εικονικές μηχανές, ή μία εφαρμογή που εκτελείται απομακρυσμένα. Όλα τα προηγούμενα παραχωρούνται προς χρήση στον αιτούντα κατόπιν "συννενοήσεως" με την μορφή της υπηρεσίας προς εξυπηρέτηση. Αυτού του είδους η "συννενόηση" δεν είναι τίποτα άλλο από μία αλληλουχία αιτημάτων και αποκρίσεων μεταξύ του αιτούμενου και του ιδιοκτήτη των πόρων (πάροχος) προκειμένου να παραχωρηθεί ο έλεγχος πρόσβασης, με την προυπόθεση ότι ο αιτούμενος την δικαιούται. Παρατηρούμε ότι το όλο μοντέλο του διαδικτυακού υπολογιστικού πλέγματος εδραιώνεται στον ***έλεγχο πρόσβασης***, ο οποίος διαδραματίζει πρωταγωνιστικό ρόλο, αφού ο χρήστης δεν έχει στην δικαιοδοσία του ούτε εφαρμογές ούτε πόρους, αλλά τις ζητάει από τον πάροχο ή έμμεσα από τρίτους που είναι συμβεβλημένοι με αυτόν. Το τελευταίο σενάριο είναι το πιο σύνηθες αφού το πλέγμα μπορεί να θεωρηθεί ως το αποτέλεσμα της συνεργασίας ενός συνόλου πάροχων που προσφέρουν πόρους σε ένα σύνολο πελατών. Εύκολα διαπιστώνει κανείς πόσο αυξάνει η πολυπλοκότητα του ελέγχου πρόσβασης, και πόσο μείζονος σημασίας είναι να σχεδιαστεί εξ αρχής με σωστό τρόπο, ώστε να μην δημιουργηθούν προβλήματα στην απόδοση του συστήματος λόγω μη ικανοποιητικής βάθμωσης του συστήματος δηλαδή να μη είναι εύκολο να εξυπηρετήσει μεγαλύτερο αριθμό πελατών.

Άξιο προσοχής είναι το πως ο πελάτης θα ζητά πρόσβαση από πολλούς διαφορετικούς υποπαρόχους με τον πλέον διαφανές τρόπο, αποφεύγοντας την συνεχή αυθεντικοποίηση με διαφορετικά διαπιστευτήρια σε διαφορετικούς εξυπηρετητές. Η αποφυγή αυτής της διαδικασίας δεν επιβάλλεται μόνο για λόγους διευκόλυνσης του πελάτη, αλλά και για ενίσχυση της ασφάλειας: η συνεχής αυθεντικοποίηση αυξάνει την πιθανότητα να διαρρεύσουν κάποια διαπιστευτήρια σε επιτιθέμενους στο σύστημα. Επίσης το γεγονός ότι διαπιστευτήρια ευρισκονται διεσπαρμένα σε διαφορετικούς εξυπηρετητές, διευκολύνει το έργο των επιτιθέμενων, προσφέροντας τους πολλαπλές επιλογές για επίθεση. Και είναι

απόλυτα λογικό ότι στα διάφορα σημεία αποθήκευσης διαπιστευτηρίων δεν θα εφαρμόζονται τα ίδια επίπεδα ασφαλείας, δίνοντας έτσι δυνατότητα επιλογής του πιό αδύναμου συστήματος, στον επιτιθέμενο.

Είναι κρίσιμο λοιπόν να αποφευχθούν κενά ασφαλείας, απόρρεια της ελλιπούς σχεδίασης του συστήματος ελέγχου πρόσβασης.

Στο κεφάλαιο αυτό θα γίνει μία μελέτη και παρουσίαση των προτεινόμενων τεχνολογιών ελέγχου πρόσβασης σε διαδικτυακό υπολογιστικό πλέγμα. Οι τεχνολογίες που προτείνονται είναι ανοιχτά πρότυπα, επεκτάσιμα και συνεχώς υπο βελτίωση από τις σημαντικότερες τεχνολογικές ομάδες.

Οπως περιγράψαμε παραπάνω ο έλεγχος πρόσβασης και η διαχείριση ταυτοτήτων των χρηστών αποτελεί μία από τις μεγαλύτερες προκλήσεις στα διαδικτυακά συστήματα διαδικτυακού υπολογιστικού πλέγματος. Οι χρήστες-πελάτες της υπηρεσίας, καλούνται να βρουν λύσεις για την μείωση του κόστους διαχείρισης πληροφοριακών συστημάτων καθώς και της πολυπλοκότητας τους αλλά την επιβολή μίας αξιόπιστης πολιτικής ασφαλείας, χωρίς όμως αυτή να περιορίζει την ευχρηστία του όλου συστήματος. Η όλη φιλοσοφία του διαδικτυακού υπολογιστικού πλέγματος στηρίζεται στην ομαδική συνεργασία διαφορετικών υπηρεσιών και εφαρμογών από διάφορους οργανισμούς. Το γεγονός αυτό καθιστά ακόμα πιο επιτακτική την λήψη επαρκών μέτρων ασφαλείας. Το κλειδί για την ομαλή μετάβαση στο διαδικτυακό υπολογιστικό πλέγμα αποτελεί η υιοθέτηση της Ενοποίησης των Ταυτοτήτων (Federated Identity) ώστε να λειτουργεί η επιχείρηση με ευελιξία και αυξημένη ασφάλεια στο διαδικτυακό πλέγμα.

Διαχείριση Ταυτοτήτων

[1]

Με την ενοποίηση των ταυτοτήτων, δημιουργούμε σχέσεις εμπιστοσύνης μεταξύ των εφαρμογών, πράγμα που αντικατοπτρίζει και τις υπηρεσιακές συνεργασίες των οργανισμών μεταξύ τους. Οι χρήστες δύνανται να κάνουν χρήση οποιαδήποτε υπηρεσίας, κάνοντας χρήση μίας ενιαίας ταυτότητας, και το πιο σημαντικό: την χρήση την κάνουν μία και μοναδική φορά εντός του συστήματος. Την επιτέλεση της εισόδου στο σύστημα μίας και μοναδικής φοράς την καλούμε ως Μοναδική Είσοδο (Single Sign On - SSO) στο παρόν κείμενο.

Για την χρήση της Ενοποιημένης Ταυτότητας, η οποία απαιτεί υψηλά μέτρα διαλειτουργικότητας, κρίνεται απαραίτητη η χρήση ανοιχτών προτύπων. Η SAML, ένα πρότυπο για την επικοινωνία των στοιχείων αυθεντικοποίησης είναι η πιο

κατάλληλη επιλογή. Η XACML αντίστοιχα συστήνεται ως το καταλληλότερο πρότυπο για την επεξεργασία και συγγραφή των πολιτικών ασφαλείας. Η χρήση κλασσικών μέτρων ασφαλείας όπως μετάδοση δεδομένων μέσω εικονικού δικτύου, είναι απόλυτα επίκαιρη και έγκυρη καθώς στην πλειοψηφία τους, τα προβλήματα ασφαλείας του πλέγματος είναι κοινά με αυτά που αντιμετωπίζει μία επιχείρηση που δεν ανήκει στο πλέγμα. Στο επόμενο τμήμα θα παρουσιαστεί η αρχιτεκτονική των τεχνολογιών αυτών μέσα από ενα πρακτικό παράδειγμα πρόσβασης ιατρικών φακέλων σε ένα νοσοκομείο.

Ο ρόλος της SAML (Security Assertion Markup Language)

Για την ομαλή συνεργασία όλων των φορέων κάτω από ένα κοινό μηχανισμό διαχείρισης ταυτοτήτων, είναι αναγκαίο να να ακολουθηθεί ένα κοινό πρότυπο. Το συστηνόμενο πρότυπο για αυτό τον μηχανισμό, αποτελεί η χρήση της τεχνολίας της SAML.

Η SAML είναι ένα πρωτόκολο το οποίο χρησιμοποιείται για να απεικονίσουμε πληροφορίες ασφαλείας. Βασίζεται στην XML και αναπαριστά πληροφορίες αυθεντικοποίησης, χαρακτηριστικών του υποκειμένου και αιτήσεις εξουσιοδότησης. Η XML αναπαράσταση διευκολύνει στην τυποποίηση του πρωτοκόλου και στην διαλειτουργικότητα με όλες τις ιατρικές εφαρμογές.

Οι πληροφορίες ασφαλείας περιγράφονται στην συνέχεια μέσω ενός τυπικού καθημερινού παραδείγματος προσβασης φακέλου ασθενούς σε ένα νοσοκομείο: Ένας ιατρός δηλώνει τον ρόλο του (χειρούργος) μέσω του πεδίου «χαρακτηριστικό υποκειμένου». Δηλώνει ότι επιθυμεί πρόσβαση στον φάκελο του ασθενή Χ με σκοπό να αποθηκεύσει νέα από τελέσματα από τις εξετάσεις του μαγνητικού τομογράφου μέσω του πεδίου «αίτηση εξουσιοδότησης». Τέλος στο πεδίο «αυθεντικοποίησης» δηλώνει τα προσωπικά του στοιχεία, τα οποία χρησιμοποιούνται από την αρχή αυθεντικοποίησης προκειμένου να επιβεβαιώσει ότι είναι αυτός που ισχυρίζεται και στην συνέχεια να εκδόσει ένα SAML κουπόνι (assertion) με όλες αυτές τις πληροφορίες και αιτήσεις του υποκειμένου.

Το σύστημα αποτελείται από ένα SAML asserting party το οποίο θα το ονομάζουμε ως αιτούμενη οντότητα και το SAML relying party η οντότητα που εξυπηρετεί τις αιτήσεις. Πρακτικά μία αιτούμενη οντότητα είναι για παράδειγμα μία ιατρός η οποία επιθυμεί να διαβάσει το συνταγολόγιο του ασθενούς και πραγματοποιεί μία αίτηση για ανάγνωση του συγκεκριμένου τμήματος του φακέλου. Η οντότητα αποδέχεται τις αιτήσεις στηριζόμενη σε μία σχέση εμπιστοσύνης μεταξύ εκείνης και του διαχειριστή ταυτοτήτων που πιστοποιεί ότι η οντότητα είναι όντως η Ιωάννα

Φράγκου και είναι ιατρός στο ΝΙΜΤΣ. Η οντότητα, ανάλογα με την πολιτική, εξυπηρετεί ή απορρίπτει το αίτημα. Η οντότητα αυτή είναι το πληροφοριακό σύστημα υγείας, το οποίο δέχεται αιτήσεις (SAML assertions) και αντλώντας την κατάλληλη πολιτική που έχει δημιουργηθεί για αυτήν, υπο τις συγκεκριμένες συνθήκες που ορίζει το πλαίσιο της αίτησης (πχ ώρα αίτησης, όνομα αιτούμενης και προυπάρχουσα δικαιοδοσία – φερ΄ ειπείν ανήκει η συγκεκριμένη ιατρός στην λίστα των ατόμων που έχουν πρόσβαση;) καταλήγει σε μία απόφαση εξουσιοδότησης.

Ένα από τα κύρια προβλήματα για την αποκάλυψη της ιδιωτικότητας αποτελεί η επανηλειμμένη αυθεντικοποίηση των υποκειμένων στους παρόχους υπηρεσιών. Το γεγονός αυτό εγκυμονεί τον κίνδυνο της αυξημένης πιθανότητας αποκάλυψης των διαπιστευτήριων πρόσβασης του ιατρού, από κάποιον που παρεμβάλεται στο κανάλι της επικοινωνίας είτε εντός του νοσοκομείου είτε εκτός. Η SAML λύνει το πρόβλημα της αναγκαιότητας της πολλαπλής αυθεντικοποίησης από τους υπάρχοντες μηχανισμούς με την υλοποίηση της Μοναδικής Είσόδου (Single Sign On). Με τον μηχανισμό αυτό, το υποκείμενο αυθεντικοποιείται μία φορά μόνο σε ένα υπεύθυνο διαχειριστή ταυτοτήτων. Στην συνέχεια ο πάροχος αυτός διακομίζει SAML κουπόνια που δηλώνουν την ταυτότητα του υποκειμένου σε οποιοδήποτε πάροχο υπηρεσιών: πχ το κέντρο ακτινολογίας της Λάρισσας, το καρδιολογικό τμήμα του Ωνασείου κ.ο.κ. Αναγκαίο προαπαιτούμενο είναι να βασίζονται όλοι οι φορείς σε μία σχέση εμπιστοσύνης με τον εγγυητή ταυτότητας, με την χρήση τεχνικών δημοσίου κλειδιού.

Αυτός ο μηχανισμός της μονής εισόδου με τον τρόπο που υλοποιείται προσφέρει ένα επιπλέον σημαντικό πλεονέκτημα: η διατήρηση των διαπιστευτηρίων γίνεται σε ένα κεντρικό εξυπηρετητή και όχι σε όλους τους εξυπηρετητές. Με αυτόν τον τρόπο αντί να έχουμε να επιλέξουμε από Ν εξυπηρετητές προκειμένου να εισβάλλουμε στην βάση δεδομένων και να αποσπάσουμε τα διαπιστευτήρια, μπορούμε να επικεντρωθούμε σε ένα εξυπηρετητή όσον αφορά την επιβολή των μέτρων ασφαλείας. Επιτυγχάνουμε την μεταφορά ευθυνών σε οντότητες οι οποίες είναι εξ αρχής σχεδιασμένες να υποστηρίζουν το επιχειρησιακό μοντέλο για το οποίο προορίζονται – διαχειριστές ταυτοτήτων για την αυθεντικοποίηση και παροχείς υπηρεσιών για την τέλεση των λειτουργιών.

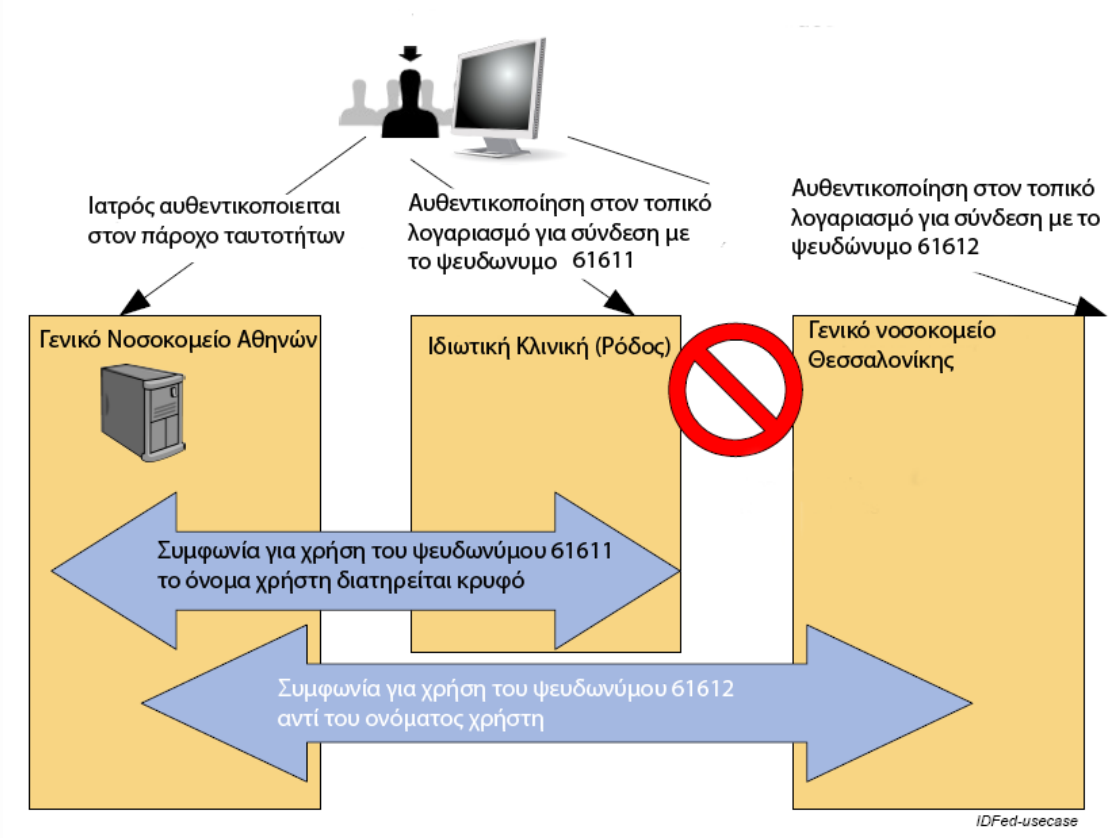
Παρόλα αυτά η λογική της μοναδικής αυθεντικοποίησης δεν έχει εισαχθεί με την SAML. Εξειδικευμένα πακέτα λογισμικού ήδη προσέφεραν υλοποιήσεις μοναδικής αυθεντικοποίησης τα οποία όμως διακατέχονταν από δύο σημαντικά μειονεκτήματα: α) το όλο σύστημα θα έπρεπε να εξοπλιστεί με πακέτα λογισμικού συγκεκριμένης εταιρείας προκειμένου να διασφαλιστεί η διαλειτουργικότητα και β) ο μηχανισμός μονής αυθεντικοποίησης επιτελούνταν με την χρήση των cookies, γεγονός το οποίο εισήγαγε αδυναμίες στην ασφάλεια των συστημάτων. Τα cookies

περιέχουν σημαντικές πληροφορίες αποθηκευμένες, οι οποίες είναι εύκολα προσπελάσιμες σε κακόβουλες τρίτες οντότητες.

Στο επόμενο τμήμα θα δωθεί ένα παράδειγμα το οποίο παρουσιάζει τον μηχανισμό επικοινωνίας των παρόχων μέσω του πρωτοκόλλου SAML. Μέσα από το πρακτικό παράδειγμα θα δωθεί και ο τρόπος με τον οποίο εξασφαλίζεται η πλήρης ανωνυμία στον χρήστη του πληροφοριακού συστήματος.

Ο ιατρός έχει εισέλθει στον εξυπηρετητή του νοσοκομείου και ταυτόχρονα έχει αυθεντικοποιηθεί αφού το νοσοκομείο τυγχάνει να είναι ο διαχειριστής ταυτοτήτων. Στην περίπτωση που θελήσει να λάβει δεδομένα ακτινογραφιών από το νοσοκομείο της Λάρισας, τότε εκείνο θα κάνει ανακατεύθυνση προς την κεντρική μονάδα διαχείρισης των ταυτοτήτων του ιατρικού προσωπικού της χώρας το οποίο έχει οριστεί να είναι το Γενικό νοσοκομείο Αθηνών " Γ. Γεννηματάς ".

Το παράδειγμα που θα παρουσιάσουμε εμπλέκει το Γενικό νοσοκομείο Αθηνών το οποίο έχει και την ιδιότητα του διαχειριστή ταυτοτήτων καθώς και μία ιδιωτική κλινική στην Ρόδο και το Γενικό Νοσοκομείο Παπαγεωργίου στην Θεσσαλονίκη τα οποία αποτελούν τους πάροχους υπηρεσιών.



