ΑΠΟΚΕΝΤΡΩΜΕΝΗ ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΣΒΑΣΗΣ ΓΙΑ ΟΜΟΣΠΟΝΔΙΑΚΕΣ ΥΠΗΡΕΣΙΕΣ ΑΠΟΘΗΚΕΥΣΗΣ ΔΕΔΟΜΕΝΩΝ

Η
ΜΕΤΑΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΕΞΕΙΔΙΚΕΥΣΗΣ

Υποβάλλεται στην

ορισθείσα από την Γενική Συνέλευση Ειδικής Σύνθεσης
του Τμήματος Πληροφορικής
Εξεταστική Επιτροπή

από τον

Νικόλαο Μπουντουρόπουλο

ως μέρος των Υποχρεώσεων

για τη λήψη

του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΔΙΠΛΩΜΑΤΟΣ ΣΤΗΝ ΠΛΗΡΟΦΟΡΙΚΗ

ΜΕ ΕΞΕΙΔΙΚΕΥΣΗ ΣΤΑ ΥΠΟΛΟΓΙΣΤΙΚΑ ΣΥΣΤΗΜΑΤΑ

Ιούνιος 2009

ΑΦΙΕΡΩΣΗ

Η εργασία αυτή αφιερώνεται στους γονείς μου, τον αδερφό μου και στην Μερόπη.

ΕΥΧΑΡΙΣΤΙΕΣ

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω όλους τους ανθρώπους που ενεπλάκησαν είτε άμεσα είτε έμμεσα στην ολοκλήρωση της διατριβής αυτής.

Αρχικά θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Στέργιο Αναστασιάδη για τις πολύτιμες συμβουλές του, από τα πρώτα έως τα τελευταία στάδια του σχεδιασμού. Παρ'όλο που η βασική μου παιδεία στον προπτυχιακό κύκλο είναι το πτυχίο του μαθηματικού μου έδωσε την ευκαιρία να εντρυφήσω στον συγκεκριμένο τομέα της πληροφορικής.

Αισθάνομαι την ανάγκη να εκφράσω την βαθύτερη ευγνωμοσύνη για τους γονείς μου για όλα όσα έχουν κάνει μέχρι σήμερα. Τους ευχαριστώ για την ψυχική υποστήριξη και ενθάρρυνση που μου έδειξαν όλα αυτά τα χρόνια.

Τέλος πρέπει να αναφέρουμε πως η παρούσα εργασία χρηματοδοτήθηκε από το έργο INTERSTORE (No I2101005) της Κοινοτικής Πρωτοβουλίας INTEREG IIIA (Ελλάδα Ιταλία) 2000-2006.

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ

ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ

ΠΕΡΙΛΗΨΗ

Νικόλαος Μπουντουρόπουλος του Δημητρίου και της Μαρίας. Msc, Τμήμα Πληροφορικής, Πανεπιστήμιο Ιωαννίνων, Ιούνιος 2009 Αποκεντρωμένη διαχείριση πρόσβασης για ομοσπονδιακές υπηρεσίες αποθήκευσης δεδομένων. Επιβλέποντας Στέργιος Αναστασιάδης.

Μελετάμε το πρόβλημα της διαχείρισης ελέγχου πρόσβασης αρχείων μεταξύ διαφόρων ανεξάρτητων οργανισμών. Οι υπάρχουσες λύσεις εγκαθιδρύουν σύνθετες συσχετίσεις μεταξύ διαφόρων οργανισμών ή απαιτούν ενημερώσεις για την πιστοποίηση του χρήστη και την εξουσιοδότηση κατά την προσπέλαση των απομακρυσμένων αρχείων. Για να μπορέσουμε να αντιμετωπίσουμε το πρόβλημα ορίζουμε την κλάση ως μια πολυπεπίπεδη δομή ομαδοποίησης. Ειδικότερα θεωρούμε δύο επίπεδα, όπου το ανώτερο επίπεδο διαμορφώνεται από διάφορους οργανισμούς, ενώ το κατώτερο περιλαμβάνει τους συγκεκριμένους χρήστες που ανήκουν σε κάθε οργανισμό. Έτσι κατορθώνουμε να κρατήσουμε χαμηλό το κόστος της απομακρυσμένης πρόσβασης με ελάχιστο κόστος ενημερώσεων μεταξύ των διαφόρων οργανισμών που συμμετέχουν. Έχουμε αναπτύξει μια πρωτότυπη υλοποίηση της αρχιτεκτονικής μας βασισμένη στον GridFTP διακομιστή. Πειραματικά αποδείξαμε το χαμηλό της κόστος. Για την εξουσιοδότηση μιας απομακρυσμένης πρόσβασης η αίτηση περιλαμβάνει τις κλάσεις στις οποίες ανήκει ο χρήστης, ενώ ο έλεγχος πρόσβασης πραγματοποιείται στον διακομιστή αποθήκευσης,

EXTENDED ABSTRACT IN ENGLISH

Boudouropoulos Nikolaos Msc Computer Science Department, University of Ioannina, Greece. June 2009 Nepheli: Scalable Decentralized Authorization through Partnerships.

Thesis Supervisor : Stergios V. Anastasiadis

We describe the frequent need of independent organizations to form federations and contribute storage resources for mutual data sharing among their users. We also define the type of the credentials that the users need to achieve this. Credentials may authorize a user to access certain resources or can be used as a proof of authentication. There are different type of credentials generally used in systems.

One basic problem in the support of data sharing is the access control of user requests that originate from remote organizations. The existing solutions either manage the authentication and authorization information centrally or they distribute it periodically from the users' organization directories to the providers of data access services. This hypothetical need to distribute the information require heavyweight update operations among the authentication and authorization services. In the present work, we introduce a decentralized security architecture called Nepheli that separates the authentication from the authorization management. We assign the user authentication to the users' organization and the access authorization to the service provider. We group the users in classes according to their access rights and transfer the class authentication certificate along with the access requests. We built a prototype architecture based on the open source implementation of the Community Authorization Service(CAS). We use the GridFTP facility as a file service example to demonstrate the scalability of our our approach.

We describe the necessary modifications that we applied to CAS and GridFTP in order to incorporate the Nepheli architecture into their operation. We split the CAS schema into separate collections of tables, the CAS-Client and the CAS-Server. The CAS-Client is located at the organization of the user and contains the tables that associate users to classes and certifications authorities. Thus, the CAS-Client plays the role of an authentication service for remote access requests. The CAS-Server maintains the resources, services, actions and policies. We expand the policy specification to include the class of the organization that belongs to. We achieve to move the entire definition and enforcement of access policy from the central CAS to the resource managers residing at each participating organization.

The user initially receives a long-term certificate from the certification authority and subsequently creates a proxy certificate. The user creates a request with the proxy certificate and submits it to the CAS-Client. The CAS-Client returns an extended certificate based on SAML (System Assertion Markup Language) language to specify the classes that the users belongs to. Finally the user submits the extended certificate to the remote GridFTP who consults the CAS-Server to decide for the remote access or not.

We conclude that the proposed security architecture reduces the overall cost of accessing a remote resource. In fact, the credential carried by a request only specifies the classes of the user instead of the actual rights that apply to the user request. Thus, the same credential can be used across multiple requests of the same user, which eliminates the need for creation of new credential for each request often needed by existing systems.

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

1.1. Στόχοι της Εργασίας

Το Υπολογιστικό Πλέγμα είναι ένα μοντέλο που παρέχει τη δυνατότητα κοινοχρησίας υπολογιστικών πόρων. Είναι βασισμένο σε ένα ανοικτό σύνολο προτύπων πρωτοκόλλων επικοινωνίας και ανταλλαγής δεδομένων, που επιτρέπει την επικοινωνία μεταξύ ετερογενών και γεωγραφικά διασκορπισμένων συστημάτων. Υλοποιεί μια εικονική αρχιτεκτονική με πολλούς δικτυωμένους υπολογιστές, όπου διαμοιράζει τις εκτελεστικές εργασίες. Το υπολογιστικό πλέγμα συμβάλλει στην επίτευξη της καλύτερης διαχείρισης των πόρων διάφορων συστημάτων και συμπεριλαμβάνει την αποτελεσματικότερη διαχείριση και επεξεργασία τεράστιων όγκων δεδομένων. Χαρακτηριστικό παράδειγμα χρήσης της τεχνολογίας αυτής είναι αυτό της αποθήκευσης και επεξεργασίας δεδομένων στο διεθνές ερευνητικό κέντρο CERN που υπολογίζεται ότι μέσα σε ένα χρόνο πειραμάτων θα παράγει δεδομένα της τάξεως των 10 Petabytes. Η επεξεργασία και αποθήκευση των δεδομένων αυτών σε ένα και μόνο οργανισμό είναι αδύνατη. Γι'αυτό επιβάλλεται οι διάφοροι οργανισμοί που θα ασχοληθούν με την επεξεργασία των δεδομένων τέτοιου μεγέθους να συνεισφέρουν τους απαραίτητους πόρους που διαθέτουν δημιουργώντας διάφορους εικονικούς οργανισμούς (Virtual Organization).

Κατά τη δημιουργία των εικονικών οργανισμών προκύπτουν πολλά τεχνικά ζητήματα, όπως είναι η πρόσβαση των χρηστών στους πόρους που συνεισφέρονται. Γενικότερα το πρόβλημα έγκειται στην δημιουργία μια κοινής πλατφόρμας για τη διαχείριση ετερογενών πόρων διαφορετικών οργανισμών. Πέρα από την πολιτική που διέπει την πρόσβαση των πόρων που ανήκουν στον εικονικό οργανισμό θα πρέπει με κάποιο τρόπο να γίνουν σεβαστές και οι τοπικές πολιτικές διαχείρισης και ασφάλειας που ο εκάστοτε οργανισμός θέλει να εφαρμόσει στους πόρους του.

Ένα βασικό χαρακτηριστικό που πρέπει να διέπει την πλατφόρμα αυτή είναι η έλλειψη κεντρικοποιημένης διαχειριστικής αρχής. Θέλουμε ο κάθε οργανισμός να είναι υπεύθυνος για την διαχείριση των πόρων του έτσι ώστε να μπορεί να επιλύει άμεσα τα όποια προβλήματα προκύψουν και να μην είναι υποχρεωμένος να είναι υπόλογος σε ένα εξωτερικό διαχειριστή. Η παραπάνω βασική σχεδιαστική αρχή συνεπάγεται τη δημιουργία ενός πρωτοκόλλου το οποίο θα επιτρέπει την αρμονική συνεργασία διαφόρων λειτουργικών συστημάτων.

Σκοπός της παρούσας εργασίας είναι καταρχήν να περιγράψουμε και να αναδείξουμε τα προβλήματα ασφαλείας ενός ευρείας κλίμακας κατανεμημένου περιβάλλον πλέγματος (grid computing) και να αναφερθούμε στις υπάρχουσες πολιτικές που έχουν προταθεί και αντιμετωπίσει είτε επιτυχώς ή ανεπιτυχώς το πρόβλημα αυτό. Στην συνέχεια προτείνουμε λύσεις τις οποίες αξιολογούμε πειραματικά.

1.2. Αντικείμενο και διάρθρωση της εργασίας

Όπως αναφερθήκαμε παραπάνω η ύπαρξη ενός πλέγματος συνεπάγεται μια πληθώρα προβλημάτων που πρέπει να αντιμετωπιστούν. Μερικά από αυτά είναι η διαχείριση των τεράστιων όγκων των δεδομένων, η ταυτοποίηση των χρηστών και η δρομολόγηση μιας διεργασίας σε διάφορα επεξεργαστικά κέντρα.

Πιο συγκεκριμένα ένα τέτοιο περιβάλλον μπορεί να αποτελείται από χιλιάδες χρήστες, που επιθυμούν να έχουν πρόσβαση σε μεγάλο όγκο δεδομένων για να μπορέσουν να τον επεξεργαστούν. Η επεξεργασία μπορεί να συνεπάγεται διάφορες ενέργειες όπως η τροποποίηση των δεδομένων αυτών, η διαγραφή τους και η μεταφορά τους. Βασικότερο πρόβλημα όλων αυτών είναι η ταυτοποίηση του χρήστη και η εξουσιοδότηση του.

Το πρόβλημα αυτό δεν είναι καινούργιο. Στο παρελθόν, έχουν προταθεί λύσεις τις οποίες ισχυριζόμαστε ότι δεν είναι αποδοτικές και δεν εναρμονίζονται με τις βασικές αρχές του πλέγματος ή έχουν χαμηλή απόδοση.

Στο Κεφάλαιο 1 γίνεται μια σύντομη εισαγωγή στο πρόβλημα και τις δυσκολίες που μπορεί να αντιμετωπίσουμε. Στο Κεφάλαιο 2 γίνεται μια σύντομη αναφορά στην βασική ορολογία καθώς και για τον διαχωρισμό και τα ιδιαίτερα χαρακτηριστικά που πρέπει να έχει ένα σύστημα διαχείρισης πιστοποιητικών. Επίσης περιγράφονται αρχιτεκτονικές διαφόρων συστημάτων που προσπαθούν να επιλύσουν το πρόβλημα που επεξεργαζόμαστε. Στο κεφάλαιο 3 περιγράφεται η δομή του συστήματος που προτείνουμε (το «Νεφέλη»(Nepheli)) καθώς και οι αλλαγές που έχουν γίνει για την αποδοτικότερη λειτουργία του. Στο κεφάλαιο 4 παρουσιάζονται τα πειραματικά αποτελέσματα που αξιολογούν την απόδοση του συστήματος. Τέλος στο κεφάλαιο 5 συνοψίζονται τα συμπεράσματα και παρουσιάζονται μελλοντικές επεκτάσεις της παρούσας έρευνας.

ΚΕΦΑΛΑΙΟ 2. ΣΧΕΤΙΚΗ ΕΡΕΥΝΑ

2.1. Εισαγωγή

Στο κεφάλαιο αυτό κάνουμε μια βιβλιογραφική αναφορά στις πιο σημαντικές λύσεις που έχουν προταθεί και υλοποιηθεί και μια κριτική στα προβλήματα που λύνουν ή αφήνουν ανοιχτά. Αρχικά αποσαφηνίζουμε κάποιους ορισμούς σχετικά με τα πιστοποιητικά και τους τύπους που μπορούν να κατηγοριοποιηθούν. Στην συνέχεια περιγράφουμε διάφορα συστήματα που προσπαθούν να αντιμετωπίσουν το πρόβλημα αυτό.

2.2. Τύποι των πιστοποιητικών

Σε ένα σύστημα κάθε χρήστης έχει μια μοναδική ταυτότητα που τον διαχωρίζει από άλλους χρήστες. Για να ταυτοποιηθεί ένας χρήστης θα πρέπει να παρουσιάσει ένα πιστοποιητικό (credentials) που να βεβαιώνει ότι είναι αυτός που ισχυρίζεται ότι είναι. Το πιστοποιητικό επιπλέον μπορεί να χρησιμοποιηθεί για να εξουσιοδοτήσει ένα χρήστη για τη χρησιμοποίηση ορισμένων πόρων ενός συστήματος και συνήθως έχει περιορισμένη διάρκεια ζωής. Η ασφαλής διαχείριση των πιστοποιητικών αυτών

είναι μια πρόκληση που απαιτεί ιδιαίτερη προσοχή στον σχεδιασμό οποιουδήποτε συστήματος που τα χρησιμοποιεί.

Συγκεκριμένα θα μπορούσαμε να τα κατηγοριοποιήσουμε ως εξής:

- Πιστοποιητικά ταυτότητας (identity credentials): Αποδεικνύουν την ταυτότητα του χρήστη. Στα συστήματα που εξετάζουμε συνήθως είναι κάποιες ψηφιακές υπογραφές που έχουν πιστοποιηθεί από κάποιο εγκεκριμένο φορέα πιστοποίησης, δηλαδή υπάρχει μια αρχή που εγγυάται την ταυτότητα του χρήστη.
- Πιστοποιητικά ταυτοποίησης (authentication credentials): Είναι παρόμοια με τα παραπάνω. Η ουσιώδης διαφορά τους έγκειται στο ότι τα πιστοποιητικά ταυτοποίησης έχουν περιορισμένη διάρκεια ζωής. Συνήθως τα πιστοποιητικά ταυτότητας χρησιμοποιούνται για να αποκτηθούν τα πιστοποιητικά ταυτοποίησης. Χαρακτηριστικό παράδειγμα είναι η διαδικασία απόκτησης άδειας παραμονής σε μια χώρα. Χορηγείται από την κυβέρνηση του εκάστοτε πολίτη αλλά έχει ισχύ σε μια άλλη χώρα. Για την χορήγηση της ο πολίτης πρέπει να προσκομίσει κάποια πιστοποιητικά ταυτότητας. Επομένως όταν κάποιος χρήστης έχει πιστοποιήσει την ταυτότητα του σε ένα φορέα τότε ο φορέας του παρέχει ένα πιστοποιητικό ταυτοποίησης για να μπορέσει να έχει πρόσβαση σε ένα άλλον.
- Πιστοποιητικά εξουσιοδότησης (authorization credentials): Δίνονται για να εξουσιοδοτήσουν τους χρήστες στην πρόσβαση διαφόρων πόρων.

2.3. Χαρακτηριστικά των συστημάτων διαχείρισης πιστοποιητικών

Η ομάδα εργασίας Ασφαλής Διαθεσιμότητα Πιστοποιητικών (Secure Available Credential-SACRED) στον Οργανισμό Ανάπτυξης Προτύπων για το Διαδίκτυο (Internet Engineering Work Force-IETF) ασχολείται με τα ζητήματα ασφάλειας και τη διαχείριση των πιστοποιητικών σε ένα διαδικτυακό περιβάλλον. Αναπτύσσει λύσεις που να υποστηρίζουν τη χρήση των ίδιων πιστοποιητικών σε διαφορετικούς διακομιστές διαδικτύου και την ασφαλή αποθήκευση τους. Η ομάδα αυτή έχει αναπτύξει κάποιες προτάσεις (RFC:Requests for Comments) και έχει θέσει ένα πλαίσιο που πρέπει να ικανοποιούν τα συστήματα αυτά που αναφέρονται παρακάτω:

- Μετάδοση πιστοποιητικών (credential transmission): Τα πιστοποιητικά πρέπει να μεταδίδονται με ασφαλή (κρυπτογραφημένα) τρόπο σε ένα περιβάλλον με αναξιόπιστους διαύλους επικοινωνίας. Επίσης θα πρέπει να είναι πιστοποιημένα από την αρχή που τα εξέδωσε.
- Αποθήκευση πιστοποιητικών (credential storage): Η αποθήκευση αυτών των ευαίσθητων δεδομένων θα πρέπει να γίνεται με προσοχή. Ειδικότερα να αποθηκεύονται σε κρυπτογραφημένη μορφή και μόνο ο ιδιοκτήτης τους να μπορεί να τα ανακτήσει.
- Ετερογένεια (heterogeneity): Διαφορετικών τύπων πιστοποιητικά και η χρήση διαφορετικών κρυπτογραφικών πρωτοκόλλων θα πρέπει να υποστηρίζονται από όλους τους φορείς που συμμετέχουν. Αυτό κυρίως απαιτείται σε τεχνολογίες πλέγματος.

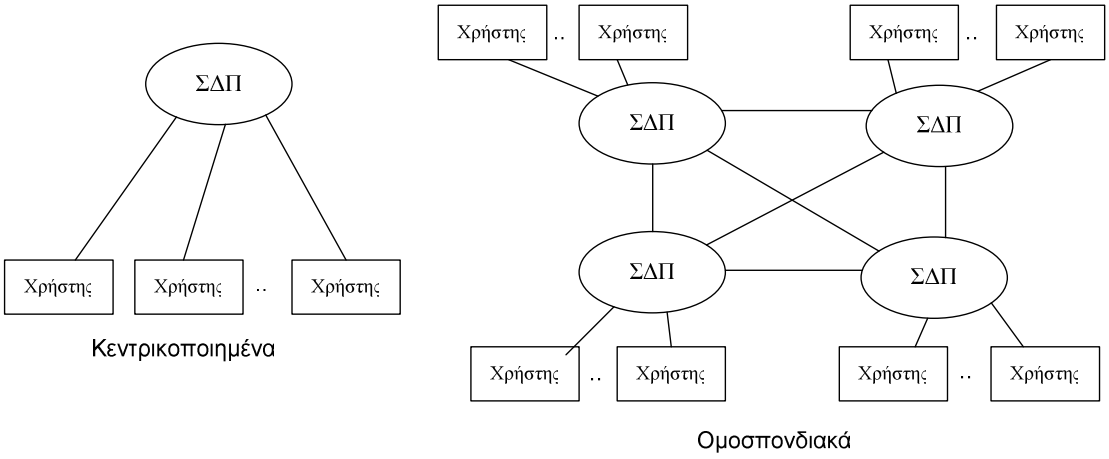
Με βάση τις προαναφερθείσες σχεδιαστικές αρχές είναι προφανές ότι ένα σύστημα διαχείρισης πιστοποιητικών πρέπει να παρέχει ασφαλή μετάδοση, αποθήκευση και να είναι συμβατό με διαφορετικού τύπου συστήματα και μηχανισμούς. Τα βασικά χαρακτηριστικά ενός συστήματος διαχείρισης πιστοποιητικών είναι τα εξής:

- Έναρξη (Initiation): Μετά την ταυτοποίηση του χρήστη με διάφορους μηχανισμούς (εισαγωγή προσωπικού κωδικού, εισαγωγή βιομετρικών χαρακτηριστικών κ.λ.π.) κάθε σύστημά διαχείρισης πιστοποιητικών πρέπει να παρέχει πιστοποιητικά.
- Ασφαλής αποθήκευση (Secure storage): Ειδικά τα πιστοποιητικά του τύπου μεγάλης διάρκειας (long-term) και τα ιδιωτικά κλειδιά πρέπει να αποθηκεύονται με ασφαλή τρόπο. Η κλοπή των μακροπρόθεσμων πιστοποιητικών μπορεί να ισοδυναμεί με μακροπρόθεσμη παραβίαση της ασφάλειας του συστήματος.
- Προσιτότητα (Accessibility): Το σύστημά διαχείρισης πιστοποιητικών πρέπει να μπορεί να παράσχει πιστοποιητικά κάθε φορά που θα ζητηθεί από τον χρήστη.

- Ανανέωση (Renewal): Τα περισσότερα πιστοποιητικά έχουν περιορισμένη περίοδο ζωής. Το σύστημά διαχείρισης πιστοποιητικών πρέπει να μπορεί να διαχειριστεί σωστά τα εκπρόθεσμα πιστοποιητικά.
- Μετάφραση (Translation): Αυτό το χαρακτηριστικό είναι ζωτικής σημασίας εάν υπάρχουν πολλαπλά συστήματα καθένα από οποία χρησιμοποιεί διαφορετικούς μηχανισμούς ταυτοποίησης και ασφάλειας. Πρέπει να υπάρχει τρόπος μετάφρασης των πιστοποιητικών για να μπορούν να χρησιμοποιηθούν από τις ετερογενείς διασκορπισμένες οντότητες.
- Έλεγχος (Delegation): Το σύστημα διαχείρισης πιστοποιητικών πρέπει να παρακολουθεί και να διεξάγει εξονυχιστικούς ελέγχους για τα πιστοποιητικά που παρέχονται στους χρήστες.
- Ανακάλεση (Revocation): Κάθε σύστημα διαχείρισης πιστοποιητικών πρέπει να έχει την δυνατότητα να ανακαλέσει ένα πιστοποιητικό εάν διαπιστωθεί ότι κάποιος χρήστης το έχει παράνομα στην κατοχή του.

2.4. Κατηγοριοποίηση των συστημάτων διαχείρισης πιστοποιητικών

Τα συστήματα διαχείρισης πιστοποιητικών-ΣΔΠ μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες. Η πρώτη είναι τα συστήματα διαχείρισης αποθήκευσης πιστοποιητικών (ή κεντρικοποιημένα) που είναι υπεύθυνα για την αποθήκευση και μερικές φορές για την άμεση δημιουργία των πιστοποιητικών μόλις ζητηθεί από τον χρήστη. Η δεύτερη είναι τα ομοσπονδιακά συστήματα διαχείρισης πιστοποιητικών που είναι υπεύθυνα για την κατανομή τους στους χρήστες μεταξύ διαφόρων οργανισμών που συμμετέχουν (σχήμα 2.1).



Σχήμα 2.1 Κεντρικοποιημένα και ομοσπονδιακά συστήματα διαχείρισης πιστοποιητικών (ΣΔΠ)

Για να εισέλθουμε στον οργανισμό όπου ανήκουμε χρησιμοποιούμε (συνήθως) την ταυτότητα και το κωδικό που δίνουν πρόσβαση στα έγγραφα και τους πόρους του οργανισμού. Αντίστοιχα έχουμε τα πιστοποιητικά που χρησιμοποιούνται σε ένα κεντρικοποιημένο σύστημα διαχείρισης πιστοποιητικών. Ωστόσο τα κεντρικοποιημένα συστήματα δεν μπορούν να εξυπηρετήσουν όλους τους σκοπούς. Για παράδειγμα, ας υποθέσουμε ότι σχεδιάζουμε να επισκεφτούμε μια πόλη του εξωτερικού. Υπάρχουν δύο οργανισμοί ο Χ και ο Υ. Ο πρώτος διαχειρίζεται τη μεταφορά και ο δεύτερος τη διαμονή. Αφού έχουμε (λογικά) δύο διαφορετικούς λογαριασμούς ή πιστοποιητικά θα πρέπει να παράσχουμε τις ίδιες πληροφορίες δύο φορές. Αντιθέτως εάν διαμοιράζονταν οι κοινές αυτές πληροφορίες μεταξύ των δύο οργανισμών δεν θα χρειαζόταν η υποβολή διαφορετικών πιστοποιητικών σε κάθε οργανισμό. Αυτό είναι ένα χαρακτηριστικό παράδειγμα ενός ομοσπονδιακού συστήματος διαχείρισης πιστοποιητικών. Πρέπει τα πιστοποιητικά να ανταλλάσσονται μεταξύ οντοτήτων που εμπιστεύονται η μία την άλλη.

