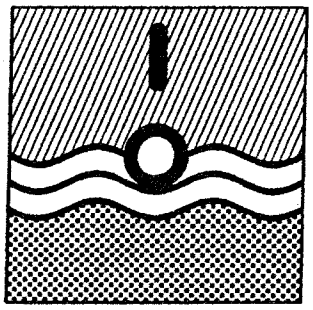
ΥΔΡΟΣΚΟΠΙΟ

ΠΡΟΓΡΑΜΜΑ STRIDE ΕΛΛΑΣ

ΔΗΜΙΟΥΡΓΙΑ ΕΘΝΙΚΗΣ ΤΡΑΠΕΖΑΣ
ΥΔΡΟΛΟΓΙΚΗΣ ΚΑΙ
ΜΕΤΕΩΡΟΛΟΓΙΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΟΜΕΑΣ ΥΔΡΑΥΛΙΚΗΣ ΚΑΙ ΤΕΧΝΙΚΗΣ ΠΕΡΙΒΑΛΛΟΝΤΟΣ

ARISTOTLE UNIVERSITY OF THESSALONIKI
FACULTY OF TECHNOLOGY
DIVISION OF HYDRAULICS AND ENVIRONMENTAL ENGINEERING



ΑΝΑΠΤΥΞΗ ΓΕΝΙΚΟΥ ΛΟΓΙΣΜΙΚΟΥ

Ανάπτυξη - υλοποίηση - τεκμηρίωση χρέωσης και παρακολούθησης λογ/σμών για τοπική και απομακρυσμένη πρόσβαση

GENERAL SOFTWARE DEVELOPMENT

Development - realisation - documentation of security, charging policy and account monitoring for local and remote access

Π. Αναστασιάδης, Ν. Γεωργιάδης, Σ. Λαδάς
Π. Λατινόπουλος, Κ. Κατσιφαράκης,

P. Anastasidis, N. Georgiadis, S. Ladas
P. Latinopoulos, K. Katsifarakis

Αριθμός τεύχους 2/23
Report number

HYDROSCOPE

STRIDE HELLAS PROGRAMME

DEVELOPMENT OF A NATIONAL DATA BANK FOR HYDROLOGICAL AND METEOROLOGICAL INFORMATION

ΘΕΣΣΑΛΟΝΙΚΗ - ΔΕΚΕΜΒΡΙΟΣ 1993
THESSALONIKI - DECEMBER 1993

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Το τεύχος αυτό αναφέρεται στην εργασία 4 της ανάπτυξης γενικού λογισμικού, που έχει τίτλο "Ανάπτυξη - υλοποίηση - τεκμηρίωση χρέωσης και παρακολούθησης λογαριασμών για τοπική και απομακρυσμένη πρόσβαση". Περιγράφονται α) το λογισμικό που αναπτύχθηκε για την ασφάλεια τόσο του χρήστη όσο και της Βάσης Δεδομένων β) τα δικαιώματα και οι υποχρεώσεις των διαφόρων ομάδων χρηστών και γ) η διαδικασία παρακολούθησης των εργασιών του χρήστη για τη δίκαια χρέωσή του.

ABSTRACT

This issue deals with task 4 of General Software Development under the title "Development - realisation - documentation of security, charging policy and account monitoring for local and remote access". The following entities are described: i) software, which has been developed for the security of both the database and the user ii) the rights and obligations of the various user groups and iii) the process of user activities monitoring in order to achieve fair charging.

1. ΕΙΣΑΓΩΓΗ

Στόχοι Ασφάλειας ΥΔΡΟΣΚΟΠΙΟΥ

1. Σωστή Διαχείριση και Ακεραιότητα του Συστήματος (Unix, Ingres, DataBase-Hydroscope)

2. Ασφαλής Πρόσβαση του Χρήστη στο Λογαριασμό

3. Ασφαλή Πρόσβαση στην Βάση Δεδομένων και Λογισμικού

Συνδυάζοντας τους τρεις στόχους μπορεί να υλοποιηθεί η ασφαλής διαχείριση των δεδομένων.

2. ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Σκοπός της πολιτικής που ακολουθείται ως προς την Ασφάλεια του Υδροσκοπίου είναι να διατηρηθεί η απλότητα και η λειτουργικότητα στη χρήση της εφαρμογής χωρίς να παραβιάζονται τα δικαιώματα άλλων χρηστών ή να αλλοιώνονται τα δεδομένα.
Η πολιτική αυτή δημιουργεί απαιτήσεις για δυο επίπεδα ασφάλειας:

α. χρήστη και
β. βάσης δεδομένων.

2.1. Επίπεδο Χρήστη

Κάθε χρήστης για να χρησιμοποιήσει το Υδροσκόπιο πρέπει να έχει λογαριασμό στο κόμβο (workstation) της υπηρεσίας του.
Ο χρήστης ανήκει σε μια από τις ακόλουθες Γενικές Ομάδες, όπως προτάθηκε σε προηγούμενη εργασία (Παπακώστας Α., Πιπιλή Κ.):

1. Κοινό: Χρήστες που δεν απασχολούνται άμεσα στη βάση δεδομένων. Το μόνο δικαίωμα πρόσβασης που τους χορηγείται είναι να βλέπουν (Select) τα δεδομένα, επεξεργασμένα ή μη επεξεργασμένα.

2. Εισαγωγέας Δεδομένων: Στην ομάδα αυτή ανήκουν οι χρήστες που έχουν αναλάβει την εισαγωγή των δεδομένων στη βάση (select / insert).

3. Ελεγκτής Εισαγωγής: Στη ομάδα αυτή ανήκουν οι χρήστες που έχουν αναλάβει τον έλεγχο των εισαχθέντων δεδομένων. Τα δεδομένα αυτά εξετάζονται ως προς την ορθότητα τους και οι χρήστες έχουν το δικαίωμα εμφάνισης, εισαγωγής, τροποποίησης και διαγραφής των δεδομένων (select / insert / update / delete).

4. Διαχειριστής Κόμβου: Στην ομάδα αυτή ανήκουν οι χρήστες που είναι υπεύθυνοι για τη σωστή λειτουργία και διαχείριση του κόμβου και έχουν το δικαίωμα εμφάνισης, εισαγωγής, τροποποίησης και διαγραφής για όλα τα αντικείμενα της ΒΔ (select / insert / update / delete). Ο ρόλος τους είναι ταυτόσημος με εκείνου του Διαχειριστή Βάσεως Δεδομένων (ΔΒΔ).

Στη συνέχεια παρουσιάζονται οι ομάδες όπως επίσης και τα δικαιώματα τους σε σχέση με την ΒΔ.
Αρχικά ο χρήστης πρέπει να ζητήσει από το Διαχειριστή του κόμβου τη δημιουργία λογαριασμού.
Το επόμενο βήμα του χρήστη είναι να εισέλθει στον λογαριασμό του εισάγοντας το χαρακτηριστικό όνομα του (User Name), όπως επίσης και ένα σύνθημα-password.
Με τον τρόπο αυτό αποκλείεται η είσοδος στο σύστημα τρίτων ατόμων. Το πιο πάνω στάδιο είναι το σημαντικότερο τόσο για την ασφάλεια του συστήματος όσο και για την προστασία του χρήστη και των δικαιωμάτων του. Αντίστοιχα όσο πιο πολλά δικαιώματα έχει ο χρήστης, τόσο η ευθύνη του είναι μεγαλύτερη για τη διαφύλαξη των στοιχείων.

2.2. Επίπεδο Βάσης Δεδομένων (ΒΔ)

Ο χρήστης δεν μπορεί να έχει πρόσβαση στους πίνακες της ΒΔ από το λειτουργικό σύστημα παρά μόνο μέσα από την Ingres (εφόσον βέβαια του επιτρέπεται η πρόσβαση) και από την εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ. Η βάση δεδομένων Ingres που επιλέχθηκε για το Υδροσκόπιο παρέχει στο Διαχειριστής Βάσης Δεδομένων ένα πολύ ικανοποιητικό σύστημα ασφάλειας, όπως θα περιγραφεί παρακάτω.