Εικόνα 15:Μονή αυθεντικοποίηση και χρήση ψευδωνύμων

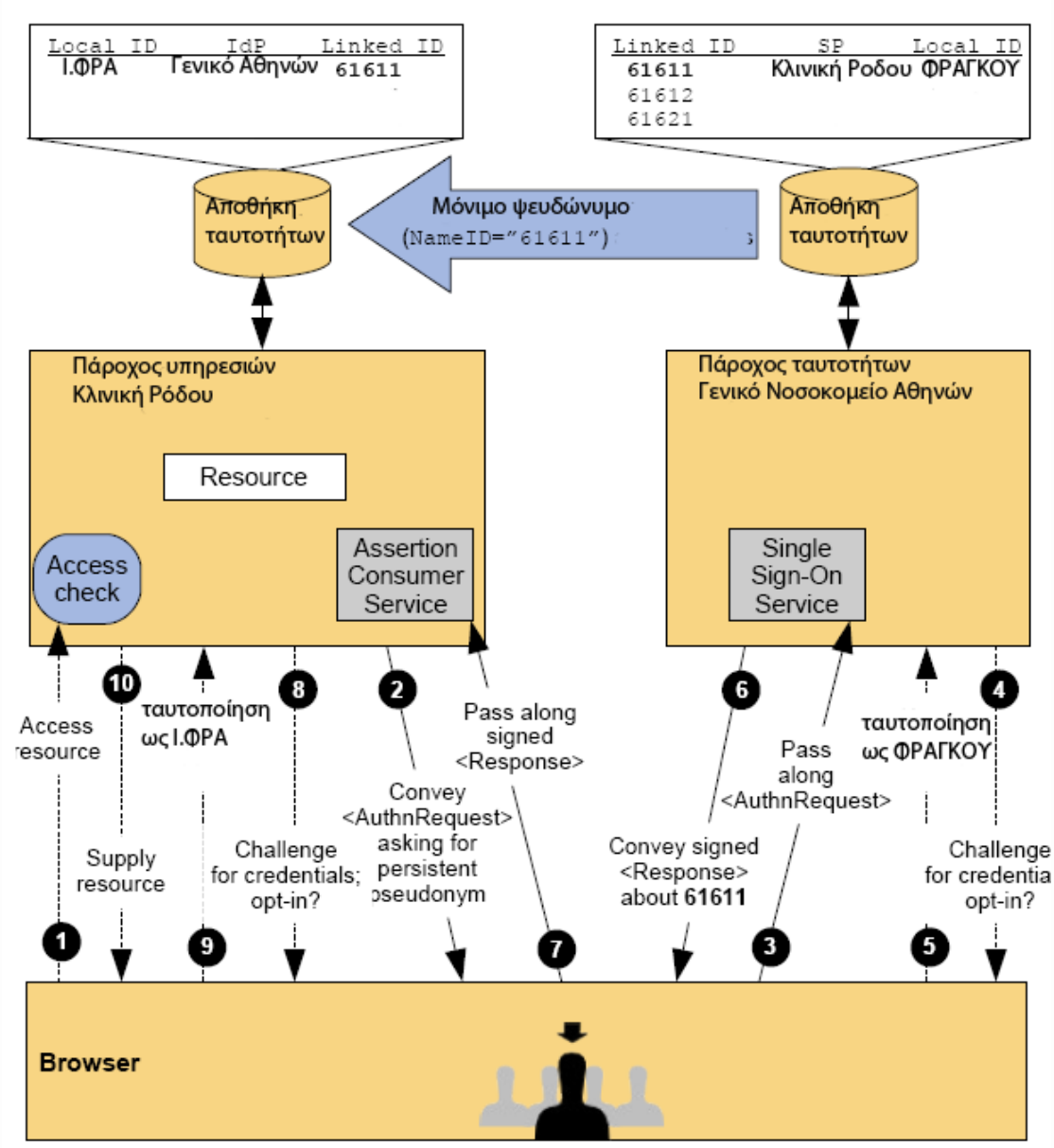
Επεξήγηση μηχανισμού πρόσβασης σε ένα πληροφοριακό σύστημα υγείας υλοποιημένο με SAML πρωτόκολο

Η ιατρός Ι.Φ η οποία εργάζεται στο Γενικό νοσοκομείο Αθηνών καλείται να λάβει τα αποτελέσματα αιματολογικών εξετάσεων ενός ασθενούς σε μία κλινική στην Ρόδο προκειμένου να χρησιμοποιηθούν για την έκδοση κατάλληλης αγωγής του ίδιου ασθενούς ο οποίος νοσηλεύεται στο Γενικό Αθήνας. Η Ι.Φ αυθεντικοποιείται στον διαχειριστή ταυτοτήτων ο οποίος στην προκειμένη περίπτωση είναι το Γενικό Αθηνών. Σε άλλο παράδειγμα θα μπορούσε να ήταν το Γενικό Θεσσαλονίκης οπότε σε αυτήν την περίπτωση το Γενικό Αθηνών θα έκανε ανακατεύθυνση της αίτησης για αυθεντικοποίηση προς το Γενικό Θεσσαλονίκης, το οποίο και θα πραγματοποιήσει την είσοδο της Ι.Φ στο σύστημα, και θα εκδόσει ένα κουπόνι αυθεντικοποίησης (assertion) το οποίο θα περιέχει το όνομα και τον ρόλο της (ιατρός) Ι.Φ αποτυπωμένο στις πληροφορίες «αυθεντικοποίησης» (authentication) και «χαρακτηριστικών» (attributes). Στο πεδίο «αίτηση εξουσιοδότησης» (authorization request) αναγράφεται η ενέργεια η οποία είναι η ανάγνωση των αιματολογικών εξετάσεων του ασθενούς. Μετά την επιτυχή αυθεντικοποίηση στον διαχειριστή ταυτοτήτων, η ιατρός ερωτάται αν επιθυμεί να ενοποιήσει τους δύο διαφορετικούς λογαριασμούς: τον λογαριασμό πρόσβασης στο Γενικό Αθηνών με τον λογαριασμό πρόσβασης στην κλινική της Ρόδου. Αν επιλέξει την ενοποίηση, τότε αποκτά πρόσβαση στην κλινική της Ρόδου χωρίς να χρειαστεί να εισάγει τα στοιχεία πιστοποίησης που διατηρεί εκεί και που προφανώς θα είναι ένα διαφορετικό σετ όνομα χρήστη και κωδικού πρόσβασης. Η όλη επικοινωνία μεταξύ των δύο νοσοκομείων γίνεται αποδίδοντας στην ιατρό ένα ψευδώνυμο (το 61611). Αυτό προσφέρει ανωνυμία καθώς δεν γίνεται συσχέτιση του ιατρικού προσωπικού με τους φακέλους των ασθενών. Το ψευδώνυμο είναι διαφορετικό για κάθε πάροχο υπηρεσιών. Στην περιπτωση που η ιατρός επιθυμούσε να συλλέξει αποτελέσματα της μαγνητικής τομογραφίας ασθενούς στο Γενικό Νοσοκομείο Θεσσαλονίκης, τότε ο διαχειριστής ταυτοτήτων του Γενικού Αθήνας θα προωθούσε το άιτημα αποδίδοντας ένα διαφορετικό ψευδώνυμο στο όνομα χρήστη (το 61612 του παραδείγματος).

Η λειτουργία ανάθεσης διαφορετικών ψευδωνύμων κατά υπηρεσία, είναι πολύ σημαντική. Ένας που παρακολουθεί το κανάλι επικοινωνίας δεν είναι δυνατόν να εξάγει συμπεράσματα βάσει των αιτήσεων του ιατρικού προσωπικού. Στην περίπτωση που χρησιμοποιούνταν ένα γενικό ψευδώνυμο για κάθε χρήστη, ίδιο για κάθε αίτημα του προς κάθε υπηρεσία, τότε ο επιτιθέμενος, θα μπορούσε να προσδιορίσει σε αρκετές περιπτώσεις την ταυτότητα του αιτούμενου μετα την συλλογή όλων των αιτήσεων στις διάφορες υπηρεσίες. Ακόμη χειρότερα, θα μπορούσε να αποσπάσει και την ταυτότητα του ασθενούς υπο ορισμένες

προυποθέσεις. Αν για παράδειγμα είναι γνωστό ότι η Ι.Φ έχει 5 ασθενείς υπο την επίβλεψη της, τότε ένας που διαπιστώνει ότι αιτείται προσβαση η ίδια γιατρός – το οποίο προδίδεται απο το καθολικό ψευδώνυμο – στον αιματολογικό, στο πνευμονολογικό και στο ακτινολογικό, μπορεί ένας να συμπεράνει ποιος από τους 5 ασθενείς είναι και μάλιστα να εξάγει πιο πολλές λεπτομέρειες για την κατάσταση της υγείας του. Για παράδειγμα ο ασθενής βρίσκεται σε προχωρημένο στάδιο καρκίνου αφου η ιατρός επικοινωνεί τακτικά με το τμήμα της χημειοθεραπείας.

Στο παράδειγμα μας το ψευδώνυμο είναι συγκεκριμένο για κάθε πάροχο υπηρεσιών και αναπαρίσταται στο ακόλουθο σχήμα:

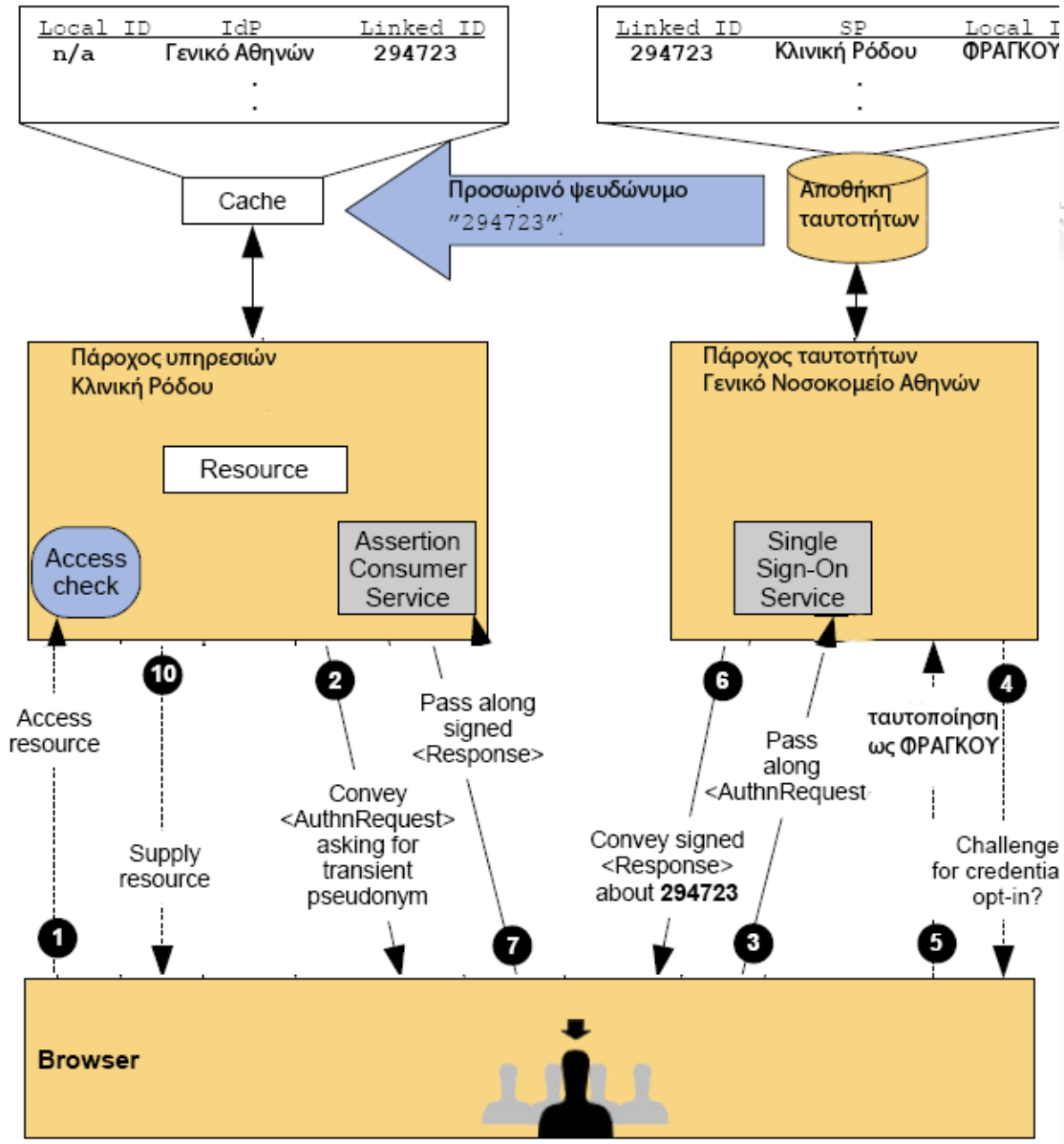


Εικόνα 16:Αναλυτική ροή χρήσης ψευδωνύμων

Το μόνιμο ψευδώνυμο 61611 έχει συσχετιστεί με την ιατρό Ι.Φ όπου ο πάροχος υπηρεσιών διαπιστώνει στην δική του βάση δεδομένων ότι πρόκειται για την συγκεκριμένη ιατρό. Η συσχέτιση γίνεται από το ψευδώνυμο και το διαχειριστή ταυτοτήτων τα οποία συνδέονται με τον τοπικό λογαριασμό της ιατρού στην κλινική της Ρόδου.

Παρόλα αυτά το σύστημα διακατέχεται από μία αδυναμία. Η ανάγκη τήρησης λογαριασμών σε κάθε πάροχο υπηρεσιών οι οποίοι μάλιστα συνδέονται με σταθερά προκαθορισμένα ψευδώνυμα εγκυμονεί κινδύνους για την ιδιωτικότητα στην περίπτωση που ένας αποκτήσει πρόσβαση σε μία βάση δεδομένων. Σε αυτήν την περίπτωση, αποκαλύπτεται η συσχέτιση του ψευδωνύμου με τον χρήστη και ακυρώνεται η ιδιωτικότητα στην επικοινωνία.

Για την αντιμετώπιση της αδυναμίας αυτής η τελευταία έκδοση της SAML υποστηρίζει την έννοια των δυναμικών ψευδωνύμων. Σύμφωνα με την τελευταία αυτή τεχνολογία, η διατήρηση τοπικών λογαριασμών σε κάθε πάροχο δεν είναι αναγκαία. Το προσωπικό διατηρεί αποκλειστικά ένα λογαριασμό ο οποίος διατηρείται στην βάση δεδομένων του Γενικού Νοσοκομείου Αθηνών. Στο παρακάτω σχήμα δεικνύεται πως επιτυγχάνεται η πλήρης ανωνυμία ενός χρήστη του πληροφοριακού συστήματος το οποίο χρησιμοποιεί την τεχνική των δυναμικών ψευδωνύμων:



Εικόνα 17:Αναπαράσταση χρήσης δυναμικών ψευδωνύμων

Ο μηχανισμός βασίζεται στην σχέση εμπιστοσύνης των παρόχων. Ο διαχειριστής ταυτοτήτων (Γενικό Αθηνών) παράγει ένα τυχαίο ψευδώνυμο και στέλνει το αίτημα στην κλινική της Ρόδου. Αυτή με την σειρά της, εμπιστευεται το Γενικό Αθηνών και συσχετίζει τον αιτούμενο χρήστη αποκλειστικά με το ψευδώνυμο. Στην συνέχεια αποφασίζει αν θα δώσει ή όχι πρόσβαση στην ιατρό – ανάλογα με την πολιτική της κλινικής.

Χαρακτηριστικό είναι ότι το ψευδώνυμο είναι συγκεκριμένο για κάθε αίτηση. Η ιατρός δεν συσχετίζεται με ένα συγκεκριμένο ψευδώνυμο όταν προσπελαύνει τον συγκεκριμένο πάροχο όπως προηγουμένως, αλλά σε κάθε συνέδρια ο διαχειριστής ταυτοτήτων της προσδίδει νέο ψευδώνυμο. Ο ωτακουστής του καναλιού δεν είναι σε θέση να αντιληφθεί πληροφορίες παρακολουθώντας το προφιλ των αιτήσεων

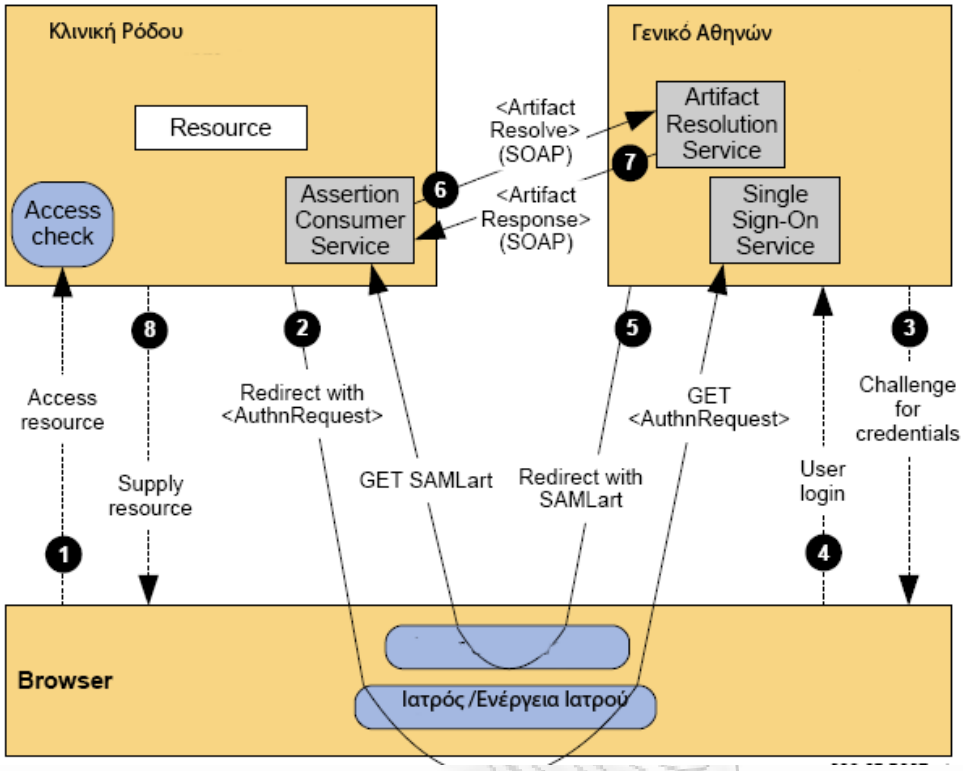
ενός χρήστη γιατι η ακύρωση της αντιστοιχίας ψευδωνύμου με χρήστη έχει ακυρωθεί και επομένως δεν είναι σε θέση να διακρίνει τους χρήστες.

Μία επιπλέον δικλείδα ασφαλείας που ενισχύει την ιδιωτικότητα είναι η άμεση διαγραφή της συσχέτισης του ψευδωνύμου με τον χρήστη με το πέρας της συνέδριας. Επομένως για την περίπτωση που κάποιος εισέλθει στην κεντρική βάση δεδομένων δεν είναι σε θέση να αντιληφθεί την ταυτότητα του χρήστη με το συγκεκριμένο ψευδώνυμο.

Ωστόσο υπάρχει μία περίπτωση που χρήζει προσοχής: αν ο επιτιθέμενος υποκλέψει ένα SAML άιτημα και εξαγει το ψευδώνυμο του αιτούμενου και αποκτήσει πρόσβαση στην κεντρική βάση δεδομένων πριν το περας της συνέδριας, τότε μπορεί να απομονώσει την ταυτότητα του αιτούμενου. Η SAML V2.0 αντιμετωπίζει το ενδεχόμενο αυτό, ενσωματώνοντας ένα νέο είδος πρωτοκόλλου επικοινωνίας το επονομαζόμενο «Artifact Protocol».

Το πρωτόκολο απεικονίζεται στο ακόλουθο σχήμα. Παρατηρούμε ότι η διαβίβαση του αιτήματος της ιατρού δεν επιτελείται μέσω του Web Browser. Αντί αυτού, το αίτημα βρίσκεται καταχωρημένο στον κεντρικό διαχειριστή ταυτοτήτων, και ο τελευταίος στέλνει ένα «δείκτη» προς την κλινική της Ρόδου. Στην συνέχεια η κλινική ανοίγει ένα απ' ευθείας ασφαλές προσωπικό κανάλι επικοινωνίας με το Γενικό Αθηνών και χρησιμοποιώντας τον δείκτη προσπελαύνει το αίτημα της γιατρού. Μετά την λήψη του αιτήματος, ο δείκτης σβήνεται από την βάση.

Βάσει των παραπάνω, ο επιτιθέμενος δεν είναι σε θέση να υποκλέψει το αίτημα της γιατρού. Το μόνο που έχει υποκλέψει είναι ένας δείκτης, ο οποίος όμως σβήνεται μετά την μεταφορά του αιτήματος στην κλινική της Ρόδου. Γενικότερα η εφαρμογή καθορισμένου χρονικού πλαισίου ισχύος του κάθε αιτήματος (timestamp) περιορίζει στο ελάχιστο τις επιθέσεις από υποκλοπές και επαναμετάδοση αιτημάτων.



Εικόνα 18:Αναπαράσταση λειτουργίας Artifact πρωτοκόλλου

Ο ρόλος της XACML

Η πιο σημαντική πρόκληση, για μία εταιρεία που μεταφέρει τα δεδομένα της στο διαδικτυακό υπολογιστικό πλέγμα, είναι η ταυτοποίηση οντοτήτων και ο καθορισμός ενός αποτελεσματικού συστήματος ελέγχου πρόσβασης, που θα μειώνει στο ελάχιστο το ρίσκο στην ασφάλεια.

Η εισαγωγή της έννοιας "πολιτική ασφαλείας" καλείται να λύσει τις αδυναμίες του υπάρχοντος συστήματος αυθεντικοποίησης με βάση τον χρήστη και μόνο. Ένα τέτοιο σύστημα, χρησιμοποιεί έλεγχο πρόσβασης χαμηλής ακρίβειας (coarse grain) καθώς οποιοσδήποτε χρήστης που αυθεντικοποιείται στο σύστημα έχει πλήρη πρόσβαση σε όλους τους πόρους. Ένα τέτοιο σύστημα κρίνεται ως ανασφαλές και χαμηλών προδιαγραφών ιδιωτικότητας. Δημιουργείται η ανάγκη να καθορίσουμε ένα πιο ακριβές μοντέλο (fine grain) ελέγχου πρόσβασης, με το οποίο θα λαμβάνουμε υπ'όψιν όχι μόνο ποιός χρήστης αυθεντικοποιείται, αλλά και τι επίπεδο πρόσβασης έχει σε κάθε υπομονάδα πόρων του συστήματος. Σε αυτό το σημείο, η XACML καλείται να καλύψει αυτές τις ανάγκες, προσφέροντας την δυνατότητα συγγραφής λεπτομερών πολιτικών ασφαλείας που καθορίζουν το επίπεδο πρόσβασης των χρηστών ή/και ομαδών χρηστών. [1]

Ο οργανισμός που χρησιμοποιεί το διαδικτυακό υπολογιστικό πλέγμα, θα πρέπει να εξασφαλίσει την απρόσκοπτη διαλειτουργικότητα των εφαρμογών του με ένα πλήρως εξωτερικευμένο σύστημα διαχείρισης εξουσιοδότησης. Στην ουσία αυτό σημαίνει ότι οι εφαρμογές θα πρέπει να είναι σχεδιασμένες με τέτοιο τρόπο ώστε να μπορούν να είναι συμβατές και να επεξεργάζονται πληροφορία δομημένη σύμφωνα με το πρότυπο XACML (eXtensible Access Control Markup Language).