Από τα παραπάνω παραδείγματα φαίνεται ότι τα ομοσπονδιακά συστήματα διαχείρισης πιστοποιητικών μπορεί να είναι χρήσιμα μόνο για τη διαχείριση της ταυτότητας του χρήστη σε διάφορους οργανισμούς. Ωστόσο σε συστήματα πλέγματος η εφαρμογή τους μπορεί να μην είναι προφανής. Τα περισσότερα συστήματα που

έχουν σχεδιαστεί παρέχουν κεντρικοποιημένο έλεγχο των πόρων. Ωστόσο όταν οι οργανισμοί συνεργάζονται για την δημιουργία εικονικών οργανισμών έτσι ώστε να χρησιμοποιήσουν από κοινού τους πόρους είναι αναγκαίο να «συνεργαστούν» οι διάφοροι τοπικοί μηχανισμοί ταυτοποίησης. Για παράδειγμα έχουμε τρεις οργανισμούς που έχουν διαφορετικούς μηχανισμούς ταυτοποίησης, όπως ο Kerberos και τα X.509 πιστοποιητικών. Οι οργανισμοί αυτοί θέλουν να συνεργαστούν και να μοιραστούν τους πόρους που διαθέτουν. Επομένως είναι αναγκαίο να γίνει διαχείριση διαφορετικών τύπων πιστοποιητικών σε διάφορα συστήματα με διαφορετικούς μηχανισμούς ταυτοποίησης. Συμπερασματικά μερικά χαρακτηριστικά που πρέπει να υπάρχουν σε κάθε ομοσπονδιακό σύστημα διαχείρισης πιστοποιητικών είναι:

- Αποθήκευση ετερογενών πιστοποιητικών (Repository of Heterogeneous Credentials): Ένα ομοσπονδιακό σύστημα διαχείρισης πιστοποιητικών απαιτεί την ασφαλής αποθήκευση των διαφόρων τύπων πιστοποιητικών.
- Μεταφορά πιστοποιητικών (Credential Transfer): Πρέπει να μεταφέρονται τα πιστοποιητικά στα διάφορα συστήματα με ασφαλή τρόπο.
- Μετάφραση πιστοποιητικών (Credential Translation): Απεικόνιση ανάμεσα σε διαφορετικών τύπων πιστοποιητικά ώστε ο χρήστης να μπορεί να κάνει εγγραφή και να υποβάλλει κάποιες εργασίες σε διαφορετικού τύπου σύστημα διαχείρισης πιστοποιητικών που χρησιμοποιεί ο οργανισμός στον οποίο εκτελείται η εργασία.

2.5. Self-certifying File System.

Το πρόβλημα που αντιμετωπίζει το σύστημα Self-certifying File System-SFS[7] είναι η ταυτοποίηση χρηστών σε ένα παγκόσμιο σύστημα αρχείων. Αναλυτικότερα υπάρχουν χρήστες οι οποίοι θέλουν να προσπελάσουν κάποια αρχεία που βρίσκονται σε έναν απομακρυσμένο διακομιστή διαφορετικού οργανισμού. Το κυριότερο πρόβλημα που προκύπτει είναι αυτό της εξακρίβωσης της ταυτότητας του χρήστη, έτσι ώστε να μπορούμε να τον εμπιστευτούμε και να του παράσχουμε το δικαίωμα να τροποποιήσει τα αρχεία που διαχειριζόμαστε.

Όταν ένας χρήστης θέλει να προσπελάσει ένα διακομιστή αρχείων, τότε αυτός ο διακομιστής αρχείων στέλνει ένα αίτημα στον διακομιστή πιστοποίησης του χρήστη για να γίνει η ταυτοποίηση του. Ο διακομιστής πιστοποίησης παραδίδει ένα σύνολο από πιστοποιητικά για τον χρήστη στο διακομιστή αρχείων. Ο διακομιστής χρησιμοποιεί τα πιστοποιητικά αυτά σε συνδυασμό με τη Λίστα Ελέγχου Πρόσβασης (ACL: Access Control List) για να αποφασίσει εάν θα επιτρέψει στον χρήστη να «διαχειριστεί» τα αρχεία. Η ACL είναι μια λίστα που καθορίζει με ακρίβεια ποιος μπορεί να εκτελέσει κάποια εργασία πάνω σε ένα αντικείμενο και τι είδους εργασία θα είναι αυτή. Στην περίπτωση μας η ACL περιέχει απομακρυσμένες οντότητες που έχουν οριστεί και υφίστανται διαχείριση από διαφορετικούς οργανισμούς. Για παράδειγμα ένας τοπικός χρήστης μπορεί να επιθυμεί να συμπεριλάβει ένα απομακρυσμένο χρήστη στην ACL του έτσι ώστε να του δώσει πρόσβαση στα δεδομένα του με απώτερο σκοπό την ανάπτυξη μιας συνεργασίας.

Συνήθως την πρώτη φορά που δίδεται πρόσβαση στον χρήστη αυτομάτως εγγράφεται στην ACL. Με αυτό τον τρόπο την επόμενη φορά που θα χρειαστεί ο χρήστης να προσπελάσει τα ίδια αρχεία, απλώς το σύστημα συμβουλεύετε την ACL και ανάλογα του επιτρέπει την πρόσβαση ή όχι. Όταν ο χρήστης παύει να ανήκει στον τοπικό διακομιστή που του παρείχε τα πιστοποιητικά πρέπει να γίνει μία αναβάθμιση στην ACL, έτσι ώστε να μην του επιτραπεί η πρόσβαση. Επομένως η λίστα θα πρέπει να ανανεώνεται περίπου κάθε μια ώρα (χωρίς αποτυχίες στο διαδίκτυο).

Για την ταυτοποίηση του χρήστη, το SFS στηρίζεται στην κρυπτογραφία δημοσίου κλειδιού[11]. Ένα πρόγραμμα που καλείται SFS-πράκτορας (SFS-agent) εκτελείται από την μεριά του χρήστη και δημιουργεί μια αίτηση πιστοποίησης (authentication request) εκ μέρους του χρήστη υπογεγραμμένη με το ιδιωτικό του κλειδί. Ο χρήστης στέλνει αυτή την αίτηση στον διαχειριστή αρχείων, που είναι υπεύθυνος για τα αρχεία που θέλει να προσπελάσει. Αυτός με την σειρά του τα στέλνει στον διακομιστή πιστοποίησης (authentication server) του χρήστη που πιστοποιεί ότι η υπογραφή είναι από τον χρήστη και ειδοποιεί το διαχειριστή αρχείων. Κάθε επόμενη επικοινωνία που γίνεται με το διαχειριστή αρχείων ανατρέχει στην ACL και διαπιστώνει την εγκυρότητα του χρήστη.

2.6. Secure Virtual Enclaves.

Ο κύριος σκοπός του συστήματος των Ασφαλών Εικονικών Τόπων (Secure Virtual Enclaves-SVE)[19] είναι να αναπτύξει ένα σύστημα ενδιάμεσου λογισμικού (middleware) με σκοπό να μπορέσουν οι διάφοροι οργανισμοί να συνενώσουν τους πόρους τους. Πάντως ο κάθε οργανισμός διατηρεί τις πολιτικές ασφαλείας που εφαρμόζει πάνω στους πόρους του. Ο λόγος που η συγκεκριμένη προσέγγιση επιλέγει το ενδιάμεσο λογισμικό είναι επειδή μπορούν να συνεργαστούν διάφορα λειτουργικά συστήματα από διαφόρους οργανισμούς και να δημιουργηθούν εύκολα κατανεμημένες εφαρμογές.

Ο *τόπος* είναι ένα σύνολο από πόρους που υφίστανται διαχείριση από τον ίδιο οργανισμό και εφαρμόζεται πάνω σε αυτούς η ίδια πολιτική ασφαλείας. Ένα σύνολο από πολλούς τόπους αποτελεί έναν SVE. Ένας τόπος μπορεί να ανήκει σε διαφορετικούς SVE. Ο όρος συνεργασία (collaboration) αναφέρεται σε χρήστες που ανήκουν σε διαφορετικούς τόπους και τους επιτρέπεται πρόσβαση σε εκατέρωθεν πόρους. Οι έλεγχοι ασφαλείας προσφέρουν σε αυτούς που έχουν κάνει την συνεργασία την προαποφασισμένη πολιτική πρόσβασης πόρων. Ο όρος τοπική αυτονομία έχει ξεχωριστή σημασία. Περιγράφει έναν οργανισμό που προσφέρει τους πόρους του και διασφαλίζει ότι έχει την κύρια ευθύνη της διαχείρισης τους. Επιπλέον καθορίζει τους πόρους μπορεί να συνεισφέρει. Τέλος με τον όρο κατανεμημένες εφαρμογές εννοούμε τις εφαρμογές που έχουν δημιουργηθεί με ενδιάμεσο λογισμικό, όπως είναι π.χ. η JAVA RMI.

Η γραφική διεπαφή πολιτικής επιτρέπει στον διαχειριστή να εξελίσσει και να διατηρεί τι υπάρχουσες πολιτικές ασφαλείας για τους τοπικούς πόρους. Ο ελεγκτής ανταλλαγών ασφαλείας (SVE Policy Exchange Controller-SPEX) μεταδίδει τις πολιτικές ασφαλείας στους άλλους τόπους του SVE. Επίσης ο SPEX δέχεται εντολές από τον διαχειριστή του για την εισαγωγή ενός τόπου στο SVE ή την αποχώρηση του. Οι παρεμβαλλόμενοι/εκτελεστές (Interceptor/Enforcers) λαμβάνουν τις αιτήσεις των χρηστών για πόρους. Στην συνέχεια ρωτούν έναν υπολογιστή πρόσβασης για την απόφαση της διαχείρισης του πόρου και είτε την αποδέχονται είτε την απορρίπτουν. Κάθε διαχειριστής ενός τόπου δημιουργεί και διατηρεί την τοπική πολιτική πρόσβασης για κάθε έναν SVE στον οποίο ανήκει.

Ο κύριος σκοπός του SVE είναι η ανάπτυξη μιας πλατφόρμας ενδιάμεσου λογισμικού, που επιτρέπει διάφορους τόπους να εμπλέκονται σε υπολογισμούς χρησιμοποιώντας κατανεμημένες εφαρμογές διατηρώντας την αυτονομία της πολιτικής του κάθε τόπου για τους πόρους που προσφέρει. Δύο ή περισσότεροι οργανισμοί αποφασίζουν να χρησιμοποιήσουν από κοινού πόρους τους. Ο διαχειριστής του ενός ξεκινά να ονοματίζει και δημιουργεί ένα SVE και παρατηρεί ποιοι άλλοι τόποι μπορεί να εμπιστευτεί για να εισαχθούν στην συνεργασία. Ο δημιουργός του είναι το μοναδικό μέλος ολόκληρου του SVE. Στο επόμενο βήμα ο διαχειριστής καθορίζει ποιοι θα είναι οι τοπικοί πόροι, την πολιτική πρόσβασης των πόρων αυτών, καθώς και τις τοπικές οντότητες που θα έχουν την εξουσιοδότηση να έχουν πρόσβαση στους πόρους του SVE. Οι διαχειριστές των υπόλοιπων τόπων που δεν έχουν εισαχθεί σε αυτό το SVE προωθούν μια αίτηση για την εισαγωγή τους. Αφού η αίτηση έχει υποβληθεί, η διεκπεραίωση της διαδικασίας είναι αυτοματοποιημένη. Τα συνιστώμενα μέρη ενός τόπου επικοινωνούν με τα αντίστοιχα μέρη του άλλου για να καθιερώσουν την συνεργασία. Τέλος οι χρήστες πλέον μπορούν να έχουν πρόσβαση σε όλους τους πόρους σε όποιο τόπο και αν ανήκουν.

2.7. Το σύστημα CRISIS.

Το CRISIS[2] είναι ένα σύστημα ασφαλείας ενός διαδικτυακού λειτουργικού συστήματος (WebOS: Web Operating System). Τα WebOS είναι λειτουργικά συστήματα που τρέχουν κατευθείαν μέσα από τον περιηγητή στο διαδίκτυο. Περιέχουν πολλές εφαρμογές οι οποίες μπορούν να αντικαταστήσουν ή να συμπληρώσουν αυτές που ήδη χρησιμοποιείται με το τρέχον (κανονικό) λειτουργικό σύστημα, ενώ κάποια από αυτά προσφέρουν και διάφορα επιπρόσθετα όπως δωρεάν αποθηκευτικός χώρος.

Οι βασικοί στόχοι που εξυπηρετεί η συγκεκριμένη αρχιτεκτονική ασφαλείας είναι δύο. Αρχικά οι χρήστες πρέπει να έχουν «ασφαλή» πρόσβαση σε ό,τι αφορά τους κοινούς πόρους, όπως είναι αρχεία, επεξεργαστική ισχύς ή αποθήκευση δεδομένων. Οι πάροχοι αυτών των πόρων χρειάζονται κατάλληλους μηχανισμούς για να κάνουν

την ταυτοποίηση κάθε χρήστη που απαιτεί την χρησιμοποίηση τους και να παρέχουν την πρόσβαση με τα κατάλληλα πιστοποιητικά.

Για την μετέπειτα περιγραφή του συστήματος ορίζουμε τρεις βασικές οντότητες:

- Πρόσωπα (Principals): Είναι οποιεσδήποτε οντότητες κάνουν αιτήσεις για πόρους. Επιπλέον τα πρόσωπα διατυπώνουν αιτήματα και έχουν ονόματα. Παραδείγματα προσώπων είναι οι χρήστες και οι υπολογιστές.
- Αντικείμενα (Objects): Τα αντικείμενα είναι πόροι που χρησιμοποιούνται από όλους όπως αρχεία, επεξεργαστική ισχύς, μνήμη, κ.τ.λ.
- Παρατηρητές Αναφορών (Reference Monitors): Μόλις πιστοποιηθεί μια αίτηση πρόσβασης από μια οντότητα για ένα αντικείμενο οι παρατηρητές αναφορών αποφασίζουν εάν θα δοθεί η τελική πρόσβαση ή όχι.

Η μεγαλύτερη καινοτομία που εισάγει το CRISIS είναι η αρχή που υπογράφει τα πιστοποιητικά. Είναι προφανές πως την αρχή αυτή θα πρέπει να εμπιστεύονται όλες οι οντότητες που συμμετέχουν στο σύστημα. Αυτή η αρχή καλείται Αρχή Πιστοποίησης-ΑΠ (Certification Authority). Η ΑΠ αντιστοιχίζει δημόσια κλειδιά σε οντότητες και διατηρεί μια Λίστα Κατάργησης Πιστοποιητικών απαριθμώντας όλα εκείνα τα κλειδιά που έχουν αλλάξει ή έχουν υποκλαπεί. Στο CRISIS, η ΑΠ υπογράφει όλα τα πιστοποιητικά ταυτότητας με μια υπογραφή που διαρκεί μερικές εβδομάδες. Επιπλέον υπάρχει μια τοπική συνεχώς συνδεδεμένη οντότητα-ΣΣΟ (OLA: on line agent) που είναι υπεύθυνη για τις δεύτερες υπογραφές μικρής διάρκειας που έχουν επίσης τα πιστοποιητικά. Κάθε πιστοποιητικό για θεωρηθεί έγκυρο πρέπει να είναι υπογεγραμμένο και από τις δύο παραπάνω οντότητες.

Ο διαχωρισμός ΑΠ/ΣΣΟ προσφέρει σημαντικά πλεονεκτήματα. Για την αποτελεσματική κλοπή ενός κλειδιού πρέπει και οι δύο υπηρεσίες να υπονομευτούν ή η ΑΠ να υπονομευτεί χωρίς όμως να το αντιληφθούμε. Επιπλέον η ΑΠ για το μεγαλύτερο χρονικό διάστημα παραμένει ανενεργή αυξάνοντας την ασφάλεια του συστήματος αφού σε μια τέτοια κατάσταση είναι δύσκολο να πραγματοποιηθεί οποιαδήποτε επίθεση. Ένα ακόμα πλεονέκτημα του διαχωρισμού είναι ότι μια Α.Π που έχει υπονομευτεί δεν μπορεί να ανακαλέσει το κλειδί ενός χρήστη και υποδυθεί τον χρήστη κάποιος χωρίς την συμμετοχή της ΣΣΟ. Η ανάκληση του κλειδιού ενός

χρήστη συνεπάγεται την υπογραφή του κλειδιού του από την οντότητα ΣΣΟ. Τέλος ένα ΣΣΟ που έχει υπονομευτεί το μόνο επιβλαβές που μπορεί να επιφέρει στο σύστημα είναι άρνηση της υπηρεσίας (DoS:Denial of Service) που σε αυτή την περίπτωση αντιμετωπίζεται με την ΑΠ να τροφοδοτεί με νέα πιστοποιητικά μια νέα ΣΣΟ.

2.8. Το σύστημα Maat

Το συγκεκριμένο σύστημα αρχείων αποτελείται από τρία μέρη: τον πελάτη, ένα διακομιστή μεταδιδόμενων και μια συστοιχία από μηχανές αποθήκευσης. Επιπλέον οι μηχανές αποθήκευσης δεν γνωρίζουν τα δικαιώματα των χρηστών επειδή τη σχετική πληροφορία αποθηκεύει και διαχειρίζεται ο διακομιστής μεταδεδομένων. Ένας πελάτης που θέλει να δημιουργήσει ένα αρχείο παράγει ένα ζεύγος δημοσίου και ιδιωτικού κλειδιού και δημιουργεί το αρχείο εκ μέρους του δημόσιου κλειδιού. Το ιδιωτικό κλειδί διανέμεται σε όλους τους χρήστες που θέλουν να έχουν πρόσβαση στο αρχείο αυτό.

Μια βασική σχεδιαστική αρχή του Maat[9] είναι τα εκτεταμένα πιστοποιητικά (extended capabilities). Ένα απλό πιστοποιητικό θα μπορούσε να αναφέρει πως ο χρήστης Α έχει δικαίωμα να διαβάσει το αντικείμενο Υ. Τώρα όμως το νέο αυτό πιστοποιητικό μπορεί να αναφέρει ότι οι χρήστες Α,Β και C έχουν δικαίωμα να διαβάσουν τα αρχεία Χ.Υ και Ζ. Με συνδυασμό δικαιωμάτων ο διακομιστής μεταδεδομένων μπορεί να παράγει λιγότερα πιστοποιητικά αφού ένα εκτεταμένο μπορεί να αντικαταστήσει πολλά πιστοποιητικά παλιότερης αρχιτεκτονικής. Αυτό συνεπάγεται ότι οι μηχανές αποθήκευσης πρέπει να επιβεβαιώσουν λιγότερα πιστοποιητικά και έτσι μπορούν να ικανοποιήσουν περισσότερα I/O αιτήματα.

2.9. Το σύστημα GSI

Η Υποδομή Ασφαλείας Πλέγματος (Grid Security Infrastructure-GSI)[3] χρησιμοποιείται στο σύστημα που έχουμε κατασκευάσει. Θα κάνουμε εκτενή περιγραφή όσο για την αρχιτεκτονική και το περιβάλλον για το οποίο προορίζεται να χρησιμοποιηθεί. Η GSI είναι μέρος του Globus Project και έχει σχεδιαστεί έτσι ώστε

να παρέχει ασφάλεια σε ένα κατανεμημένο περιβάλλον. Εστιάζει κυρίως σε θέματα ταυτοποίησης και ελέγχου πρόσβασης. Ειδικότερα παρέχει μηχανισμούς ταυτοποίησης σε ένα χρήστη, στις διεργασίες που μπορεί να εκτελέσει αυτός ο χρήστης, στη δέσμευση των πόρων που χρησιμοποιούνται από τον χρήστη καθώς και ένα μηχανισμό αμοιβαίας ταυτοποίηση όλων των παραπάνω οντοτήτων. Επίσης επιτρέπει τη λειτουργία τοπικών μηχανισμών ελέγχου χωρίς ιδιαίτερες αλλαγές.

Για την επίτευξη των παραπάνω στόχων έχουν δημιουργηθεί τέσσερα πρωτόκολλα. Με το Πρωτόκολλο 1 ένας χρήστης κάνει μια σύνδεση (log on) στο σύστημα πλέγματος δημιουργώντας έναν προσωρινό πληρεξούσιο χρήστη (user proxy). Ο πληρεξούσιος χρήστης με την χρήση του Πρωτοκόλλου 2 μπορεί να δεσμεύσει πόρους για την εκτέλεση μιας εφαρμογής. Με την χρήση του Πρωτοκόλλου 3 μια διεργασία μπορεί να δεσμεύσει και αυτή όσους πόρους κρίνεται απαραίτητο άμεσα. Τέλος το Πρωτόκολλο 4 ορίζει μια αντιστοίχηση από σφαιρικές σε τοπικές οντότητες.

Πριν αναφέρουμε για το πως εφαρμόζεται όλο αυτό το σύστημα ταυτοποίησης πρέπει πρώτα να ορίσουμε τον πληρεξούσιο χρήστη. Ο πληρεξούσιος χρήστης είναι μια οντότητα που ενεργεί εκ μέρους του χρήστη. Συγκεκριμένα είναι μια διεργασία που ξεκινά από τον χρήστη σε κάποια τοποθεσία κοντά σε αυτόν. Ο χρήστης μπορεί να επιτρέψει στον πληρεξούσιο του να ενεργεί εκ μέρους του χρήστη παρέχοντας του συγκεκριμένα πιστοποιητικά.

Ο πληρεξούσιος χρήστης συμπεριφέρεται σαν να ήταν ο ίδιος ο χρήστης. Έχει τα δικά του πιστοποιητικά έτσι ώστε να μην χρειάζεται ο χρήστης να είναι συνδεδεμένος συνέχεια κατά την διάρκεια των υπολογισμών που έχει ζητήσει. Επίσης εξαλείφει την ανάγκη να έχει διαθέσιμα τα μακροπρόθεσμα πιστοποιητικά του χρήστη συνεχώς. Επιπλέον ο πληρεξούσιος χρήστης είναι υπό τον απόλυτο έλεγχο του χρήστη και μπορεί να τερματιστεί (συνήθως η διάρκεια ζωής του ορίζεται ως η διάρκεια των υπολογισμών). Αυτό σημαίνει ότι στην περίπτωση που υποκλαπούν τα πιστοποιητικά του οι επιπτώσεις δεν θα είναι και τόσο βλαβερές όσο θα ήταν εάν είχαν κλαπεί τα μακροπρόθεσμα πιστοποιητικά (long-lived credentials) του χρήστη που χρησιμοποιούνται για την δημιουργία των βραχυπρόθεσμων.

Άλλη μια σημαντική οντότητα που πρέπει να ορίσουμε είναι ο πληρεξούσιος διαχειριστής πόρων (resource proxy). Πρόκειται για μια διεπαφή (interface) ανάμεσα στην ασφάλεια του πλέγματος και στην τοπική ασφάλεια του κάθε πόρου. Αναλαμβάνει στην ουσία να «μεταφράσει» τις έγκυρές δεσμεύσεις των πόρων στους τοπικούς μηχανισμούς ασφαλείας.

Όπως αναφέραμε πιο πάνω το Πρωτόκολλο 1 περιγράφει τον τρόπο με τον οποίο δημιουργείται ο πληρεξούσιος χρήστης. Για την λειτουργία του θα πρέπει να δημιουργηθεί ένα προσωρινό πιστοποιητικό. Αυτό γίνεται κυρίως για δύο σημαντικούς λόγους. Αφ'ενός θέλουμε να περιορίσουμε όσο το δυνατόν περισσότερο την περίπτωση εκείνη όπου χρησιμοποιούνται τα μακροπρόθεσμα πιστοποιητικά και αφ'εταίρου μας επιτρέπεται να οριοθετήσουμε ένα χρονικό διάστημα που το βραχυπρόθεσμο πιστοποιητικό μπορεί να είναι ενεργό. Έτσι λοιπόν δημιουργείται ένα βραχυπρόθεσμο πιστοποιητικό που το συμβολίζουμε C_{UP} το οποίο ο χρήστης το πιστοποιεί υπογράφοντάς με κάποιο ιδιωτικό κλειδί του. Το C_{UP} έχει περιορισμένη διάρκεια ζωής καθώς και άλλους περιορισμούς που προσδιορίζονται από τον χρήστη. Περιγράφουμε το Πρωτόκολλο 1 παρακάτω:

- Ο χρήστης αποκτά πρόσβαση σε ένα υπολογιστή, οπού θα δημιουργηθεί ο πληρεξούσιος χρήστης. Η ταυτοποίηση σε αυτή τη φάση μπορεί να γίνει χρησιμοποιώντας οποιοδήποτε είδος τοπικού μηχανισμού ασφαλείας.
- Ο χρήστης δημιουργεί το πιστοποιητικό που θα χρησιμοποιηθεί από το πληρεξούσιο χρήστη το C_{UP} χρησιμοποιώντας τα μακροπρόθεσμα πιστοποιητικά που έχει. Στην ουσία το νέο πιστοποιητικό που δημιουργείται είναι μια σειρά πληροφοριών που έχει υπογραφεί από τα μακροπρόθεσμα πιστοποιητικά Οι πληροφορίες αυτές είναι το όνομα του χρήστη (user-id), το όνομα του τοπικού φορέα (local host), η διάρκεια ζωής του C_{UP} και οποιαδήποτε άλλη πληροφορία που απαιτείται από το πρωτόκολλο πιστοποίησης.