3. ΓΕΝΙΚΑ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΚΟΜΒΟΥ - ΔΙΚΤΥΟΥ

3.1. Ασφάλεια Κόμβου

Η ασφάλεια του ΥΔΡΟΣΚΟΠΙΟΥ στηρίζεται στη σωστή ασφάλεια σε κάθε κόμβο (workstation). Για την υλοποίηση της, τρεις ρόλοι χρηστών με τα αντίστοιχα δικαιώματα είναι απαραίτητοι:

α. ο διαχειριστής του λειτουργικού συστήματος (System administrator)
β. ο διαχειριστής της Ingres (Ingres administrator) και
γ. ο διαχειριστής της βάσης δεδομένων κόμβου (Database administrator).

Οι παραπάνω ρόλοι είναι δυνατόν να συγκεντρωθούν σε ένα φυσικό πρόσωπο για να απλοποιηθούν οι διαδικασίες της χορήγησης δικαιωμάτων χρήσης της βάσης δεδομένων.

3.1.1. Διαχειριστής Λειτουργικού Συστήματος (ΔΛΣ)

Ευθύνη του ΔΛΣ είναι η σωστή λειτουργία των μηχανών (hardware) και του λογισμικού (software) του κόμβου όπως επίσης και η επίβλεψη και εξυπηρέτηση των χρηστών του συστήματος. Ο ΔΛΣ έχει στην κατοχή του το λογαριασμό "root" και συνεργάζεται με το Διαχειριστή της Ingres για την ομαλή και απρόσκοπτη λειτουργία μεταξύ του λειτουργικού συστήματος και της εγκατάστασης της Ingres.
Είναι υποχρέωση του ΔΛΣ για την εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ εκτός από τις άλλες παραπάνω εργασίες, να ανοίγει λογαριασμό (open an account) στον χρήστη της εφαρμογής και να δίνει τον κωδικό χρήσης (user name) και το σύνθημα (password).
Ανάλογα με το περιβάλλον (shell) που θα δουλεύει ο χρήστης πρέπει να προστεθούν κάποιες εντολές στο αρχείο του για την εύκολη πρόσβασή του στην Ingers. Το αρχείο, που το αποκτά ο χρήστης με τη δημιουργία του λογαριασμού του, είναι το .profile στο Bourne ή K shell και .login στο C shell. Για παράδειγμα, οι εντολές που προστίθενται στο αρχείο .profile είναι οι ακόλουθες:

```
$II-SYSTEM=/usr/ingres
export II-SYSTEM
PATH=$II-SYSTEM/ingres/bin:$II-SYSTEM/ingres/utility:$PATH
export PATH
```

Επίσης εάν δε θα επιτραπεί στον συγκεκριμένο χρήστη να χρησιμοποιεί τα εργαλεία της Ingres τότε θα πρέπει να προστίθενται και μερικές ακόμη εντολές έτσι ώστε ο χρήστης κατά την είσοδο στον λογαριασμό του αμέσως να τρέχει η εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ χωρίς να παρεμβάλετε το περιβάλλον του λειτουργικού. Αυτές οι εντολές μπορεί να είναι το κάλεσμα ενός "script" που ανεβάζει το περιβάλλον "Xwindows" και εισάγει το χρήστη στην εφαρμογή.

Οι χρήστες του κόμβου χωρίζονται σε ομάδες για την καλύτερη οργάνωση κόμβου. Οι ομάδες χαρακτηρίζονται από αριθμούς αντί για ονόματα. Π.χ. ο διαχειριστής της Ingres ανήκει στην ομάδα με αριθμό 1000, ενώ ο διαχειριστής της ΒΔ στην ομάδα με αριθμό 2000. Ο ΔΛΣ δημιουργεί επίσης και άλλες δύο ομάδες. Στην πρώτη ομάδα ανήκουν οι τοπικοί χρήστες του κόμβου (με αριθμό 3000) και στη δεύτερη οι απομακρυσμένοι χρήστες (με αριθμό 5000).