Το XACML αποτελεί το κυρίαρχο πρότυπο γενικού σκοπού για την περιγραφή και επεξεργασία πολιτικών διαχείρισης δεδομένων και για τον καθορισμό αποφάσεων πρόσβασης. Το πρότυπο αυτό καθορίζει ένα συντακτικό μίας γλώσσας εκπεφρασμένης σε XML, καθώς και ένα μοντέλο διαχείρισης και επεξεργασίας των πολιτικών. Ο κύριος στόχος του προτύπου είναι να προσφέρει στους οργανισμούς μία στάνταρντ μεθοδολογία προς όλα τα συστήματα και τις εφαρμογές μέσω μίας κοινής γλώσσας, μιας κοινής και παγιωμένης μεθοδολογίας ελέγχου πρόσβασης και επιβολής πολιτικής. Το βασικό πλεονέκτημα είναι, ότι είναι ένα ανοιχτό πρότυπο που χρησιμοποιείται ευρέως από τους παρόχους, με αποτέλεσμα ο οργανισμός που το χρησιμοποιεί, αποφεύγει το κόστος που θα επέβαλλε η εναρμόνιση των εφαρμογών του με εξειδικευμένες και κλειστές αρχιτεκτονικές ελέγχου πρόσβασης που ακολουθούν διαφορετικές υλοποιήσεις από πάροχο σε πάροχο. Σύμβαση με πάροχο που ακολουθεί εξειδικευμένες λύσεις αναγκάζει τον πελάτη να αναδιαμορφώσει τις εφαρμογές του σε περίπτωση που αλλάξει πάροχο, αυξάνοντας το κόστος. Επιπλέον, στην περίπτωση της εξιδικευμένης αρχιτεκτονικής, ο πελάτης επαφίεται πλήρως στην πρωτοβουλία του συγκεκριμένου παρόχου σχετικά με την παροχή διορθώσεων, και αναβαθμίσεων του μοντέλου πράγμα που είναι πολύ περιοριστικό, συγκρίνοντας το με ένα ανοιχτό και συνεχώς εξελισσόμενο πρότυπο, στο οποίο συμμετέχουν ένα σύνολο από οργανισμούς για την βελτίωση και την εξέλιξη του. [2]

Πολιτική ασφάλειας με XACML

Η επέκταση των υπηρεσιών πρόσβασης μίας επιχείρησης στο διαδικτυακό υπολογιστικό πλέγμα επιτελείται από τον πάροχο. Το μειονέκτημα είναι ότι το όλο πλαίσιο εφαρμογής είναι σε αρκετά πρωτογενές επίπεδο. Παρόλα αυτά, η κατάσταση είναι δυνατόν να βελτιωθεί σημαντικά, με την προυπόθεση ότι ο πελάτης λάβει υπ' όψιν του ορισμένα μέτρα. Καταρχάς αναγκαίο είναι να συμφωνήσει με τον πάροχο σχετικά με την υιοθέτηση ανοιχτών προτύπων για την διαχείριση πρόσβασης. Με αυτόν τον τρόπο εξασφαλίζουμε την λειτουργία ενός συστήματος ευρείας αποδοχής και συνεπώς αντικείμενο συνεχούς εξελίξεως από τις πιό σημαντικές επιστημονικές ομάδες/οργανισμούς. Με την εφαρμογή ενός κοινώς αποδεκτού προτύπου, ο πελάτης θα πρέπει να επιδιώξει την υλοποίηση

ενός κεντρικού συστήματος διαχείρισης πρόσβασης εντός της έδρας του. Θα πρέπει να λάβει υπ 'όψιν του ότι η έκθεση των υπηρεσιών του στο διαδίκτυο επιβάλλει την συγγραφή κατάλληλων πολιτικών και διαδικασιών.

Για την αποτελεσματική διαχείριση των ταυτοτήτων σε ένα διαδικτυακό υπολογιστικό πλέγμα, ιδιαίτερη μέριμνα θα πρέπει να ληφθεί για την διαμόρφωση του συστήματος με δημιουργία και διαγραφή των χρηστών. Ο κάθε χρήστης συνδέεται με μία ταυτότητα, η οποία ορίζει τα δικαιώματα του όσον αφορά την πρόσβαση στο σύστημα. Παρατηρούμε λοιπόν, ότι αυτή η διαδικασία σχετίζεται άμεσα με τον έλεγχο πρόσβασης. Η διαδικασία αυτή θα πρέπει να επιτελείται ταχέως και με αυτοματοποιημένο τρόπο.

Για αυτόν τον λόγο χρησιμοποιείται η SPML (Service Provisioning Markup Language), υποδομή βασισμένη σε XML η οποία αναπτύσσεται από το OASIS γκρουπ, της οποίας ο στόχος είναι να προσφέρει με ένα κοινώς συμφωνημένο τρόπο την έκδοση υπηρεσιών ιστού και εφαρμογών, μεταξύ οργανισμών δια μέσω του διαδικτύου.

Οι πολιτικές ασφαλείας μεγάλων οργανισμών είναι ως επί το πλείστον πολύπλοκες και εφαρμόζονται σε πολλά διαφορετικά σημεία και από πολλά διαφορετικά κέντρα επιβολής. Για παράδειγμα, στοιχεία πολιτικής μπορεί να ασκούν τα τμήματα ανθρωπίνου δυναμικού, πληροφοριακών συστημάτων, νομικό ή το τμήμα οικονομικών. Ο τρόπος επιβολής ποικίλει: μία πολιτική μπορεί να επιβληθεί είτε μέσω ηλεκτρονικού ταχυδρομείου, WAN, ή και από συστήματα απομακρυσμένου ελέγχου. Η πρακτική που ασκούν τα σύγχρονα συστήματα είναι να τηρείται μία αυτόνομη διαχείριση πολιτική ασφαλείας σε κάθε σημείο ώστε να επιτυγχάνεται ο όσο το δυνατόν ακριβέστερος καθορισμός πολιτικής για το συγκεκριμένο σημείο επιβολής. Αυτό έχει ως αποτέλεσμα να καθιστά την μεταβολή μίας πολιτικής ως μία διαδικασία χρονοβόρα, πολύπλοκη και με μεγάλο κόστος. Επιπλέον με αυτό το πλαίσιο υλοποίησης πολιτικών, δεν είναι δυνατόν να έχουμε μία σαφή καθολική εικόνα για το επίπεδο ασφάλειας του οργανισμού. Για την διαχείριση των δικαιωμάτων στο διαδικτυακό υπολογιστικό πλέγμα, είναι αναμενόμενο ότι θα απαιτηθεί σημαντικός χρόνος προκειμένου να διασφαλιστεί η αρμονική λειτουργία των συστημάτων και εφαρμογών με μία εξωτερική υπηρεσία διαχείρισης δικαιωμάτων. Επιβάλλεται για αυτόν τον λόγο η χρήση ενός προτύπου με το οποίο θα καθορίζουμε πολιτικές πρόσβασης και αποφάσεις εξουσιοδότησης κάνοντας χρήση μίας κοινής γλώσσας. Η XML έχει αποδειχτεί ως η καταλληλότερη γλώσσα από άποψη ευκολίας στην εκμάθηση αλλά και στην επέκταση της προκειμένου να υποστηρίξει νέες έννοιες. Το πρότυπο XACML (eXtensible Access Control Markup Language) εξυπηρετεί με τον καλύτερο τρόπο όλες αυτές τις νέες απαιτήσεις. Αποτελεί το κυρίαρχο πρότυπο, και συγκροτείται από μία γλώσσα και μία μέθοδο για έλεγχο πρόσβασης και επιβολή πολιτικής. Η XACML συμπληρώνει το SAML πρότυπο: Ενώ η SAML καθορίζει το τρόπο που επικοινωνούν οι οντότητες και

διαβιβάζουν μεταξύ τους πληροφορίες ασφάλειας, η XACML καθορίζει τον τρόπο που υλοποιούνται και επεξεργάζονται οι πολιτικές ασφαλείας. Η XACML είναι συμβατή με την SAML αλλά ανεξάρτητη.

Στην συνέχεια θα δώσουμε ορισμούς για βασικές έννοιες στην XACML.

κατάσταση: έκφραση κατηγορημάτων. Το αποτέλεσμα μίας συνάρτησης που καλείται για να αποφανθεί στις καταστάσεις: "αληθές" , "ψευδές", "απροσδιόριστο".

απαίτηση για απόφαση: Η απαίτηση από ένα κέντρο επιβολής πολιτικής προς ένα κέντρο απόφασης προκειμένου το τελευταίο να εκδόσει απόφαση εξουσιοδότησης.

απόφαση εξουσιοδότησης: το αποτέλεσμα αξιολόγησης μίας εφαρμοζόμενης πολιτικής που επιστρέφει το κέντρο απόφασης στο κέντρο επιβολής πολιτικής. Είναι το αποτέλεσμα κλήσης συνάρτησης που έχει τις ακόλουθες τιμές εξόδου:"αποδοχή", "απόρριψη", "απροσδιόριστο", "μη εφαρμοζόμενο".

πλαίσιο: η απεικόνιση μίας απαίτησης για απόφαση και μίας απόφασης εξουσιοδότησης.

διαχειριστής πλαισίου: η οντότητα η οποία μετατρέπει ***απαιτήσεις για απόφαση*** από το εξειδικευμένο φόρματ της δομής της κλήσης του συστήματος, σε XACML κανονικοποιημένο. Αντίστοιχα μετατρέπει ***αποφάσεις εξουσιοδότησης*** εκπεφρασμένες σε μορφή XACML, στην μορφή που απαιτεί η δομή απόκρισης του συστήματος.

κανόνας: τμήμα μίας πολιτικής το οποίο είναι ο σκοπός, αποτέλεσμα ή κατάσταση.

πόρος: δεδομένα, υπηρεσία ή τμήμα συστήματος.

απόφαση: το αποτέλεσμα της αξιολόγησης ενός κανόνα, πολιτικής ή σετ πολιτικών.

πολιτική: ένα σύνολο κανόνων, ο καθορισμός ενός συγκεκριμένου αλγορίθμου συνδιασμού των κανόνων, και προαιρετικά ένα σύνολο από υποχρεώσεις ή συμβουλές.

Κέντρο Διαχείρισης Πολιτικών: η οντότητα που δημιουργεί πολιτικές ή σετ πολιτικών.

Κέντρο Αποφάσεων Πολιτικών: Η οντότητα που αξιολογεί τις πολιτικές και καθορίζει μία απόφαση εξουσιοδότησης.

Κέντρο Επιβολής Πολιτικών: Η οντότητα που επιτελεί τον έλεγχο πρόσβασης δια μέσω απαιτήσεων για απόφαση και επιβάλλοντας αποφάσεις εξουσιοδότησης.

Κέντρο Πληροφοριών Πολιτικών: οντότητα που παρέχει τις τιμές των διαφόρων χαρακτηριστικών που εμπεριέχονται στις πολιτικές.

κατηγόρημα:δήλωση για τα χαρακτηριστικά τα οποία είναι προς αξιολόγηση.

υποκείμενο: η οντότητα για την οποία καλείται το σύστημα να αποφανθεί για παραχώρηση προς αυτήν την αιτούμενη πρόσβαση.

Οι βασικές απαιτήσεις που καλύπτει η γλώσσα πολιτικής ασφαλείας είναι οι παρακάτω:

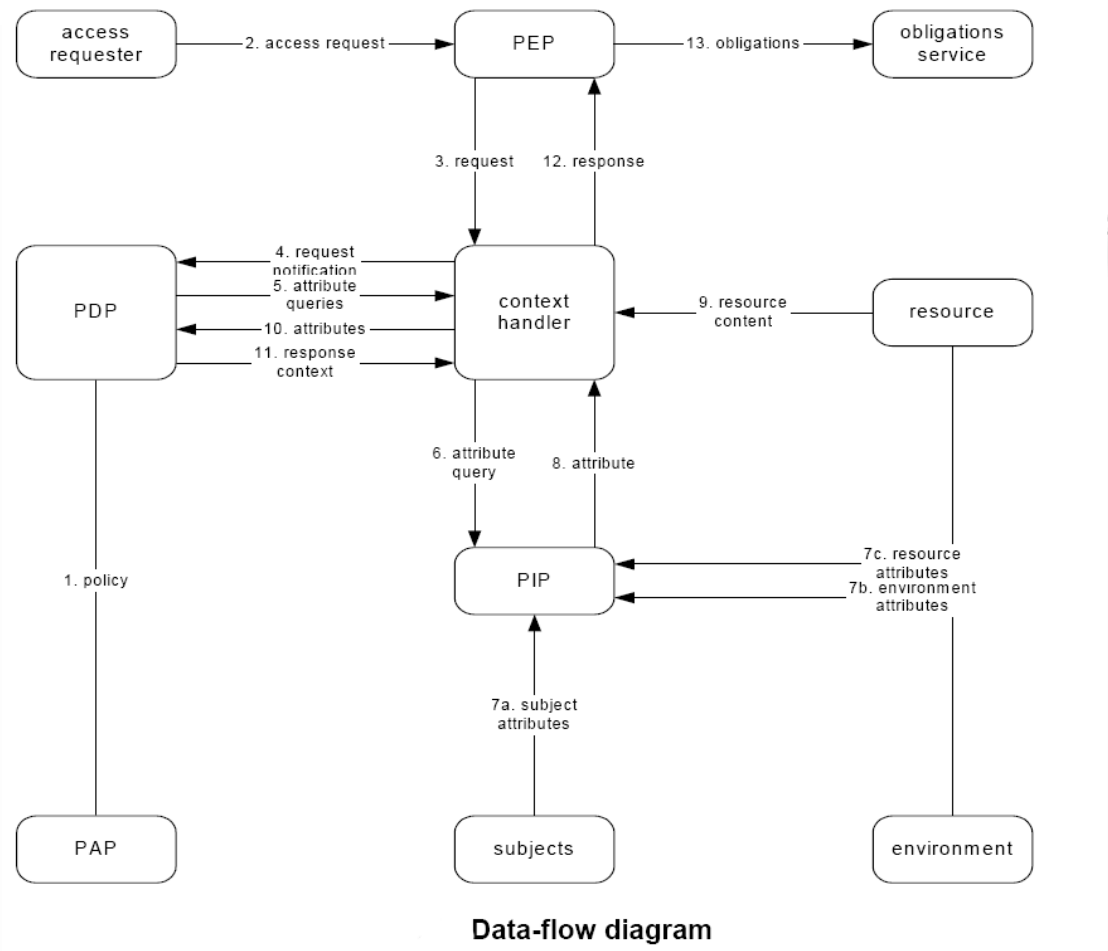
- Παροχή μεθόδου με την οποία συνδιάζονται κανόνες και πολιτικές σε ένα ενιαίο σετ πολιτικών, στο οποίο αντιστοιχεί μία συγκεκριμένη απαίτηση για απόφαση.
- Υπάρχει ευελιξία στην περιγραφή της διαδικασίας με την οποία οι κανόνες και οι πολιτικές συνδιάζονται.
- Παροχή υποστήριξης για πολλαπλά υποκείμενα καθώς και για χαρακτηριστικά που λαμβάνουν πολλαπλές τιμές.
- Παροχή μεθόδου για διαμόρφωση απόφασης εξουσιοδότησης βασισμένης σε χαρακτηριστικά του υποκειμένου καθώς και στους πόρους του υποκειμένου.
- Παροχή σετ λογικών και μαθηματικών τελεστών για την επεξεργασία των χαρακτηριστικών του υποκειμένου και των πόρων.
- Παροχή μεθόδου για εύρεση της πολιτικής που αντιστοιχεί σε συγκεκριμένη δράση, βασισμένη σε τιμές χαρακτηριστικών των υποκειμένων και πόρων.
- Παροχή επιπέδου αφαιρετικότητας στον συγγραφέα της πολιτικής όσον αφορά την εφαρμογή και το περιβάλλον υλοποίησης.

Αρχιτεκτονικό Μοντέλο της XACML

Το παρακάτω σχήμα απεικονίζει το μοντέλο ροής των δεδομένων της XACML καθώς και τις οντότητες που συγκροτούν την αρχιτεκτονική. Οι αρμοδιότητες της κάθε οντότητας θα περιγραφούν κατά την ανάλυση της αρχιτεκτονικής.

Ως πρώτο στάδιο, ένα υποκείμενο αιτείται πρόσβαση σε ένα πόρο, οπότε στέλνει μία απαίτηση στο **Κέντρο Επιβολής Πολιτικής (ΚΕΠ).** το **ΚΕΠ** είναι δυνατόν να έχει διάφορες μορφές. Είναι δυνατόν να είναι τμήμα ενός εξυπηρετητή διαδικτύου, ενός εξυπηρετητή ηλεκτρονικού ταχυδρομείου ή ακόμα και μία απομακρυσμένη πύλη.

Για αυτόν τον λόγο οι αιτήσεις, δεν έχουν όλες το ίδιο φόρματ, παρά ποικίλουν, ανάλογα με την μορφή του **ΚΕΠ**. Το γεγονός αυτό θα δημιουργούσε την απαίτηση να γραφούν οι πολιτικές σε διαφορετικά φορμάτ, ένα για κάθε τύπο **ΚΕΠ**. Αυτό είναι αναποτελεσματικό από άποψη συντήρησης του συστήματος: μία οποιαδήποτε αλλαγή στην πολιτική θα απαιτούσε αλλαγή σε όλες τις μορφές πολιτικών. Για τον λόγο αυτό, γεννιέται η ανάγκη να παρέχουμε την αίτηση για απόφαση σε μία κανονικοποιημένη μορφή, συμβατή με όλους τους τύπους των **ΚΕΠ**. Την κανονικοποίηση της φόρμας αίτησης προς μία φόρμα τύπου XACML την αναλαμβάνει ο *διαχειριστής πλαισίου*. Στην συνέχεια την νέα φόρμα, την μεταβιβάζει στο **Κέντρο Απόφασης Πολιτικής (ΚΑΠ)**. Το **ΚΑΠ** επεξεργάζεται την αίτηση και αν κρίνεται αναγκαίο επιτελεί μία σειρά ερωτημάτων στον *διαχειριστή πλαισίου* για περαιτέρω πληροφορίες. Αυτές οι πληροφορίες μπορεί να αφορούν *χαρακτηριστικά, πόρους, ενέργειες* και *γενικές πληροφορίες* του περιβάλλοντος της εφαρμογής. Στην περίπτωση αυτή, ο *διαχειριστής πλαισίου* λαμβάνει τις επιπρόσθετες πληροφορίες από το **Κέντρο Πληροφοριών Πολιτικής (ΚΠΠ).** Το **ΚΠΠ** διαβιβάζει όλες τις πληροφορίες στον *διαχειριστή πλαισίου* και ο τελευταίος με την σειρά του τις προωθεί στο **ΚΑΠ**. Στο **Κέντρο Διαχείρισης Πολιτικής (ΚΔΠ)** συγγράφονται οι πολιτικές και τα σετ πολιτικών, τα οποία είναι διαθέσιμα προς πρόσβαση από το **ΚΑΠ**. Το **ΚΑΠ** προσπελαύνει την βάση δεδομένων και λαμβάνει την πολιτική που αντιστοιχεί προς αυτήν την αίτηση πρόσβασης. Επιτελείται μία αξιολόγηση της πολιτικής, και στην συνέχεια επιστρέφει στον *διαχειριστή πλαισίου,* την *απόφαση εξουσιοδότησης*. Τέλος, ο διαχειριστής πλαισίου την μετατρέπει στο φόρματ που αντιστοιχεί στο **ΚΕΠ**, και την προωθεί σε αυτό. Το ΚΕΠ, αφού εκτελεί αν υπάρχουν, τις υποχρεώσεις, τελικώς επιτρέπει ή απορρίπτει το αίτημα στον αιτούμενο.