- Στο τελευταίο βήμα δημιουργείται ο πληρεξούσιος χρήστης και του δίνουμε το C_{UP}. Επίσης θα πρέπει να προστατεύει το C_{UP} με τους τοπικούς μηχανισμούς ασφαλείας.

Η παραπάνω ιδέα της δημιουργίας του πληρεξούσιου χρήστη δεν είναι μοναδική. Γενικότερα πολλά συστήματα χρησιμοποιούν την ίδια τεχνική που τα μακροπρόθεσμα πιστοποιητικά του χρήστη χρησιμοποιούνται για να δημιουργία κάποιων πιστοποιητικών περιορισμένης διάρκειας. Αυτό που διαφοροποιεί την αρχιτεκτονική του GSI από τις υπόλοιπες είναι η αλληλεπίδραση που επιτρέπεται μεταξύ του πληρεξούσιου χρήστη και του διαχειριστή πόρων.

Το Πρωτόκολλο 2 επιτρέπει στο πληρεξούσιο χρήστη να δεσμεύει πόρους. Η δέσμευση πόρων μπορεί να γίνει είτε από το πληρεξούσιο χρήστη είτε από μια διεργασία. Συνοπτικά ένα πληρεξούσιο χρήστη ζητά πρόσβαση σε ένα πόρο αναζητώντας παράλληλα και την ταυτότητα του διαχειριστή του συγκεκριμένου πόρου. Στην συνέχεια καταθέτει ένα αίτημα στο συγκεκριμένο διαχειριστή. Εάν το αίτημα αυτό ολοκληρωθεί με επιτυχία τότε ο πόρος δεσμεύεται και δημιουργείται μια διεργασία σε αυτό τον πόρο. Η διαδικασία θα ήταν εντελώς παρόμοια εάν ο σκοπός μας ήταν να δεσμεύσουμε ένα πόρό για λογαριασμό μιας διεργασίας, ένα πόρο όπως υπηρεσίες δικτύου ή αποθήκευσης. Για λόγους συντομίας υποθέτουμε ότι η δημιουργία διεργασίας έχει ως άμεσο επακόλουθο την δέσμευση ενός πόρου.

Επίσης πρέπει να αναφερθεί πως η απάντηση στην αίτηση του διαχειριστή πόρων μπορεί να απορριφτεί για διάφορους λόγους. Μπορεί ο πόρος να μην είναι διαθέσιμος, ο χρήστης να μην αναγνωρίζεται, ή ο χρήστης να μην είναι εξουσιοδοτημένος να χρησιμοποιήσει τον πόρο αυτό με τον τρόπο που θέλει. Ο διαχειριστής πόρων μπορεί να ενσωματώσει την τοπική πολιτική ασφαλείας που εφαρμόζεται στον κάθε πόρο. Περιγράφουμε το Πρωτόκολλου 2 την αναλύουμε παρακάτω:

1. Το πληρεξούσιο χρήστη και ο διαχειριστής πόρων κάνουν αμοιβαία ταυτοποίηση ο ένας στον άλλο χρησιμοποιώντας τα C_{UP} και C_{RP} (το πιστοποιητικό του διαχειριστή πόρων) αντίστοιχα. Μέρος της διαδικασίας

αυτής είναι ο έλεγχος της εγκυρότητας των πιστοποιητικών του πληρεξούσιου χρήστη από τον διαχειριστή πόρων κυρίως για την χρονοσφραγίδα που περιέχουν.

2. Μόλις γίνει ο απαραίτητος έλεγχος της ταυτοποίησης το πληρεξούσιο χρήστη παρουσιάζει ένα υπογεγραμμένο αίτημα στον διαχειριστή πόρων.
3. Ο διαχειριστής πόρων ελέγχει εάν ο χρήστης που έχει υπογράψει το πιστοποιητικό του πληρεξούσιο χρήστη είναι εξουσιοδοτημένος από την τοπική πολιτική ασφαλείας να δεσμεύσει τον πόρο.
4. Στην περίπτωση που η έκβαση όλων των παραπάνω είναι θετική ο διαχειριστής πόρων δημιουργεί ένα πιστοποιητικό πόρου (Resource-Credential) που περιέχει το όνομα του χρήστη για τον οποίο δεσμεύτηκε ο πόρος, το όνομα του πόρου και άλλες πληροφορίες.
5. Ο διαχειριστής πόρων με ιδιαίτερη ασφάλεια παραδίνει το πιστοποιητικό χρήστη στο πληρεξούσιο χρήστη.
6. Το πληρεξούσιο χρήστη εξετάζει προσεκτικά το πιστοποιητικό πόρου και εάν αποφασίσει να το εγκρίνει το υπογράφει και δημιουργείται το C_P ένα πιστοποιητικό για τη δέσμευση του πόρου.
7. Ο χρήστης με ασφάλεια δίνει το C_P στο διαχειριστή πόρων.
8. Τέλος ο διαχειριστής πόρων δεσμεύει τον πόρο και τον παραδίδει στην νέα διεργασία και το C_P δίνει την δυνατότητα στην διεργασία να πιστοποιεί τον εαυτό της και την ταυτότητα του χρήστη που τη ζήτησε.

Το πρόβλημα που αντιμετωπίζει το τελευταίο πρωτόκολλο αυτό είναι η δημιουργία μιας σωστής αντιστοίχισης μεταξύ σφαιρικών (global) οντοτήτων και τοπικών οντοτήτων. Στην ουσία καταχωρούμε σε ένα πίνακα που τον διαχειρίζεται ο διαχειριστής πόρων όλες τις αντιστοιχίσεις μεταξύ σφαιρικών και τοπικών οντοτήτων. Τον πίνακα αντιστοίχιση θα μπορούσε να τον διαχειριστεί ο τοπικός διαχειριστής του συστήματος. Αυτή η προσέγγιση προσθέτει κάποιο φορτίο.

Η βασική ιδέα πάνω στην οποία υλοποιείται το Πρωτόκολλο 4 είναι ο χρήστης να αποδείξει ότι κατέχει πιστοποιητικά και για την σφαιρική και για την τοπική οντότητα. Αυτό επιτυγχάνεται κάνοντας πιστοποίηση σφαιρικά και άμεσα στο

διαχειριστή πόρων χρησιμοποιώντας την τοπική μέθοδο πιστοποίησης. Ο χρήστης τότε δημιουργεί την αντιστοίχηση μεταξύ σφαιρικών και τοπικών οντοτήτων. Την αντιστοίχηση αυτή τη δέχεται ο διαχειριστής πόρων οπότε είναι σε θέση να πιστοποιήσει και σφαιρικά και τοπικά πιστοποιητικά.

2.10. Το σύστημα Kerberos

Ο Kerberos[13] θα μπορούσε να χαρακτηριστεί ως ένα μοντέλο που χρησιμοποιείται κυρίως για την ταυτοποίηση των χρηστών. Πρακτικά είναι μια βάση δεδομένων που περιέχει όλες τις οντότητες που απαρτίζουν το σύστημα μας και γνωρίζει το ιδιωτικό κλειδί της κάθε μιας. Θα περιγράψουμε τον τρόπο λειτουργίας του, θα εξηγήσουμε πως καταφέρνει την ταυτοποίηση των χρηστών και τέλος θα αιτιολογήσουμε τα προβλήματα που αντιμετωπίζει ο Kerberos σε ένα περιβάλλον πλέγματος. Το σύμβολο K_{χ} παριστάνει το κλειδί του χρήστη χ. Το σύμβολο $K_{\chi,\psi}$ παριστάνει το κλειδί επικοινωνίας μεταξύ των οντοτήτων χ,ψ. Το $T_{\chi,\psi}$ παριστάνει το «εισιτήριο» μεταξύ των οντοτήτων χ,ψ και περιέχει όλες τις απαραίτητες πληροφορίες για την ασφαλή επικοινωνία των χ,ψ.

(1) Ο χρήστης εισάγει το όνομα του. Στη συνέχεια στέλνεται ένα αίτημα στο διακομιστή πιστοποίησης και επίσης το όνομα μιας ειδικής υπηρεσίας γνωστής ως διακομιστής παροχής εισιτηρίων (Ticket Granting Server-TGS).

(2) Ο διακομιστής πιστοποίησης ελέγχει εάν γνωρίζει τον χρήστη και στην συνέχεια απαντά με το αρχικό εισιτήριο που περιέχει:

- Το κλειδί $K_{c,tgs}$ που θα χρησιμοποιηθεί για την επικοινωνία μεταξύ χρήστη και της υπηρεσίας TGS.
- Ένα εισιτήριο $T_{c,tgs}$ κρυπτογραφημένο με το ιδιωτικό κλειδί του TGS και κατά συνέπεια μόνο ο TGS μπορεί να το «διαβάσει». Το εισιτήριο αυτό πιστοποιεί την ταυτότητα του χρήστη

(3) Με το που το λάβει ο χρήστης του ζητείται να δώσει το κωδικό του. Ο κωδικός μετατρέπεται στο K_c που χρειάζεται για την αποκωδικοποίηση του μηνύματος. Αφού

το αποκωδικοποιήσει στέλνει στο TGS ένα αίτημα το οποίο είναι για ένα εισιτήριο για τον διακοσμητή (που παρέχει την υπηρεσία) που θέλει να συνδεθεί.

(4) Ο TGS απαντά με ένα εισιτήριο κατάλληλα κρυπτογραφημένο που χρησιμοποιεί ο χρήστης για να προσπελάσει τον διακοσμητή που παρέχει την υπηρεσία που μας ενδιαφέρει.

(5)Τέλος ο χρήστης γνωρίζοντας το $K_{c,tgs}$ χρησιμοποιεί το εισιτήριο αυτό για να αποδείξει την ταυτότητα του και το κλειδί που υπάρχει μέσα στο εισιτήριο για την περαιτέρω επικοινωνία ώσπου αυτή να λήξει.

Όπως γνωρίζουμε ένα περιβάλλον πλέγματος αποτελείται από πολλούς οργανισμούς. Το πρόβλημα της διασταύρωσης πιστοποιητικών αναφέρεται στην επέκταση των χρηστών ενός οργανισμού σε ένα άλλον. Η αρχική ιδέα πάνω στην οποία στηρίζεται είναι να μοιραστεί ένα μυστικό κλειδί ανάμεσα σε δύο οργανισμούς. Το κλειδί αυτό θα διανεμηθεί από το TGS.

Το πρόβλημα που μπορεί να προκύψει από την παραπάνω προσέγγιση είναι το εξής. Ένα σύνολο από N οργανισμούς που θα πρέπει να ανταλλάξουν μεταξύ τους ένα σύνολό περίπου ένα σύνολο N^2 διαφορετικών κλειδιών (συγκεκριμένα $\binom{n}{2} = \frac{n!}{2!(n-2)!}$). Μάλιστα τα κλειδιά αυτά θα πρέπει να ανταλλαχθούν διαμέσου ασφαλών διαύλων επικοινωνίας.

Σε αντίθεση, η 5^{η} έκδοση του Kerberos υποστηρίζει την ιεραρχική διανομή των κλειδιών. Οι οργανισμοί κατανέμονται ιεραρχικά και κάθε οργανισμός μοιράζεται κλειδιά με τα θυγατρικά του και με τον γονικό του. Για παράδειγμα θέλουμε ο χρήσης που ανήκει στον οργανισμό K1 να επικοινωνήσει με ένα άλλο οργανισμό K2 και να ζητήσει ένα εισιτήριο για ένα διακοσμητή που διαχειρίζεται ο K2. Πρώτα θα εκτελέσει την πιστοποίηση στο τοπικό οργανισμό στο οποίο ανήκει. Στην συνέχεια θα ακολουθήσει την ιεραρχική δομή του μονοπατιού φτάνοντας στον K2 ζητώντας του ένα εισιτήριο για την υπηρεσία του διακομιστή που θέλει να προσπελάσει.

Η λίστα όλων των οργανισμών τα οποία έχει διασχίσει η αίτηση του χρήστη καταγράφεται στο τελικό εισιτήριο και ο διακοσμητής πιστοποίησης του απομακρυσμένου οργανισμού πραγματοποιεί την τελική απόφαση για το κατά πόσο μπορεί να εμπιστευτεί το μονοπάτι που ακολουθήθηκε. Η επιλογή μικρότερων διαδρομών υποστηρίζεται από το μοντέλο, καθ' ότι μπορούν να βελτιώσουν σημαντικά την απόδοση της διαδικασίας.

2.11. Community Authorization Service

Το πρόβλημα που προσπαθεί να λύσει το Σύστημα Κοινοτικής Εξουσιοδότησης (Community Authorization Service-CAS)[15] είναι η εναρμόνιση των διάφορων πολιτικών πρόσβασης μεταξύ των διαφόρων οργανισμών που συμμετέχουν σε ένα εικονικό οργανισμό (virtual organization). Το CAS μπορεί να χαρακτηριστεί ως μια έμπιστη αντικειμενική αρχή (trusted third party authority) την οποία αποδέχονται όλοι.

Όλες οι πληροφορίες που χρειάζονται για τον διαχειρισμό δικαιωμάτων των πόρων βρίσκονται αποθηκευμένες στην βάση δεδομένων του CAS. Σε μια συνοπτική περιγραφή θα μπορούσαμε να πούμε ότι ο χρήστης κάνει μια αίτηση στον CAS που απαντά παρέχοντας στον χρήστη ένα πιστοποιητικό (capability) που αναγράφεται αναλυτικά σε αυτό τα δικαιώματα που έχει ο χρήστης. Αυτό το πιστοποιητικό ο χρήστης παρουσιάζει στον εκάστοτε διαχειριστή πόρων και ανάλογα πραγματοποιείται ή όχι η επιθυμία του.

Θα πρέπει να αναφέρουμε πως ο CAS ασχολείται κυρίως με το θέμα της εξουσιοδότησης. Στην υλοποίηση του CAS το θέμα της ταυτοποίησης πραγματοποιείται από τον μηχανισμό του GSI (Globus Security Infrastructure) που στηρίζεται στα προσωρινά πιστοποιητικά (proxy credentials) και γενικότερα στην κρυπτογραφία του δημόσιου κλειδιού.

Πιο συγκεκριμένα ο CAS διακομιστής γνωρίζει όλους όσους συμμετέχουν στον οργανισμό. Περιέχει πληροφορίες που καθορίζουν ποιος έχει την άδεια, για ποιό πόρο

είναι η άδεια αυτή και τι άδεια χρήσης δίνουμε. Για παράδειγμα ο χρήστης user1 (ποιος) έχει πρόσβαση στον πόρο (για ποια) /tmp/test.txt να την διαγράψει (τι).

Η παραπάνω δομή προσφέρει μια δραματική μείωση στην δημιουργία των απαραίτητων σχέσεων εμπιστοσύνης (trust relationships) από $C \times P \rightarrow C + P,$ (όπου C είναι ο καταναλωτής και P ο παραγωγός). Ως καταναλωτή ορίζουμε οποιαδήποτε οντότητα που μπορεί να δεσμεύσει κάποιο πόρο. Ως παραγωγό ορίζουμε οποιαδήποτε οντότητα που μπορεί να προσφέρει πόρους. Κάθε καταναλωτής πρέπει να είναι γνωστός και να τον εμπιστεύεται ο CAS διακομιστή και δεν χρειάζεται να ξέρει κάθε παραγωγό. Κάθε παραγωγός πρέπει να είναι γνωστός και να τον εμπιστεύεται ο CAS και δεν χρειάζεται να ξέρει κάθε καταναλωτή. Όπως είναι προφανές σαφώς και μπορεί να προκαλέσει επιβράδυνση αφού ο CAS δουλεύει κάπως κεντρικοποιημένα. Ένας τρόπος με τον οποίο θα μπορούσε να αντιμετωπιστεί αυτό είναι κάποιες μέθοδοι αντιγραφής της βάσης. Για να πραγματοποιηθεί η υλοποίηση του έπρεπε να επεκταθούν τρεις GSI μηχανισμοί:

(1)Περιορισμένα Πιστοποιητικά Εξουσιοδότησης (Restricted Proxy Credentials)
Είναι μια επέκταση των ήδη υπαρχόντων πιστοποιητικών του GSI που καθορίζουν σε κάθε χρήστη τα δικαιώματα που ορίζονται από την πολιτική της εκάστοτε κοινότητας.

(2)Γλώσσα πολιτικής ασφάλειας (Policy Language)
Για την υλοποίηση του CAS υπάρχει μια γλώσσα πολιτικής που αποτελείται από μια λίστα δικαιωμάτων. Κάθε δικαίωμα αποτελείται από μία λίστα από αντικείμενα(object) και μια λίστα ενεργειών(action) πάνω σε αυτά τα αντικείμενα.

(3)Βιβλιοθήκες και Διεπαφές Εφαρμογής Προγραμμάτων (Libraries and APIs)
Η γλώσσα πολιτικής ασφαλείας που υπάρχει διατυπωμένη στα εμπιστευτικά πιστοποιητικά εξουσιοδότησης πρέπει να μπορούν να διερμηνευτούν από τους διαχειριστές πόρων που τα αποδέχονται.

2.12. Σύγκριση όλων των παραπάνω αποτελεσμάτων

Σε αυτό το σημείο θα μπορούσαμε να κάνουμε μια σύγκριση στην προσέγγιση των παραπάνω τεχνικών. Η SVE έχει κάποια κοινά χαρακτηριστικά με το CAS. Και οι δύο επιτρέπουν την διαχείριση των τοπικών πόρων από τους τοπικούς διαχειριστές και να καθορίζουν την πολιτική πρόσβασης που θα έχει ως προς την κοινότητα που θα ανήκουν. Η SVE προσέγγιση επιτρέπει σ'ένα τόπο να παραχωρήσει πόρους σε έναν η περισσότερα SVE, ενώ η CAS επιτρέπει στους παρόχους πόρων να δίνουν πρόσβαση σε περισσότερες από μια κοινότητα.

Πέρα από τις ομοιότητες υπάρχουν και σημαντικές διαφορές. Το SVE μοντέλο επικεντρώνει περισσότερο την προσοχή του στις σχέσεις μεταξύ των διαφόρων οργανισμών, ενώ το CAS μοντέλο εστιάζει στην σχέση μεταξύ χρηστών και κοινοτήτων. Το SVE μοντέλο επιτρέπει την ενσωμάτωση των πόρων εφόσον ανήκουν σε κάποιο τόπο, ενώ στο CAS μοντέλο δεν έχουμε αντίστοιχο περιορισμό. Στο SVE οι πολιτικές για τους πόρους εκτελούνται από τους τοπικούς διαχειριστές. Στο CAS, αφού πρώτα καθοριστούν από τους τοπικούς διαχειριστές, στην συνέχεια υφίστανται διαχείριση από το ίδιο το CAS. Συμπερασματικά συγκρίνοντας τις δύο αυτές προσεγγίσεις το CAS είναι μια πιο πρακτική λύση. Το CRISIS και το Globus είναι παρόμοια συστήματα με την έννοια ότι στοχεύουν στην διαχείριση των κατανεμημένων πόρων και δημιουργία κατανεμημένων υπολογισμών σε ένα ευρύ δίκτυο. Κοινά χαρακτηριστικά των δύο συστημάτων είναι το πρωτόκολλο SSL και τα πιστοποιητικά X.509 που χρησιμοποιούν.

Το CRISIS είναι μια πιο ολοκληρωμένη αρχιτεκτονική ασφαλείας αλλά και πιο δαπανηρή. Αξιοσημείωτο είναι να αναφερθεί πως δεν προσαρμόζεται στους τοπικούς μηχανισμούς ασφαλείας. Ένας από τους πρωτεύοντες στόχους που πρέπει να θέσουμε είναι να παράσχουμε ένα λεπτό στρώμα ομοιογένειας για τους διάφορους τοπικούς μηχανισμούς ασφαλείας.

Επίσης το CRISIS δεν συμπεριφέρεται σε μια διεργασία ως ξεχωριστή οντότητα. Αυτή είναι μια βασική διαφορά με το Globus επειδή επιτρέπει στις διεργασίες να συμπεριφέρονται αυτόνομα, για παράδειγμα να δεσμεύουν κάποιούς πόρους ή να ξεκινήσουν μια άλλη διεργασία εάν χρειαστεί. Αυτό μετατρέπει τη διεργασία σε μια

προσωρινή διαχειριστική αρχή. Τέλος μια ακόμη ουσιαστική διαφορά είναι ότι σε ένα τέτοιο περιβάλλον μια διεργασία πλέγματος πρέπει να την αντιλαμβανόμαστε ως μια δυναμική ομάδα διεργασιών που χρησιμοποιεί διαφορετικούς πόρους σε διαφορετικούς οργανισμούς. Λόγω του σχεδιασμού του το CRISIS είναι περισσότερο μια αρχιτεκτονική για απομακρυσμένη εκτέλεση διεργασιών και όχι για μια τυπική διεργασία πλέγματος.

Συμπερασματικά για να μπορέσουμε να αντιμετωπίσουμε το πρόβλημα της πιστοποίησης σε ένα περιβάλλον πλέγματος θα πρέπει να υιοθετήσουμε μια τεχνική που να συμπεριλαμβάνει όσο το δυνατόν τα θετικά γνωρίσματα των παραπάνω προσεγγίσεων. Το πρώτο που πρέπει να αποσαφηνίσουμε είναι ότι θα χρησιμοποιήσουμε την ήδη υπάρχουσα υλοποιημένη λύση του CAS. Θα προσπαθήσουμε να την τροποποιήσουμε με τέτοιο τρόπο ώστε να γίνει όσο το δυνατόν περισσότερο αποκεντρικοποιημένη. Σε ένα περιβάλλον πλέγματος η αποκέντρωση είναι ένας βασικός παράγοντας που πρέπει να λαμβάνεται υπόψιν.

ΚΕΦΑΛΑΙΟ 3. ΤΟ ΣΥΣΤΗΜΑ ΝΕΦΕΛΗ

3.1. Εισαγωγή

Εξετάζουμε την συχνή ανάγκη ανεξάρτητων οργανισμών να σχηματίζουν ομοσπονδίες και να συνεισφέρουν πόρους αποθήκευσης για αμοιβαίο διαμοιρασμό στους χρήστες τους. Τέτοιες δομές επιτρέπουν την ευέλικτη δημιουργία συνεργασιών και εξυπηρετούν ένα μεγάλο εύρος εφαρμογών στην επιστήμη, τη μηχανική και τις επιχειρήσεις. Οι υπάρχουσες λύσεις δεν είναι ιδιαίτερα επεκτάσιμες σε πρόσβαση δεδομένων εξαιτίας της πολυπλοκότητας που απαιτείται στην ασφαλή εξαγωγή των δεδομένων σε απομακρυσμένους χρήστες. Υποθέτουμε ότι κάθε οργανισμός (site ή realm) έχει μια ανεξάρτητη διοικητική δομή σε συνδυασμό με μια πολιτική ασφαλείας. Ο οργανισμός αυτός συμπεριλαμβάνει χρήστες και ομάδες που δημιουργούνται από αυτούς. Επιπλέον ο κάθε οργανισμός έχει διαχειριστές των πόρων που εξετάζουν τα αιτήματα πρόσβασης στους τοπικούς πόρους που διαθέτουν. Κάθε οργανισμός διαχειρίζεται ένα μηχανισμό ταυτοποίησης που παρέχει πιστοποιητικά τους χρήστες του για να αποδεικνύουν την ταυτότητα τους. Ο μηχανισμός ταυτοποίησης προσδιορίζει μια λίστα από ιδιότητες για ένα συγκεκριμένο χρήστη όπως είναι οι ομάδες που ανήκει. Η πληροφορία αυτή είναι απαραίτητη για τους διαχειριστές των πόρων προκειμένου να αποφασίσουν εάν θα ικανοποιήσουν το αίτημα ή όχι.

Μία απλή προσέγγιση στη λύση του προβλήματος είναι να έχουμε τον διαχειριστή του κάθε οργανισμού να προσθέτει ο ίδιος απομακρυσμένους χρήστες στον τοπικό μηχανισμό ταυτοποίησης. Ακόμα και εάν το τοπικό σύστημα μπορεί να αναγνωρίσει σφαιρικές ταυτότητες αυτή η τεχνική μπορεί να είναι αποτελεσματική σε μικρής κλίμακα σενάρια χωρίς σημαντική επιβάρυνση. Μια παρόμοια τεχνική αντιμετώπισης θα μπορούσε να επιτρέψει στον οργανισμό να κάνει εξαγωγή των ομάδων στον

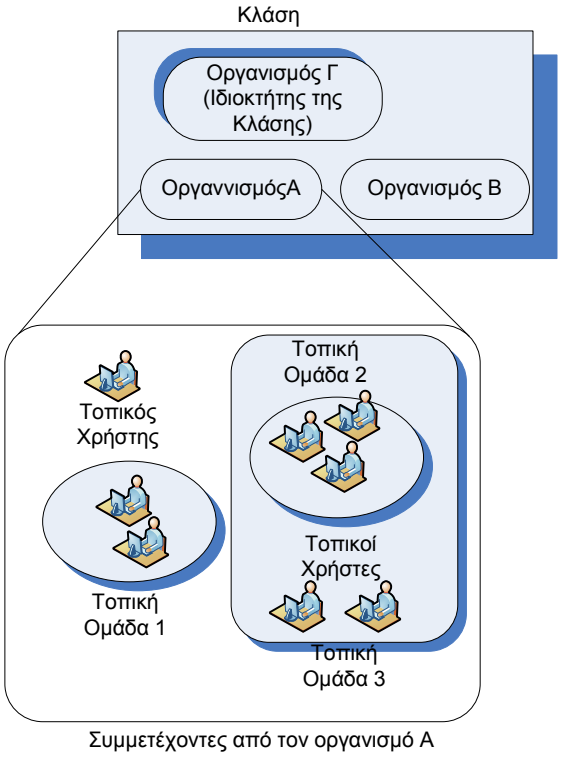
διαχειριστή των πόρων για να μπορέσει να επιτύχει μια απομακρυσμένη πρόσβαση. Για λόγους καλύτερης απόδοσης οι διαχειριστές των πόρων περιοδικά ενημερώνουν την υπηρεσία εξουσιοδότησης με τις ομάδες που περιέχουν τοπικούς και απομακρυσμένους χρήστες. Αυτό έχει ως άμεση συνέπεια μεγαλύτερο φορτίο στο δίκτυο και είναι ευάλωτο σε αποσυνδέσεις.