3.1.2. Διαχειριστής Ingres (ΔΙ)

Ο ΔΙ είναι υπεύθυνος για την ομαλή λειτουργία της εγκατάστασης της Ingres (εγκατάσταση αρχείων, ξεκίνημα, σταμάτημα και επίβλεψη "servers", ξεκίνημα και σταμάτημα της Ingres, ορισμός παραμέτρων περιβάλλοντος), όπως επίσης για τη δήλωση χρηστών και τη χρησιμοποίηση της Ingres.
Οι υποχρεώσεις του διαχειριστή της Ingres, για την εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ, είναι να επιτρέψει στον χρήστη την πρόσβαση του στην Ingres, όπως επίσης και η δημιουργία των ομάδων που ανήκουν οι χρήστες (θα αναλυθούν λεπτομερέστερα παρακάτω).
Ο διαχειριστής μέσω της accessdb (Ingres utility) εκτός των άλλων:

i) επιτρέπει την πρόσβαση του χρήστη στην Ingres δίνοντας του τα ελάχιστα δικαιώματα, δηλαδή χωρίς δικαίωμα δημιουργίας βάσης δεδομένων (Create Database), διαχειριστή (Super User), ενημέρωσης των καταλόγων του συστήματος (Update System Catalogs), και τοποθέτησης "σημαιών" μέσα στην Ingres (Set Trace Flags), όπως επίσης τη δήλωση του χρήστη σε "default group" (βλέπε παρακάτω),

ii) τροποποιεί τα δικαιώματα του χρήστη,

iii) διαγράφει έναν υπάρχοντα χρήστη,

vi) βλέπει τη λίστα των δηλωμένων χρηστών που χρησιμοποιούν την Ingres και

v) επιτρέπει την πρόσβαση του χρήστη σε μια "private" βάση δεδομένων.

Εάν ο διαχειριστής θέλει να εισαγάγει περισσότερους από ένα χρήστες, τότε μπορεί να χρησιμοποιήσει το αρχείο "users" που βρίσκεται κάτω από το $II-SYSTEM/ingres/files. Μέσα σε αυτό το αρχείο εισάγει μαζικά τους χρήστες δίνοντας τα αντίστοιχα δικαιώματα, και στη συνέχεια αντιγράφει τις αλλαγές του αρχείου "users" μέσα στους καταλόγους του συστήματος (βλέπε DBA manual, 2-11).

Δεύτερη υποχρέωση του ΔΙ είναι η δημιουργία των ομάδων χρηστών.
Η δημιουργία ομάδων χρηστών αποτελεί μεγάλη ευκολία για την ασφάλεια της βάσης γιατί ο ΔΒΔ (όπως θα διευκρινιστεί παρακάτω) μπορεί να χορηγήσει δικαιώματα στην ομάδα για αντικείμενα της βάσης δεδομένων ή ακόμη και στην ίδια τη βάση. Μόνον ο ΔΙ μπορεί να δημιουργήσει και να καταστρέψει "group", ή να ορίσει τους χρήστες που ανήκουν σε ένα συγκεκριμένο "group" μέσα από την τροποποίηση των δεδομένων της Ingres "iidbdb".
Η δημιουργία ενός "group" υλοποιείται με την εντολή "create group". Π.χ.

create group groupid (όπου groupid το όνομα του "group")
προαιρετικό with users = (userid, ...) (όπου userid το όνομα του χρήστη)

Η πρόσθεση ή αφαίρεση χρηστών από ένα "group" υλοποιείται με την εντολή "alter group". Π.χ.

alter group grouid
και add users (userid, ...)
ή drop users (userid, ...)

ή drop all (διαγραφή όλων των χρηστών που ανήκουν στο αντίστοιχο "group")

Η καταστροφή ενός "group" υλοποιείται με την εντολή "drop group" με την προϋπόθεση ότι στην ομάδα αυτή δεν υπάρχει κανένας χρήστης δηλαδή έχουν διαγραφεί όλοι. Π.χ.

drop group grouid, ...