Εικόνα 19:Διάγραμμα ροής ενεργειών στο μοντέλο αρχιτεκτονικής XACML

Μελέτη ασφάλειας SAML/XACML

Τα προβλήματα ασφάλειας στον περιβάλλον του διαδικτυακού υπολογιστικού πλέγματος δεν είναι νεόφερτα. Ως επί το πλείστον είναι κλασσικά προβλήματα ασφάλειας, με την διαφορά ότι συνυπάρχουν σε ένα νέο πεδίο, το οποίο τα κάνει πιό σημαντικά από άποψη επιπτώσεων. [3]

Η ασφάλεια στην SAML

Γενικά η SAML δεν περιγράφει μηχανισμούς για την προστασία της ακεραιότητας και εμπιστευτικότητας των αιτημάτων της. Αυτά αναπαρίστανται σε XML μορφή και μεταδίδονται μεταξύ των παρόχων μέσω του πρωτοκόλλου SOAP. Ένας ωτακουστής του καναλιού επικοινωνίας δύναται να υποκλέψει και να διασαφηνίσει την πηγή και τον τελικό αποδέκτη του αιτήματος. Ακόμα και το ίδιο το αίτημα, το οποίο περικλείει την αίτηση εξουσιοδότησης αποκαλύπτει από μόνη του, τους φυσικούς πόρους του παρόχου μειώνοντας την ιδιωτικότητα του συστήματος.

Για παράδειγμα, ο ωτακουστής μαθαίνει ότι στην συγκεκριμένη τοποθεσία υπάρχει ακτινολογικό εργαστήριο ή κέντρο ελέγχου για τον υιο HIV.

Για την περαιτέρω ενίσχυση της ιδιωτικότητας, κρίνεται απαραίτητο να εφαρμοστεί κρυπτογράφηση για την επίτευξη της εμπιστευτικότητας και υπογραφή για την εξασφάλιση της ακεραιότητας των δεδομένων σε ένα SAML αίτημα. Επιπλέον μέτρα ασφαλείας, όπως HTTP over SSL/TLS μπορούν να χρησιμοποιηθούν σε επίπεδο μεταφοράς μηνυμάτων. Επίσης εφαρμογή IPsec κάτω από το επίπεδο του SOAP είναι μια καλή λύση η οποία μας επιτρέπει να αποφύγουμε την αναγκαιότητα για γράψιμο των εφαρμογών από την αρχή ώστε να υπακούει τις τεχνικές των ασφαλών πρωτόκολλων επικοινωνίας όπως με την περίπτωση του SSL.

Τεχνικές επίθεσεις με εισαγωγή αιτημάτων από τον επιτιθέμενο είναι δυνατόν να προκαλέσει κατάρρευση του συστήματος ή και υποκλοπή πληροφοριών. Μία προσφερόμενη λύση είναι η χρήση του πεδίου “InResponseTo” όπου συσχετίζει ένα συγκεκριμένο αποτέλεσμα με την αντίστοιχη αίτηση. Σε αυτήν την περίπτωση ο επιτιθέμενος θα πρέπει να μεσολαβήσει μετά την αίτηση και να παρεμβάλει την τεχνητή απόκριση, γεγονός που αυξάνει την δυσκολία του όλου εγχειρήματος.

Τεχνικές αλλοίωσης αιτημάτων είναι ικανές να προκαλέσουν απώλεια ιδιωτικότητας αλλά και ρήξη στην όλη ασφάλεια του συστήματος. Ο επιτιθέμενος δύναται να προσθέσει επιπλέον χαρακτηριστικά σε ένα αίτημα και στην συνέχεια, υποκλέπτοντας την απόκριση του συστήματος να εκμαιεύσει πληροφορίες για το σύστημα/αιτούμενο/ασθενή. Τέλος είναι σε θέση να μεταβάλλει και αποφάσεις εξουσιοδότησης πράγμα πολύ σοβαρό τόσο για την ιδιωτικότητα όσο και για την ασφάλεια. Κλασσικά αντίμετρα όπως υπογραφή σε επίπεδο XML (XML signature) βοηθούν να αποτραπούν αυτές οι ενέργειες.

Η χρήση του Artifact πρωτοκόλλου βοηθάει αποτελεσματικά στην διατήρηση της ιδιωτικότητας της πληροφορίας σε ένα SAML αίτημα.

Αξιοποίηση Web Services Standards στο πληροφοριακό σύστημα υγείας

Η SAML έχει το πλεονέκτημα ότι είναι επεκτάσιμη. Για αυτόν τον λόγο έχει υιοθετηθεί από διάφορα standards όπως τα WS-Security. Το standard αυτό προσφέρει μέτρα εξασφάλισης SOAP μηνυμάτων. Προσφέρει Αυθεντικοποίηση, ακεραιότητα δεδομένων, και εμπιστευτικότητα. Το WS-Security ενσωματώνεται σε ένα SOAP μήνυμα με το <Security> πεδίο εντός της SOAP επικεφαλίδας. Αυτό το πεδίο περικλείει πληροφορία σχετικά με τον τύπο της εφαρμοζόμενης ασφάλειας που χρησιμοποιείται για την προστασία του SOAP μηνύματος. Το WS-Security χρησιμοποιεί το XML Encryption και XML Signature για την κρυπτογράφηση και υπογραφή των μηνυμάτων και επιπλέον υποστηρίζει την τεχνική προσάρτησης

«χρονοσφραγίδας» (timestamp) στα μηνύματα. Τα αιτήματα στο WS-Security μπορεί να είναι:

- Δυαδικής μορφής XML (X509 certificates, Kerberos tickets)
- Δομημένης μορφής XML (SAML assertions)

Συμπερασματικά η χρήση τεχνολογίας WS-Security προσφέρει ασφάλεια σε επίπεδο SOAP μηνύματος, ενισχύοντας την ακεραιότητα και την εμπιστευτικότητα των αιτημάτων που πραγματοποιεί ο εκάστοτε χρήστης του πληροφοριακού συστήματος υγείας, είτε είναι ένας ασθενής είτε ο βασικός γιατρός της μονάδας.

Η ασφάλεια στην XACML

Το μοντέλο απειλής υποθέτει ότι ο επιτιθέμενος έχει αποκτήσει πρόσβαση στο κανάλι επικοινωνίας και είναι σε θέση να εισάγει, να μεταβάλλει και να σβήνει μηνύματα. Τα κύρια σημεία τα οποία είναι ευάλωτα στις επιθέσεις είναι τα κέντρα επιβολής πολιτικής, κέντρα απόφασης και κέντρα διαχείρισης. Στο ακόλουθο τμήμα θα επικεντρωθούμε στην ανάλυση των απειλών σε ένα ιατρικό σύστημα βασισμένο στην XACML.

Η XACML από μόνη της, δεν προσφέρει μηχανισμούς για να εγγυηθεί την εμπιστευτικότητα. Για την εμπιστευτικότητα είναι αναγκαία η χρήση της κρυπτογράφησης των μηνυμάτων στο μοντέλο ροής της XACML. Η εισαγώγη μηνυμάτων μπορεί να αποφευχθεί με αμοιβαία αυθεντικοποίηση με SSL και με συνδυασμό χρήσης αρίθμησης μηνυμάτων (sequence numbers).

Είναι σημαντικό να διασφαλιστεί ότι το υποκείμενο όχι μόνο έχει αυθεντικοποιηθεί αλλά έχει και εξουσιοδότηση να στέλνει αιτήσεις.

Σημαντικό ρόλο διαδραματίζει η γνώση του υπεύθυνου ασφαλείας του συστήματος. Περιπτώσεις όπου δεν γνωρίζει λεπτομερώς το σύστημα και την απόκριση του είναι ικανές να καταρρίψουν της ιδιωτικότητα του συστήματος. Για παράδειγμα ας υποθέσουμε ότι στο Γενικό νοσοκομείο Αθηνών έχουμε το ιατρικό προσωπικό και το βοηθητικό προσωπικό, και έχουμε γράψει μία πολιτική σύμφωνα με την οποία μόνο το ιατρικό προσωπικό έχει πρόσβαση στα άκρως ευαίσθητα αποτελέσματα εξετάσεων HIV. Αν ενοποιήσουμε το τμήμα αυτό του νοσοκομείου με ένα άλλο στο οποίο απότελείται από το ιατρικό προσωπικό αλλά το βοηθητικό προσωπικό έχει διαφορετική ονομασία ομάδας, για παράδειγμα « πρόσθετο προσωπικό» , τότε η ενοποίηση των τμημάτων θα έχει ως αποτέλεσμα να μην αναγνωρίσει η πολιτική την νέα ομάδα (πρόσθετο προσωπικό) και να μην την αποκλείσει από την ανάγνωση των αποτελεσμάτων όπως θα έπρεπε. Το αποτέλεσμα είναι ότι το προσθετο

προσωπικό θα αποκτήσει δικαιώματα της ιατρικής ομάδας. Ένα δεύτερο παράδειγμα είναι η χρήση αρνητικών κανόνων. Αν δίνουμε για παράδειγμα πρόσβαση στους φακέλους σε όλους τους γιατρούς εκτός από τους παθολόγους και υπάρχει η περίπτωση λανθασμένης διαμόρφωσης του κέντρου απόφασης, η πολιτική θα εκτελεστεί και ο αρνητικός κανόνας απλά θα παραβλεφτεί! Αυτό θα έχει ως αποτέλεσμα να αποκτήσουν πλήρη πρόσβαση στο σύστημα οι παθολόγοι. Σημαντικό ρόλο παίζει και η διαμόρφωση του πληροφοριακού συστήματος. Χαρακτηριστικό παράδειγμα αποτελεί η απειλή των «NotApplicable» αποτελεσμάτων. Ο επιτιθέμενος στέλνει μία αίτηση ούτως ώστε να μην είναι σε θέση να βρεθεί μία αντίστοιχη πολιτική από το κέντρο διαχείρισης και να έχουμε απόκριση με την ένδειξη «NotApplicable». Αυτή η απόκριση μεταφράζεται ως επιτροπή για πρόσβαση από την πλειονότητα των εξυπηρετητών. Ο επιτιθέμενος αποκτά πρόσβαση με αυτόν τον τρόπο. Ο διαχειριστής θα πρέπει να γνωρίζει καλά την συμπεριφορά του συστήματος σε κάθε περίπτωση και να το καθορίζει. Στην προκειμένη περίπτωση συνίσταται να συσχετίσει την απόκριση «NotApplicable» με άρνηση εξυπηρέτησης.

Από τα παραπάνω συμπεραίνουμε ότι είναι αναγκαία η αυθεντικοποίηση του κέντρου επιβολής πολιτικής στο κέντρο απόφασης πολιτικής και το αντίστροφο. Στην πρώτη περίπτωση αποφεύγουμε την αποστολή αποφάσεων εξουσιοδότησης σε μη επιτρεπτά κέντρα επιβολής πολιτικής, και στην δεύτερη περίπτωση αποφεύγουμε την αποστολή αιτημάτων για πρόσβαση σε μη πιστοποιημένα κέντρα τα οποία υποκλέπτουν πληροφορίες. Η εμπιστευτικότητα επιτυγχάνεται μέσω καναλιού SSL και σε επίπεδο μηνύματος με κρυπτογράφηση του XACML μηνύματος. Οι πολιτικές αποτελούν την καρδιά ενός συστήματος και είναι απαραίτητο να υπογράφονται ώστε να αποφύγουμε την τροποποίηση τους από τρίτους και την μη εξουσιοδοτημένη λήψη ελέγχου πληροφοριών απόρρητων. Η πιστοποίηση των πολιτικών δεν θα πρέπει να γίνεται μόνο με κριτήριο του ποιος υπέγραψε την πολιτική.

Επίσης θα πρέπει να δωθεί προσοχή στο σύστημα διαχείρισης των πολιτικών ασφαλείας. Κάθε πολιτική θα πρέπει να συσχετίζεται με ένα μοναδικό κωδικό. Οποιαδήποτε αδυναμία τήρησης μοναδικού αναγνωριστικού για κάθε πολιτική έχει σαν αποτέλεσμα την εκτέλεση λανθασμένης πολιτικής με συνέπεια την λήψη εξουσιοδότησης για χρήση πόρων τους οποίους δεν έχει δικαιοδοσία.

Τέλος τα κέντρα επιβολής πολιτικής και κέντρα απόφασης θα πρέπει να έχουν σχέση εμπιστοσύνης μεταξύ τους. Ο οργανισμός διατηρεί σε μία και μοναδική κόπια τα δεδομένα ταυτοποίησης των χρηστών τα οποία διαχειρίζεται το σύστημα διαχείρισης ταυτοτήτων και δεν τα μοιράζεται ή κοινοποιεί σε ουδεμία οντότητα εντός ή εκτός του οργανισμού. Στην συνέχεια, και βασιζόμενος στην σχέση εμπιστοσύνης μεταξύ του οργανισμού και των διαφόρων εξωτερικών υπηρεσιών, το

σύστημα διαχείρισης ταυτοτήτων ανταλλάσσει στοιχεία μη ιδιωτικής φύσεως με τις εκάστοτε υπηρεσίες και στην συνέχεια αυτές αποδέχονται το αίτημα για εξυπηρέτηση από τον χρήστη. Η όλη εμπειρία που αποκομίζει ο χρήστης είναι απόλυτα θετική: με απόλυτη διαφάνεια χρησιμοποιεί όλες τις υπηρεσίες επιτελώντας μία και μοναδική απόδοση διαπιστευτηρίων στο σύστημα. Καταργείται η αναγκαιότητα πολλαπλής αυθεντικοποίησης με διαφορετικά ζεύγη ονομάτων/κωδικών. Εκτός αυτού, η αποθήκευση των διαπιστευτηρίων σε ένα κεντρικό σημείο ενισχύει δραματικά την ασφάλεια.

Βιβλιογραφία Κεφαλαίου

[1] m. K. L. K. a. B. T. Kevin Hamlen, «Security Issues for Cloud Computing,» The Univerity of Texas Department of Computer Science, Dallas, 2010.

[2] D. McGuire, «CACloud E-Guide».

[3] «Evaluating IaaS security risks,» [Ηλεκτρονικό]. Available: SearchCloudSecurity.com.

[4] OASIS, «eXtensible Access Control Markup LAnguage (XACML) Version 3.0,» 2010.

[5] P. G. M. J. R. M. J. M. E. S. J. S. Richard Chow, «Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control».

[6] S. Cantor, «Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID saml-core-2.0-os.,» 2005.

[7] F. Hirsch, «Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID saml-secconsider- 2.0-os,» 2005.

[8] T. Moses, «OASIS eXtensible Access Control Markup Language (XACML),» OASIS XACML-TC,, 2005.

[9] «IDENTITY FEDERATION IN A HYBRID CLOUD COMPUTING ENVIRONMENT SOLUTION GUIDE implementation guide,» Juniper Networks.

Κεφάλαιο 4

Πρακτική Εφαρμογή Διαδικτύου με Εξουσιοδότηση βασισμένη στο πρότυπο XACML

Περιγραφή του περιβάλλοντος ανάπτυξης της εφαρμογής

Στα πλαίσια της παρούσας εργασίας, υλοποιήθηκε μία διαδικτυακή εφαρμογή στην γλώσσα προγραμματισμού Java. Η εφαρμογή αυθεντικοποιεί και εξουσιοδοτεί χρήστες για πρόσβαση στους πόρους του συστήματος, οι οποίοι στην συγκεκριμένη περίπτωση είναι το σύστημα αρχείων. Ο σκοπός της εφαρμογής ήταν να αξιοποιηθεί η υποδομή βιβλιοθηκών XACML που υποστηρίζει ο JBoss Application Server.

Σημείωση: *Η διαδικτυακή εφαρμογή που υλοποιήθηκε, είναι εγκατεστημένη σε ένα Virtual Machine το οποίο παραδίδεται στην παρούσα Διπλωματική εργασία σε ένα DVD. Το παραδοτέο, περιλαμβάνει:*

- *το project με τον πηγαίο και εκτελέσιμο κώδικα Στο Eclipse Indigo IDE περιβάλλον.*
- *εγκατάσταση του JBoss Application Server για την εκτέλεση της εφαρμογής.*
- *πολιτικές XACML που έχουν γραφτεί για την μελέτη ποικίλλων σεναρίων εξουσιοδότησης σε περιβάλλον διαδικτυακού υπολογιστικού πλέγματος, αλλά και για την επαλήθευση της λειτουργικότητας που έχει αναπτυχθεί στα πλαίσια της εργασίας.*

Ο JBoss Application Server (AS) , ανήκει στην κατηγορία του ανοιχτού λογισμικού και βασίζεται σε εφαρμογές γραμμένες σε Java Enterprise Edition (EE). Η Java EE, αποτελεί μία επέκταση της JAVA, και ενισχύει την τελευταία, με την προσθήκη ενός συνόλου διεπαφών και λειτουργικότητας που αφορούν τις υπηρεσίες ιστού και τα δίκτυα, προσανατολισμένες σε επιχειρησιακό λογισμικό με γνώμονα την αξιοπιστία και ασφάλεια. Ο JBoss AS ανήκει πλέον στην Red Hat. [1]

Ο JBoss AS ενσωματώνει από την έκδοση 5.0 την ονομαζόμενη ως JBoss XACML βιβλιοθήκη. Αυτή αποτελεί μία υλοποίηση του XACML V2.0 προτύπου όπως αυτό έχει καθοριστεί από τον οργανισμό OASIS. Καθορίζει διεπαφές για ανάγνωση και επεξεργασία πολιτικών και προσφέρει ένα object model συμβατό με JAXB v2.0 το οποίο μπορεί να χρησιμοποιηθεί για δημιουργία πολιτικών και αιτημάτων και

αποκρίσεων συμβατών με το XACML πρότυπο. Η JAXB (Java Architecture for XML Binding) αποτελεί ένα μοντέλο το οποίο επιτρέπει την αντιστοίχιση Java κλάσεων σε δομές XML [2]. Εν κατακλείδι. ο σκοπός της βιβλιοθήκης JBoss XACML, είναι να προσφέρει ένα έλεγχο εξουσιοδότησης υψηλής ακρίβειας (fine grain) στις εφαρμογές γραμμένες σε Java EE.

Περιγραφή και εκτέλεση της εφαρμογής

Η διαδικτυακή εφαρμογή που αναπτύχθηκε, εχει ως στόχο την υλοποίηση της εξουσιοδότησης σε χρήστες, βασισμένο σε ρόλους αλλά και χαρακτηριστικά αυτών. Η αιτούμενη πρόσβαση είναι μία διαδρομή καταλόγου,και πραγματοποιείται κατόπιν επιτυχούς αυθεντικοποίησης του χρήστη και έπειτα από παροχή εξουσιοδότησης για πρόσβαση από τον μηχανισμό XACML. Η επιτυχής πρόσβαση έχει ως αποτέλεσμα την απεικόνιση των αρχείων του ζητούμενου καταλόγου.

Για τον έλεγχο πρόσβασης, επιλέχτηκε το πρότυπο XACML, το οποίο βασίζεται σε χαρακτηριστικά. Για λόγους πληρότητας της υλοποίησης, τροποποιήθηκε ο μηχανισμός, ώστε να υποστηρίζει και ρόλους υποκειμένων. Συνεπώς, για την απόφαση της εξουσιοδότησης, λαμβάνεται υπ'όψιν ένα σύνολο χαρακτηριστικών, καθώς και ο ρόλος του υποκειμένου. Η δυνατότητα της ομαδοποίησης των χρηστών σε ρόλους, προσφέρει ένα επιπλέον βαθμό ελευθερίας στον διαχειριστή του συστήματος κατά την διαδικασία της συγγραφής και διαμόρφωσης των πολιτικών.

Η εφαρμογή, επιτρέπει την αποθήκευση χρηστών σε μία βάση δεδομένων. Οι πληροφορίες που αποθηκεύονται είναι το όνομα χρήστη, ο κωδικός πρόσβασης και ο ρόλος.

Το πρώτο στάδιο ελέγχου είναι η αυθεντικοποίηση με βάση το όνομα και τον κωδικό πρόσβασης. Στην συνέχεια, και αφού αυθεντικοποιηθεί επιτυχώς ο χρήστης, λαμβάνονται υπ'οψιν η διαδρομή καταλόγου η οποία έχει δωθεί στο αίτημα, και προσπελαύνει την βάση δεδομένων για να εξάγει τον ρόλο του χρήστη, χρησιμοποιώντας ως κλειδί το όνομα του. Το επόμενο στάδιο αφορά την μελέτη μία προς μία όλες όλων των πολιτικών του συστήματος, χρησιμοποιώντας για δεδομένα το

- όνομα του χρήστη
- ρόλος του χρήστη
- διαδρομή καταλόγου

Το Κέντρο Επιβολής της Πολιτικής προσκομίζει όλα τα παραπάνω στοιχεία χρήστη στο Κέντρο Απόφασης Πολιτικής, το οποίο με την σειρά του συνδιάζει τα στοιχεία αυτά και εκδίδει αποφάσης για κάθε πολιτική του συστήματος.

Να τονίσουμε ότι για λόγους ασφαλείας, η απόφαση "Not Applicable" δεν θεωρείται ως κατάφαση για την εξουσιοδότηση πρόσβασης. Επίσης, αν έστω και ένα αποτέλεσμα επεξεργασίας πολιτικής είναι αρνητικό, τότε υπερισχύει των όποιων θετικών αποτελεσμάτων και αυτόματα απορρίπτεται η πρόσβαση στον χρήστη (Deny Overrides).