Ένας άλλος τρόπος για να επιτρέψουμε την απομακρυσμένη πρόσβαση σε διάφορους οργανισμούς είναι η χρήση μονοπατιών πιστοποίησης (delegation path) μέσα από ιεραρχικούς δεσμούς εμπιστοσύνης (hierarchical trust relationship) [2,13]. Αυτά τα μονοπάτια δεν απαιτούν μεγάλο φορτίο για την ταυτοποίηση, αλλά απαιτούν την δημιουργία ιεραρχικών συνδέσεων που εξαρτώνται άμεσα από τους οργανισμούς που την απαρτίζουν. Υπάρχει επίσης και η δυνατότητα δημιουργίας ενός σφαιρικού μηχανισμού πιστοποίησης που περιέχει πλήρη γνώση για τα μέλη του κάθε οργανισμού [15] και τον πόρων στους οποίους μπορούν να έχουν πρόσβαση. Σε αυτή την περίπτωση υπάρχει ένα κόστος ενημέρωσης διατηρώντας τις πληροφορίες αυτές με συνέπεια ως προς τους οργανισμούς που αλλάζουν τους χρήστες τους ή τους πόρους τους ή τις δικαιοδοσίες που παρέχει ο ένας στον άλλον στο πέρασμα του χρόνου. Επιπλέον υπάρχει και ένα σημαντικότερο κόστος. Ο κάθε χρήστης για να μπορέσει να προσπελάσει ένα πόρο πρέπει να επικοινωνήσει με το κεντρικό διακομιστή να πάρει το απαραίτητο πιστοποιητικό και με την σειρά του ο χρήστης να το προωθήσει στον διαχειριστή του πόρου για την ενέργεια που θέλει να κάνει.

Ο κύριος λόγος της αυξήσεως της πολυπλοκότητας των παραπάνω λύσεων προκύπτει από την υποθετική ανάγκη για εξαγωγή όλων των δομών ομάδων των χρηστών από ένα οργανισμό σε ένα άλλο. Έτσι ένας οργανισμός θα μπορέσει να ορίσει τους απομακρυσμένους χρήστες και τις ομάδες που θα αποκτήσουν πρόσβαση στα τοπικά αρχεία. Για να μπορέσουμε να ξεπεράσουμε τον περιορισμό αυτό ορίζουμε την έννοια της *κλάσης* (class) μεταξύ διαφόρων οργανισμών. Μια κλάση είναι μια πολυεπίπεδη ομάδα όπου διακεκριμένοι οργανισμοί συνεισφέρουν τοπικούς χρήστες και ομάδες. Στην περίπτωση μας η κλάση αποτελείται από δύο επίπεδα. Το ανώτερο επίπεδο αναφέρεται σε οργανισμούς και το κατώτερο αποτελείται από χρήστες που συμμετέχουν από κάθε οργανισμό. Γενικά πάντως μια κλάση μπορεί να περιέχει

πολλαπλά επίπεδα ομάδων εξαρτώμενοι από την δομή των συμμετεχόντων οργανισμών.

Το ιδιαίτερο χαρακτηριστικό της κλάσης είναι ότι η πολυεπίπεδη δομή δεν είναι πλήρως ορατή στους οργανισμούς που συμμετέχουν. Όταν ένας οργανισμός δίνει δικαιοδοσίες σε μια κλάση οι αντίστοιχοι διαχειριστές πόρων πρέπει να ξέρουν τους συγκεκριμένους οργανισμούς που ανήκουν στην κλάση. Είναι ευθύνη των οργανισμών να πιστοποιούν τους χρήστες τους και να τους τροφοδοτούν με τα αντίστοιχα πιστοποιητικά για την πρόσβαση στους απομακρυσμένους πόρους. Κατά κύριο λόγο ο κάθε οργανισμός αποφασίζει ποιους τοπικούς χρήστες ή ομάδες θα συμμετέχουν στην κλάση, ενώ κρατάνε έξω από την κλάση την δομή της ιεραρχίας τους (σχήμα 3.1). Για να μπορέσει να επιβεβαιώσει σ'ένα διαχειριστή πόρων κάποιος χρήστης ότι ανήκει σε μια κλάση απαιτεί ελάχιστο κόστος σε σύγκριση με τις εναλλακτικές προσεγγίσεις που περιλαμβάνουν την εγκαθίδρυση ιεραρχικών δομών ή πλήρη γνωστοποίηση των μελών των ομάδων σ'όλη την ομοσπονδία.



Σχήμα 3.1 Κάθε οργανισμός συνεισφέρει στη κλάση ένα αυθαίρετο αριθμό χρηστών και ομάδων. Για την απομακρυσμένη πρόσβαση μεταφέρεται μόνο η συμμετοχή του χρήστη στη κλάση αυτή.

3.2. Αρχιτεκτονική

3.2.1. Ορισμοί

Υποθέτουμε ότι ο κάθε οργανισμός χαρακτηρίζεται από ένα μοναδικό όνομα όπως το όνομα τόπου στο διαδίκτυο (domain name). Κάθε οργανισμός παρέχει ένα μηχανισμό πιστοποίησης που τροφοδοτεί πιστοποιητικά στους χρήστες του για τοπικές ή απομακρυσμένες αιτήσεις. Ένας οργανισμός σχηματίζει μια κλάση με την χρήση ενός μοναδικού ονόματος μαζί με μια λίστα από άλλους οργανισμούς (ονομάζεται ομάδα οργανισμών-sitegroups) που με ασφάλεια συμπεριλαμβάνουν την ονομασία αυτή στα πιστοποιητικά της κλάσης (class certificates). Καλούμε *ιδιοκτήτη* τον οργανισμό που δημιουργεί και διατηρεί την κλάση. Κάθε οργανισμός που είναι μέλος της κλάσης συνεισφέρει τοπικές ομάδες χρηστών.

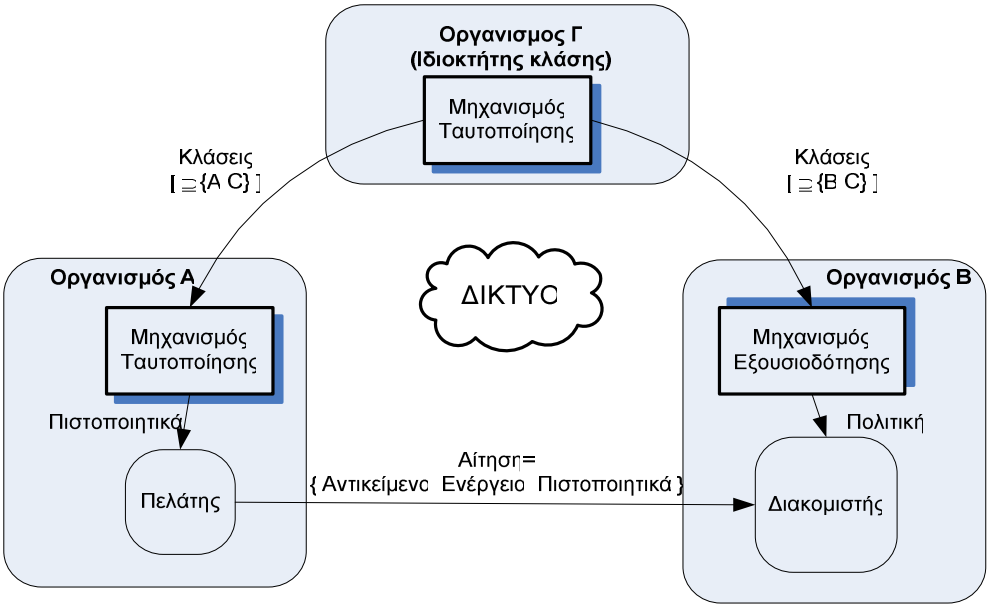
3.2.2. Υποθέσεις

Υποδιαίρεση πρόσβασης. Η υποδιαίρεση της πρόσβασης (Access Granularity) στα δεδομένα επηρεάζει άμεσα το υφιστάμενο κόστος εξουσιοδότησης και πιστοποίησης. Ο παράγοντας αυτός δικαιολογεί τον ξεχωριστό σχεδιασμό που παραδοσιακά ακολουθήθηκε για να υποστηρίζει λήψη αρχείων σε σύγκριση με προσπελάσεις βασισμένες σε μπλόκ. Τυπικά οι λήψεις ολόκληρων αρχείων είναι πιο συνηθισμένες σε ευρείας κλίμακα δίκτυα ενώ οι προσπελάσεις βασισμένες σε μπλοκ περιορίζονται στα όρια ενός κτίριου ή ενός πανεπιστήμιου. Καθώς οι ταχύτητες των δικτύων βελτιώνονται ο παραπάνω διαχωρισμός δεν είναι ευδιάκριτος με τις βασισμένες σε μπλοκ προσβάσεις να απαιτούνται όλο και πιο συχνά σε μεγάλες αποστάσεις. Η πρόκληση είναι να ενεργοποιήσουμε την ασφαλή λειτουργία τους χωρίς να υπονομεύσουμε την γρήγορη απόκριση και την διαχείριση με χαμηλό κόστος.

Κατανομή της πολιτικής. Η πολιτική πρόσβασης καθορίζει τις δικαιοδοσίες διαφορετικών χρηστών σε διαφορετικές προσφερόμενές υπηρεσίες. Προηγούμενες έρευνες έχουν προτείνει την χρήση των πιστοποιητικών ως μέσο για την αποκέντρωση των συστημάτων ασφαλείας και την εγκαθίδρυση τους σε διάφορα τμήματα ενός κατανεμημένου συστήματος [8]. Κατά συνέπεια οι χρήστες μπορούν να αντέξουν το κόστος που απαιτείται για να μεταφέρουν τις πολιτικές από το μέρος που καθορίστηκαν στο μέρος που θα τις επεξεργαστούν και θα τις εφαρμόσουν. Στο μοντέλο μας οι διαχειριστές πόρων είναι υπεύθυνοι και για την πολιτική ασφαλείας και για την εφαρμογή της. Ωστόσο το κόστος της κλάσης προσθέτει ένα επιπλέον επίπεδο για το καθορισμό των οντοτήτων και την διάσπαση της διαδικασίας πιστοποίησης ανάμεσα στον οργανισμό του χρήστη και στον οργανισμό που είναι ο ιδιοκτήτης της κλάσης. Ο στόχος μας είναι να ελαχιστοποιήσουμε το όγκο των δεδομένων που μεταφέρεται στους διάφορους οργανισμούς κατά την διάρκεια αιτημάτων πρόσβασης.

- Διαχείριση: Ο πληθυσμός των χρηστών είναι συνήθως πολύ μεγαλύτερος από τον αριθμό των οργανισμών. Έτσι λοιπόν η πιστοποίηση για τη συμμετοχή ενός οργανισμού σε μια κλάση είναι αμελητέα σε σύγκριση με την συμμετοχή ενός χρήστη σε μια κλάση. Τα αιτήματα πρόσβασης κατευθύνουν τα πιστοποιητικά από τον οργανισμό που ανήκει ο χρήστης στον διαχειριστή

πόρων, ενώ ο διαχειριστής πόρων εξάγει την πληροφορία της κλάσης από τον οργανισμό στον οποίο ανήκει ο χρήστης. Πρακτικά η πιστοποίηση γίνεται κατά κύριο λόγο στον οργανισμό του χρήστη, ενώ η εξουσιοδότηση παραμένει κύρια ευθύνη του διαχειριστή των πόρων (σχήμα 3.2). Η ικανότητα να μεταφέρουμε δικαιώματα από μια αρχή σε μια άλλη είναι ζωτικής σημασίας για την εύκολη δημιουργία μιας κλάσης με ένα αυθαίρετο αριθμό απομακρυσμένων χρηστών κάνοντας διαθέσιμους κάποιους πόρους, όπως δεδομένα αρχείων, με απομακρυσμένες υπηρεσίες. Στο μοντέλο μας περιορίσαμε το κόστος διαχείρισης που απαιτείται για την μεταφορά δικαιωμάτων πρόσβασης σε απομακρυσμένες οντότητες, αλλά δεν το εξαλείψαμε εντελώς. Ο διαχειριστής ενός οργανισμού πρέπει να αποδείξει την συμμετοχή του οργανισμού του σε μια κλάση πριν οι χρήστες του από τον οργανισμό αυτό απαιτήσουν την πρόσβαση σε απομακρυσμένους πόρους που συνεισφέρουν στην κλάση αυτή. Η εναλλακτική προσέγγιση του προβλήματος δίνοντας άμεσα δικαιοδοσία στους απομακρυσμένους χρήστες στο σύστημα προσθέτει προσαρμοστικότητα στο σύστημα με κόστος όμως τον περιορισμό της επεκτασιμότητας.



Σχήμα 3.2 Η αρχιτεκτονική του συστήματος «Νεφέλη» διαχωρίζει τον μηχανισμό ταυτοποίησης από τον μηχανισμό εξουσιοδότησης. Η συμμετοχή του χρήστη στην κλάση είναι η μόνη πληροφορία που χρειάζεται για να επιτραπεί η απομακρυσμένη πρόσβαση

3.2.3. Σχεδιαστικά Θέματα

Μια κλάση καθιερώνει ένα ευρύτερο πλαίσιο για διαμοιρασμό πόρων μεταξύ ανεξάρτητων οργανισμών. Ως αφηρημένη ιδέα συσχετίζει την ομοσπονδία και τις ομάδες της με τις κοινές απαιτήσεις για πόρους.

- Πιστοποίηση: Κάθε οργανισμός χρησιμοποιεί ένα μακροπρόθεσμο πιστοποιητικό υπογεγραμμένο από μια αρχή πιστοποίησης για τη διαχείριση των πιστοποιητικών που παραδίδει στους χρήστες. Η γνησιότητα του πιστοποιητικού αυτού επικυρώνεται μια φορά και έχει ισχύ για ένα μεγάλο χρονικό διάστημα (συνήθως η προεπιλογή είναι πέντε χρόνια). Ο χρήστης έχει ένα παρόμοιο μακροπρόθεσμο πιστοποιητικό. Και οι δύο οντότητες χρησιμοποιούν τα πιστοποιητικά αυτά για να μπορέσουν να παράγουν βραχυπρόθεσμα πιστοποιητικά που θα χρησιμοποιηθούν για να γίνει αμοιβαία αναγνώριση.

Έτσι ο χρήστης πιστοποιεί την ταυτότητα του με τον τοπικό μηχανισμό ασφαλείας παρουσιάζοντας το βραχυπρόθεσμο πιστοποιητικό που έχει δημιουργήσει. Στην συνέχεια δημιουργώντας μια αίτηση με το βραχυπρόθεσμο πιστοποιητικό παραλαμβάνει ένα εκτεταμένο πιστοποιητικό υπογεγραμμένο από το μυστικό κλειδί της υπηρεσίας που συσχετίζει τον χρήστη με τις κλάσεις που ανήκει. Το πιστοποιητικό αυτό είναι έγκυρο για ένα συγκεκριμένο χρονικό διάστημα που περιορίζει την έκθεση του συστήματος σε μια αναπάντεχη υπονόμευση της ασφάλειας. Το εκτεταμένο πιστοποιητικό περιέχει την ταυτότητα του οργανισμού που ανήκει ο χρήστης και «υπογράφει» μια λίστα από τις κλάσεις που ο χρήστης ανήκει. Για τοπική ή απομακρυσμένη πρόσβαση ο χρήστης χρησιμοποιεί το εκτεταμένο πιστοποιητικό στον διαχειριστή πόρων.

Ως μια βελτιστοποίηση για να μειωθεί το κόστος της πληροφορίας της πιστοποίησης που μεταδίδεται στο δίκτυο, τα αιτήματα πρόσβασης περιέχουν μόνο τις κλάσεις που περιέχονται τόσο στον τοπικό όσο και στον απομακρυσμένο οργανισμό. Έτσι μειώνουμε επιπλέον το κόστος επεξεργασίας για την εξουσιοδότηση στον απομακρυσμένο οργανισμό. Υποθέτουμε ότι τα ονόματα των απομακρυσμένων υπηρεσιών διανέμονται στους χρήστες μέσα από ένα κατάλογο τόπων (Domain Registry)

- Εξουσιοδότηση: Οι διαχειριστές πόρων σε κάθε οργανισμό διατηρούν λίστες ελέγχου πρόσβασης για να καθορίσουν τις δικαιοδοσίες που δίνονται σε διαφορετικές κλάσεις. Οι λίστες ελέγχου πρόσβασης χρησιμοποιούνται συχνά σε συστήματα αρχείων επειδή παρέχουν ευελιξία σε αιτήματα πρόσβασης και λογαριασμούς χρηστών για τα αιτήματα τους σε σύγκριση με εναλλακτικές επιλογές, όπως τα πιστοποιητικά[12]. Έτσι λοιπόν όταν φτάνει ένα απομακρυσμένο αίτημα οι διαχειριστές πόρων συγκρίνουν τα πιστοποιητικά που έλαβαν με τη λίστα ελέγχου πρόσβασης για το ζητούμενο αρχείο. Το αίτημα ικανοποιείται εάν μια τουλάχιστον από τις κλάσεις στην οποία ανήκει ο χρήστης υπάρχει στην άδεια πρόσβασης.

- Ανάκληση: Στο μοντέλο μας η ανάκληση των δικαιωμάτων ενός χρήστη επιβάλλεται από τη λήξη των αντίστοιχων πιστοποιητικών και την ανάγκη για ανανέωση από τον τοπικό μηχανισμό πιστοποίησης. Παρόμοια, η συμμετοχή ενός μέλους μιας ομοσπονδίας θα μπορούσε περιοδικά να λήγει και απαιτεί νέα πιστοποίηση από τον ιδιοκτήτη. Μέχρι στιγμής μια τέτοια υπηρεσία δεν υποστηρίζεται από εμάς αλλά είναι στα άμεσα σχέδια μας η υλοποίηση της υπηρεσίας αυτής. Έτσι μπορούμε εν δυνάμει να διαχειριστούμε τις τροποποιήσεις στη λίστα των οργανισμών που συμμετέχουν σε κάθε κλάση. Επιπλέον η αρχιτεκτονική μας θα μπορούσε να επιτρέψει διαχειριστές πόρων να λαμβάνουν λίστες ανάκλησης από απομακρυσμένους διακομιστές πιστοποίησης με σκοπό να επιτρέψουν ανάκληση της άδειας σε ένα ολόκληρο οργανισμό που συμμετέχει στην κλάση και έχει πλέον αποφασίσει να αποσύρει τους πόρους του. Μια τέτοια λύση παρέχει άμεση εκτέλεση της πολιτικής στους διαχειριστές πόρων αλλά προσθέτει μια περισσότερο πολύπλοκη δομή στην ασφάλεια.

- Εκπροσώπηση: Το δικαίωμα του χρήστη για πρόσβαση σε ένα απομακρυσμένο πόρο επιτρέπεται όπως αποδείξαμε με την προσκόμιση του εκτεταμένου πιστοποιητικού. Επίσης εξαρτάται από την τοπική πολιτική κατά πόσον ο οργανισμός μπορεί να υποστηρίξει τις δικαιοδοσίες που αναφέρονται στο εκτεταμένο πιστοποιητικό. Στη συνηθισμένη περίπτωση οι ομοσπονδίες

δημιουργούνται για να εξυπηρετήσουν συγκεκριμένους σκοπούς της κλάσης που με ακρίβεια καθορίζουν ποιος θα συμμετέχει από κάθε οργανισμό, τον πραγματικό ρόλο του στην κλάση και το πλήθος των πόρων που θα συνεισφέρουν. Συνεπώς ο προσδιορισμός χρηστών στις κλάσεις γίνεται από διαχειριστές του κάθε οργανισμού που γνωρίζουν επαρκώς τις απαιτήσεις των κλάσεων που δημιουργούνε και μπορούν να διαχειριστούν το πλήθος και τις δικαιοδοσίες των χρηστών.

- Λογοδότηση: Οι χρήστες είναι υπόλογοι για τα αιτήματα που κάνουν και τους πόρους που πραγματικά χρησιμοποιούν από τους διάφορους οργανισμούς. Αυτό υλοποιείται με την ενσωμάτωση που περιέχεται στα εκτεταμένα πιστοποιητικά που μεταφέρονται σε κάθε αίτημα και κρυπτογραφικά πιστοποιούνται με ένα αδιαμφισβήτητο τρόπο από τον οργανισμό στον οποίο ανήκει ο χρήστης. Έτσι μπορούμε να παρακολουθήσουμε την ανάλωση των πόρων σε κάθε απομακρυσμένο οργανισμό και να εντοπίσουμε ίχνη κακόβουλης συμπεριφοράς που προκύπτουν στο σύστημα από τον οργανισμό που ανήκει ο χρήστης που τα προκάλεσε. Σε μια τέτοια περίπτωση μπορούμε να απαγορεύσουμε την πρόσβαση όλου του οργανισμού στους πόρους που διαχειριζόμαστε.

3.2.4. Επικεφαλαίωση

Σε αυτή την φάση της εργασίας μπορούμε να περιγράψουμε τα πλεονεκτήματα της προσέγγισης μας για τη λύση του προβλήματος:

- Αποκέντρωση. Δεν υπάρχει ανάγκη να δημιουργηθεί μια κεντρική διαχειριστική αρχή που να γνωρίζει όλους τους χρήστες και όλες τους προσβάσιμους πόρους. Οι ιδιοκτήτες και οι συμμετέχοντες της κλάσης είναι κατανεμημένοι σε διάφορους οργανισμούς με τον ίδιο τρόπο που είναι και οι χρήστες.
- Ανανέωση. Οι αλλαγές στον πληθυσμό ενός οργανισμού μπορούν να αντικατοπτριστούν από τα αιτήματα των χρηστών. Τα αιτήματα αυτά εξαρτώνται από τη συχνότητα της ανάγκης που εμφανίζεται στον χρήστη για να ανανεώσει τα πιστοποιητικά του από τον οργανισμό του.

- Κόστος Υπηρεσίας. Για να εκπληρωθεί ένα αίτημα χρειάζεται το πιστοποιητικό που περιέχει την συμμετοχή του χρήστη στην κλάση. Την πληροφορία αυτή περιέχουν τόσο ο τοπικός όσο και ο απομακρυσμένος διακομιστής αντίστοιχα.
- Κόστος Ενημέρωσης. Έχουμε μειώσει το κόστος ενημέρωση γιατί κρατάμε σε κάθε οργανισμό την συμμετοχή του σε κλάσεις. Επιπλέον μπορούμε να διαχειριστούμε τις αποσυνδέσεις του δικτύου και να αποφύγουμε την πολυπλοκότερη κατανομή πολιτικών ασφάλειας.

3.3. Υλοποίηση πρωτότυπου

Ο σχεδιασμός του συστήματος που προτείνουμε αναφέρεται κυρίως σε περιβάλλοντα κοινοχρησίας συστημάτων αποθήκευσης δεδομένων. Θεωρούμε ότι ένας οργανισμός ορίζει μια *ομάδα οργανισμών* (sitegroup) προκειμένου να σχηματίσει έναν εικονικό οργανισμό. Ένας χρήστης που είναι μέλος ενός τέτοιου οργανισμού θα πρέπει να μπορεί να προσπελάσει τους πόρους ενός άλλου οργανισμού της ίδιας ομάδας εφόσον παρέχει τη δυνατότητα αυτή ο απομακρυσμένος οργανισμός. Στα πλαίσια ενός εικονικού οργανισμού επιτρέπουμε τη δημιουργία *ομάδων χρηστών* (user group) στις οποίες ένας οργανισμός επιλεκτικά μπορεί να προσφέρει δυνατότητες πρόσβασης για διάφορους πόρους του. Όπως περιγράψαμε ήδη, οι υπάρχουσες αρχιτεκτονικές απομακρυσμένης προσπέλασης εναλλακτικά (α) συγκεντρώνουν σε μια κεντρική βάση δεδομένων τις πληροφορίες περιγραφής των χρηστών, των πόρων και των πολιτικών προσπέλασης, (β) περιοδικά μεταφέρουν τις πληροφορίες των χρηστών στους διαχειριστές πόρων, ή (γ) περιοδικά ανταλλάσσουν τις πολιτικές απομακρυσμένης προσπέλασης μεταξύ των διαφορετικών διαχειριστών πόρων.