Ο ΔΙ αλλά και οποιοσδήποτε χρήστης μπορεί από τους πίνακες του συστήματος iiusergroup ή iiuser που βρίσκεται μέσα στην iidbdb να δει ποιες ομάδες υπάρχουν και ποιοι χρήστες ανήκουν στις αντίστοιχες ομάδες.

Ο ΔΙ πρέπει να έχει δηλωμένους στην Ingres τους ακόλουθους χρήστες:

root:	διαχειριστής του κόμβου,
ingres:	διαχειριστής της Ingres (δηλαδή τον εαυτό του),
hydro:	διαχειριστής της ΒΔ του ΥΔΡΟΣΚΟΠΙΟΥ,
hydronet:	διαχειριστής του δικτύου και της κατανεμημένης ΒΔ του ΥΔΡΟΣΚΟΠΙΟΥ.

Ακολουθούν δώδεκα απομακρυσμένοι χρήστες που πρέπει να βρίσκονται σε κάθε κόμβο για να μπορούν οι χρήστες των άλλων κόμβων να έχουν πρόσβαση στην εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ. Κάθε τέτοιος χρήστης μπορεί να έχει μέχρι δέκα τον αριθμό (από 0 μέχρι 9) λογαριασμούς στον κόμβο. Ο τελευταίος αριθμός (9) είναι κατειλημμένος από ένα "δαίμονα" (daemon) που σκοπό έχει να ενημερώνει τους πίνακες που ανήκουν στις διαχειριστικές πληροφορίες της ΒΔ στους απομακρυσμένους κόμβους. Οι απομακρυσμένοι αυτοί χρήστες είναι οι ακόλουθοι:

ntua0..9:	κόμβος ΕΜΠ (5001-5009),
nms0..9:	κόμβος ΕΜΥ (5010-5019),
ma0..9:	κόμβος (5020-5029),
meppw0..9:	κόμβος ΥΠΕΧΩΔΕ (5030-5039),
noa0..9:	κόμβος ΕΑΑ (5040-5049),
ppc0..9:	κόμβος ΔΕΥ (5050-5059),
wssca0..9:	κόμβος ΕΥΔΑΠ (5060-5069),
ua0..9:	κόμβος ΕΚΠΑ (5070-5079),
miet0..9:	κόμβος ΥΒΕΤ (5080-5089),
autdhee0..9:	κόμβος ΑΠΘΤΥΤΠ (5090-5099),
autde0..9:	κόμβος ΑΠΘΕΤ (5100-5109),
nrcpsd0..9:	κόμβος ΕΚΕΦΕΔ (5110-5119).

Οι ομάδες του ΥΔΡΟΣΚΟΠΙΟΥ που πρέπει να δημιουργηθούν από το ΔΙ είναι οι ακόλουθες:

hydro: στην ομάδα αυτήν ανήκουν ο διαχειριστής του συστήματος, ο διαχειριστής της Ingres και ο διαχειριστής της ΒΔ,

hrusers: στην ομάδα αυτήν ανήκουν όλοι οι χρήστες των απομακρυσμένων κόμβων όπως αυτοί ορίστηκαν παραπάνω,

husers: στην ομάδα αυτήν ανήκουν όλοι οι τοπικοί χρήστες του κόμβου που έχουν δικαίωμα χρήσης της εφαρμογής του ΥΔΡΟΣΚΟΠΙΟΥ,

hdatainsert: στην ομάδα αυτήν ανήκουν χρήστες που έχουν δικαίωμα εισαγωγής δεδομένων,

hdataupdate: στην ομάδα αυτήν ανήκουν χρήστες που έχουν δικαίωμα ενημέρωσης δεδομένων,

hadmininsert: στην ομάδα αυτήν ανήκουν χρήστες που έχουν δικαίωμα εισαγωγής δεδομένων και εισαγωγής άλλων στοιχείων που αφορούν τη διαχείριση του ΥΔΡΟΣΚΟΠΙΟΥ (η ομάδα αυτή έχει περισσότερα δικαιώματα από την ομάδα hdatainsert),

hadminupdate: στην ομάδα αυτήν ανήκουν χρήστες που έχουν δικαίωμα ενημέρωσης δεδομένων όπως επίσης ενημέρωσης άλλων στοιχείων που έχει εισάγει η ομάδα hadmininsert (η ομάδα αυτή έχει περισσότερα δικαιώματα από την ομάδα hdataupdate).