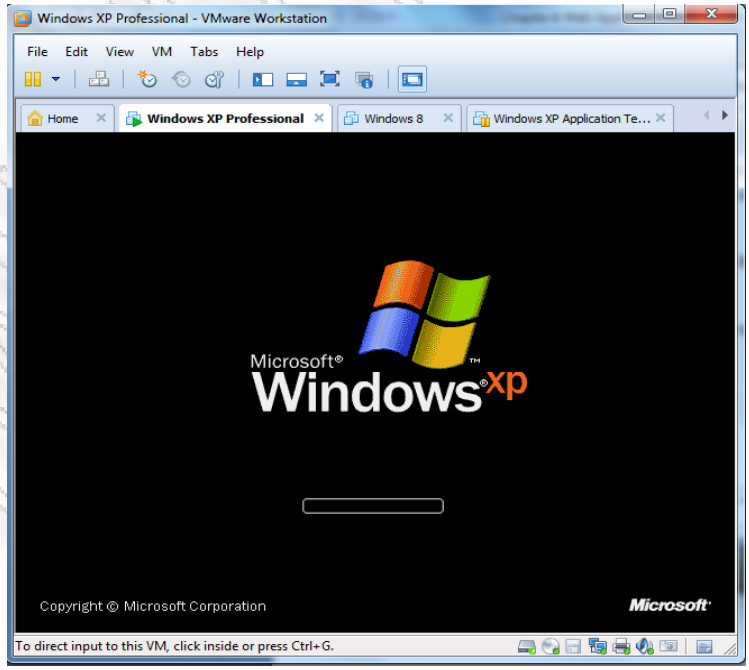
Στο επόμενο τμήμα θα παρουσιάσουμε την εφαρμογή και τον τρόπο εκτέλεσης καθώς και ένα σύνολο παραδειγμάτων πολιτικών και αποφάσεων.

Το παραδοτέο της διπλωματικής εργασίας είναι μία εικονική μηχανή με το λειτουργικό των Windows XP εγκατεστημένο. Στο λειτουργικό αυτό έχουμε εγκαταστήσει τον JBoss Application Server, το Eclipse IDE, καθώς και το project σε μορφή πηγαίου αλλά και εκτελέσιμου κώδικα.

Το πρώτο βήμα είναι να αντιγράψουμε τα περιεχόμενα του DVD σε ένα κατάλογο, στον εξυπηρετητή.

Για την φόρτωση του εικονικού μηχανήματος, υπάρχουν εργαλεία διαφορετικών εταιρειών. Για την παρουσίαση χρησιμοποιήθηκε το VMWare Workstation 8.

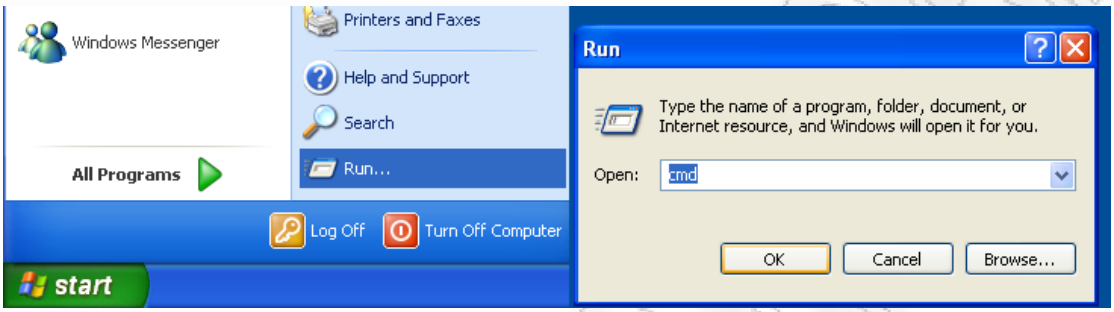
Επιλέγοντας File -> Open και το αρχείο "Windows XP Professional", δίνουμε στην συνέχεια την επιλογή "I copied it" και εκκινεί το λειτουργικό σύστημα:



Εικόνα 20:Εκκινώντας την εικονική μηχανή του DVD

Για την εκκίνηση της εφαρμογής θα φορτώσουμε μία συνεδρία του JBoss Application Server.

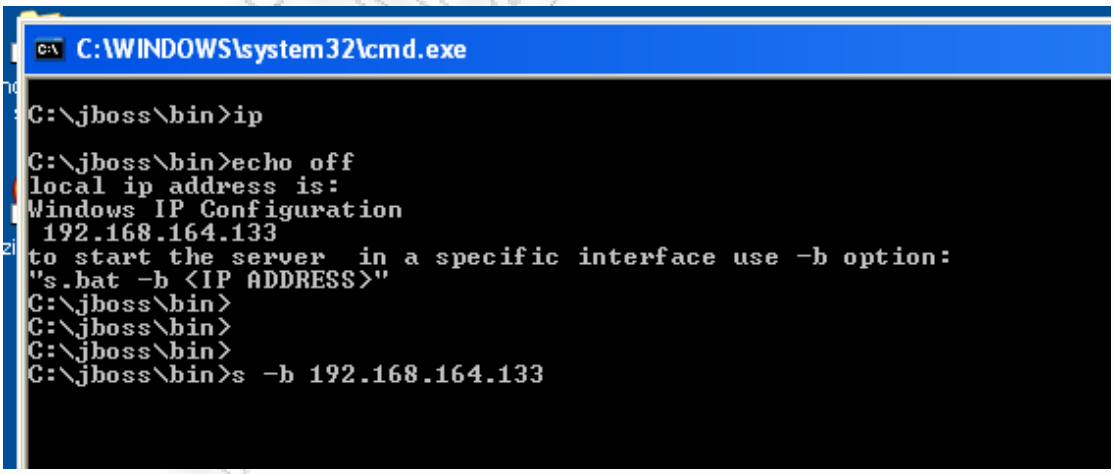
Εκκινούμε την γραμμή εντολών επιλέγοντας το "Run" και δίνοντας cmd.



Εικόνα 21:Ανοίγωντας παράθυρο γραμμής εντολών

Στην γραμμή εντολών, μετακινούμαστε στον κατάλογο c:\jboss\bin και εκτελούμε το αρχείο ip.bat για να εξάγουμε την IP Address του συστήματος. Αυτή θα χρησιμοποιηθεί για να φορτώσουμε τον JBoss ώστε να ακούει αιτήματα σταλμένα αποκλειστικά σε αυτήν την διεύθυνση.

ο JBoss εκτελείται καλώντας το αρχείο **s.bat**. Για την εκτέλεση του στην διεύθυνση του συστήματος που στην προκειμένη περίπτωση είναι η 192.168.164.133 , χρησιμοποιούμε την επιλογή **-b** όπως απεικονίζεται στο σχήμα παρακάτω:



Εικόνα 22: Εκκινώντας τον JBoss Application Server σε συγκεκριμένη IP

Ο Server θα φορτώσει με την σειρά του την διαδικτυακή μας εφαρμογή, η οποία την έχουμε ονομάσει ως *"jboss-as-policy"*. Ένδειξη ότι η εφαρμογή έχει φορτώσει και

είναι έτοιμη να δεχτεί αιτήματα, αποτελεί η τελευταία γραμμή όπως φαίνεται στην επόμενη εικόνα, η οποία αναφέρει ότι: *Deployed "jboss-as-policy.war".*

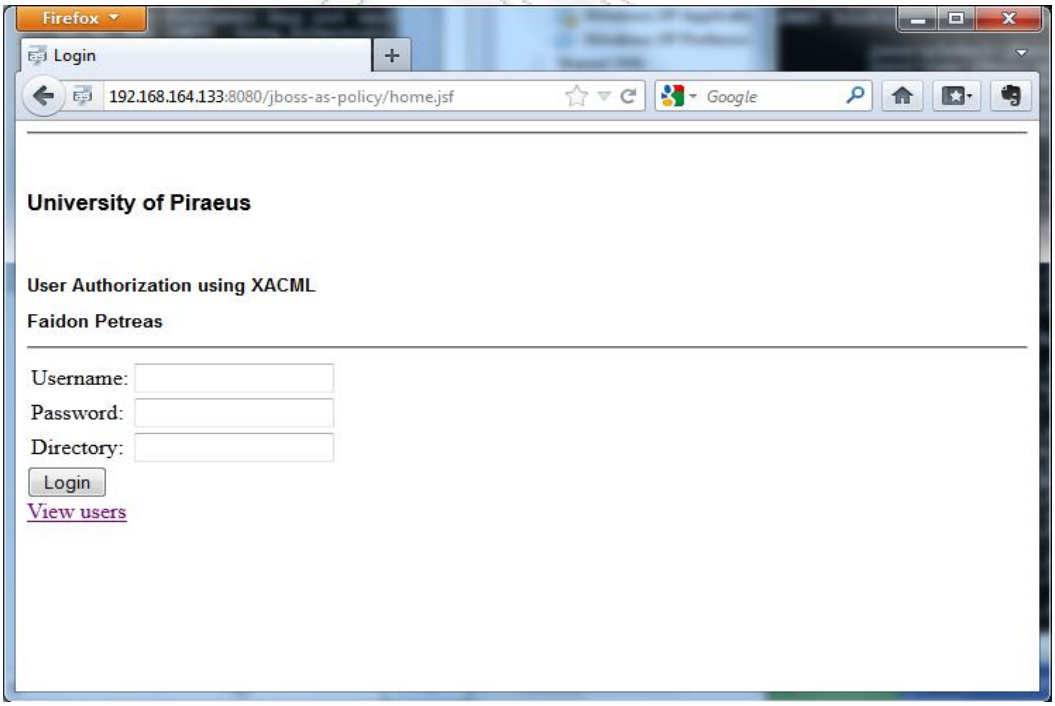
Εικόνα 23: Ολοκλήρωση της φόρτωσης της διαδικτυακής εφαρμογής αυθεντικοποίησης και εξουσιοδότησης

Η εφαρμογή έχει φορτωθεί σε μία συνέδρια του JBoss Application Server, και ελιναι προσπελάσιμη από οποιοδήποτε φυσικό ή εικονικό μηχάνημα του δικτύου, μέσω της διεύθυνσης 192.168.164.133 και πόρτας 8080.

Ανοίγουμε ένα περιηγητή ιστοσελίδων και δίνουμε ως διεύθυνση ιστού την:

http://192.168.164.133:8080/jboss-as-policy/home.jsf

Η εισαγωγική οθόνη της εφαρμογής παραθέτει τρία στοιχεία για συμπλήρωση από τον χρήστη:



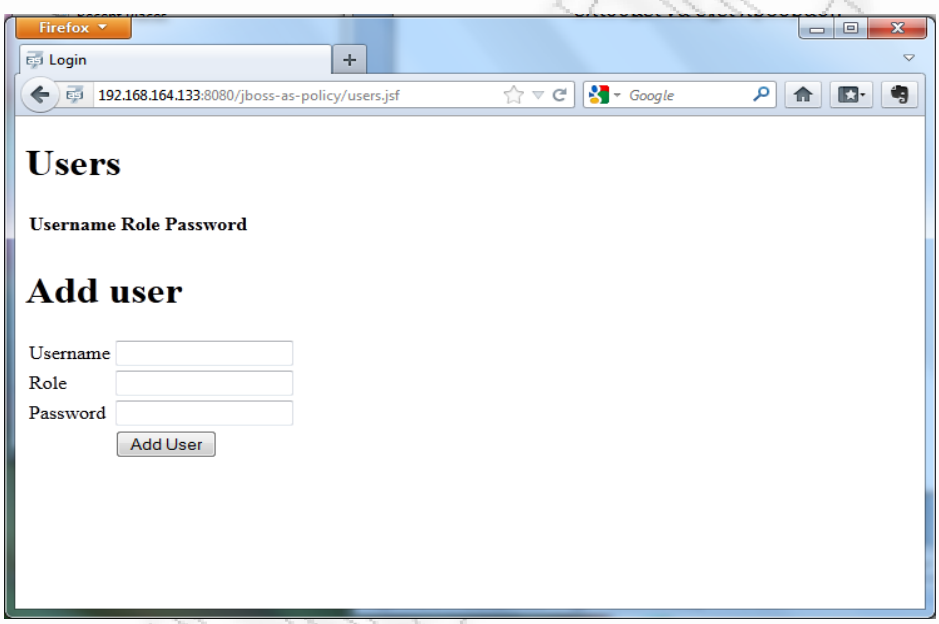
Εικόνα 24: Αρχική οθόνη της εφαρμογής

Το όνομα, τον κωδικό πρόσβασης και τέλος την διαδρομή καταλόγου στην οποία επιθυμεί να έχει πρόσβαση.

Πατώντας την επιλογή "View Users" παρατηρούμε τους χρήστες του συστήματος που έχουν αποθηκευτεί.

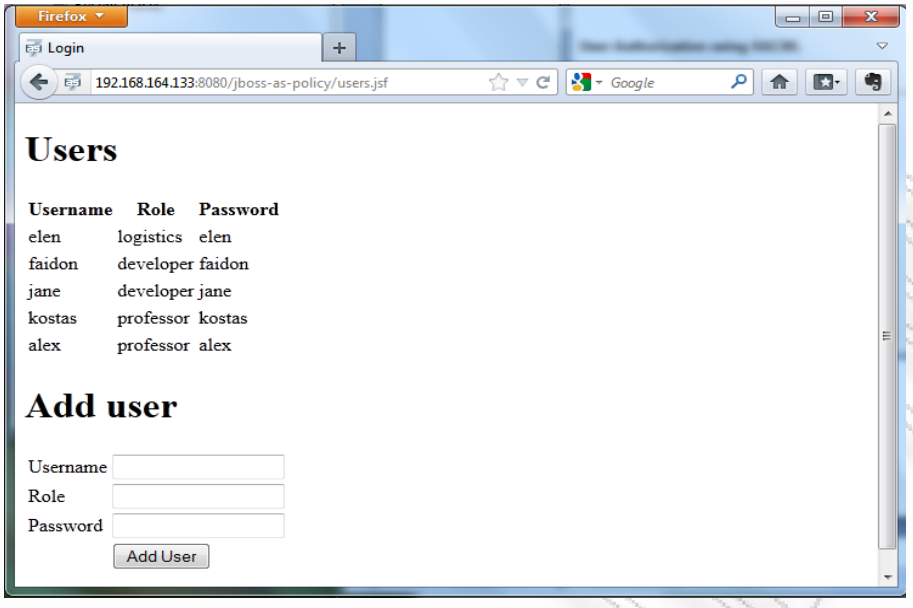
Σημείωση: για την μεγαλύτερη διευκόλυνση κατά την εκτέλεση της εφαρμογής, κρίθηκε μη σκόπιμη η επιβολή κωδικού administrator για το μενού "View Users". Σε περιβάλλον επιχειρησιακό φυσικά θα πρέπει να επιβληθεί κωδικός, αλλά για τα δεδομένα που επιθυμούμε να παρουσιάσουμε στην παρούσα εργασία κρίθηκε ως μη απαραίτητος.

Αρχικά το σύστημα δεν έχει χρήστες:



Εικόνα 25: Απεικόνιση βάσης δεδομένων χρηστών

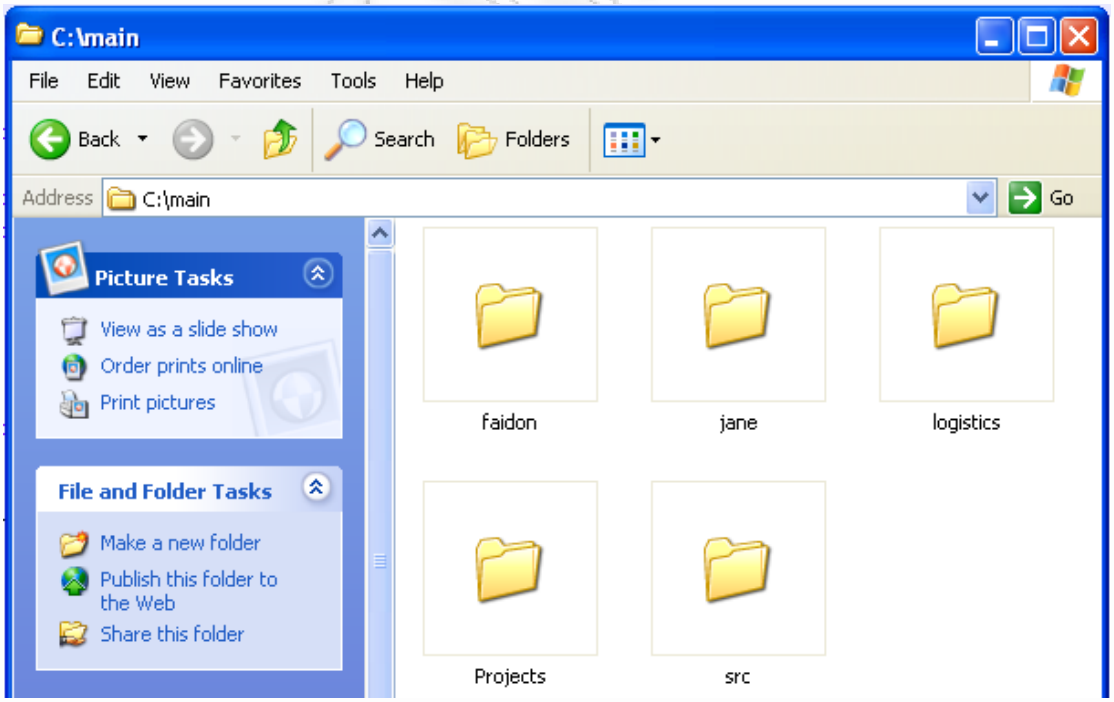
Προσθέτουμε έναν προς έναν τους χρήστες ώστε στο τέλος να έχουμε την εξής βάση δεδομένων:



Εικόνα 26: Η βάση δεδομένων, μετά την διαμόρφωση

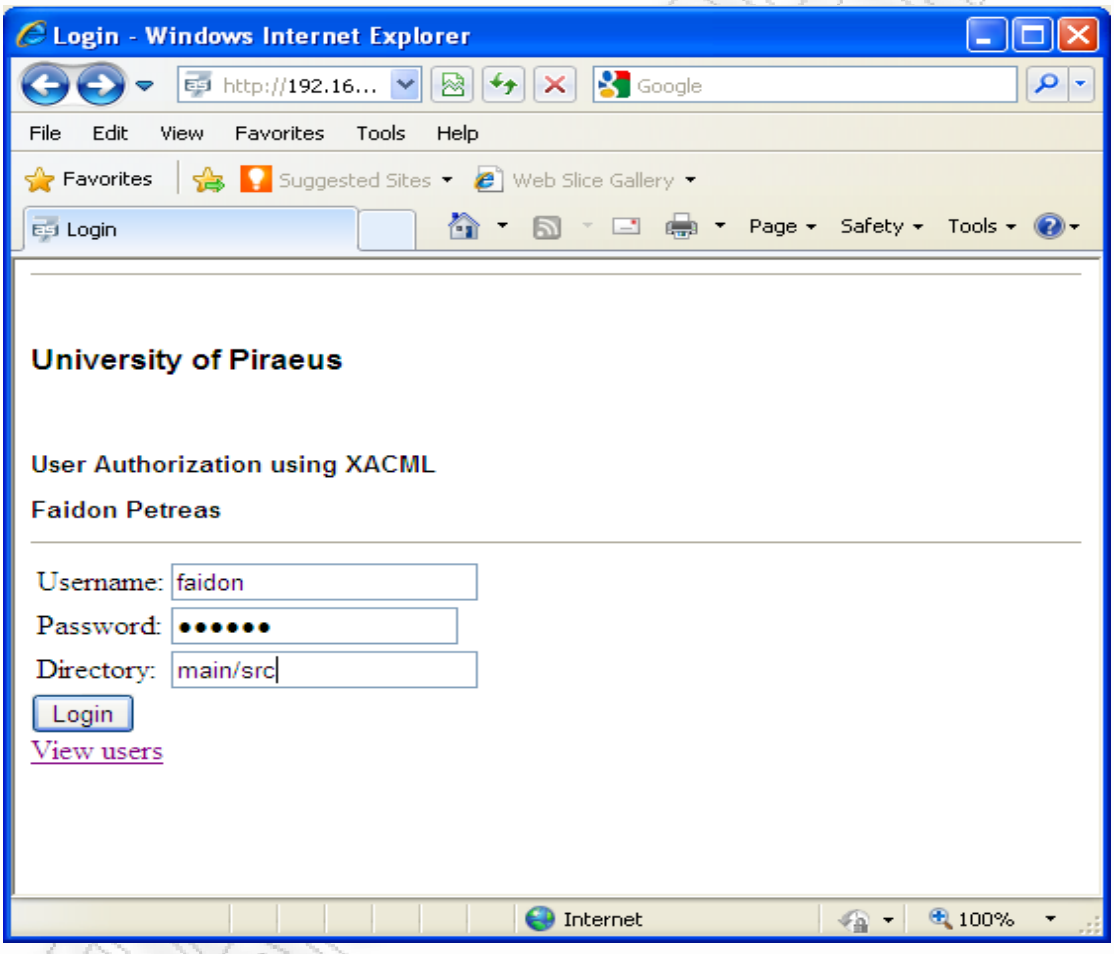
Για λόγους απλούστευσης, οι κωδικοί πρόσβασης συμπίπτουν με το όνομα του χρήστη.