Η υλοποίηση που πραγματοποιήσαμε επιτεύχθηκε με κατάλληλη τροποποίηση του λογισμικού ανοιχτού κώδικα του συστήματος CAS. Η βασική επέκταση που κάναμε ήταν να εισαγάγουμε στο πιστοποιητικό που λαμβάνει ο χρήστης από το CAS τις κλάσεις οργανισμών που ανήκει ο τοπικός οργανισμός καθώς και τις αντίστοιχες ομάδες των κλάσεων στις οποίες ανήκει ο χρήστης. Η πληροφορία αυτή μεταφέρεται στο διακομιστή που διαχειρίζεται τον εκάστοτε πόρο, όπως είναι τα αρχεία δεδομένων στην περίπτωσή μας. Ο διακομιστής επεξεργάζεται το αίτημα ανακτώντας

από την τοπική βάση τη λίστα ελέγχου πρόσβασης του αιτούμενου πόρου και προσδιορίζει αν επιτρέπεται ή όχι η πρόσβαση για το συγκεκριμένο χρήστη με βάση τις κλάσεις στις οποίες ανήκει ο τελευταίος.

Χρησιμοποιήσαμε την υπηρεσία GridFTP ως μια υπηρεσία αρχείων για να αποδείξουμε την επεκτασιμότητα της προσέγγισης μας, παρ'ολο που ένας πειραματισμός με συστήματα αρχείων βασισμένα σε μπλόκ είναι μέρος των μελλοντικών μας σχεδίων. Παρακάτω περιγράφουμε τις απαραίτητες τροποποιήσεις που εφαρμόσαμε στο CAS και στον GridFTP για να ενσωματώσουμε την αρχιτεκτονική του Νεφέλη στην δικιά τους.

3.3.1. Ο CAS και ο GridFTP

Η *ανοιχτή αρχιτεκτονική ασφάλειας πλέγματος* (Open Grid Security Architecture – OGSA) είναι μια πρότυπη αρχιτεκτονική για ασφαλή ανάπτυξη υπηρεσιών πλέγματος που καθιερώθηκε από το Global Grid Forum. Στα πλαίσια του OGSA ορίζεται μια διεπαφή που επιτρέπει την δρομολόγηση και εκτέλεση εφαρμογών σε απομακρυσμένα υπολογιστικά συστήματα. Αντίστοιχα, το *πλαίσιο πόρων υπηρεσιών ιστού* (Web Services Resource Framework – WSRF) προσδιορίζει τον τρόπο με τον οποίο μπορούμε να δημιουργήσουμε υπηρεσίες στον παγκόσμιο ιστό. Το Globus Toolkit 4 (GT4)[5,6] αποτελείται από πέντε κατηγορίες υποσυστημάτων:

- Ασφάλεια
- Εύρεση, μεταφορά και πρόσβαση δεδομένων
- Δρομολόγηση και εκτέλεση εργασιών
- Παρακολούθηση και εύρεση πόρων
- Εργαλεία ανάπτυξης λογισμικού

Επίσης μπορούσαμε να χωρίσουμε τις υπηρεσίες σε δύο μεγάλες κατηγορίες με βάση το άν είναι ή όχι υπηρεσίες διαδικτύων.

3.4. Ο αρχικός CAS και GridFTP

Το πρότυπο του CAS διακομιστή αποτελείται από μια υπηρεσία διαδικτύου δημιουργημένη σε μια περιγραφή WSDL (Web Service Definition Language) που είναι προσβάσιμη μέσω μηνυμάτων που δημιουργούνται από *πρωτόκολλο απλών αντικειμένων πρόσβασης* (Simply Object Access Protocol-SOAP), μια σχεσιακή βάση δεδομένων που απαντά σε SQL ερωτήματα (PostgreSQL) και κάποιο κώδικα διεπαφής που συνδέει τα παραπάνω[5,15]. Τα SOAP μηνύματα χρησιμοποιούνται από υπηρεσίες διαδικτύου για την επικοινωνία πελάτη διακομιστή. Η σχεσιακή βάση δεδομένων, διαχειρίζεται κεντρικοποιημένα ένα σύνολο από πίνακες που περιέχουν πληροφορίες σχετικά με τους χρήστες τους πόρους, τις ενέργειες και τις εφαρμόσιμες πολιτικές. Η αρχιτεκτονική του CAS διοργανώνει τους χρήστες σε ομάδες και καθορίζει την συγκεκριμένη αρχή πιστοποίησης που παρέχει μακροπρόθεσμα πιστοποιητικά στον χρήστη. Επιπλέον, μπορεί να ομαδοποιήσει τις ενδεχόμενες ενέργειες που μπορούμε να εφαρμόσουμε. Κάθε προσβάσιμος πόρος είναι στην ουσία ένα αντικείμενο. Τα αντικείμενα μπορούν επίσης να ομαδοποιηθούν και να συσχετιστούν με κάποιο ονοματοχώρο (namespace). Οι ορισμοί πολιτικής συσχετίζουν ομάδες χρηστών με αντικείμενα και τις επιτρεπόμενες ενέργειες που μπορούν να εφαρμοστούν στα αντικείμενα αυτά.

Ο GridFTP αποτελείται από ένα πρωτόκολλο μεταφοράς δεδομένων και μια συλλογή από εργαλεία πελάτη-διακομιστή που επιτρέπουν γρήγορες μεταφορές αρχείων σε δίκτυα[6]. Το πρωτόκολλο έχει σχεδιαστεί έτσι ώστε να παρέχει αποτελεσματικά και αξιόπιστα με ένα τρόπο που να είναι συμβατός με τους υπάρχοντες μηχανισμούς ασφαλείας. Προσθέτει ευελιξία σε σχέση με παραδοσιακές μεθόδους αντιγραφής, αφού δημιουργεί παράλληλες μεταφορές σε πολλαπλές ροές δεδομένων. Η υλοποίηση του CAS επιτρέπει στον πελάτη να κάνει χρήση ενός βραχυπρόθεσμου πιστοποιητικού που έχει υπογράψει με τα μακροπρόθεσμα πιστοποιητικά που έχει πάρει από μια έμπιστη αρχή πιστοποίησης με σκοπό να ζητήσει από τον CAS ένα νέο εκτεταμένο πιστοποιητικό που περιέχει τα δικαιώματα πρόσβασης στους πόρους. Μετέπειτα ο πελάτης προωθεί το εκτεταμένο πιστοποιητικό στον απομακρυσμένο GridFTP διακομιστή. Ο διακομιστής χρησιμοποιεί το πιστοποιητικό για να μπορέσει να αποφανθεί ότι ο χρήστης μπορεί να εφαρμόσει τις ενσωματωμένες πολιτικές πρόσβασης που υπάρχουν στο πιστοποιητικό και επιτρέπουν την κατάλληλη ενέργεια.

Αξιοσημείωτο είναι να αναφερθεί πως το εκτεταμένο πιστοποιητικό στην αρχιτεκτονική αυτή περιέχει τους πόρους και τα δικαιώματα σε αυτούς που έχει ο εκάστοτε χρήστης που ζητάει το πιστοποιητικό αυτό.

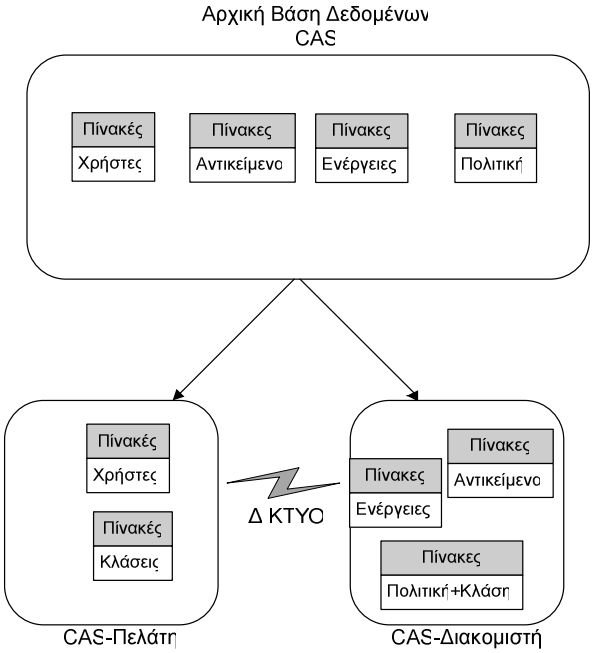
3.5. Το Πρωτότυπο Νεφέλη

Στην προσέγγιση που ακολουθούμε, θέτουμε ως βασικό στόχο να μειώσουμε στο ελάχιστο απαραίτητο το φορτίο ενημέρωσης μεταξύ των διαφορετικών οργανισμών. Για το σκοπό αυτό κρατούμε σε κάθε οργανισμό τις πληροφορίες που προσδιορίζουν τις κλάσεις, στις οποίες ανήκει ο κάθε τοπικός χρήστης. Αντίστοιχα, περιορίζουμε σε κάθε διαχειριστή πόρων την πληροφορία ελέγχου προσπέλασης των κλάσεων της κάθε ομάδας οργανισμών στους οποίους ανήκει ο διαχειριστής πόρων. Η βασική ακολουθία βημάτων για την απομακρυσμένη προσπέλαση ενός πόρου από ένα χρήστη περιλαμβάνει τη λήψη ενός πιστοποιητικού από τον τοπικό διαχειριστή που προσδιορίζει τις κλάσεις χρηστών στις οποίες ανήκει ο συγκεκριμένος χρήστης. Η αίτηση απομακρυσμένης προσπέλασης του χρήστη με τη βοήθεια του πιστοποιητικού μεταφέρει στον απομακρυσμένο διακομιστή αρχείων την πληροφορία για τον απαραίτητο έλεγχο προσπέλασης. Ο διακομιστής αρχείων συγκρίνει τις κλάσεις του χρήστη με αυτές στις οποίες παρέχεται η αιτούμενη πρόσβαση και είτε αποδέχεται το αίτημα και επιστρέφει τα δεδομένα ή το απορρίπτει.

Ο κύριος σκοπός του αρχικού συστήματος ήταν να ελέγχει κεντρικοποιημένα τις πολιτικές προσβάσεις για κάθε χρήστη σε ένα ομοσπονδιακό περιβάλλον ενώ το Νεφέλη επιτρέπει σε κάθε συμμετέχοντα οργανισμό να καθορίζει τις δικές του πολιτικές πρόσβασης στο σύνολο όλης της κλάσης. Για να μπορέσουμε να συγκρίνουμε τις δύο εναλλακτικές αρχιτεκτονικές διαχωρίσαμε την βάση του CAS σε δύο διαφορετικά σύνολα πινάκων, τον CAS-Πελάτη και τον CAS-Διακομιστή. Ο CAS-Πελάτη βρίσκεται στον οργανισμό που ανήκει ο χρήστης και περιέχει τους πίνακες εκείνους που συσχετίζουν τους χρήστες με τις κλάσεις και τις αρχές πιστοποίησης. Έτσι λοιπόν ο CAS-Πελάτη παίζει τον ρόλο μιας υπηρεσίας ταυτοποίησης για απομακρυσμένα αιτήματα πρόσβασης. Εκμεταλλευτήκαμε το πρότυπο X.509 με σκοπό να πιστοποιήσουμε την συμμετοχή του χρήστη σε διάφορους οργανισμούς. Συμπερασματικά οι διαχειριστές πόρων επιτρέπουν άμεσα

την πρόσβαση στους απομακρυσμένους χρήστες εξετάζοντας την πληροφορία που αφορά τις κλάσεις που ανήκει ο χρήστης. Μια παρόμοια τεχνική ακολουθήθηκε από το κατανεμημένο σύστημα αρχείων NFSv4 που χρησιμοποιεί συγκεκριμένες ονοματολογικές συμβολοσειρές για να κάνει μοναδική σφαιρική αναγνώριση της ταυτότητας κάθε χρήστη και άμεσα να καθορίσει τις προσβάσεις στα εξαγόμενα αρχεία σε μεγάλα δίκτυα[14].

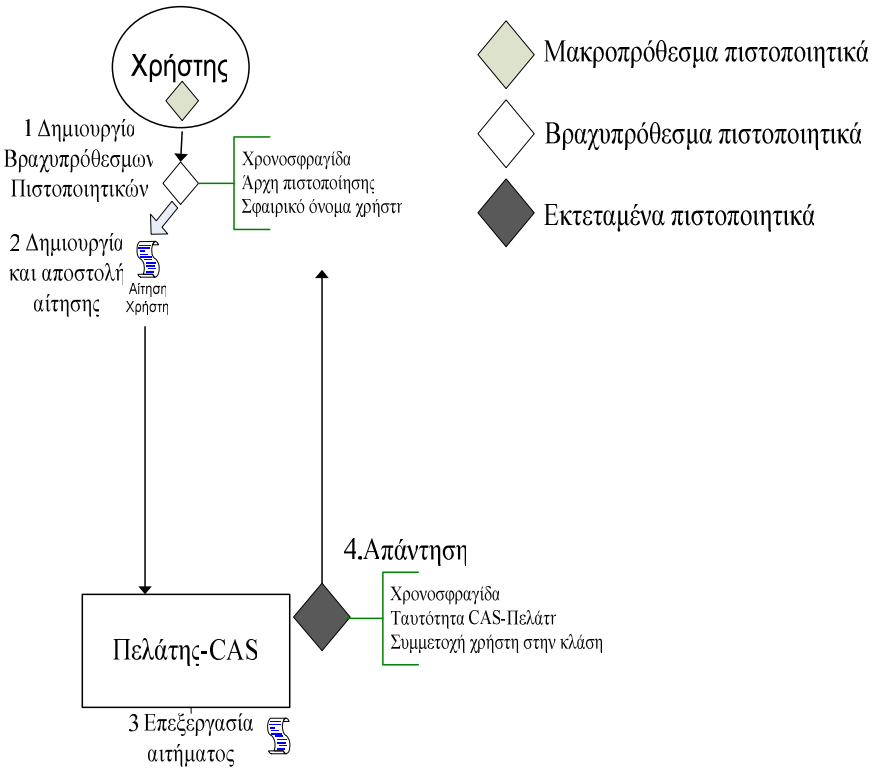
Έχουμε επεκτείνει το σχήμα CAS-Πελάτη με πίνακες που καθορίζουν ιδιόκτητες κλάσεων και συσχετίζουν χρήστες με τοπικές και απομακρυσμένες κλάσεις. Υποθέτουμε ότι οι χρήστες έχουν ένα μοναδικό σφαιρικό όνομα που μπορεί να πιστοποιηθεί από τον τοπικό μηχανισμό πιστοποίησης. Ο CAS-Διακομιστή διαχειρίζεται τους πόρους, τις ενέργειες που επιτρέπονται στους πόρους, και την πολιτική πρόσβασης. Έχουμε κρατήσει το μεγαλύτερο μέρος των πινάκων από τον αρχικό σχεδιασμό, αλλά έχουμε επεκτείνει τον πίνακα των πολιτικών να συμπεριλαμβάνει κλάσεις εν αντιθέσει με χρήστες και ομάδες χρηστών που είχε ο αρχικός (σχήμα 3.3). Με αυτό τον τρόπο έχουμε μεταφέρει εξ’ολοκλήρου την εφαρμογή της πολιτική πρόσβασης από τον κεντρικοποιημένο CAS στους διαχειριστές πόρων και πλέον εδρεύει σε κάθε οργανισμό. Η υπηρεσία του GridFTP μπορεί να υποστηρίξει μια σειρά ενεργειών στα δεδομένα αρχεία ή καταλόγους όπως ανάγνωση (read), εγγραφή (write), εύρεση (lookup), δημιουργία (creation), διαγραφή (delete) και αλλαγή προκαθορισμένου καταλόγου (chdir, εφαρμογή μόνο σε κατάλογο).



Σχήμα 3.3 Η διάσπαση της αρχικής βάσης δεδομένων στον CAS-Πελάτη και CAS-Διακομιστή. Ο χρήστης λαμβάνει από τον CAS-Πελάτη το πιστοποιητικό με τις κλάσεις που ανήκει και το προσκομίζει τον CAS-Διακομιστή για να του επιτρέψει την προσπέλαση.

Αρχικά ο χρήστης λαμβάνει τα μακροπρόθεσμα πιστοποιητικά του από μια αρχή πιστοποίησης και δημιουργεί τα βραχυπρόθεσμα πιστοποιητικά. Την αρχή πιστοποίησης πρέπει να την γνωρίζει ο CAS-Πελάτη για να μπορέσει να εξακριβώσει την ταυτότητα του χρήστη. Αρχικά ο χρήστης με την εισαγωγή κάποιου κωδικού παράγει τα βραχυπρόθεσμα πιστοποιητικά του (Βήμα 1, σχήμα 3.4). Τα βραχυπρόθεσμα πιστοποιητικά περιέχουν την σφαιρική ταυτότητα του χρήστη, το σφαιρικό όνομα της Αρχής Πιστοποίησης που τα έχει προμηθευτεί και μια χρονοσφραγίδα διάρκειας συνήθως δώδεκα ωρών. Στην συνέχεια με τα βραχυπρόθεσμα πιστοποιητικά που έχει δημιουργήσει ο χρήστης δημιουργεί και υποβάλει αίτηση στον CAS-Πελάτη για να αποκτήσει το εκτεταμένο πιστοποιητικό που θα του επιτρέψει να κάνει την απομακρυσμένη πρόσβαση (Βήμα 2). Ο CAS-Πελάτη ανατρέχει στην βάση του και κάνει ερώτηση κατά πόσο γνωρίζει τον συγκεκριμένο χρήστη και την αρχή που του έδωσε τα μακροπρόθεσμα πιστοποιητικά. Στην περίπτωση που τον γνωρίζει ξεκινά την διαδικασία να βρει σε ποιες κλάσεις ανήκει ο χρήστης αυτός (Βήμα 3). Μόλις τις εντοπίσει δημιουργεί ένα νέο

εκτεταμένο πιστοποιητικό βασισμένο στην γλώσσα SAML (System assertion Markup Language)[16] που εμπεριέχει όλες τις κλάσεις που ανήκει ο χρήστης καθώς και την ταυτότητα του οργανισμού που ανήκει ο χρήστης (βήμα 4). Η SAML είναι παράγωγο βασισμένο στην XML(Extensible Markup Language) που είναι μια γλώσσα, ένας μηχανισμός που καθορίζει δομές σε ένα κείμενο, και έχει σχεδιαστεί για την ανταλλαγή πληροφοριών ταυτοποίησης και εξουσιοδότησης μεταξύ διαφορετικών μηχανισμών ασφαλείας. Συγκριτικά η αυθεντική έκδοση του CAS περιέχει και αυτή εκτεταμένα πιστοποιητικά με δικαιώματα πρόσβασης για κάθε αρχείο-φάκελο που διαχειρίζεται ο GridFTP ενώ εδώ το εκτεταμένο πιστοποιητικό περιέχει κλάσεις.

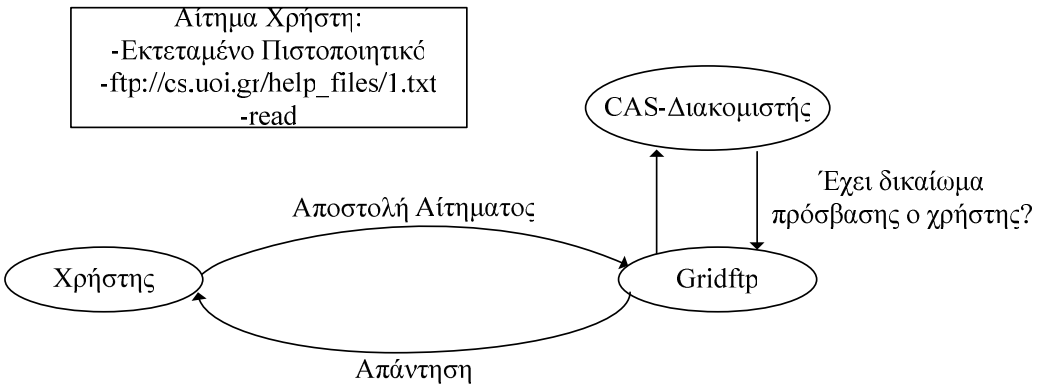


Σχήμα 3.4 Επικοινωνία χρήστη και CAS-Πελάτη

Εδώ θα πρέπει να τονίσουμε μια σημαντική διαφορά. Το εκτεταμένο πιστοποιητικό της δικιάς μας αρχιτεκτονικής περιέχει τις κλάσεις που ανήκει ο χρήστης μια πληροφορία ίδια για όλα τα μέλη της ομοσπονδίας. Έτσι λοιπόν στην περίπτωση που θέλουμε να προσπελάσουμε ένα άλλο αρχείο ενός διαφορετικού διαχειριστή αρχείων που ανήκει στην κλάση αυτή δεν χρειάζεται να επαναλάβουμε την ίδια διαδικασία

παραλαβής εκτεταμένου πιστοποιητικού που είναι και πολυδάπανη. Στην αρχική αρχιτεκτονική έχουμε δύο εναλλακτικές λύσεις για να αντιμετωπίσουμε το πρόβλημα αυτό. Η πρώτη είναι να ζητήσουμε από τον CAS ή να ενσωματώσει περισσότερη πληροφορία σχετικά τους πόρους που θέλουμε να προσπελάσουμε, πράγμα που επιβαρύνει το κόστος της απάντησης ή ζητάμε ένα δεύτερο πιστοποιητικό που θα περιέχει τα δικαιώματα των πόρων που διαχειρίζεται ένας άλλος διακομιστής αρχείων. Σε κάθε περίπτωση υπάρχει ένα μεγάλο κόστος που είναι προφανές στα πειραματικά αποτελέσματα.

Στην συνέχεια ο χρήστης προωθεί το εκτεταμένο πιστοποιητικό στον GridFTP που διαχειρίζεται το αρχείο που θέλει να προσπελάσει. Ωστόσο επειδή εξωτερικά το πιστοποιητικό είναι το ίδιο δεν χρειάστηκε καμία αλλαγή στον πελάτη που χρησιμοποιούμε για να κάνουμε μια απομακρυσμένη αίτηση στον GridFTP. Ο GridFTP λαμβάνει το πιστοποιητικό του χρήστη, το όνομα του αρχείου που θέλει να προσπελάσει και τι είδους ενέργεια θέλει να κάνει. Με τη σειρά του ο GridFTP θέτει ερώτημα στον CAS-Διακομιστή για την απομακρυσμένη πρόσβαση. Εάν επιτρέπεται η ενέργεια αυτή για τις κλάσεις που ανήκει ο χρήστης δίνεται η πρόσβαση αλλιώς απορρίπτεται. Το παρακάτω σχήμα (σχήμα 3.5) αντικατροπτίζει την διαδικασία της απομακρυσμένης πρόσβασης.



Σχήμα 3.5 Αποστολή Αιτήματος στον απομακρυσμένο διαχειριστή

Για καλύτερη κατανόηση ας δούμε αναλυτικά την δομή των πινάκων που χρησιμοποιούμε σε κάθε οντότητα και την λειτουργία και σκοπό που έχει ο καθένας.

Στο τέλος θα κάνουμε ένα απλό παράδειγμα για να γίνει καλύτερα κατανοητή η όλη τροποποίηση. Πρώτα περιγράφουμε την δομή των πινάκων του CAS- Πελάτη.

Πίνακας Αρχών Πιστοποίησης.

Οι πίνακες αυτοί περιγράφουν κάθε αρχή που μπορεί να παράγει μακροπρόθεσμα πιστοποιητικά για τους χρήστες. Όπως αναφέραμε πιο πριν, κάθε χρήστης έχει ένα βραχυπρόθεσμο πιστοποιητικό τύπου X.509 που επιβεβαιώνει την ταυτότητα του. Το πιστοποιητικό αυτό συνήθως έχει διάρκεια ζωής μερικών ωρών. Ο χρήστης για να μπορέσει να το δημιουργήσει προμηθεύεται από μια έμπιστη αρχή κάποια μακροπρόθεσμα πιστοποιητικά τα οποία χρησιμοποιεί για να υπογράψει τα βραχυπρόθεσμα πιστοποιητικά που παράγει. Στον πίνακα αυτόν αποθηκεύονται όλες οι απαραίτητες πληροφορίες για την έμπιστή αρχή από την οποία ο χρήστης έχει προμηθευτεί τα μακροπρόθεσμα πιστοποιητικά.

Πιο συγκεκριμένα όπως βλέπουμε ο πίνακας αποτελείται από τρία πεδία (σχήμα 3.6). Στο πρώτο πεδίο αποθηκεύουμε το ψευδώνυμο της αρχής. Το ψευδώνυμο είναι μια πληροφορία που χρησιμοποιείται εσωτερικά στην βάση του και μάλιστα υπάρχει περιορισμός να είναι μοναδική. Το δεύτερο κομμάτι αφορά τη μέθοδο με την οποία γίνεται η πιστοποίηση που στην περίπτωση μας δεν είναι άλλη από την κρυπτογραφία δημοσίου κλειδιού με τα X.509 πιστοποιητικά. Στο τελευταίο πεδίο αποθηκεύουμε το σφαιρικό όνομα της αρχής που υπάρχει στα πιστοποιητικά που θα υπογράψει.

Πίνακας χρηστών

Όπως είναι προφανές στον δεύτερο πίνακα αποθηκεύουμε τους χρήστες (σχήμα 3.6). Ο πίνακας αυτός αποτελείται από τρία πεδία. Στο πρώτο πεδίο υπάρχει ένα ψευδώνυμο του χρήστη που χρησιμοποιείται εσωτερικά στην βάση. Ο εκάστοτε διαχειριστής αποφασίζει πιο θα είναι όταν τον καταχωρήσει. Στο επόμενο πεδίο αποθηκεύουμε το σφαιρικό όνομα του χρήστη που υπάρχει στο X.509 πιστοποιητικό του. Είναι μοναδικό γιατί κάθε αρχή πιστοποίησης που εκδίδει τα μακροπρόθεσμα πιστοποιητικά του χρήστη φροντίζει να έχει ένα διακεκριμένο όνομα. Στο τελευταίο πεδίο υπάρχει το ψευδώνυμο της αρχής πιστοποίησης από τον οποίο έχει προμηθευτεί

τα μακροπρόθεσμα πιστοποιητικά ο χρήστης με σκοπό να κατασκευάζει βραχυπρόθεσμα.