Αναλυτικά τα δικαιώματα κάθε ομάδας περιγράφονται στην παρακάτω ενότητα. Ο διαχειριστής της ΒΔ είναι υπεύθυνος να δώσει δικαιώματα για τη δική του ΒΔ στην κάθε αντίστοιχη ομάδα.

3.2 Διαχειριστής Βάσης Δεδομένων (ΔΒΔ)

ΔΒΔ ονομάζεται ο δημιουργός της βάσης δεδομένων. Δικαίωμα της δημιουργίας μιας βάσης δεδομένων δίνει ο ΔΙ όταν ορίζει τα δικαιώματα του συγκεκριμένου χρήστη στην Ingres.
Ευθύνη του ΔΒΔ είναι να δώσει τα κατάλληλα προνόμια στους χρήστες κατά την πρόσβαση τους στη δική του βάση δεδομένων όπως επίσης και στα αντικείμενα που βρίσκονται μέσα σε αυτήν (tables, views, και procedures).
Επίσης, ο ΔΒΔ μπορεί να δημιουργήσει και να καταστρέψει μια βάση δεδομένων που δημιούργησε, να συντηρήσει τη βάση δεδομένων, να δημιουργήσει αντικείμενα βάσης δεδομένων για τους άλλους χρήστες, και έχει την ευθύνη του "back up".

Υποχρέωση του ΔΒΔ για την εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ είναι να δώσει προνόμια στα "groups" (ή αν θελήσει και σε μεμονωμένους χρήστες) για την πρόσβαση είτε στη βάση δεδομένων είτε στους πινάκες της.

Τονίζεται ότι ο ΔΒΔ είναι ο ιδιοκτήτης της ΒΔ της εφαρμογής. Η ΒΔ είναι "private" και ΔΒΔ έχει την πλήρη ευθύνη.
Στην εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ η τοπική ΒΔ ονομάζεται db0.

Μέσα από τη ΒΔ ο ΔΒΔ μπορεί να δώσει δικαίωμα "grant" σε ένα ή περισσότερα αντικείμενα. Η γενική σύνταξη της εντολής είναι

grant "δικαίωμα" on "αντικείμενο" to "όνομα"

Ο ΔΒΔ είναι υπεύθυνος για τον έλεγχο της απόδοσης των δικαιώματος "grant" μόνο στους συγκεκριμένους και εγκεκριμένους χρήστες ή ομάδες.

Θα εξεταστούν παρακάτω δύο περιπτώσεις:
οταν το αντικείμενο (object) είναι πίνακας και
όταν το αντικείμενο είναι η ίδια η βάση δεδομένων.

Αλλα αντικείμενα που ο ΔΒΔ είναι μπορεί δώσει προνόμια είναι:

οι όψεις (views),
οι διαδικασίες (procedures) και
τα γεγονότα (events).

Προνόμια που μπορούν να δοθούν σε ένα πίνακα σε "group" ή σε χρήστη και θα χρησιμοποιηθούν στην εφαρμογή είναι τα ακόλουθα:

-- select (επιλογή)
-- insert (εισαγωγή)
-- delete (διαγραφή)
-- update (ενημέρωση)
-- all (σε όλα από τα παραπάνω)

Τα παραπάνω προνόμια θα δοθούν από το ΔΒΔ στα αντίστοιχα "groups" για την απόκτηση αντίστοιχων δικαιωμάτων.