Ο χρήστης αιτείται για πρόσβαση στο σύστημα αρχείων κάτω από τον κατάλογο ***"c:\main"***



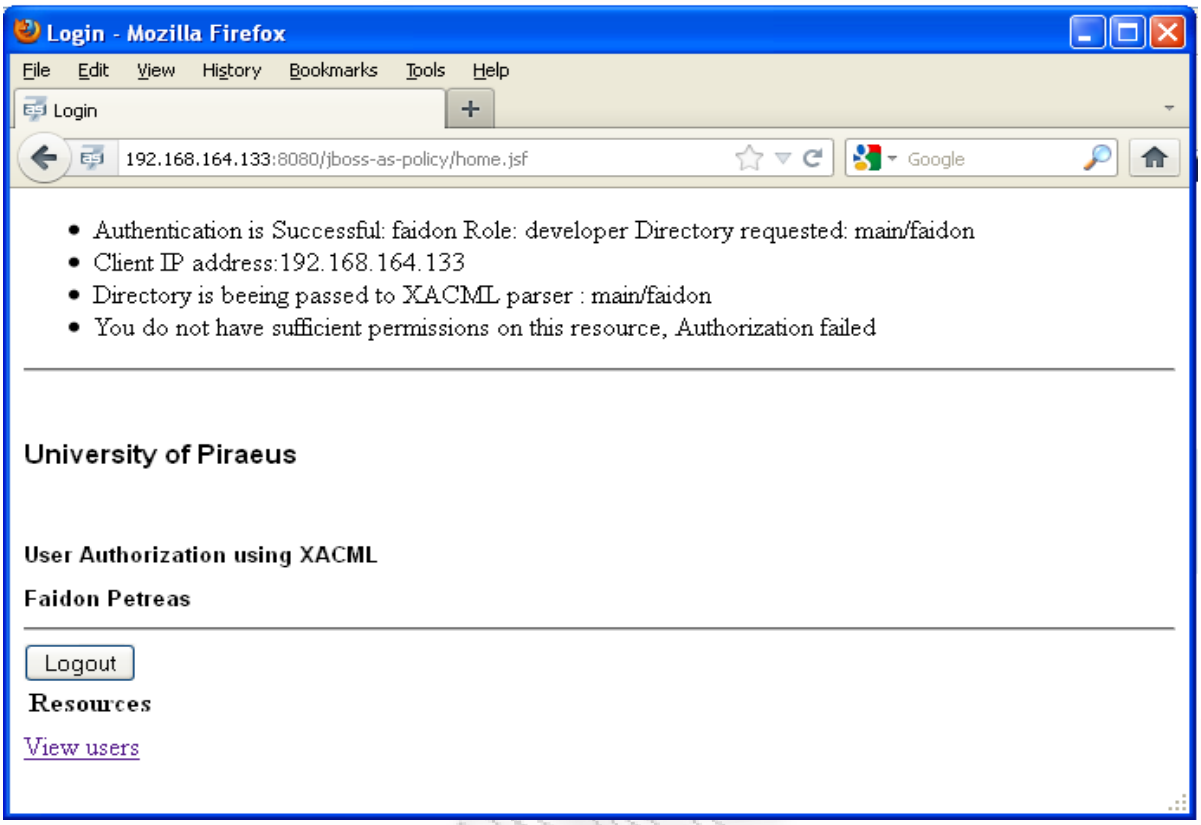
Εικόνα 27: Το σύστημα υποκαταλόγων για το οποίο παρέχεται η πρόσβαση

Στην παρούσα κατάσταση, έχουμε διαμορφώσει το σύστημα με τέτοιο τρόπο ώστε να ορίζουμε ποιοι χρήστες έχουν πρόσβαση και ποιοι είναι οι ρόλοι που συνδέονται με κάθε χρήστη. Ωστόσο, δεν έχουν καθοριστεί πολιτικές, και ως συνέπεια, αν θα δωθεί ένα από τα ονόματα χρηστών που έχουμε ορίσει, τότε ναι μεν θα η φάση της αυθεντικοποίησης θα ολοκληρωθεί επιτυχώς, αλλά λόγω μη ύπαρξης πολιτικών, στην φάση της εξουσιοδότησης, το σύστημα θα απορρίψει την πρόσβαση. Στην επόμενη εικόνα επιχειρούμε είσοδο δίνοντας όνομα χρήστη "faidon" και τον σωστό κωδικό πρόσβασης, όπως είναι καταχωρημένο στην βάση δεδομένων.



Εικόνα 28: Απόπειρα εισόδου: χρήστης καταχωρημένος, αλλά χωρίς πολιτική που να καθορίζει την πρόσβαση

Το αποτέλεσμα είναι να λάβουμε άρνηση εξουσιοδότησης από το σύστημα όπως δεικνύεται στην παρακάτω εικόνα:



Εικόνα 29:Μη ύπαρξη σχετικής πολιτικής: άρνηση εξουσιοδότησης

Συνεπώς, το επόμενο βήμα είναι ο καθορισμός των πολιτικών πρόσβασης.

Πολιτικές συστήματος

Σε αυτό το τμήμα θα δωθούν οι πολιτικές που δημιουργηθήκαν για την κάλυψη του ελέγχου πρόσβασης των χρηστών που αποθηκεύσαμε.

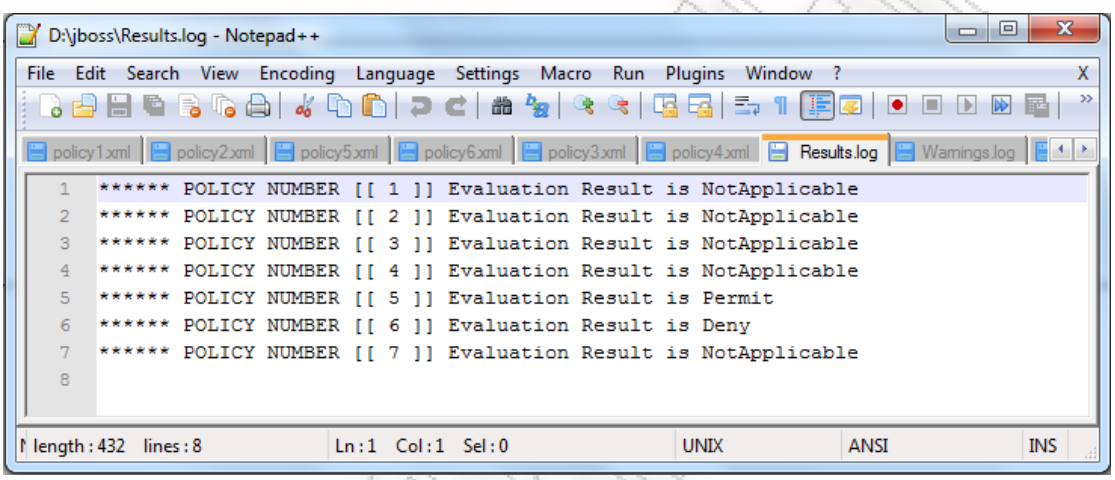
Απαραίτητες προυποθέσεις για την σωστή λειτουργία:

1. Οι πολιτικές του συστήματος πρέπει να αποθηκεύονται κάτω από τον κατάλογο c:\jboss
2. Οι πολιτικές θα πρέπει να έχουν συγκεκριμένη ονοματολογία, όπου το όνομα κάθε αρχείου συγκροτείται από το "policy", τον αριθμό της πολιτικής, ξεκινώντας από το 1 πάντα, και την επέκταση ".xml".
3. Η αρίθμηση των πολιτικών θα πρέπει να είναι συνεχής!

Σημαντικό: αν οποιαδήποτε από τις άνω συνθήκες δεν ικανοποιηθεί, η εφαρμογή δεν θα λειτουργήσει όπως προβλέπεται!

Αρχεία καταγραφής

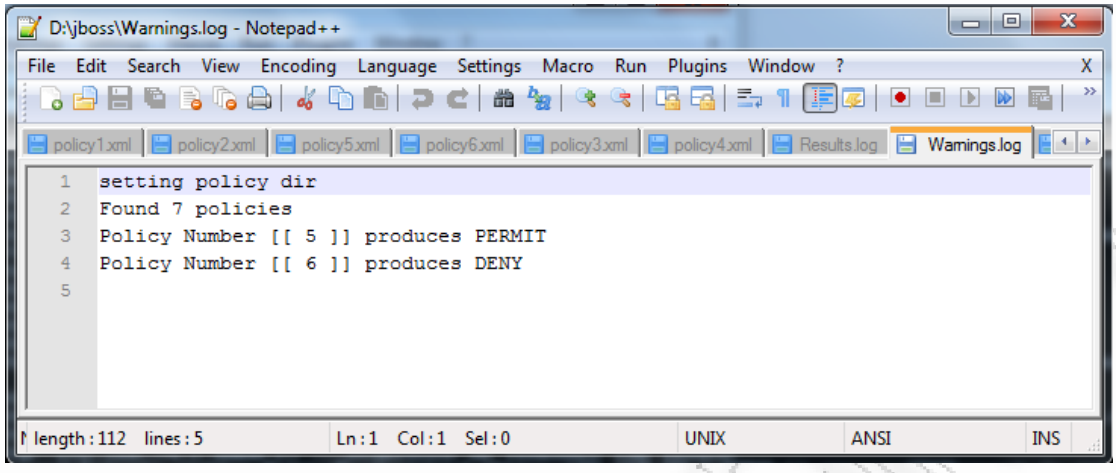
Για τον έλεγχο των αποτελεσμάτων του συστήματος εξουσιοδότησης αποφάσεων, δημιουργούνται κάθε φορά τα αρχεία "warnings.log" και "results.log" στον υποκατάλογο c:\jboss. Το αρχείο "results.log" ενημερώνει για τις αποφάσεις σε κάθε εκτέλεση πολιτικής ενώ το "warnings.log" υποδεικνύει σημεία προσοχής. Η εκτέλεση της εισόδου του χρήστη **"jane"** στον υποκατάλογο **"/main/src"** προκύπτει από την αποδοχή σύμφωνα με την εκτέλεση της πολιτικής 5 και 6. Αυτό μπορεί να επιβεβαιωθεί ανοίγωντας το αρχείο "results.log", όπου και βλέπουμε για κάθε πολιτική ποιά ήταν η απόφαση:



Εικόνα 30: Τα περιεχόμενα του αρχείου Results.txt

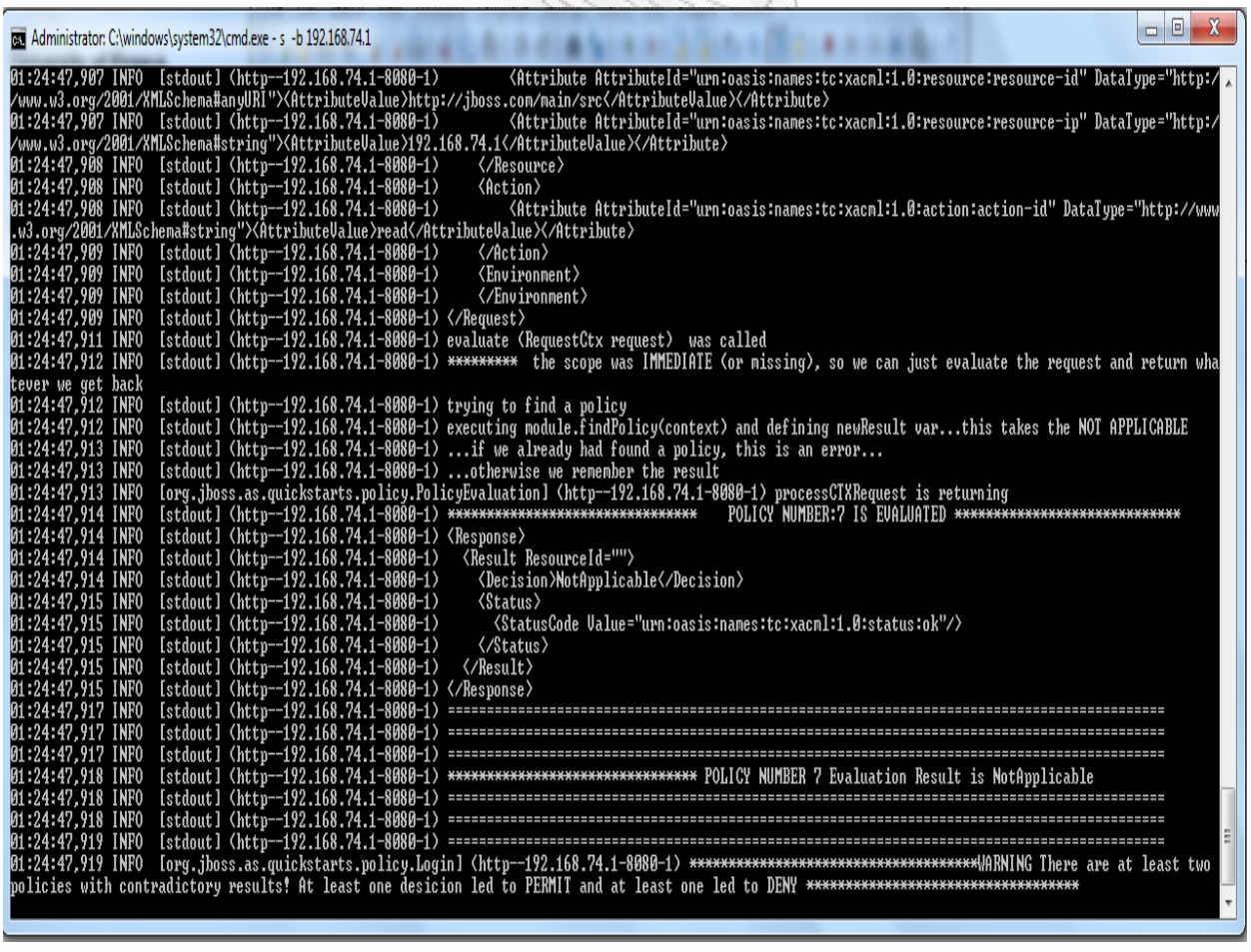
Στο παράδειγμα μας η πολιτική 5 έδωσε την εξουσιοδότηση στο όνομα χρήστη "jane" μέσω του γενικού κανόνα απόδοσης πρόσβαση στο main/src για όλους τους developers. Ωστόσο η πολιτική 6 απαγόρευσε την πρόσβαση καθώς έχει ανασταλλεί η πρόσβαση του καταλόγου αυτού συγκεκριμένα για την "jane".

Σε αυτήν την περίπτωση έχουμε δύο αντικρουόμενες αποφάσεις, οπότε συμπληρώνεται το αρχείο καταγραφών **"warnings.log"** προκειμένου να ελεγχθεί από τον αρμόδιο για τον καθορισμό των πολιτικών και να προβεί σε τυχούσα διορθωτική ενέργεια. Στην συγκεκριμένη περίπτωση βέβαια δεν χρήζει κάποια διόρθωση το σύστημα καθώς οι πολιτικές 5 και 6 παίζουν συμπληρωματικό ρόλο μεταξύ τους. Σε μία άλλη όμως περίπτωση για την οποία ενώ θα επιθυμούσαμε αποδοχή εισόδου, και λαμβάναμε απόρριψη, αυτό θα χρησίμευε για να ανιχνεύσουμε ποία πολιτική προκάλεσε αυτό το αποτέλεσμα με σκοπό την διόρθωση της ή την διαγραφή της.



Εικόνα 31:Τα περιεχόμενα του αρχείου Warnings.txt

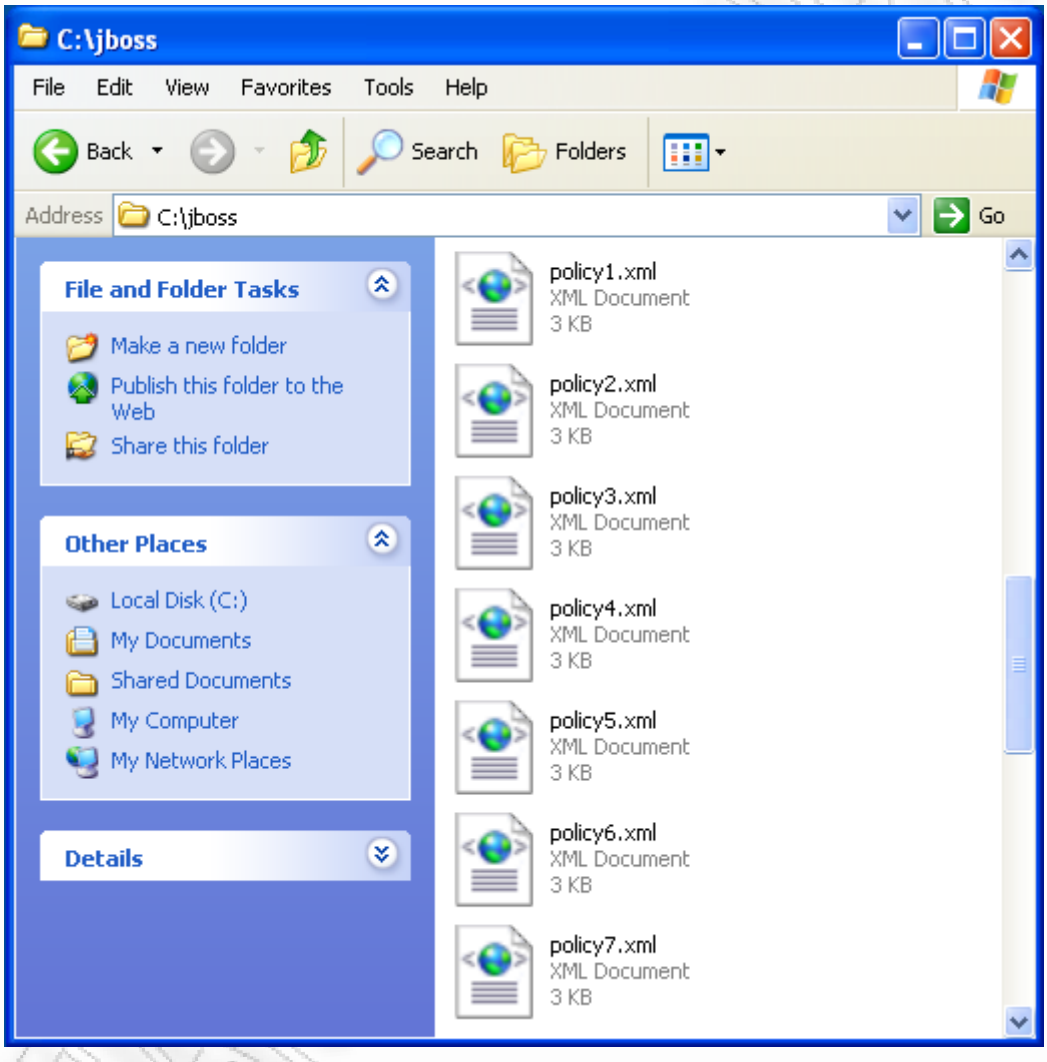
Παράλληλα με τα αρχεία καταγραφών, έχει ληφθεί μέριμνα για την ενημέρωση του χρήστη στο παράθυρο φόρτωσης της εφαρμογής, από όπου μπορούμε να δούμε συγκεντρωτικά όλη την παραπάνω πληροφορία:



Εικόνα 32: Στιγμιότυπο πληροφοριών εξόδου, κατόπιν εξυπηρέτησης αιτήματος

Το αίτημα του χρήστη επίσης αποθηκεύεται στον κατάλογο "c:\main" και ονομάζεται ως "request.xml". Η XML αναπαράσταση της απόφασης κάθε πολιτικής ευρίσκεται επίσης στο ίδιο κατάλογο και ονομάζεται ως "responseX.xml" όπου X ο αριθμός της πολιτικής που αντιστοιχεί η συγκεκριμένη απόφαση.