Πίνακας κλάσεων

Ο πίνακας αυτός αποτελείται από ένα πεδίο μόνο (σχήμα 3.6). Στο πεδίο αυτό αναγράφουμε όλες τις κλάσεις που ανήκει ο οργανισμός μας.

Πίνακας συσχέτισης Χρήστης_Κλάση_Ομάδα

Τέλος ο πίνακας Χρήστης_Κλάση_Ομάδα συσχετίζει τις προηγούμενες οντότητες (σχήμα 3.6). Συγκεκριμένα αναφέρει ποιος χρήστης ανήκει σε ποια κλάση σε ποια ομάδα της σύμπραξης αυτής. Για να μπορέσει να γίνει μια τέτοια καταχώρηση πρέπει στους παραπάνω πίνακες να έχουν καταχωρηθεί τα ονόματα αυτά.

Πίνακας 3.1 Πίνακας Αρχών Πιστοποίησης

Πεδία Τιμών	**Πληροφορίες Πίνακα**
ψευδώνυμο αρχής	default Trust Anchor
μέθοδο πιστοποίησης	X.509
δεδομένα πιστοποίησης	O=Grid /.../CN=Globus Simple CA

Πίνακας 3.2 Πίνακας Χρηστών

Πεδία Τιμών	**Πληροφορίες Πίνακα**
ψευδώνυμο χρήστη	nikolas
σφαιρικό όνομα χρήστη	O=Grid/.../CN=Nikos Boudouropoulos
ψευδώνυμο αρχής	default Trust Anchor

Πίνακας 3.3 Πίνακας Κλάσης

Πεδία Τιμών	**Πληροφορίες Πίνακα**
ονομασία κλάσης	mathematician

Πίνακας 3.4 Πίνακας Χρήστης_Κλάση_Ομάδα

Πεδία Τιμών	**Πληροφορίες Πίνακα**
ψευδώνυμο χρήστη	nikolas
όνομα ομάδας	algebra
όνομα κλάσης	mathematician

Σχήμα 3.6 Οι πίνακες του CAS-Πελάτη

Στην συνέχεια θα περιγράψουμε και τους πίνακες του CAS-Διακομιστή. Στην αρχική αρχιτεκτονική οι πόροι που διαχειριζόταν ο CAS βρίσκονταν σε ένα πίνακα αντικειμένων (object). Για την περίπτωση που ενδιαφερόμαστε τα αντικείμενα που διαχειριζόμαστε είναι τα αρχεία. Έτσι λοιπόν στον πίνακα αντικειμένων θα έχουμε μόνο καταχωρήσεις που αφορούν αρχεία. Ο πίνακας αποτελείται από τα πεδία:

Σε αυτό τον πίνακα περιέχονται όλα τα αρχεία-φάκελοι που υπάρχουν στον απομακρυσμένο διαχειριστή αρχείων. Ο χαρακτήρας «*»(wildcard) σημαίνει πως το αντικείμενο αυτό συμπεριλαμβάνει όλα τα αρχεία και του υποφακέλους που βρίσκονται σε μεγαλύτερο βάθος. Το πρώτο πεδίο αποτελεί «κλειδί» για κάθε πλειάδα που υπάρχει σε αυτό τον πίνακα. Το τελευταίο πεδίο είναι ένα αναγνωριστικό, ότι το αντικείμενο αυτό μπορεί να το διαχειριστεί μόνο ο GridFTP διακομιστής. Ο CAS έχει υλοποιηθεί για να διαχειρίζεται διάφορους πόρους από οργανισμούς. Οι πόροι αυτοί μπορεί να είναι διάφορα πράγματα πέραν των δεδομένων, όπως υπολογιστική ισχύς, αποθήκευση κτλ. Ο GridFTP για να καταλάβει ποια αντικείμενα αφορούν αυτό το πεδίο αυτό πρέπει να είναι συμπληρωμένο με την συμβολοσειρά «FTPDirectoryTree». Ας υπενθυμίσουμε ότι ο CAS έχει υλοποιηθεί μόνο για τον διαχειρισμό αρχείων.

Τέλος ο πιο σημαντικός πίνακας που υπάρχει είναι ο πίνακας πολιτικής. Περιέχει πληροφορίες που καθορίζουν επακριβώς την πρόσβαση στα τοπικά αρχεία των απομακρυσμένων χρηστών. Ας το δούμε πιο αναλυτικά.

Το πρώτο στοιχείο αποτελεί κλειδί για κάθε πλειάδα που υπάρχει στον πίνακα. Το δεύτερο πεδίο προσδιορίζει την ονομασία της κλάσης. Το τρίτο πεδίο προσδιορίζει την ομάδα της κλάσης. Το τέταρτο και το πέμπτο αναφέρονται στην ενέργεια που μπορώ να κάνω στο αντικείμενο. Πιο συγκεκριμένα το πέμπτο πεδίο είναι μια αναφορά προς τον πίνακα ενεργειών. Στην περίπτωση μας είναι περιορισμένα και αφορούν ενέργειες πάνω σε αρχεία όπως ανάγνωση, εγγραφή διαγραφή κτλ. Το έκτο και το έβδομο πεδίο αφορούν το αντικείμενο στο οποίο αναφερόμαστε. Για λόγους βελτιστοποίησης θα μπορούσαμε να δημιουργήσουμε και πίνακες με ομάδες ενεργειών και πίνακες με ομάδες αντικειμένων. Έτσι για παράδειγμα σε μία ομάδα ενεργειών θα μπορούσαμε να συμπεριλάβουμε την ανάγνωση και την διαγραφή και στην ομάδα των αντικειμένων αρκετά αρχεία. Έτσι θα μπορούσαμε να δηλώσουμε στον πίνακα αυτό ότι σε μία μόνο πρόταση ότι η «χ» κλάση που μπορεί να εκτελέσει τις ενέργειες «y» μπορεί να τροποποιήσει την ομάδα των αρχείων «ζ». Σε αυτή την περίπτωση θα έπρεπε να αλλάξουν οι αναφορές στο πέμπτο και το έβδομο πεδίο και να αναφέρονται στους αντίστοιχους πίνακας που θα συμπεριλαμβάνουν τις αντίστοιχες ομαδοποιήσεις.

Πίνακας 3.5 Πίνακας Αντικειμένων

Πεδία Τιμών	**Πληροφορίες Πίνακα**
αναγνωριστικό αντικειμένου	5
όνομα αντικειμένου	ftp://cs.uoi.gr/help_files/*
όνομα διαχειριστή πόρου	FTPDirectoryTree

Πίνακας 3.6 Πίνακας Ενέργειες_Υπηρεσίες

Πεδία Τιμών	**Πληροφορίες Πίνακα**
αναγνωριστικό ενέργειας	18
όνομα υπηρεσίας	file
ενέργεια υπηρεσίας	read

Πίνακας 3.7 Πίνακας Πολιτική

Πεδία Τιμών	**Πληροφορίες Πίνακα**
αναγνωριστικό πολιτικής	7
όνομα κλάσης	mathematician
όνομα ομάδας της κλάσης	algebra
ενέργεια	18
καθορισμός ενέργειας	Ενέργειες_Υπηρεσίες
αντικείμενο	5
καθορισμός αντικειμένου	Αντικείμενα

Σχήμα 3.7 Οι πίνακες του CAS-Διακομιστή

Ας υποθέσουμε ότι ο χρήστης έχει προμηθευτεί τα μακροπρόθεσμα πιστοποιητικά του από μια αρχή πιστοποίησης και τον γνωρίζει ο CAS-Πελάτη. Στην συνέχεια χρησιμοποιεί τα πιστοποιητικά αυτά για να δημιουργήσει τα βραχυπρόθεσμα πιστοποιητικά. Αυτά περιέχουν το σφαιρικό όνομα που έχει από την αρχή πιστοποίησης και το όνομα της αρχής αυτής καθώς και το χρονικό διάστημα για το οποίο είναι έγκυρα. Δηλαδή το πιστοποιητικό αυτό περιέχει τις πληροφορίες (σφαιρικό όνομα χρήστη, όνομα αρχής, χρονοσφραγίδα). Η προκαθορισμένη διάρκεια της σφραγίδας αυτή είναι δώδεκα ώρες. Τόσο στο μηχάνημα που δημιουργεί ο χρήστης το πιστοποιητικό τόσο και το μηχάνημα του CAS-Πελάτη θα πρέπει να έχουν συγχρονισμένα ρολόγια. Στην περίπτωση που ένας εκ των δύο παραβαίνει τον κανόνα αυτό δεν θα μπορέσει να ολοκληρωθεί η διαδικασία αυτή. Γι’άυτό όλες οι οντότητες που απαρτίζουν την αρχιτεκτονική χρησιμοποιούν το πρωτόκολλο NTP(Network Time Protocol).

- Ταυτοποίηση

Ο χρήστης έχει στην κατοχή κάποια μακροπρόθεσμα πιστοποιητικά που τα έχει υπογράψει μια αρχή πιστοποίησης. Με την βοήθεια αυτών των πιστοποιητικών παράγει κάποια βραχυπρόθεσμα πιστοποιητικά που περιέχουν το σφαιρικό όνομα της αρχής που του έχει προμηθεύσει τα μακροπρόθεσμα. Αρχικά εξετάζει εάν υπάρχει το σφαιρικό όνομα της αρχής που υπογράφει τα μακροπρόθεσμα πιστοποιητικά του χρήστη βάση του. Στην περίπτωση αυτή συνεχίζεται η διερεύνηση αφού πρώτα

εντοπίσει το ψευδώνυμο της αρχής αυτής. Γνωρίζοντας το ψευδώνυμο της αρχής και το σφαιρικό όνομα του χρήστη που αναγράφεται στο πιστοποιητικό είναι σε θέση πλέον να εντοπίσει το ψευδώνυμο του χρήστη. Για παράδειγμα ο χρήστης που έχει την σφαιρική ονομασία “Nikos Boudouropoulos” δημιουργεί ένα βραχυπρόθεσμο πιστοποιητικό που περιέχει την σφαιρική του ονομασία την αρχή πιστοποίησης που το έχει υπογράψει “Globus Simple CA” και μια χρονοσφραγίδα. Ανατρέχοντας στη βάση μπορούμε να διαπιστώσουμε ότι η αρχή πιστοποίησης “Globus Simple CA” περιέχεται στην βάση και μάλιστα με την ψευδώνυμο “defaultTrustAnchor”. Στην συνέχεια γνωρίζοντας το ψευδώνυμο της αρχής πιστοποίησης σε συνδυασμό με την σφαιρική ταυτότητα του χρήστη που αναγράφεται στο πιστοποιητικό, από τον πίνακα των χρηστών μπορεί να εντοπίσει το μοναδική ψευδώνυμο που έχει ο χρήστης στην βάση του CAS-Πελάτη. Στο συγκεκριμένο παράδειγμα το ψευδώνυμο του χρήστη όπως φαίνεται και από τους πίνακες είναι “nikolas”.

Εφόσον έχουμε εντοπίσει το ψευδώνυμο του χρήστη και είμαστε πλέον σίγουροι ότι τον έχουμε κατοχυρωμένο στην βάση το τελευταίο που μένει να ελέγξουμε είναι την χρονοσφραγίδα του πιστοποιητικού. Η χρονοσφραγίδα είναι ένα διάστημα δώδεκα ωρών. Η ώρα του μηχανήματος που είναι ρυθμισμένος ο CAS-Πελάτης εάν ανήκει στο συγκεκριμένο διάστημα ολοκληρώνει τον έλεγχο της ταυτοποίησης.

- Πιστοποίηση

Μετά την ολοκλήρωση της διαδικασίας της ταυτοποίησης πρέπει να ξεκινήσει η διαδικασία της πιστοποίησης. Έχοντας εντοπίσει το ψευδώνυμο του χρήστη εξετάζει τον πίνακας που συνδέει το ψευδώνυμο με τις κλάσεις που ανήκει ο χρήστης. Στην περίπτωση που εντοπίσει έστω και μία εγγραφή (nikolas, algebra, mathematician) τότε επιστρέφει στον χρήστη ένα εκτεταμένο πιστοποιητικό που πιστοποιεί την συμμετοχή στην αντίστοιχη κλάση και την ομάδα αυτής (υποθέτουμε ότι κάθε κλάση διαθέτει κάποιες ομάδες για αποτελεσματικότερη ομαδοποίηση των χρηστών που την απαρτίζουν). Στην περίπτωση που ο χρήστης ανήκει σε μία ακόμα κλάση ή σε μια διαφορετική ομάδα της ίδιας κλάσης δεν αποτελεί πρόβλημα για την υλοποίηση μας. Στην πρότυπο αυτό που κατασκευάσαμε η προεπιλογή είναι να εγγράφεται στον εκτεταμένο πιστοποιητικό του χρήστη όλες οι κλάσεις και οι ομάδες των κλάσεων που ανήκει. Στα μελλοντικά μας σχέδια είναι να υλοποιήσουμε ένα μηχανισμό όπου ο

χρήστης θα καθορίζει ποιες κλάσεις και ομάδες των κλάσεων θέλει να συμπεριληφθούν με σκοπό να ελαχιστοποιήσουμε το κόστος παραλαβής του πιστοποιητικού. Το εκτεταμένο αυτό πιστοποιητικό περιέχει όλες τις απαραίτητες πληροφορίες για την εξουσιοδότηση της απομακρυσμένης πρόσβασης. Πέραν από τις κλάσεις και τις ομάδες που ανήκει ο χρήστης περιέχει μια χρονοσφραγίδα και την σφαιρική ταυτότητα του CAS-Πελάτη.

- Προσπέλαση

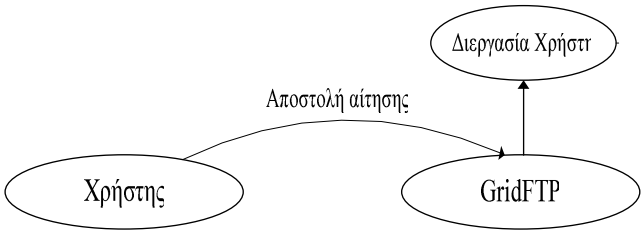
Τώρα ο χρήστης είναι έτοιμος να κάνει την προσπέλαση σε οποιοδήποτε απομακρυσμένο διαχειριστή πόρων που ανήκει στην κλάση και την ομάδα της κλάσης αυτής. Για να ολοκληρωθεί η προσπέλαση αυτή ο χρήστης πρέπει να γνωρίζει την ονομασία του πόρου-αρχείου που θέλει να προσπελάσει.

- Σύγκριση με αρχική αρχιτεκτονική GridFTP

Στον αρχικό του σχεδιασμό ο διακομιστής GridFTP έκανε απλή ανάλυση στο πιστοποιητικό και εντόπιζε απευθείας τα δικαιώματα στους εκάστοτε πόρους. Αυτό ήταν εφικτό επειδή η απαραίτητη πληροφορία για την παραπάνω ανάλυση συλλεγόταν περιοδικά στον διακομιστή CAS με την απαιτούμενη επιβάρυνση. Αντιθέτως, στην δική μας υλοποίηση αρχικά ο διακομιστής GridFTP αναλύει το πιστοποιητικό και βρίσκει τις κλάσεις και τις ομάδες στις οποίες ανήκει ο χρήστης. Στη συνέχεια ο διακομιστής GridFTP θέτει ένα ερώτημα στην τοπική του βάση για τον αποθηκευτικό πόρο που θέλει να προσπελάσει ο χρήστης και το δικαίωμα που θέλει να εξασκήσει σε αυτόν, π.χ. ανάγνωση ενός αρχείου. Κάνοντας ένα ταίριασμα με τις αντίστοιχες πληροφορίες του χρήστη μπορεί ο διακομιστής να βρει εάν επιτρέπεται η πρόσβαση στο συγκεκριμένο πόρο.

Χρησιμοποιώντας το πρόγραμμα του πελάτη για GridFTP ο χρήστης μαζί με τα στοιχεία του πόρου που θέλει να προσπελάσει στέλνει ένα αίτημα που αποτελείται {εκτεταμένο πιστοποιητικό, ftp://cs.uoi.gr/help_files/1.txt, read}. Μόλις ο GridFTP παραλάβει ένα τέτοιο αίτημα το πρώτο πράγμα που κάνει είναι να εξετάσει την υπογραφή του πιστοποιητικού. Ελέγχει την εγκυρότητα της και βρίσκει την απεικόνιση της σφαιρικής ταυτότητας που περιέχει το πιστοποιητικό στον τοπικό χρήστη του συστήματος. Αμέσως μετά ξεκινάει μια νέα διεργασία για λογαριασμό

του τοπικού αυτού χρήστη που θα αναλάβει να ολοκληρώσει το αίτημα του απομακρυσμένου χρήστη (σχήμα 3.6). Αξιοσημείωτο είναι να αναφερθεί πως η τακτική αυτή έχει δημιουργηθεί για λόγους ασφαλείας. Η εκτέλεση του GridFTP μπορεί να γίνει μόνο από τον διαχειριστή του συστήματος. Γι'αυτό οποιαδήποτε αίτηση του ζητηθεί να πραγματοποιήσει την αναθέτει στον τοπικό χρήστη που απεικονίζεται η ταυτότητα του εκτεταμένου πιστοποιητικού που έχει λάβει. Φανταστείτε ένα κακόβουλο χρήστη που θα θελήσει να βλάψει τον GridFTP. Η μόνη αποτελεσματική επίθεση που μπορεί να κάνει είναι να τον βομβαρδίζει με μια πληθώρα αιτήσεων. Ο GridFTP μόλις το αντιληφθεί θα αφαιρέσει την απεικόνιση της σφαιρικής οντότητας του πιστοποιητικού στον τοπικό χρήστη και θα απορρίπτει τις αιτήσεις του χωρίς να προκληθεί ιδιαίτερο πρόβλημα.



Σχήμα 3.8 Αποστολή και επεξεργασία της αίτησης

- Τροποποιήσεις

Η νέα διεργασία στην συνέχεια θα ενεργοποιήσει το κομμάτι του GridFTP που είναι υπεύθυνο για να εξακριβώσει την εφικτότητα της προσπέλασης του πόρου. Το κομμάτι αυτό αποτελείται από τρία μέρη:

- Αρχικοποίηση. Σε αυτό το κομμάτι αρχικοποιούνται όλες οι πληροφορίες που πρόκειται να χρησιμοποιήσουμε για να αποφανθούμε για την προσπέλαση του πόρου. Επιπλέον καλείται και ο συντακτικός αναλυτής που εξακριβώνει την ορθή σύνταξη του πιστοποιητικού.
- Εξουσιοδότηση. Εξετάζοντας διεξοδικά τις πληροφορίες του πιστοποιητικού ερχόμαστε σε επικοινωνία με τον CAS-Διακομιστή. Με μια σειρά ερωτήσεων που θα περιγραφούν εντοπίζουμε εκείνη την καταχώρηση στον πίνακα πολιτικής που επιτρέπει την προσπέλαση εάν υπάρχει.

- Αποδέσμευση. Τέλος απελευθερώνουμε ό,τι πόρους έχουμε δεσμεύσει για να μπορέσει το σύστημα να εξυπηρετήσει άλλες αιτήσεις από απομακρυσμένους χρήστες.

Στο πρώτο μέρος δε χρειάστηκε να κάνουμε κάποιες ιδιαίτερες αλλαγές. Στην αρχική αρχιτεκτονική το εκτεταμένο πιστοποιητικό όπως αναφέραμε περιέχει τους πόρους και τις ενέργειες που μπορούσε ο χρήστης να κάνει στους πόρους αυτούς. Καταφέραμε να διατηρήσουμε την ίδια δομή του πιστοποιητικού για να μην χρειαστεί να αλλάξει ο συντακτικός αναλυτής. Τώρα σε κάθε εκτεταμένο πιστοποιητικό αντί να περιέχει τους πόρους και τις ενέργειες που έχουμε δικαίωμα να εκτελέσουμε σε κάθε πόρο αναγράφει τις κλάσεις που ανήκει ο χρήστης και τις αντίστοιχες ομάδες των κλάσεων αυτών.

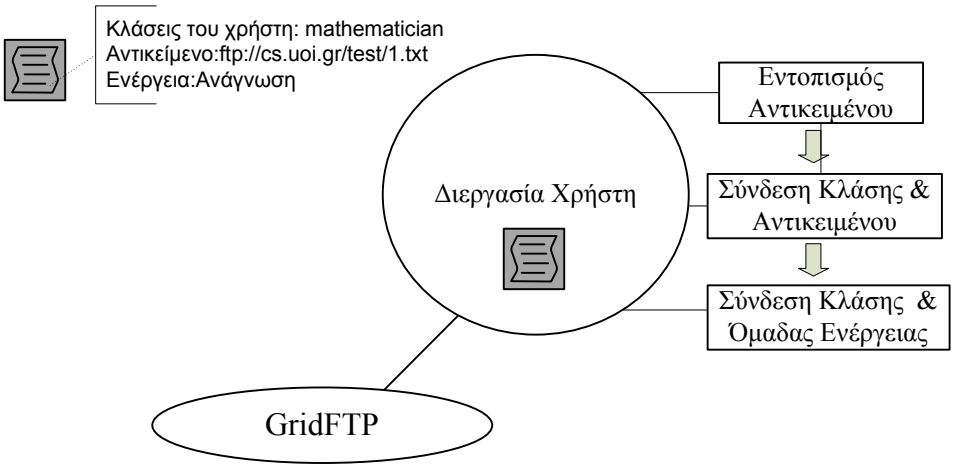
Στο δεύτερο μέρος χρειάστηκαν αρκετές αλλαγές. Για τη νέα πληροφορία που υπάρχει μέσα στο πιστοποιητικό έπρεπε να δημιουργηθούν και οι αντίστοιχες συναρτήσεις που θα επέτρεπαν την επεξεργασία τους. Αρχικά πριν προχωρήσουμε στην επεξεργασία των πληροφοριών αυτών η πρώτη ενέργεια που έπρεπε να γίνει είναι να διαπιστωθεί κατά πόσο ο πόρος-αρχείο που ζητάει ο χρήστης υπάρχει στην βάση του CAS-Διακομιστή. Σε αυτό το σημείο θα πρέπει να αποσαφηνίσουμε μια σημαντική λεπτομέρεια. Ο διαχειριστής της βάσης μπορεί στον πίνακα πολιτικής να έχει δώσει τα δικαιώματα όχι για αυτό καθ'εαυτό το αρχείο, αλλά στον κατάλογο που βρίσκεται αναδρομικά σε κάποιον από τους γονικούς καταλόγους που ανήκουν σε αυτό το μονοπάτι. Έτσι λοιπόν ο χρήστης με μια σειρά ερωτημάτων που θα ξεκινούν από το όνομα του αρχείου και θα επαναλαμβάνονται αναδρομικά ώσπου να φτάσουμε στην ρίζα του μονοπατιού θα συλλέξει τα κλειδιά των πλειάδων αυτών από τον πίνακα των αντικειμένων. Η αποθήκευση των κλειδιών αυτών για τις αντίστοιχες πλειάδες γίνεται σε μια λίστα απλά συνδεδεμένη. Στην περίπτωση που δεν υπάρχουν αντικείμενα που συσχετίζονται με την απαίτηση του χρήστη δεν μπορούμε να συνεχίσουμε την διαδικασία αυτή. Αυτό σημαίνει πως ο διαχειριστής των πόρων δεν έχει καταχωρήσει το συγκεκριμένο αντικείμενο στην βάση του Διακομιστή-CAS.

Έτσι λοιπόν στο παράδειγμα που έχούμε αναφέρει ο χρήστης θέλει να προσπελάσει το ftp://cs.uoi.gr/help_files/1.txt. Εμείς θα αναζητήσουμε καταχωρήσεις αντικειμένων που θα έχουν την ακόλουθη μορφή:

- ftp://cs.uoi.gr/help_files/1.txt
- ftp://cs.uoi.gr/help_files/
- ftp://cs.uoi.gr/help_files/*
- ftp://cs.uoi.gr/*

Στην τρίτη κατά σειρά ερώτηση έχουμε θετική απάντηση από την βάση και το αναγνωριστικό αντικειμένου έχει την τιμή πέντε. Εφόσον έχουμε εντοπίσει τα αντικείμενα που σχετίζονται με τον αρχείο που θέλουμε προχωράμε στο επόμενο βήμα. Ξεκινάμε να επεξεργαζόμαστε τις πληροφορίες που μπορούμε να αντλήσουμε από το πιστοποιητικό. Η πρώτη πληροφορία που αντλούμε είναι η κλάση στην οποία ανήκει ο χρήστης (σχήμα 3.7). Σε αυτό το σημείο ξανασυνδεόμαστε με την βάση και ρωτάμε εάν υπάρχουν στον πίνακα πολιτικής καταχωρήσεις που αφορούν τις αναγνωριστικές τιμές των αντικειμένων που έχουμε εντοπίσει και την κλάση στην οποία ανήκει ο χρήστης. Η διαδικασία αυτή επαναλαμβάνεται για κάθε μια κλάση που ανήκει ο χρήστης. Στην περίπτωση αρνητικής απάντησης απορρίπτουμε την τρέχοντα κλάση καθώς και τις ομάδες που μπορεί να περιέχει το πιστοποιητικό και προχωράμε στην επόμενη. Σε όσες κλάσεις και αναγνωριστικά αντικειμένων εντοπίσουμε θετικά αποτελέσματα αποθηκεύουμε τα κλειδιά των πλειάδων αυτών καθώς και τις αντίστοιχες ομάδες των κλάσεων αυτών. Στο παράδειγμα που έχουμε η επόμενη ερώτηση που θα γίνει είναι εάν η κλάση «mathematician» και το αναγνωριστικό αντικειμένου με τιμή πέντε υπάρχουν σε κάποια πλειάδα του πίνακα. Όπως είναι προφανές υπάρχει μια τέτοια πολιτική με αναγνωριστικό πολιτικής εφτά.