: Προνόμια που μπορούν να δοθούν στο σύνολο της ΒΔ και θα χρησιμοποιηθούν στην εφαρμογή είναι τα ακόλουθα:

-- query-row-limit (μέγιστος αριθμός γραμμών που επιτρέπεται να επιστρέφει μια ερώτηση (query))
-- create-table (δημιουργία πινάκων στον χρήστη ή "group")

Ο ΔΒΔ αλλά και κάθε χρήστης μπορεί να δει τα δικαιώματα του σε ένα ή περισσότερους πίνακες χρησιμοποιώντας την εντολή "help permit" και το όνομα του πίνακα. Τα αντίστοιχα δικαιώματα ενός χρήστη για το σύνολο της ΒΔ που αναφέρθηκαν παραπάνω μπορούν να δοθούν καλώντας την "function" "dbmsinfo". Π.χ.

select dbmsinfo('request-name')

όπου "request-name" μπορεί να είναι το "query-row-limit" ή "create table".

Επίσης στους πίνακες του συστήματος "iiusergroup" και "iidbprivileges" που βρίσκονται στην βάση "iidbdb" υπάρχουν σχετικές πληροφορίες για τα δικαιώματα που δόθηκαν από το ΔΒΔ στους χρήστες.

Η κατάργηση των δικαιωμάτων σε έναν ή περισσότερους πίνακες πραγματοποιείται με την εντολή "drop permit on".
Η γενική σύνταξη της εντολής είναι:

drop permit on "πίνακας" "ακέραιος" ή all

όπου "ακέραιος" είναι κάποιο συγκεκριμένο δικαίωμα, αριθμός που δόθηκε από την εντολή "help permit". Η επιλογή "All" χρησιμοποιείται για την κατάργηση κάθε δικαιώματος του χρήστη ή της ομάδας στον συγκεκριμένο πίνακα.
Αντίστοιχα, η κατάργηση των δικαιωμάτων στο σύνολο της ΒΔ πραγματοποιείται με την εντολή "revoke". Η γενική σύνταξη της εντολής είναι;

revoke "δικαίωμα", ... ή all
on database "ΒΔ", ...
from user ή group "όνομα", ...

Η κατάργηση δικαιωμάτων στο σύνολο της ΒΔ γίνεται μόνον από το ΔΙ και ΔΒΔ μέσα από τη βάση "iidbdb".

Τα παραπάνω δικαιώματα πρέπει να διανεμηθούν στις τρεις μεγάλες ενότητες πληροφοριών της ΒΔ.
Οι ενότητες είναι:
Πληροφορίες σχετικές με τις εφαρμογές του ΥΔΡΟΣΚΟΠΙΟΥ,
Διαχειριστικές πληροφορίες της ΒΔ και
"πραγματικά" δεδομένα.

Πίνακες με πληροφορίες σχετικές με τις εφαρμογές του ΥΔΡΟΣΚΟΠΙΟΥ.

Για αυτήν την κατηγορία οι ομάδες husers και hrusers όπως και όλες οι άλλες που αναφέρθηκαν προηγουμένως έχουν δικαίωμα επιλογής δεδομένων (select) από οποιοδήποτε πίνακα.

Ειδικά σε δύο πινάκες (stations-groups και series-macros) η ομάδα husers έχει δικαίωμα της εισαγωγής, ενημέρωσης και διαγραφής (insert / update / delete) επειδή αφορούν ενέργειες προσωπικές του χρήστη καθώς χρησιμοποιεί την εφαρμογή.

Πίνακες με διαχειριστικές πληροφορίες της ΒΔ.

Για αυτήν την κατηγορία οι ομάδες husers και hrusers όπως και όλες οι άλλες, έχουν δικαίωμα επιλογής δεδομένων (select) από όλους τους πίνακες.
Η ομάδα hadmininsert έχει δικαίωμα εισαγωγής (insert) σε όλους τους πίνακες εκτός αυτών που τελειώνουν σε "-rmt".
Η ομάδα hadmininupdate έχει δικαίωμα εισαγωγής (insert), ενημέρωσης (update) και διαγραφής (delete) σε όλους τους πίνακες εκτός αυτών που τελειώνουν σε "-rmt". Τέλος, η ομάδα hdataupdate έχει δικαίωμα εισαγωγής (insert), ενημέρωσης (update) και διαγραφής (delete) μόνο στους πίνακες "timeseries" και "events".