Για το σύστημα μας έχουν γραφτεί 7 πολιτικές, και συνεπώς η δομή θα πρέπει να είναι όπως στο παρακάτω σχήμα:



Εικόνα 33: Ακριβής τοποθεσία και ονοματολογία των πολιτικών

Πολιτική 1

policy1.xml | policy2.xml | policy5.xml | policy6.xml | policy3.xml | policy4.xml | Results.log | Warnings.log

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <Policy
3        xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
4        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5        xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
6          access_control-xacml-2.0-policy-schema-os.xsd"
7        PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:I:policy"
8        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
9     <Description>
10       Policy I.
11    </Description>
12    <Target/>
13    <Rule
14          RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:I:rule"
15          Effect="Permit">
16       <Description>
17          User with Username faidon can access path main/faidon.
18       </Description>
19       <Target>
20          <Subjects>
21             <Subject>
22                <SubjectMatch
23                      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
24                   <AttributeValue
25                         DataType="http://www.w3.org/2001/XMLSchema#string">faidon</AttributeValue>
26                   <SubjectAttributeDesignator
27                         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
28                         DataType="http://www.w3.org/2001/XMLSchema#string"/>
29                </SubjectMatch>
30             </Subject>
31          </Subjects>
32          <Resources>
33             <Resource>
34                <ResourceMatch
35                      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
36                   <AttributeValue
37                         DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://jboss.com/main/faidon</AttributeValue>
38                   <ResourceAttributeDesignator
39                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
40                         DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
41                </ResourceMatch>
42             </Resource>
43          </Resources>
44       </Target>
45    </Rule>
46 </Policy>
```

Εικόνα 34: Περιεχόμενα πολιτικής 1

Η πολιτική 1 καθορίζει ότι το αποτέλεσμα θα είναι ***"αποδοχή"*** (γρ. 15) όταν το ***υποκείμενο*** (γρ. 27) που δίδεται ισούται (γρ. 23) με το όνομα ***"faidon"*** (γρ. 25) και ο πόρος που προσπελαύνεται είναι ο κατάλογος ***"main/ faidon "*** (γρ. 37)

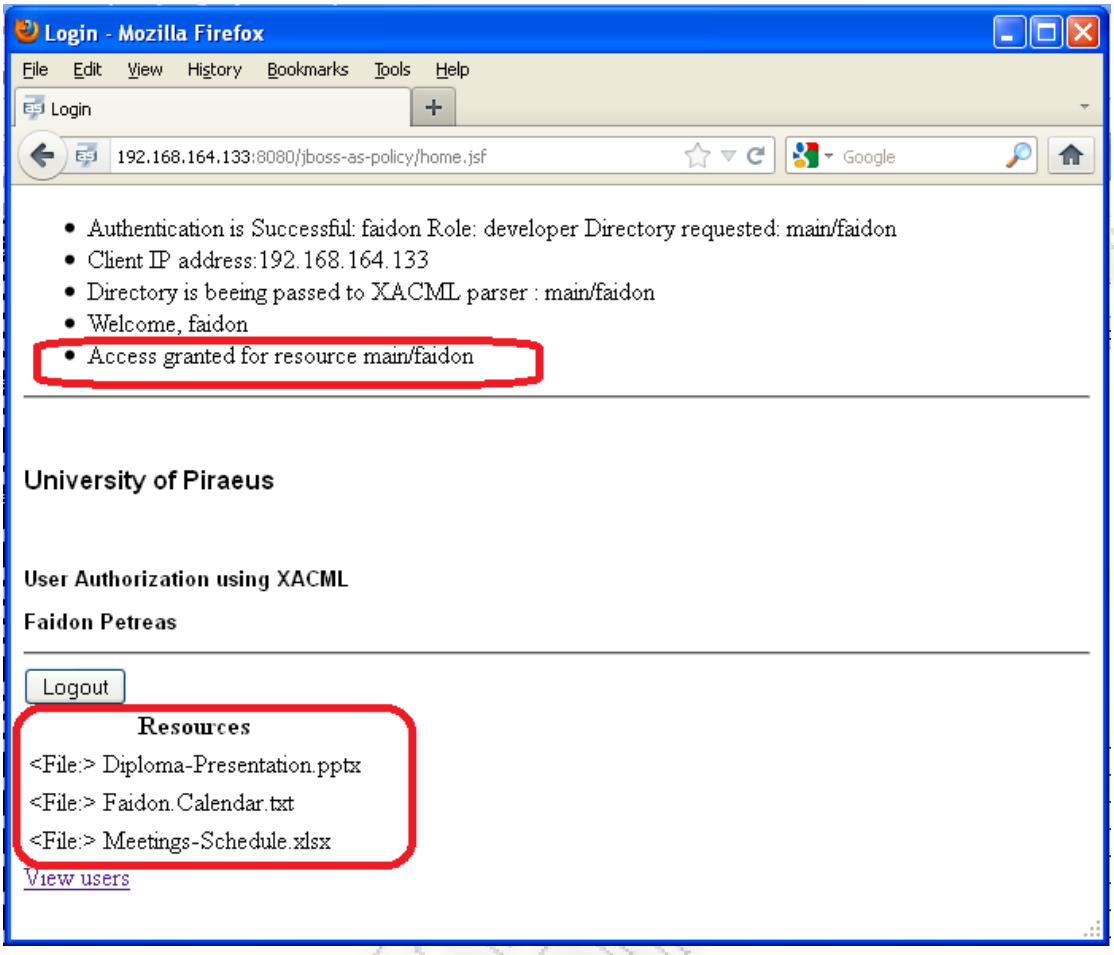
Πιστοποίηση πολιτικής:

τεστ 1: είσοδος χρήστη "faidon" στον κατάλογο "main/faidon".

Αναμενόμενο αποτέλεσμα: Επιτυχία

Ενδεικτικά, στην παρακάτω εικόνα απεικονίζουμε την εξουσιοδότηση πρόσβασης που μας παρέχει το σύστημα σε περίπτωση επιτυχίας. Μετά την εκτύπωση του μηνύματος

Access is granted for faidon, ακολουθεί η εκτύπωση της λίστας με τους ζητούμενους πόρους που ευρίσκονται στον φάκελο main/faidon:



Εικόνα 35: Επιτυχής εξουσιοδότηση για προβολή των πόρων

τεστ 2: είσοδος χρήστη με διαφορετικό όνομα του "faidon" στον κατάλογο "main/faidon".

Αναμενόμενο αποτέλεσμα: Αποτυχία

Πολιτική 2

policy1.xml | policy2.xml | policy5.xml | policy6.xml | policy3.xml | policy4.xml | Results.log | Warnings.log

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <Policy
3        xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
4        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5        xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
6          access_control-xacml-2.0-policy-schema-os.xsd"
7        PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:II:policy"
8        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
9     <Description>
10       Policy II.
11    </Description>
12    <Target/>
13    <Rule
14          RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:II:rule"
15          Effect="Permit">
16       <Description>
17          User with Username jane can access path main/jane.
18       </Description>
19       <Target>
20          <Subjects>
21             <Subject>
22                <SubjectMatch
23                      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
24                   <AttributeValue
25                         DataType="http://www.w3.org/2001/XMLSchema#string">jane</AttributeValue>
26                   <SubjectAttributeDesignator
27                         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
28                         DataType="http://www.w3.org/2001/XMLSchema#string"/>
29                </SubjectMatch>
30             </Subject>
31          </Subjects>
32          <Resources>
33             <Resource>
34                <ResourceMatch
35                      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
36                   <AttributeValue
37                         DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://jboss.com/main/jane</AttributeValue>
38                   <ResourceAttributeDesignator
39                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
40                         DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
41                </ResourceMatch>
42             </Resource>
43          </Resources>
44       </Target>
45    </Rule>
46 </Policy>
47
```

Xtensible Markup Language file | length : 2096 lines : 47 | Ln : 1 Col : 39 Sel : 0 | UNIX

Εικόνα 36: Περιεχόμενα πολιτικής 2

Η πολιτική 2 καθορίζει ότι το αποτέλεσμα θα είναι ***"αποδοχή"*** (γρ. 15) όταν το ***υποκείμενο*** (γρ. 27) που δίδεται ισούται (γρ. 23) με το όνομα ***"jane"*** (γρ. 25) και ο πόρος που προσπελαύνεται είναι ο κατάλογος ***"main/jane"*** (γρ. 37).

Πιστοποίηση πολιτικής:

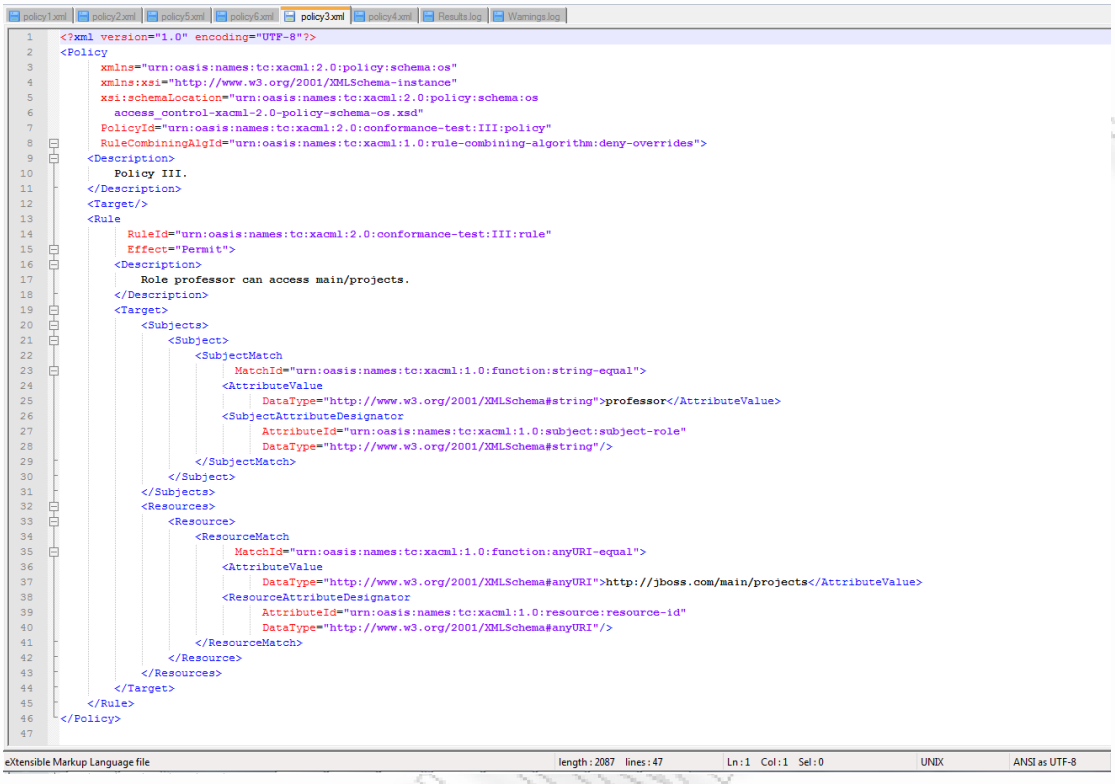
τεστ 1: είσοδος χρήστη "jane" στον κατάλογο "main/jane".

Αναμενόμενο αποτέλεσμα: Επιτυχία

τεστ 2: είσοδος χρήστη με διαφορετικό όνομα του "jane" στον κατάλογο "main/jane".

Αναμενόμενο αποτέλεσμα: Αποτυχία

Πολιτική 3



```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
      xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
        access_control-xacml-2.0-policy-schema-os.xsd"
      PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:III:policy"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
    <Description>
        Policy III.
    </Description>
    <Target/>
    <Rule
          RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:III:rule"
          Effect="Permit">
        <Description>
            Role professor can access main/projects.
        </Description>
        <Target>
            <Subjects>
                <Subject>
                    <SubjectMatch
                          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue
                              DataType="http://www.w3.org/2001/XMLSchema#string">professor</AttributeValue>
                        <SubjectAttributeDesignator
                              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-role"
                              DataType="http://www.w3.org/2001/XMLSchema#string"/>
                    </SubjectMatch>
                </Subject>
            </Subjects>
            <Resources>
                <Resource>
                    <ResourceMatch
                          MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                        <AttributeValue
                              DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://jboss.com/main/projects</AttributeValue>
                        <ResourceAttributeDesignator
                              AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                              DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                    </ResourceMatch>
                </Resource>
            </Resources>
        </Target>
    </Rule>
</Policy>
```

Εικόνα 37: Περιεχόμενα πολιτικής 3

Η πολιτική 3 καθορίζει ότι το αποτέλεσμα θα είναι ***"αποδοχή"*** (γρ. 15) όταν ο ***ρόλος*** (γρ. 27) που δίδεται ισούται (γρ. 23) με το ***"professor"*** (γρ. 25) και ο πόρος που προσπελαύνεται είναι ο κατάλογος ***"main/projects"*** (γρ. 37).

Πιστοποίηση πολιτικής:

τεστ 1: είσοδος χρήστη "kostas" στον κατάλογο "main/projects".

Αναμενόμενο αποτέλεσμα: Επιτυχία γιατί το "kostas" αντιστοιχεί σε ρόλο "professor"

τεστ 2: είσοδος χρήστη "alex" στον κατάλογο "main/projects".

Αναμενόμενο αποτέλεσμα: Επιτυχία γιατί το "alex" αντιστοιχεί σε ρόλο "professor"

τεστ 3: είσοδος χρήστη με όνομα "faidon" στον κατάλογο "main/projects".

Αναμενόμενο αποτέλεσμα: Αποτυχία γιατί το "faidon" δεν αντιστοιχεί σε ρόλο "professor"

Πολιτική 4

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
      xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
        access_control-xacml-2.0-policy-schema-os.xsd"
      PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:III:policy"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
    <Description>
        Policy IV.
    </Description>
    <Target/>
    <Rule
          RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:III:rule"
          Effect="Deny">
        <Description>
            Professor Alex is not allowed to log from 10.0.0.5
        </Description>
        <Target>
            <Subjects>
                <Subject>
                    <SubjectMatch
                          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue
                              DataType="http://www.w3.org/2001/XMLSchema#string">alex</AttributeValue>
                        <SubjectAttributeDesignator
                              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                              DataType="http://www.w3.org/2001/XMLSchema#string"/>
                    </SubjectMatch>
                </Subject>
            </Subjects>
            <Resources>
                <Resource>
                    <ResourceMatch
                          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue
                              DataType="http://www.w3.org/2001/XMLSchema#string">10.0.0.5</AttributeValue>
                        <ResourceAttributeDesignator
                              AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-ip"
                              DataType="http://www.w3.org/2001/XMLSchema#string"/>
                    </ResourceMatch>
                </Resource>
            </Resources>
        </Target>
    </Rule>
</Policy>
```

Εικόνα 38: Περιεχόμενα πολιτικής 4

Με την πολιτική 4 επιθυμούμε να συσχετίσουμε υλικούς πόρους με υποκείμενα. Συγκεκριμένα, απαγορεύουμε πρόσβαση (γρ. 15) στο όνομα υποκειμένου ***"alex"*** (γρ. 25) για πρόσβαση γενικώς, όταν και μόνο όταν, επιχειρεί πρόσβαση από το μηχάνημα με IP διεύθυνση ***10.0.0.5*** (γρ. 37).

Πιστοποίηση πολιτικής:

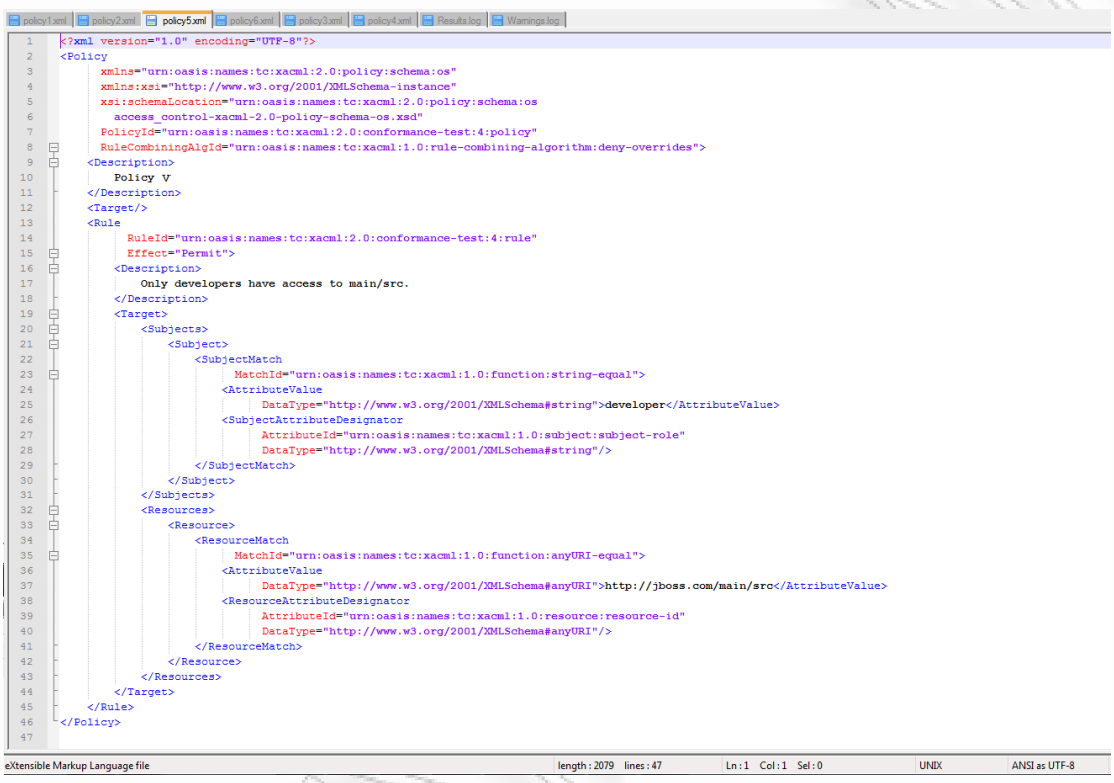
τεστ 1: είσοδος χρήστη "alex" στον κατάλογο "main/projects" από εικονικό ή φυσικό μηχάνημα με IP διεύθυνση διαφορετικής της 10.0.0.5.

Αναμενόμενο αποτέλεσμα: Επιτυχία

τεστ 2: είσοδος χρήστη "alex" στον κατάλογο "main/projects" από το εικονικό ή φυσικό μηχάνημα με IP διεύθυνση 10.0.0.5.

Αναμενόμενο αποτέλεσμα: Αποτυχία γιατί το "alex" κάνει απόπειρα εισόδου απο απαγορευμένο πόρο.

Πολιτική 5



```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <Policy
3        xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
4        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5        xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
6          access_control-xacml-2.0-policy-schema-os.xsd"
7        PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:4:policy"
8        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
9     <Description>
10       Policy V
11    </Description>
12    <Target/>
13    <Rule
14          RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:4:rule"
15          Effect="Permit">
16       <Description>
17          Only developers have access to main/src.
18       </Description>
19       <Target>
20          <Subjects>
21             <Subject>
22                <SubjectMatch
23                      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
24                   <AttributeValue
25                         DataType="http://www.w3.org/2001/XMLSchema#string">developer</AttributeValue>
26                   <SubjectAttributeDesignator
27                         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-role"
28                         DataType="http://www.w3.org/2001/XMLSchema#string"/>
29                </SubjectMatch>
30             </Subject>
31          </Subjects>
32          <Resources>
33             <Resource>
34                <ResourceMatch
35                      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
36                   <AttributeValue
37                         DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://jboss.com/main/src</AttributeValue>
38                   <ResourceAttributeDesignator
39                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
40                         DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
41                </ResourceMatch>
42             </Resource>
43          </Resources>
44       </Target>
45    </Rule>
46 </Policy>
47
```

Εικόνα 39: Περιεχόμενα πολιτικής 5

Η πολιτική 5 καθορίζει ότι το αποτέλεσμα θα είναι ***"αποδοχή"*** (γρ. 15) όταν ο ***ρόλος*** (γρ. 27) που δίδεται ισούται (γρ. 23) με το ***"developer"*** (γρ. 25) και ο πόρος που προσπελαύνεται είναι ο κατάλογος ***"main/src"*** (γρ. 37).

Πιστοποίηση πολιτικής:

Προπαιτούμενα: Απενεργοποιούμε την πολιτική 6 ή αντικαθιστούμε το Deny με Permit εντός της πολιτικής.

τεστ 1: είσοδος χρήστη "faidon" στον κατάλογο "main/src".

Αναμενόμενο αποτέλεσμα: Επιτυχία γιατί το "faidon" αντιστοιχεί σε ρόλο "developer"

τεστ 2: είσοδος χρήστη με διαφορετικό όνομα του "jane" στον κατάλογο "main/src".

Αναμενόμενο αποτέλεσμα: Επιτυχία γιατί το "jane" αντιστοιχεί σε ρόλο "developer"

Πολιτική 6

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy
      xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
        access_control-xacml-2.0-policy-schema-os.xsd"
      PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:II:policy"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
    <Description>
        Policy VI.
    </Description>
    <Target/>
    <Rule
          RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:II:rule"
          Effect="Deny">
        <Description>
            Deny Access to User with Username jane to main/src. Jane is leaving company.
        </Description>
        <Target>
            <Subjects>
                <Subject>
                    <SubjectMatch
                          MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                        <AttributeValue
                              DataType="http://www.w3.org/2001/XMLSchema#string">jane</AttributeValue>
                        <SubjectAttributeDesignator
                              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
                              DataType="http://www.w3.org/2001/XMLSchema#string"/>
                    </SubjectMatch>
                </Subject>
            </Subjects>
            <Resources>
                <Resource>
                    <ResourceMatch
                          MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                        <AttributeValue
                              DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://jboss.com/main/src</AttributeValue>
                        <ResourceAttributeDesignator
                              AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                              DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                    </ResourceMatch>
                </Resource>
            </Resources>
        </Target>
    </Rule>
</Policy>
```

Εικόνα 40: Περιεχόμενα πολιτικής 6

Η πολιτική 6 καθορίζει ότι το αποτέλεσμα θα είναι ***"απόρριψη"*** (γρ. 15) όταν το ***όνομα υποκειμένου*** (γρ. 27) που δίδεται ισούται (γρ. 23) με το ***"jane"*** (γρ. 25) και ο πόρος που προσπελαύνεται είναι ο κατάλογος ***"main/src"*** (γρ. 37).