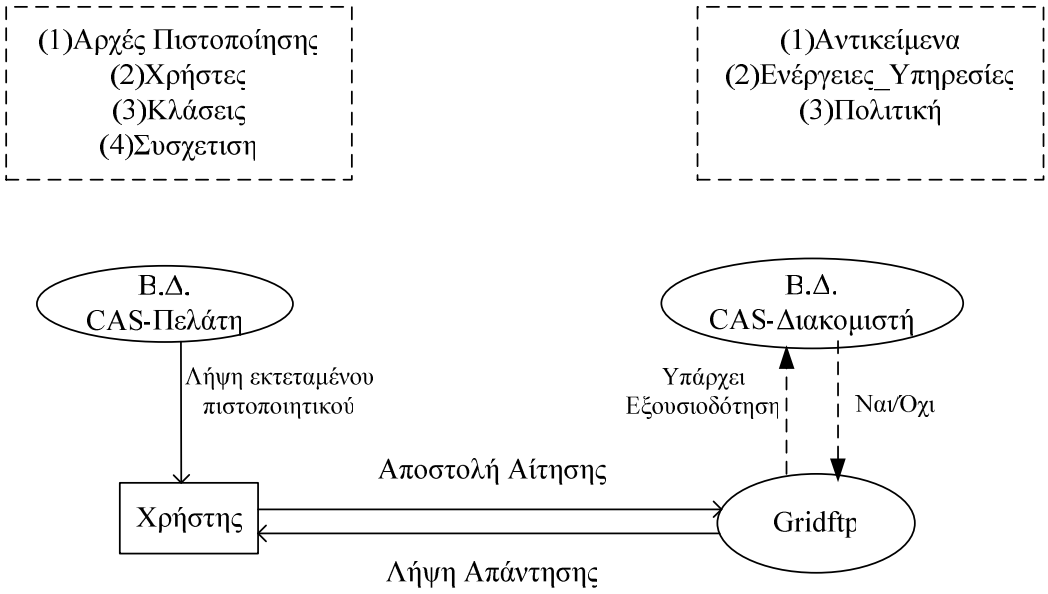
Έχουμε φτάσει λοιπόν στο σημείο που από τον πίνακα πολιτικής έχουμε εντοπίσει πλειάδες οι οποίες μπορεί να ικανοποιήσουν το αίτημα μας στα πεδία της κλάσης και του αντικειμένου. Για να ολοκληρωθεί η διαδικασία κάνουμε μια τελική ερώτηση στην βάση. Όπως καταλαβαίνουμε η ερώτηση θα αφορά τα υπόλοιπα πεδία που πρέπει να ταυτοποιηθούν. Έτσι λοιπόν για κάθε ομάδα της κλάσης αυτής σε συνδυασμό με την ενέργεια που θέλουμε να κάνουμε ρωτάμε την βάση και στην πρώτη θετική απάντηση ικανοποιούμε το αίτημα.



Σχήμα 3.9 Επεξεργασία του αιτήματος του απομακρυσμένου χρήστη

3.6. Συμπεράσματα

Συμπερασματικά οι υπάρχουσες πολιτικές ασφαλούς προσπέλασης σε περιβάλλοντα πλέγματα αντιμετώπιζαν περιορισμούς κλιμάκωσης λόγω του μεγάλου όγκου ενημερώσεων είτε μεταξύ των επιμέρους οργανισμών που συμμετέχουν στο πλέγμα ή μεταξύ των οργανισμών και μιας κεντρικής αρχής. Στην προσέγγιση που σχεδιάσαμε και υλοποιήσαμε, ο κάθε οργανισμός συντηρεί τοπικές πληροφορίες σύνθεσης για τις ομάδες χρηστών που περιέχει και οργανισμών στους οποίους ανήκει καθώς και λίστες ελέγχου πρόσβασης για τους τοπικούς πόρους. Οι πληροφορίες που ανταλλάσσονται μεταξύ των διαφορετικών οργανισμών περιορίζονται στις ελάχιστες απαραίτητες για να επιβεβαιωθεί η δυνατότητα πρόσβασης ενός χρήστη σε έναν απομακρυσμένο πόρο και να ικανοποιηθεί η εκάστοτε αιτούμενη εξυπηρέτηση εφόσον επιτρέπεται.



Σχήμα 3.10 Συνολική εικόνα του συστήματος

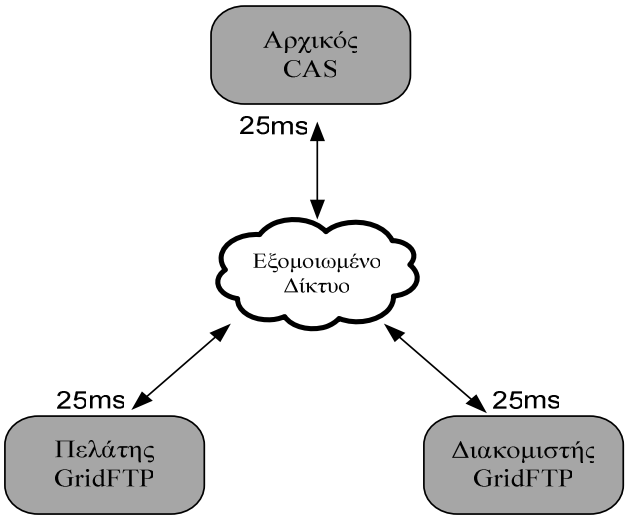
ΚΕΦΑΛΑΙΟ 4. ΠΕΙΡΑΜΑΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

4.1. Περιγραφή αποτελεσμάτων

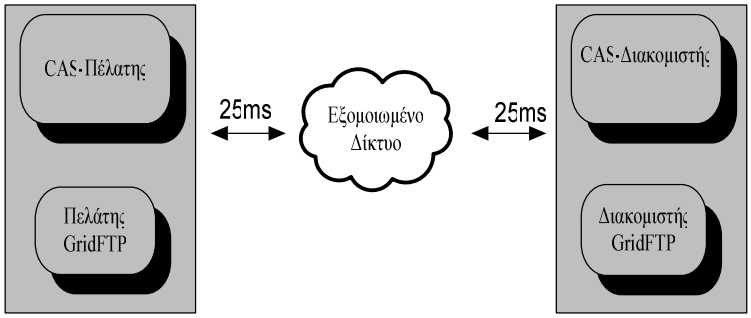
Για να μπορέσουν να ολοκληρωθούν τα πειράματα έπρεπε να γίνουν κάποιες τροποποιήσεις στον υπάρχοντα κώδικα. Όπως έχουμε προαναφέρει ο CAS είναι μια υπηρεσία διαδικτύου. Ο πελάτης που έχει κατασκευαστεί για να καλεί αυτή την υπηρεσία είναι μια εφαρμογή που έχει συνταχτεί στην γλώσσα προγραμματισμού JAVA. Από πειραματικές μετρήσεις που κάναμε καταλήξαμε στο συμπέρασμα ότι η υλοποίηση του πελάτη καταναλώνει ένα μεγάλο μέρος της υπολογιστικής ισχύος του μηχανήματος στο οποίο εκτελείται. Αυτό έχει ως αποτέλεσμα να μην μπορούμε να εξετάσουμε την συμπεριφορά του CAS σε υψηλά φορτία αφού η υπάρχουσα υλοποίηση θα απαιτούσε σημαντική υπολογιστική ισχύ πολλαπλών κόμβων. Αυτό το πρόβλημα έχει διαπιστωθεί από την τρίτη έκδοση του Globus, όταν για να αξιολογηθούν οι διαδικτυακές υπηρεσίες που προσφέρει το πακέτο χρειάστηκαν 45 κόμβοι για να δημιουργήσουν 1000 πελάτες[21]. Γι’αυτό αναγκαστήκαμε και τροποποιήσαμε τον κώδικα του πελάτη μετατρέποντας τον σε πολυνηματικό. Για κάθε μια αίτηση που δημιουργεί ο πελάτης δημιουργεί παράλληλα και ένα νήμα που είναι υπεύθυνο γι’αυτή.

Για την υλοποίηση των πειραμάτων που αφορούν την παλιά αρχιτεκτονική του CAS χρησιμοποιήσαμε δύο διαφορετικούς διακομιστές ένα για τον CAS και ένα για τον αρχικό GridFTP αντίστοιχα. Για την υλοποίηση του Νεφέλη χρησιμοποιήσαμε τρεις διαφορετικούς διακομιστές ένα για τον CAS-Πελάτη, ένα για τον Νεφέλη-GridFTP και ένα για τον CAS-Διακομιστή. Επιπλέον διεξάγουμε μία σειρά πειραμάτων σε εξομοιωμένο δίκτυο που προσθέτει χρόνο μετάβασης-επιστροφής (round trip time-RTT) με την χρήση του εξομοιωτή δικτύου (Network Emulator-Netem). Το Netem

είναι ένα εργαλείο που χρησιμοποιείται για εξομοιώσεις δικτύων και προσθέτει χρονοκαθυστερήσεις στα πακέτα που δημιουργούμε για να διακινηθούν στο δίκτυο [22]. Οι χρονοκαθυστερήσεις που έχουμε τοποθετήσει φαίνονται από τα παρακάτω σχήματα (σχήμα 4.1, σχήμα 4.2). Οι κόμβοι των μηχανημάτων που δημιουργήθηκαν οι παραπάνω οντότητες έχουν την διανομή Debian 4 του λειτουργικού συστήματος Linux με έκδοση πυρήνα 2.6.18. Κάθε κόμβος περιλαμβάνει ένα τετραπύρηνο επεξεργαστή Intel Xeon E5345 2.33GHz, 3Gb μνήμη RAM και δύο 250 Gb 7200 RPM SATA δίσκους. Αντίστοιχα κάθε κόμβος-πελάτη περιλαμβάνει ένα τετραπύρηνο επεξεργαστή Intel Xeon E5345 2.66GHz 3Gb μνήμη RAM και δύο 300Gβ 15000 RPM SATA δίσκους. Τέλος για την μεταφορά δεδομένων μεταξύ των κόμβων χρησιμοποιήθηκε ένα δίκτυο Ethernet το οποίο είχε ταχύτητα μετάδοσης δεδομένων 1Gbit/sec.



Σχήμα 4.1 Εξομοίωση δικτύου για την αρχική αρχιτεκτονική.



Σχήμα 4.2 Εξομοίωση δικτύου για την νέα αρχιτεκτονική.

Ο τρόπος που επιλέξαμε να εξομοιώσουμε το δίκτυο αντικατοπτρίζει τις πραγματικές χρονοκαθυστερήσεις που θα εμφανίζονταν στην εφαρμογή της αρχιτεκτονικής. Επιπλέον επιλέξαμε δύο φορτία ένα υψηλό και ένα χαμηλό για να μελετήσουμε την συμπεριφορά του συστήματος. Τέλος επιλέγοντας τα ίδια φορτία έχουμε διεξάγει τα πειράματα με τις ίδιες παραμέτρους χωρίς την καθυστέρηση του δικτύου.

Όταν αναφερόμαστε σε χαμηλό φορτίο για τον CAS-Πελάτη ή τον CAS έχουμε ένα κόμβο που εκτελεί δέκα πελάτες και ο κάθε πελάτης στέλνει χίλια ερωτήματα στον αντίστοιχο CAS-Πελάτη ή CAS. Στο υψηλό φορτίο έχουμε τρεις κόμβους με δέκα πελάτες. Ο κάθε πελάτης στέλνει συνολικά χίλια ερωτήματα. Τα ερωτήματα παράγονται συνεχόμενα χωρίς καμία καθυστέρηση μεταξύ τους. Για τον Grid-FTP και τον Νεφέλη-GridFTP έχουμε ένα κόμβο που δημιουργεί χίλιους πελάτες και η μέση καθυστέρηση μεταξύ των αιτήσεων είναι 0.3s και 0.15s, αντιστοίχως. Για την ορθότερη διεξαγωγή του πειράματος παράγουμε 1000 τυχαίους αριθμούς από μια γεννήτρια αριθμών και εκτελέσαμε τον μετασχηματισμό $x = -\beta \ln u$ όπου το β παίρνει τις τιμές 0.3 και 0.15 και το u είναι ένας από τους τυχαίους ομοιόμορφα κατανεμημένους αριθμούς στο [0,1]. Έτσι δημιουργούμε τα χρονικά διαστήματα μεταξύ διαδοχικών αιτήσεων.

Το πρώτο που πρέπει να σχολιαστεί είναι η προετοιμασία για την δημιουργία της αίτησης που θα κάνει ο πελάτης για το εκτεταμένο πιστοποιητικό. Πρόκειται για μια αρκετά δαπανηρή διαδικασία και ίσως μια υλοποίηση του σε διαφορετική γλώσσα προγραμματισμού να μπορούσε να μας απαλλάξει από αυτό το φορτίο. Και στις δύο

αρχιτεκτονικές διαρκεί τον ίδιο ακριβώς χρόνο. Στον χρόνο αυτό ο πελάτης διαβάζει το βραχυπρόθεσμο πιστοποιητικό που έχει δημιουργήσει για να μπορεί να δημιουργήσει την κατάλληλη αίτηση για τον διακομιστή που θα του δώσει το εκτεταμένο πιστοποιητικό. Αξιοσημείωτο είναι να αναφερθεί πως το βραχυπρόθεσμο πιστοποιητικό δημιουργείται σε 59ms.

Όπως έχουμε αναφέρει μια βασική διαφορά των δύο αρχιτεκτονικών είναι η εισαγωγή της διαφορετικής πληροφορίας στο εκτεταμένο πιστοποιητικό. Άμεσο επακόλουθο είναι να εντοπίσουμε κάποιες διαφορές στον χρόνο εξυπηρέτησης των αιτήσεων αυτών. Παρατηρούμε μικρή διαφορά στον χρόνο εξυπηρέτησης από τον κάθε διακομιστή αλλά και στον χρόνο διεκπεραίωσης της ασφαλούς επικοινωνίας και λήψης του πιστοποιητικού αυτού. Η πληροφορία που έχουμε εισάγει στο πιστοποιητικό στην νέα αρχιτεκτονική αφορά την συμμετοχή του χρήστη σε μία κλάση που καθορίζει τα αρχεία στα οποία έχει πρόσβαση ο χρήστης. Το πιστοποιητικό αυτό παρουσιάζεται στον Νεφέλη-GridFTP και αποφασίζει την πρόσβαση. Στον CAS η πληροφορία που εισάγεται στον πιστοποιητικό είναι το δικαίωμα προσπέλασης ενός απομακρυσμένου αρχείου καθώς και οι ενέργειες που επιτρέπονται σ’αυτό. Ενδεικτικά το πιστοποιητικό της νέας αρχιτεκτονικής έχει το μέγεθος των 7546 bytes και το πιστοποιητικό της παλιάς αρχιτεκτονικής 7672 bytes.

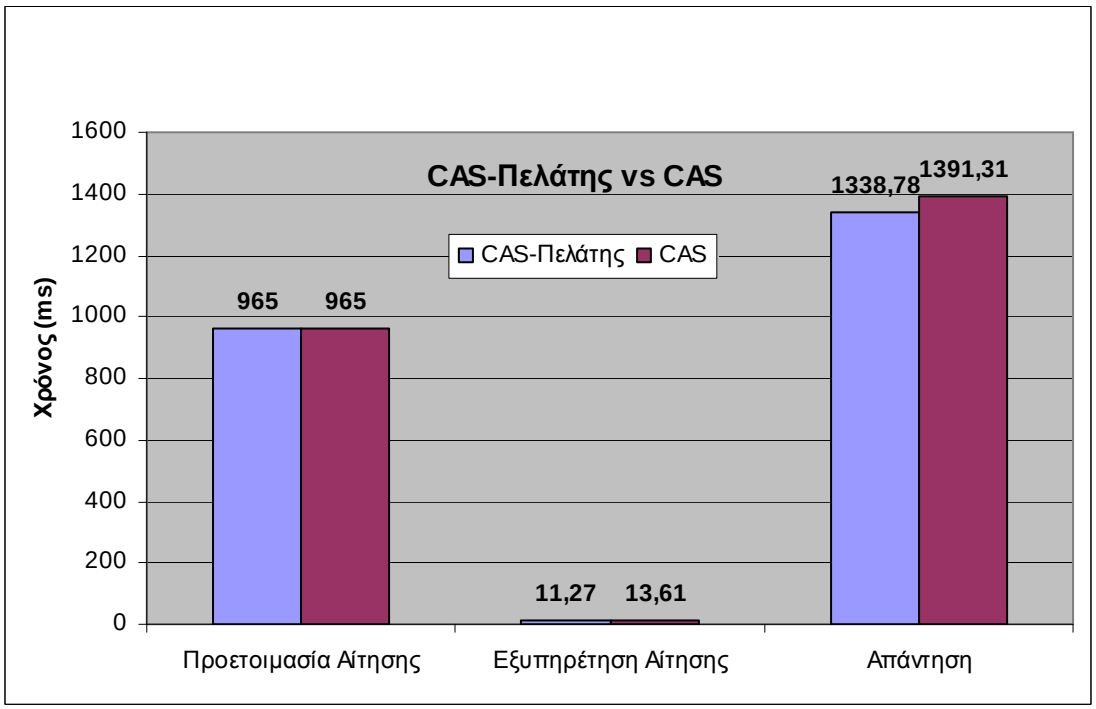
Η επικοινωνία μεταξύ χρήστη και CAS-Πελάτη (ή CAS) γίνεται με τη χρήστη του *πρωτοκόλλου μεταφοράς ασφαλούς υπερκειμένου*(-Secure HyperText Transfer Protocol-https) που είναι πολυδάπανη. Το HTTPS δεν είναι ξεχωριστό πρωτόκολλο όπως μερικοί νομίζουν, αλλά αναφέρεται στον συνδυασμό του απλού HTTP πρωτοκόλλου και των δυνατοτήτων κρυπτογράφησης που παρέχει το πρωτόκολλο ασφαλής επικοινωνία επιπέδου(Secure Socket Layer-SSL).

Στην συνέχεια ο χρήστης αφού παραλάβει το πιστοποιητικό το στέλνει στον αντίστοιχο GridFTP διακομιστή που έχει υλοποιηθεί για κάθε αρχιτεκτονική. Λογικό είναι ο Νεφέλη-GridFTP να χρειάζεται κάποιο επιπλέον χρόνο για την επεξεργασία αυτή, αφού συμβουλεύεται τον CAS-Διακομιστή για την εξουσιοδότηση της. Το κόστος της εξουσιοδότησης ανέρχεται στα 200ms περίπου. Στην περίπτωση που θέλουμε να προσπελάσουμε κάποιο άλλο αρχείο που ανήκει στην κλάση την οποία

ανήκει ο χρήστης δεν θα χρειαστεί να προμηθευτούμε εκ’ νέου κάποιο νέο εκτεταμένο πιστοποιητικό.

4.2. Πειραματικά Αποτελέσματα

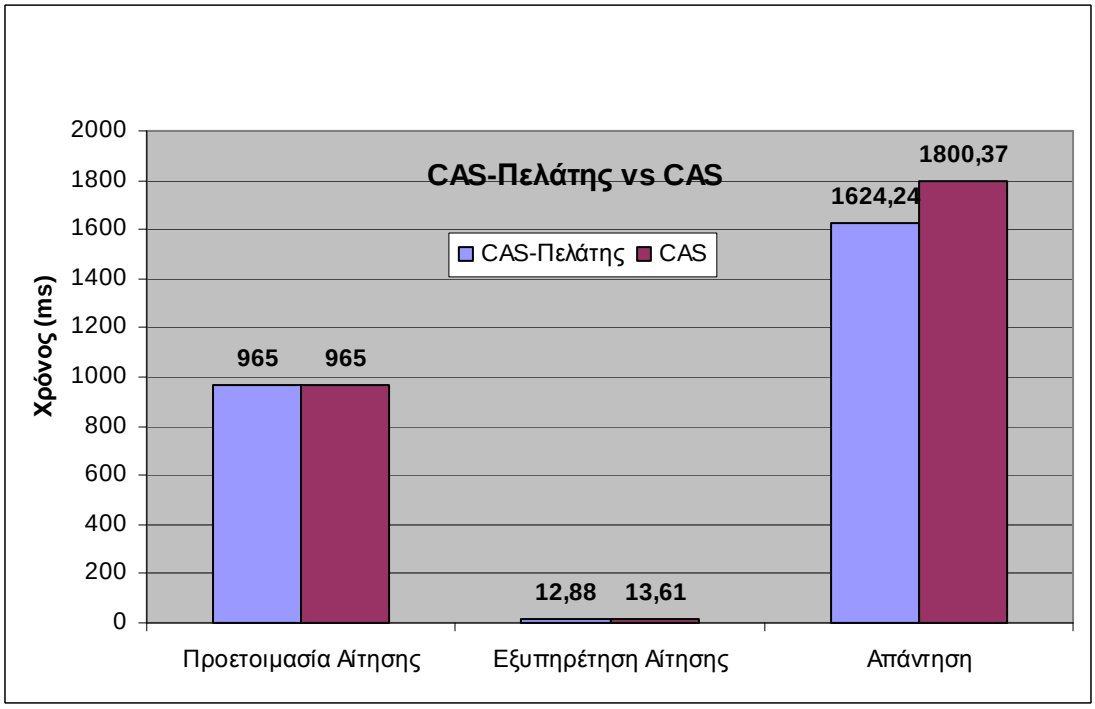
Τα πρώτα πειραματικά αποτελέσματα είναι μια σύγκριση μεταξύ του CAS-Πελάτη και του CAS σε χαμηλό φορτίο και σε τοπικό δίκτυο (σχήμα 4.3). Όπως παρατηρούμε η εξυπηρέτηση στην περίπτωση μας είναι λίγο ταχύτερη λόγω των λιγότερων ερωτήσεων που κάνουμε στην βάση του CAS. Το ποσοστό χρησιμοποίησης του επεξεργαστή στον CAS- Πελάτη είναι 25.44% ενώ στον CAS 26.41%.



Σχήμα 4.3 Λήψη πιστοποιητικού σε τοπικό δίκτυο και χαμηλό φορτίο

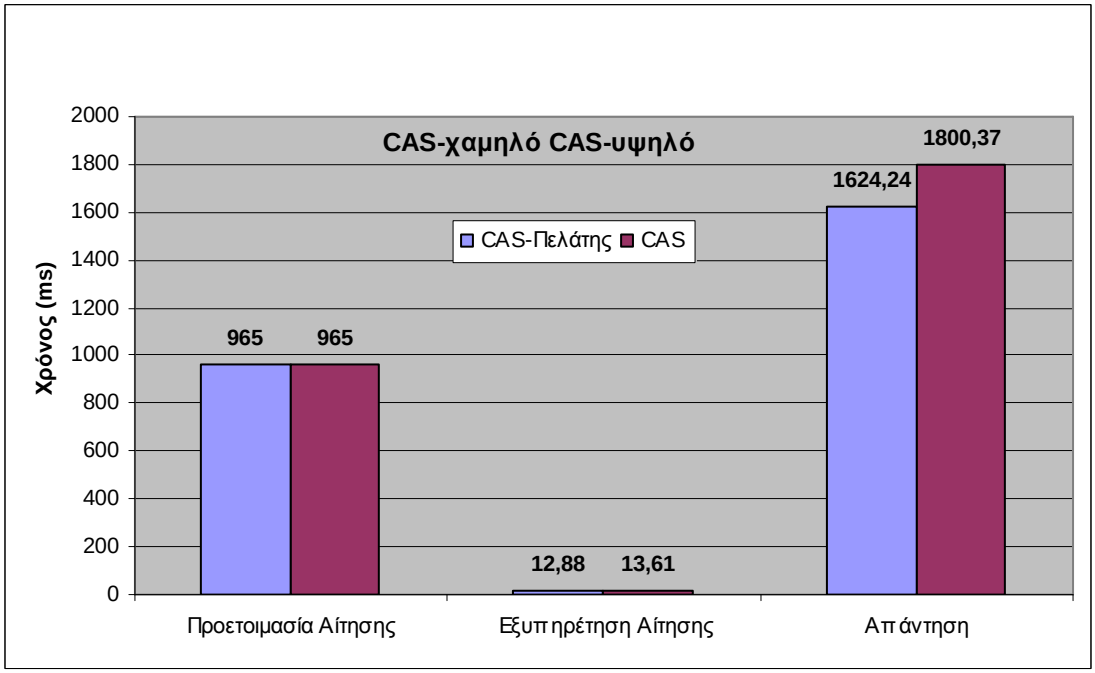
Το επόμενο πειραματικό αποτέλεσμα έχουν γίνει σε υψηλό φορτίο και σε τοπικό δίκτυο (σχήμα 4.4). Όπως είναι αναμενόμενο ο CAS με υψηλό φορτίο επιβαρύνεται σημαντικά γιατί η εξυπηρέτηση της αίτησης και η απάντηση είναι πιο δαπανηρές στο

CAS από τον CAS-Πελάτη. Το ποσοστό χρησιμοποίησης του επεξεργαστή στον CAS- Πελάτη είναι στο 73.65% ενώ στον CAS 67.15%.



Σχήμα 4.4 Λήψη πιστοποιητικού σε τοπικό δίκτυο και υψηλό φορτίο

Το τρίτο πείραμα αφορά την αρχιτεκτονική του CAS. Εκτελούμε δύο πειράματα σε υψηλό και χαμηλό φορτίο αλλά με καθυστερήσεις στο δίκτυο (σχήμα 4.5). Ο CAS ως κεντρικοποιημένη αρχή είναι πολύ πιθανόν να μην βρίσκεται κοντά στον χρήστη. Έτσι έχουμε εισάγει μια χρονοκαθυστέρηση σε κάθε πακέτο πριν εισαχθεί στο δίκτυο της τάξεως των 25ms. Το ποσοστό χρησιμοποίησης του επεξεργαστή για το χαμηλό φορτίο είναι 19.97% και για το υψηλό 53.79%.

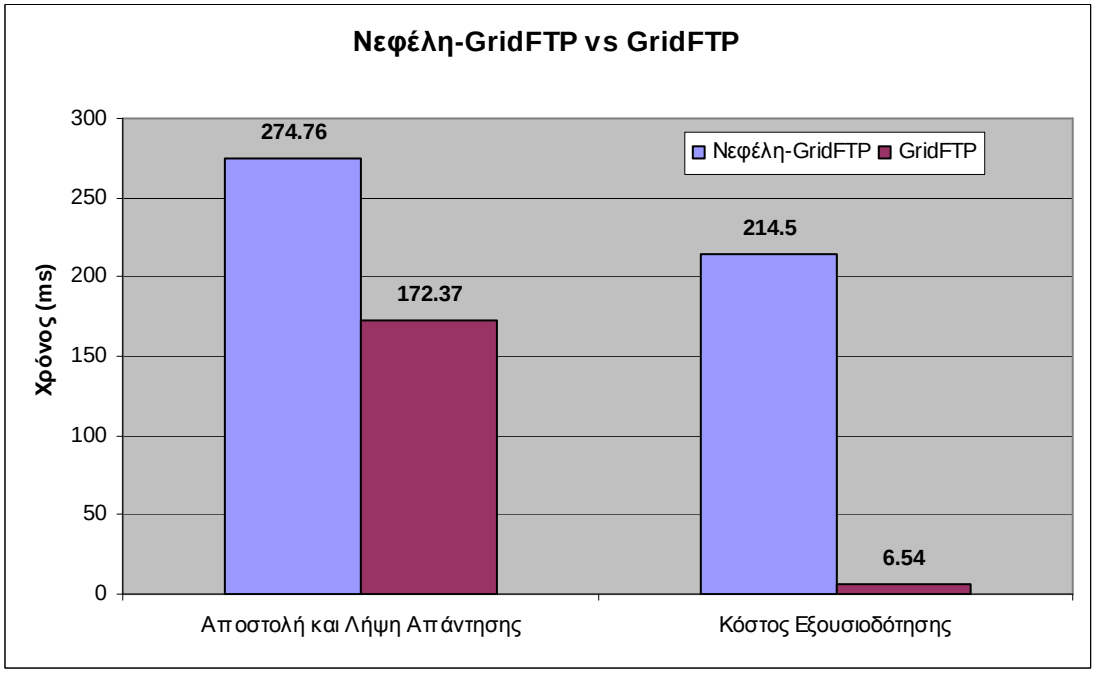


Σχήμα 4.5 CAS σε εξομοιωμένο δίκτυο (RTT 50ms) με υψηλό και χαμηλό φορτίο.

Εξουσιοδότηση

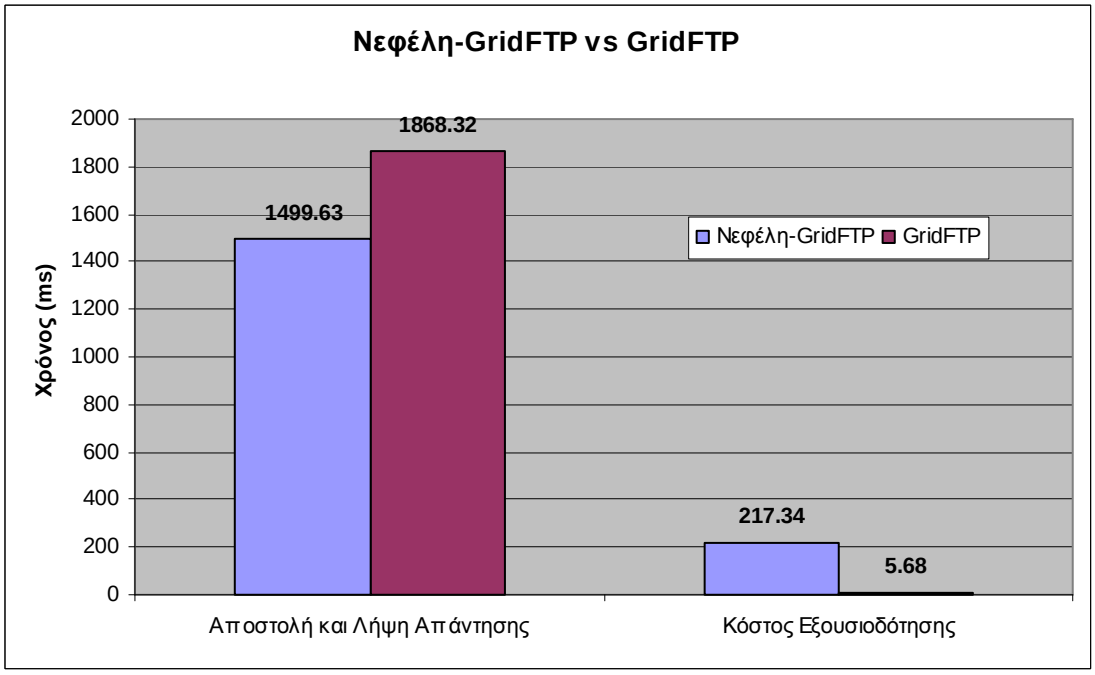
Αφού προμηθευτήκαμε το εκτεταμένο πιστοποιητικό τώρα θα κάνουμε μια προσπέλαση σε ένα απομακρυσμένο πόρο και τον διαχειρίζεται ο αρχικός GridFTP και ο Νεφέλη-GridFTP που συμβουλεύεται τον CAS-Διακομιστή. Αξιοσημείωτο είναι να αναφερθεί πως η βάση του CAS-Διακομιστή βρίσκεται σε διαφορετικό κόμβο από το διαχειριστή πόρου. Για να επικοινωνήσει μαζί του θα πρέπει να αρχικοποιήσει μια σύνδεση. Στην παρούσα υλοποίηση την αρχικοποιούμε ξεχωριστά για κάθε μια αίτηση σε τρία σημεία του προγράμματος και τον χρόνο δημιουργίας τον αφαιρούμε από τα συνολικά αποτελέσματα. Ο χρόνος δημιουργίας μιας σύνδεσης με την βάση ανέρχεται περίπου στα 300ms. Μελλοντικό μας σχέδιο είναι να αρχικοποιήσουμε την σύνδεση αυτή μια φορά και να την χρησιμοποιούν κάθε φορά όσοι την χρειάζονται αποφεύγοντας το κόστος της επαναληπτικής αρχικοποίησης της. Σε αυτό το σημείο θα πρέπει να τονίσουμε ότι με το εκτεταμένο πιστοποιητικό της νέας αρχιτεκτονικής μπορούμε να προσπελάσουμε οποιοδήποτε πόρο ανήκει στην κλάση αυτή. Η τροποποίηση αυτή μας αποδεσμεύει από το φορτίο απόκτησης ενός νέου εκτεταμένου πιστοποιητικού για κάθε διαφορετικό πόρο.

Στο πρώτο πείραμα συγκρίνουμε τον συνολικό χρόνο που κάνουμε για την αποστολή και την απάντηση μιας αίτησης καθώς και τον χρόνο που χρειάζεται για να ολοκληρωθεί η εξουσιοδότηση (σχήμα 4.6). Ο κάθε διακομιστής έχει εξυπηρετήσει χίλιες αιτήσεις που έχουν δημιουργηθεί από ένα κόμβο με μέσο ρυθμό άφιξης 0.3 sec. Σε κάθε περίπτωση διαβάζουμε ένα αρχείο μηδενικού μεγέθους. Η επιλογή αυτή έγινε για να μπορέσουμε να εκτιμήσουμε όσο το δυνατόν καλύτερα τον χρόνο εξουσιοδότησης. Ο Νεφέλη-GridFTP επιβαρύνεται με ένα κόστος των 215ms περίπου. Είναι λογικό ένα τέτοιο κόστος αφού επικοινωνεί με τον CAS-Διακομιστή για να συλλέξει όλες τις απαραίτητες πληροφορίες που χρειάζεται για να επιτρέψει ή να απαγορεύσει την εξουσιοδότηση. Μπορούμε να πληρώσουμε αυτό το κόστος αφού σε περίπτωση που θέλουμε να προσπελάσουμε κάποιο άλλο αρχείο δεν θα χρειαστεί να ξαναπληρώσουμε το αρχικό κόστος απόκτησης του πιστοποιητικού που ανέρχεται σε χρόνο μεγαλύτερο των δύο δευτερολέπτων. Η πληροφορία που περιέχουν τα πιστοποιητικά μπορούν να μας εξουσιοδοτήσουν να προσπελάσουμε οποιοδήποτε αρχείο σε όποιον διαχειριστή πόρων της κλάσης. Το ποσοστό χρησιμοποίησης του επεξεργαστή στον Νεφέλη-GrifFTP διακομιστή ανέρχεται στο 24,21% και στον αρχικό GridFTP 8,45%.



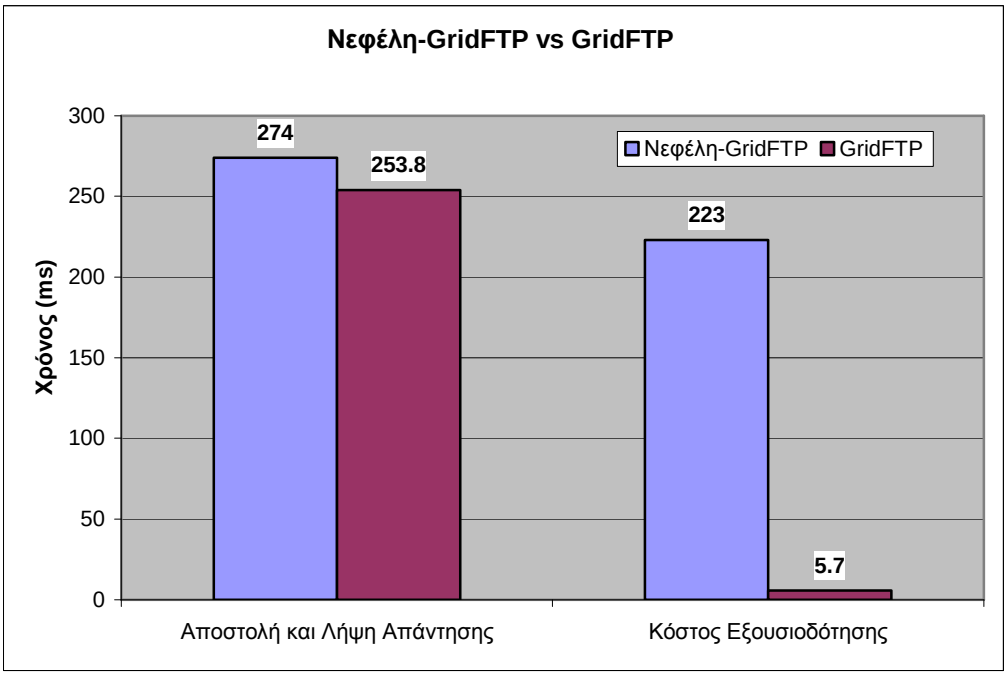
Σχήμα 4.6 Λήψη αρχείου σε τοπικό δίκτυο με χαμηλό φορτίο

Το επόμενο πείραμα έχει ολοκληρωθεί με το ίδιο ακριβώς φορτίο με την μόνη διαφορά ότι μεταξύ πελάτη και GridFTP υπάρχει η καθυστέρηση στο δίκτυο (σχήμα 4.7). Όπως είχαμε προαναφέρει ο χρόνος της απάντησης μεταξύ GridFTP και Νεφέλη-GridFTP είναι περίπου ο ίδιος. Έτσι ο μεν παλιός στο θέμα της εξουσιοδότησης είναι αρκετά πιο γρήγορος, ενώ στο θέμα της μεταφοράς καταναλώνεται χρόνος που στην δικιά μας αρχιτεκτονική χρησιμοποιείται για την εξουσιοδότηση. Το ποσοστό χρησιμοποίησης του επεξεργαστή που καταναλώθηκε στον Νεφέλη-GrifFTP διακομιστή ανέρχεται στο 24,06% και για τον αρχικό GridFTP 8,08%.



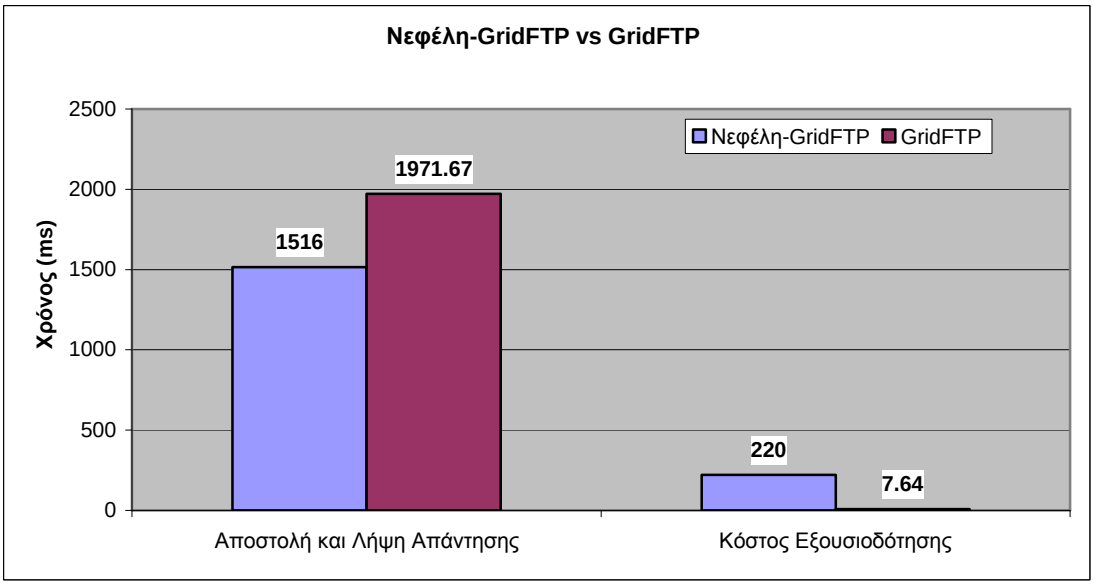
Σχήμα 4.7 Λήψη αρχείου σε εξομοιωμένο δίκτυο (RTT 50ms) με χαμηλό φορτίο

Στην επόμενη σειρά πειραμάτων αυξήσαμε τον ρυθμό υποβολής των ερωτημάτων. Το μέσο διάστημα μεταξύ των αιτήσεων ρυθμός μειώθηκε 0,15sec (σχήμα 4.8). Όπως είναι αναμενόμενο με ένα υψηλότερο φορτίο αυξάνεται και η κατανάλωση της επεξεργαστικής ισχύς καθώς και ο χρόνος της εξουσιοδότησης. Το ποσοστό χρησιμοποίησης του επεξεργαστή που καταναλώθηκε στον Νεφέλη-GrifFTP ανέρχεται στο 47.78% και για τον αρχικό GridFTP 16,06%.



Σχήμα 4.8 Λήψη αρχείου σε τοπικό δίκτυο με υψηλό φορτίο

Στο τελευταίο πείραμα έχουμε διατηρήσει τον ίδιο ρυθμό άφιξης αιτήσεων και έχουμε προσθέσει την χρονική καθυστέρηση στο δίκτυο (σχήμα 4.9). Η επεξεργαστική ισχύς που καταναλώθηκε στον Νεφέλη-GrifFTP διακομιστή ανέρχεται στο 46.9% και για τον αρχικό GridFTP 15,58%.



Σχήμα 4.9 Λήψη αρχείου σε εξομοιωμένο δίκτυο (RTT 50ms) και υψηλό φορτίο

4.3. Συμπεράσματα

Όπως διαπιστώσαμε το κόστος δημιουργίας και παραλαβής του εκτεταμένου πιστοποιητικού σε κάθε περίπτωση είναι δαπανηρό. Οι διαφορές για την απόκτηση του και στις δύο αρχιτεκτονικές είναι αμελητέες. Στη Νεφέλη το κόστος αυτό το πληρώνουμε μια φορά και όχι σε κάθε αίτηση που θα θελήσουμε να κάνουμε. Γι'αυτό η καινοτομία που έχουμε εισάγει στο σύστημα Νεφέλη είναι τα πιστοποιητικά αυτά να περιέχουν τις κλάσεις των οργανισμών και να μπορούν να χρησιμοποιηθούν σε κάθε Νεφέλη-GridFTP. Με αυτό τον τρόπο μπορούμε να έχουμε άμεση πρόσβαση σε οποιοδήποτε Νεφέλη-GridFTP ανήκει στην κλάση αυτή. Βέβαια το κόστος της εξουσιοδότησης μεταφέρεται σε κάθε Νεφέλη-GridFTP να έρθει σε επικοινωνία με τον CAS-Διακομιστή για να ολοκληρωθεί η διαδικασία.

ΚΕΦΑΛΑΙΟ 5. ΕΠΙΛΟΓΟΣ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΕΡΓΑΣΙΑ

5.1. Επίλογος

Συμπερασματικά οι υπάρχουσες πολιτικές ασφαλούς προσπέλασης σε περιβάλλοντα πλέγματα αντιμετώπιζαν περιορισμούς κλιμάκωσης λόγω του μεγάλου όγκου ενημερώσεων είτε μεταξύ των επιμέρους οργανισμών που συμμετέχουν στο πλέγμα ή μεταξύ των οργανισμών και μιας κεντρικής αρχής. Στην προσέγγιση που σχεδιάσαμε και υλοποιήσαμε, ο κάθε οργανισμός συντηρεί τοπικές πληροφορίες σύνθεσης για τις κλάσεις χρηστών που περιέχει και οργανισμών στους οποίους ανήκει καθώς και λίστες ελέγχου πρόσβασης για τους τοπικούς πόρους. Οι πληροφορίες που ανταλλάσσονται μεταξύ των διαφορετικών οργανισμών περιορίζονται στις ελάχιστες απαραίτητες για να επιβεβαιωθεί η δυνατότητα πρόσβασης ενός χρήστη σε έναν απομακρυσμένο πόρο και να ικανοποιηθεί η εκάστοτε αιτούμενη εξυπηρέτηση εφόσον επιτρέπεται.

Στην προσέγγιση που ακολουθούμε, θέτουμε ως βασικό στόχο να μειώσουμε στο ελάχιστο απαραίτητο το φορτίο ενημέρωσης μεταξύ των διαφορετικών οργανισμών. Για το σκοπό αυτό κρατούμε σε κάθε οργανισμό τις πληροφορίες που προσδιορίζουν τις κλάσεις στις οποίες ανήκει ο κάθε τοπικός χρήστης. Αντίστοιχα, περιορίζουμε σε κάθε διαχειριστή πόρων την πληροφορία ελέγχου προσπέλασης σε κάθε κλάση στους οποίους ανήκει ο διαχειριστής πόρων. Η βασική ακολουθία βημάτων για την απομακρυσμένη προσπέλαση ενός πόρου από ένα χρήστη περιλαμβάνει τη λήψη ενός πιστοποιητικού από τον τοπικό διαχειριστή χρηστών που προσδιορίζει τις κλάσεις στις οποίες ανήκει ο συγκεκριμένος χρήστης. Η αίτηση απομακρυσμένης προσπέλασης του χρήστη με τη βοήθεια του πιστοποιητικού μεταφέρει στον απομακρυσμένο διακομιστή αρχείων την πληροφορία για τον απαραίτητο έλεγχο

προσπέλασης. Ο διακομιστής αρχείων συγκρίνει τις κλάσεις του χρήστη με αυτές στις οποίες παρέχεται η αιτούμενη πρόσβαση και είτε αποδέχεται το αίτημα και επιστρέφει τα δεδομένα ή το απορρίπτει.

5.2. Μελλοντική εργασία

Στα μελλοντικά μας σχέδια εντάσσεται η μείωση του κόστους της αίτησης της απομακρυσμένης πρόσβασης. Ο Νεφέλη-GridFTP επιβαρύνεται με ένα φορτίο λόγω της σύνδεσης που πρέπει να κάνει με τον CAS-Διακομιστή. Σκοπός μας είναι να αναπτύξουμε ένα τρόπο όπου η αρχικοποίηση της σύνδεσης αυτής θα γίνεται μια φορά με την έναρξη του Νεφέλη-GridFTP και θα μπορεί να χρησιμοποιηθεί από οποιονδήποτε την ζητήσει. Έχει γίνει μια πρώτη υλοποίηση που έχει μειώσει δραματικά το κόστος εξουσιοδότησης (12ms) αλλά χρειάζεται επιπλέον εκσφαλμάτωση.

ΑΝΑΦΟΡΕΣ

[1] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell' Agnello, A. Frohner, K. Lorentey, and F. Spataro. From gridmap-file to voms: managing authorization in a grid environment. *Future Generation Computer Systems*, 21:549–558, 2005.

[2] E. Belani, A. Vahdat, T. Anderson, and M. Dahlin. The crisis wide area security architecture. In *Usenix Security Symposium*, pages 15–30, San Antonio, TX, 1998.

[3] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke. A security architecture for computational grids. In *ACM Conference on Computer and Communication Security*, pages 83–92, San Francisco, CA, Nov. 1998.

[4] Y. Fu, J. Chase, B. Chun, S. Schwab, and A. Vahdat. Sharp: An architecture for secure resource peering. In *ACM Symposium on Operating Systems Principles*, pages 133–148, Bolton Landin, NY, Oct. 2003.

[5] The Globus Alliance. *GT 4.2.0 CAS Developer's Guide*.

[6] The Globus Alliance. *GT 4.2.0 GridFTP Developer's Guide.*

[7] M. Kaminsky, G. Savvides, D. Mazieres, and M. F. Kaashoek. Decentralized user authenication in a global file system. In *ACM Symposium on Operating Systems Principles*, pages 60–73, Bolton Landing, NY, 2003.

[8] A. D. Keromytis and J. M. Smith. Requirements for scalabale access control and security management architectures. *ACM Transactions on Internet Technologies*, 7(2):1–22, May 2007.

[9] A. W. Leung, E. L. Miller, and S. Jones. Scalable security for petascale parallel file systems. In *ACM/IEEE Conference on Supercomputing (SC)*, 2007.

[10] J. Linn. *RFC 2743: The Generic Security Service API Version 2 update 1*. The Internet Society, Jan. 2000.

[11] D. Mazieres, M. Kaminsky, M. F. Kaashoek, and E. Wichel. Separating key management from file system security. In *ACM Symposium on Operating Systems Principles*, pages 124–139, Kiawah Island, SC, Dec. 1999.

[12] S. Miltchev, J. M. Smith, V. Prevelakis, A. Keromytis, and S. Ioannidis. Decentralized access control in distributed file sysems. *ACM Computing Surveys*, 40(3),Aug. 2008.

[13] B. C. Neuman and T. Ts'o. Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38, Sept. 1994.

[14] B. Pawlowski, D. Noveck, D. Robinson, and R. Thurlow. The nfs version 4 protocol. In *International System Administration and Networking Conference*, Maastricht, Netherlands, 2000

[15] L. Pearlman, V. Welch, I. Foster, and C. Kesselman. A community authorization service for group collaboration. In *IEEE Intl Workshop on Policies for Distributed Systems and Networks*, pages 50–59, Monterey, CA, 2002.

[16] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, and T. Scavo. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. Organization for the Advancement of Structured Information Standards (OASIS), Feb. 2007

[17] R. S. Sandhu and E. J. Coyne. Role-based access control models. *Computer*, 29(2):38–47, Feb. 1996.

[18] T. Scavo and V. Welch. A grid authorization model for science gateways. In *International Workshop on Grid Computing Environments*, Reno, NV, Nov. 2007.

[19] D. Shands, R. Yee, J. Jacobs, and E. J. Sebes. Secure virtual enclaves: Supporting coalition use of distributed application technologies. *ACM Transactions on Information and System Security*, 4:103–133, May 2000.

[20] V. Welch and the Globus Security Team. Globus toolkit version 4 grid security infrastructure: A standards perspective. Technical report, The Globus Alliance, 2005. Version 4.

[21] D.Chen, A.Demichev, D.Foster, V.Kalyaev A.Kryukov, M.Lamanna, V. Rose, R.Rocha, C.Wang OGSA Globus Toolkit 3 evaluation activity at CERN Nuclear Instruments and Methods in Physics Research July 2004.

[22] Net:Netem http://www.linuxfoundation.org/en/Net:Netem

ΣΥΝΤΟΜΟ ΒΙΟΓΡΑΦΙΚΟ

Ο Νικόλαος Μπουντουρόπουλος γεννήθηκε το 1981 στην Κομοτηνή όπου και ολοκλήρωσε τις λυκειακές σπουδές του το 1999. Το 2000 ξεκίνησε τις σπουδές του στο Τμήμα Μαθηματικών του Πανεπηστημίου Ιωαννίνων τις οποίες ολοκλήρωσε το 2006. Από τον Σεπτέμβριο του 2006 είναι μεταπτυχιακός φοιτητής του Τμήματος Πληροφορικής του Πανεπιστημίου Ιωαννίων. Τα ερευνητικά του ενδιαφέροντα εστιάζονται σε θέματα ασφάλειας και κρυπτογραφίας.