Πιστοποίηση πολιτικής:

τεστ 1: είσοδος χρήστη "faidon" στον κατάλογο "main/src".

Αναμενόμενο αποτέλεσμα: Επιτυχία γιατί το "faidon" αντιστοιχεί σε ρόλο "developer"

τεστ 2: είσοδος χρήστη με διαφορετικό όνομα του "jane" στον κατάλογο "main/src".

Αναμενόμενο αποτέλεσμα: Αποτυχία γιατί στο υποκείμενο με όνομα "jane" απαγορεύεται η πρόσβαση στον υποκατάλογο αυτό.

τεστ 3: είσοδος χρήστη "jane" στον κατάλογο "main/jane".

Αναμενόμενο αποτέλεσμα: Επιτυχία γιατί για το όνομα "jane" δεν έχει τεθεί περιοριστική πολιτική σχετικά με το "main/jane"

Πολιτική 7

policy1.xml | policy2.xml | policy5.xml | policy6.xml | policy3.xml | policy4.xml | Results.log | Warnings.log | ip.bat | policy7.xml

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <Policy
3        xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
4        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
5        xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
6          access_control-xacml-2.0-policy-schema-os.xsd"
7        PolicyId="urn:oasis:names:tc:xacml:2.0:conformance-test:III:policy"
8        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
9     <Description>
10       Policy VII.
11    </Description>
12    <Target/>
13    <Rule
14          RuleId="urn:oasis:names:tc:xacml:2.0:conformance-test:VII:rule"
15          Effect="Deny">
16       <Description>
17          Faidon is not allowed to log in main/src from 192.168.74.1
18       </Description>
19       <Target>
20          <Subjects>
21             <Subject>
22                <SubjectMatch
23                      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
24                   <AttributeValue
25                         DataType="http://www.w3.org/2001/XMLSchema#string">faidon</AttributeValue>
26                   <SubjectAttributeDesignator
27                         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
28                         DataType="http://www.w3.org/2001/XMLSchema#string"/>
29                </SubjectMatch>
30             </Subject>
31          </Subjects>
32          <Resources>
33             <Resource>
34                <ResourceMatch
35                      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
36                   <AttributeValue
37                         DataType="http://www.w3.org/2001/XMLSchema#string">192.168.74.1</AttributeValue>
38                   <ResourceAttributeDesignator
39                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-ip"
40                         DataType="http://www.w3.org/2001/XMLSchema#string"/>
41                </ResourceMatch>
42                <ResourceMatch
43                      MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
44                   <AttributeValue
45                         DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://jboss.com/main/src</AttributeValue>
46                   <ResourceAttributeDesignator
47                         AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
48                         DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
49                </ResourceMatch>
50             </Resource>
51          </Resources>
52       </Target>
53    </Rule>
54 </Policy>
55
```

eXtensible Markup Language file | length : 2674 lines : 55 | Ln : 29 Col : 36 Sel : 0 | Dos\Windows | ANSI

Εικόνα 41: Περιεχόμενα πολιτικής 7

Η πολιτική 7 έχει ομοιότητα με την πολιτική 4 αλλά θέτει τον περιορισμό σε ένα ορισμένο υποκατάλογο. Συγκεκριμένα, απαγορεύουμε πρόσβαση (γρ. 15) στο όνομα υποκειμένου ***"faidon"*** (γρ. 25) για πρόσβαση στον υποκατάλογο ***"main/src"*** (γρ 46), όταν και μόνο όταν, επιχειρεί πρόσβαση από το μηχάνημα με IP διεύθυνση ***192.168.74.1*** (γρ. 37)

Πιστοποίηση πολιτικής:

Προπαιτούμενα: Απενεργοποιούμε την πολιτική 6 ή αντικαθιστούμε το Deny με Permit εντός της πολιτικής.

τεστ 1: είσοδος χρήστη "faidon" στον κατάλογο "main/src" από εικονικό ή φυσικό μηχάνημα με IP διεύθυνση διαφορετικής της ***192.168.74.1***.

Αναμενόμενο αποτέλεσμα: Επιτυχία

τεστ 2: είσοδος χρήστη "jane" στον κατάλογο "main/src" από εικονικό ή φυσικό μηχάνημα με IP διεύθυνση διαφορετικής της ***192.168.74.1***.

Αναμενόμενο αποτέλεσμα: Επιτυχία

τεστ 3: είσοδος χρήστη "faidon" στον κατάλογο "main/src" από εικονικό ή φυσικό μηχάνημα με IP διεύθυνση ***192.168.74.1***.

Αναμενόμενο αποτέλεσμα: Αποτυχία γιατί το "faidon" κάνει απόπειρα εισόδου απο απαγορευμένο μηχάνημα.

τεστ 4: είσοδος χρήστη "jane" στον κατάλογο "main/src" από εικονικό ή φυσικό μηχάνημα με IP διεύθυνση ***192.168.74.1***.

Αναμενόμενο αποτέλεσμα: Επιτυχία

Παρατηρήσεις - Συμπεράσματα

Το διαδικτυακό υπολογιστικό πλέγμα, αποτελεί αναμφίβολα ένα σημαντικό νεωτερισμό, τον οποίο δεν θα πρέπει να αμελήσουν οι εταιρείες. Σύμφωνα με μελέτη του Gartner, το 2011 οι εταιρείες επένδυσαν το 40% της υποδομής τους σε εκτέλεση Εφαρμογής ώς Υπηρεσία, αποδεσμεύοντας επιλεγμένες εφαρμογές από την υλική τους υποδομή [3]. Οι κίνδυνοι που εμφανίζονται στο προσκήνιο όμως επιβάλλουν την τήρηση συγκεκριμένων μέτρων ασφαλείας, προκειμένου να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των δεδομένων. Ο ακριβής καθορισμός Όρων Χρήσης Υπηρεσιών (Service Level Agreements) με τον πάροχο βοηθά σημαντικά τον πελάτη στον καθορισμό μίας πολιτικής που θα προστατέψει τα δεδομένα του. Ακόμα και αν στηρ [4]ιχτούμε στην άποψη ότι το κόστος αγοράς υλικού ελαττώνεται σημαντικά με την εξέλιξη της τεχνολογίας, καθώς και το κοστος για την εκπαίδευση εξειδικευμένου προσωπικού δεν είναι τόσο υψηλή, από την

άλλη μεριά το κέρδος σε υπολογιστική ισχύ με την χρήση υπηρεσίας υπολογιστικού πλέγματος είναι τόσο υψηλό, ώστε να καθιστά αυτό το μοντέλο ως το επικρατέστερο για μία εταιρεία που απαιτεί σοβαρά αποθέματα υπολογιστικής ισχύος για την διεκπεραίωση των εργασιών της. Είναι σημαντικό το ότι οι οργανισμοί αποφεύγουν το βάρος της επενδυσης σε αγορά υξυπηρετητών, οι οποίοι χάνουν την αξία τους με το πέρασμα του χρόνου. Αντί αυτού βρίσκουν πιο ελκυστική την λύση της εξαγοράς ισχύος με την μορφή της υπηρεσίας. Το κόστος της υπηρεσίας προσαρμόζεται με τις εκάστοτε απαιτήσεις για ισχύ. Αναλογικά, το μοντέλο ταυτίζεται απόλυτα με το μοντέλο που χρησιμοποιούμε με την ηλεκτρική ενέργεια. Πληρώνουμε το κεντρικό δίκτυο της ΔΕΗ, με ένα ποσό που αναλογεί με την ηλεκτρική ενέργεια που καταναλώνουμε. Και φυσικά ο τελικός καταναλωτής ουδεμία σχέση έχει με τον εξοπλισμό που παράγει ρεύμα.

Όλο αυτό το κέρδος με το μοντέλο αυτό δεν έρχεται χωρίς το αντίστοιχο τίμημα στον τομέα της ασφάλειας. Στο κάτω κάτω η ίδια η φιλοσοφία του μοντέλου επιβάλλει την αποθήκευση των προσωπικών δεδομένων σε χώρο εκτός του οργανισμού. Αυτό εξ'ορισμού εισάγει προβλήματισμούς, ειδικά όταν τα δεδομένα είναι ευαίσθητα. Από τεχνικής άποψης η διαχείριση μεγάλου όγκου δεδομένων τα οποία μετακινούνται συνεχώς μεταξύ διαφορετικών γεωγραφικώ τοποθεσιών, απαιτεί

Είναι γεγονός ότι δεν έχουν λυθεί όλα τα ζητήματα ασφαλείας στο διαδικτυακό υπολογιστικό πλέγμα. Τα πρότυπα στην αρχική τους μορφή είναι αρκετά περιοριστικά. Αναλυτές έχουν επισημάνει την εξής αντιφατική άποψη εκ πρώτης όψεως: ότι η διαδικασία της προτυποποίησης δεν θα ωφελήσει το υπολογιστικό υπολογιστικό πλέγμα από άποψη εξάπλωσης. Αυστηροί κανόνες είναι δυνατόν να περιορίσουν τις δυνατότητες του και να περιορίσουν την διάδοση του. Υπάρχει ένα στάδιο αναμονής, μέχρι η αγορά του μοντέλου αυτού να σταθεροποιηθεί, και σε επόμενο στάδιο θα αρχίσουν να επιβάλλουν μέτρα προληπτικά για την ασφάλεια. Αυτό από μόνο του είναι αφήνει πολλές λαβές για εμφάνιση προβλημάτων ασφάλειας [4].

Όπως ο John Pescatore είχε αναφέρει στους New York Times: "Η ασφάλεια των υπηρεσιών διαδικτυακού υπολογιστικού πλέγματος είναι όπως το λειτουγικό σύστημα των Windows εν έτει 1999. Χρησιμοποιείται ευρέως, και απλά δεν έχει παρουσιαστεί ακόμα κάποια καταστροφική ενέργεια. Αλλά ακόμα είμαστε στο ξεκίνημα της νέας εποχής του Ίντερνετ, και είναι αναμενόμενο ότι θα συμβεί [ενέργεια με καταστροφικές συνέπειες]" [5]. Τα δεδομένα έχουν αλλάξει: εώς τώρα ένας οργανισμός, βασιζόταν στην ποιότητα του λογισμικού του, στην δική του υλική υποδομή, κια στα μέτρα ασφαλείας που θέσπιζε και εφάρμοζε ο ίδιος. Με το νεό μοντέλο, έχουμε μεταφορά της εμπιστοσύνης σε ένα άλλο επίπεδο:ο πελάτης θα πρέπει να εμπιστευτεί τον πάροχο. Η εμπιστοσύνη του πελάτη, θα πρέπει να

επεκταθεί πέρα από τον τομέα της ασφάλειας: στην αξιοπιστία, στην διαθεσιμότητα και στην συνέχιση της επιχειρηματικής δραστηριότητας του παρόχου [6]. Οι οργανισμοί θα πρέπει να είναι πολύ προσεκτικοί σχετικά με το που θα εμπιστευτούν την διαφύλαξη των δεδομένων τους. Η IBM, Cisco, SAP, EMC και άλλες σημαντικές εταιρείες, έχουν ιδρύσει ένα μανιφέστο "ανοιχτού διαδικτυακού υπολογιστικού πλέγματος" στο οποίο ορίζουν μέτρα ασφάλειας και ελέγχου υπηρεσιών του μοντέλου. Υπάρχουν ένα σύνολο από πρότυπα τα οποία καθορίζουν μέτρα ασφάλειας και πρακτικές που θα πρέπει να ακολουθεί ένας πάροχος. Το πιό σημαντικό από αυτά είανι το ISO27001 και το SAS70 ελεγκτικό πρότυπο [4].

Υπάρχουν δεκαοκτώ διαφορετικοί οργανισμοί οι οποίοι υλοποιούν πρότυπα και προγραμματιστικές διεπαφές για το διαδικτυακό υπολογιστικό πλέγμα [7].

Αξιοσημείωτο είναι, πως ενώ το μοντέλο προσφέρει εμφανή πλεονεκτήματα, δεν σπεύδουν να το ενστερνιστούν όλες οι εταιρείες, χωρίς πρώτα να αναλύσουν ολά τα ρίσκα σχετικά με την ιδιωτικότητα και την ασφάλεια, και χωρίς να αναλάβουν ειδικοί την ανάλυση της αποδοτικότητας ενός παρόχου από άποψη τεχνικού επιπέδου αλλά και του μέτρου της ηθικής του. Σε κάθε είναι ένα πολλά υποσχόμενο μοντέλο, το οποίο προσφέρει στους καταναλωτές τεράστια υπολογιστική ισχύ σε πολύ μικρό κόστος. Αναμένεται να έχει μεγάλη επίδραση στην βιομηχανία του λογισμικού. Η δραστηριότητα σε αυτό το μοντέλο έχει μεγαλώσει κατά 200% μέσα στο 2009. Λαμβάνοντας υπ'όψιν ότι τα μελλοντικά πρότυπα θα ενισχύσουν την ασφάλεια και την ιδιωτικότητα, υπολογίζεται ακόμα σημαντικότερη ανάπτυξη και διάδοση.

Εώς το 2012 πάνω από το 50% των εξυπηρετητών των επιχειρήσεων εισέρχονται στην τεχνολογία των εικονικών συστημάτων, όπως αναφέρει η έρευνα του Gartner. Επίσης, σε πέντε χρόνια, αναμένεται η ασφάλεια των εικονικών συστημάτων να είναι σε ψηλότερα επίπεδα από ότι τα παραδοσιακά συστήματα. Βέβαια όπως σημειώνει η ίδια η έρευνα για το έτος 2012, τα εικονικά συστήματα υπολείπονται των φυσικών συστημάτων στον τομέα της ασφάλειας. Η αδυναμία αυτή εστιάζεται στην μη επαρκή αξιοποίηση ομάδας υπεύθυνης ασφάλειας των συστημάτων, καθώς και στην μη ύπαρξη εξελιγμένων εργαλείων για την προστασία των συστημάτων στα νέα περιβάλλοντα [8].

Η επιτυχημένη αξιοποίηση των υπηρεσιών διαδικτυακού πλέγματος προυποθέτει πολλαπλά μέτρα. Καταρχάς πρέπει να υπάρχει κατάλληλο SLA με τον πάροχο. Ανάλογα με το είδος των υπηρεσιών θα πρέπει ο πελάης να διερευνήσει το κατα πόσο ο πάροχος εγγυάται την ασφάλεια των δεδομένων του: ποιες τεχνικές εφαρμόζει? με ποιους τρίτους συνεργάζεται? Πολλές φορές ο τρίτος αποτελεί τον αδύναμο κρίκο της αλυσσίδας, που όταν σπάσει είναι δυνατόν να φέρει σε δύσκολη θέση τόσο τον πάροχο όσο και τον πελάτη. Ένα άλλο ερώτημα είναι το κατα πόσο υποστηρίζει την προτυποποίηση ο πάροχος. Αυτό είναι πολύ σημαντικό αν

κρίνουμε ότι τα πρότυπα απολαμβάνουν της συνεχούς βελτίωσης, αλλα και προσφέρουν την πιο επιτυχημένη διαλειτουργικότητα των εφαρμογών μεταξύ πελατών που ανήκουν σε διαφορετικούς πάροχους. Χαρακτηριστικό παράδειγμα προτύπου που αναλύθηκε και υλοποιήθηκε στα πλαίσια της παρούσας διπλωματικής είναι η εξουσιοδότηση ελέγχου πρόσβασης με XACML.

Με την υλοποίηση του προτύπου, κατορθώσαμε να παράγουμε μία εφαρμογή, η οποία η κεντρική λειτουργικότητα είναι πλήρως ανεξαρτητοποιημένη από τον μηχανισμό ελέγχου πρόσβασης. Τα κύρια πλεονεκτήματα του διαχωρισμού αυτού, είναι ότι ο κώδικας σε μεγάλα έργα είναι πιο έυκολα συντηρήσιμος, με λιγότερα σφάλματα και ευκολότερα επεκτάσιμος. Επιπλέον η διαμόρφωση του συστήματος της εξουσιοδότησης επιτελείται με πολύ εύκολο τρόπο, προσθέτοντας πολιτικές ασφαλείας σε XML χωρίς να χρειάζεται μεταγλώτιση του κώδικα ή οποιαδήποτε τροποποίηση.

Ακόμα πιο σημαντικό είναι η όλη ιδέα της υιοθέτησης ενός προτύπου. Στο υποθετικό σενάριο όπου ένας πάροχος διακόπτει την λειτουργία του, η υπάρχουσα εφαρμογή του πελάτη θα μπορεί να λειτουργήσει σε έναν άλλο πάροχο που ακολουθεί το πρότυπο. Μη υιοθέτηση προτύπων θα οδηγούσε σε μεγάλα κόστη συντήρησης λογισμικού, προκειμένου να γίνει συμβατό με την νέα πλατφόρμα του παρόχου.

Η τεχνολογία του διαδικτυακού υπολογιστικού πλέγματος κεντρίζει το ενδιαφέρον της βιομηχανίας. Αναμένεται να παρατηρηθεί αυξημένη ζήτηση για εξειδικευμένο και υψηλά αμοιβόμενο προσωπικό στον τομέα αυτό. Για λογαριασμό έρευνας της IBM, (Global Trends Survey) 2000 επαγγελματίες από τον χώρο της πληροφορικής κρίνουν ότι η τάση για ανάπτυξη εφαρμογών για κινητές συσκευές και για το διαδικτυακό πλέγμα θα παρουσιάσει ανοδική πορεία στα επόμενα πέντε χρόνια. Το επίκεντρο θα είναι συσκευές φορητές, όπως έξυπνα κινητά, ταμπλέτες και ανάπτυξη λογισμικού το οποίο θα είναι συμβατό με υπηρεσίες διαδικτυακού πλέγματος, όπως σημειώνει η Alice Chou διευθύντρια στο developerWorks της IBM. Οι προγραμματιστές καλούνται να εξοικοιωθούν με ένα σύνολο τεχνολογιών προσανατολισμένο στις υπηρεσίες διαδικτυακού πλέγματος, κλειδί για την επαγγελματική τους επιτυχία αλλά και για την ευημερία των επιχειρήσεων [9].

Βιβλιογραφία Κεφαλαίου

[1] «JBoss application server,» [Ηλεκτρονικό]. Available: http://en.wikipedia.org/wiki/Jboss.

[2] A. J. Saldhana, «User Guide for JBoss XACML,» [Ηλεκτρονικό]. Available: http://docs.jboss.org/jbosssecurity/docs/jbossxacml/html/jbossxacml.html.

[3] R. Westervelt, «Cloud computing group to tackle security concerns,» [Ηλεκτρονικό]. Available: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1352540,00.html#.

[4] D. Binning, «Top five cloud computing security issues,» [Ηλεκτρονικό]. Available: http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm .

[5] «What's New in the Amazon Cloud?: Security Vulnerability in Amazon EC2 and SimpleDB Fixed (7.5 Months After Notification),» [Ηλεκτρονικό]. Available: http://cloudsecurity.org/blog/2008/12/18/whats-new-in-the-amazon-cloud-security-vulnerability-in-amazon-ec2-and-simpledb-fixed-75-months-after-notification.html.

[6] B. Schneier, «Be Careful When You Come to Put Your Trust in the Clouds,» [Ηλεκτρονικό]. Available: http://www.schneier.com/essay-274.html.

[7] J. Zipadelli, «All Backed Up: Cloud Computing Security Issues,» [Ηλεκτρονικό]. Available: http://www.digitalmediabuzz.com/2009/11/cloud-computing-security-2/.

[8] A. Moscaritolo, «NIST issues virtualization security guidance,» 2011. [Ηλεκτρονικό]. Available: http://www.scmagazine.com/nist-issues-virtualization-security-guidance/article/195756/.

[9] M. O'Connell, «New developerWorks survey shows dominance of cloud computing and mobile application development,» [Ηλεκτρονικό]. Available: http://www.ibm.com/developerworks/aboutdw/2010survey-results/.

[10] S. Microsystems, «sunxacml.sourceforge,» 2003-2004. [Ηλεκτρονικό]. Available: http://sunxacml.sourceforge.net/guide.html#xacml.