Πίνακες με "πραγματικά" δεδομένα.

Για αυτήν την κατηγορία οι ομάδες husers και hrusers όπως και όλες οι άλλες έχουν δικαίωμα επιλογής δεδομένων (select) από όλους τους πίνακες. Εξαιρούνται οι πίνακες με κατάληξη "-tmp" όπου η ομάδα hrusers δεν έχει δικαίωμα επιλογής δεδομένων ενώ αντίθετα η ομάδα husers έχει εκτός του δικαιώματος επιλογής και εισαγωγής (insert).
Ακολουθεί η ομάδα hdatainseert που έχει δικαίωμα εισαγωγής (insert) στους πινάκες με πρόθεμα "const-", "raw-" και "aggr-".
Στους ίδιους πίνακες η ομάδα hdataupdate έχει τα ίδια δικαιώματα με την ομάδα hdatainsert και επιπλέον το δικαίωμα της ενημέρωσης(update) και διαγραφής (delete).
Οι ομάδες hadmininsert και hadminupdate έχουν για αυτήν την κατηγορία πινάκων τα ίδια δικαιώματα.

Όσον αφορά τα δικαιώματα των ομάδων ή χρηστών ως προς τη ΒΔ, αυτοί δεν έχουν δικαίωμα να δημιουργήσουν δικούς τους πίνακες ούτε "procedures" (συναρτήσεις). Αντιθέτως, όλοι οι χρήστες έχουν δικαίωμα να εκτελούν "database procedures".

4. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ

Η πρωτοπορία της εφαρμογής του ΥΔΡΟΣΚΟΠΙΟΥ στην χρήση κατανεμημένης βάσης αναγκάζει την εφαρμογή στην επέκταση της ασφάλειας σε επίπεδο δικτύου.
Οπως έχει ήδη αναφερθεί παραπάνω, δημιουργήθηκαν χρήστες που αντιπροσωπεύουν τους άλλους κόμβους (ntua0..nms0..9, κτλ) και δημιουργήθηκε η ομάδα "hrusers" για αυτούς τους απομακρυσμένους χρήστες. Η ομάδα αυτή έχει τα λιγότερα δικαιώματα από όλες τις ομάδες. Ο ΔΙ του τοπικού κόμβου πρέπει να δηλώσει μέσω του netu (εργαλείο της Ingres) όλους τους λογαριασμούς των απομακρυσμένων κόμβων έτσι ώστε οι τοπικοί χρήστες να έχουν πρόσβαση σε αυτούς.

5. ΑΣΦΑΛΕΙΑ ΕΦΑΡΜΟΓΗΣ

Η εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ εκτός της ασφάλειας που παρέχει η Ingres δημιουργεί το δικό της σύστημα ασφάλειας. Κατά αυτόν τον τρόπο, δημιουργείται φιλικότερο περιβάλλον επικοινωνίας της εφαρμογής με το χρήστη. Έτσι στον χρήστη παρουσιάζονται μόνο οι δυνατές επιλογές (εργασίες που μπορεί να εκτελέσει) σύμφωνα με τα δικαιώματα που έχει. Ο χρήστης δεν εμπλέκεται στις διαδικασίες στις οποίες δεν έχει δικαιώματα εκτέλεσης και κατά συνέπεια δεν εμφανίζονται τα απαγορευτικά μηνύματα λάθους από την Ingres.

Κατά την είσοδο του χρήστη στην εφαρμογή παίρνουν κατάλληλες τιμές διάφορες γενικές μεταβλητές (global variables).
Μία ομάδα τέτοιων μεταβλητών σκοπό έχει να καθορίσει τα δικαιώματα του χρήστη σύμφωνα με την ομάδα στην οποία ανήκει. Είναι ευθύνη εκείνων που αναπτύσσουν τις εφαρμογές να χρησιμοποιήσουν αυτές τις γενικές μεταβλητές και να αφήνουν το χρήστη να εκτελεί μόνο τις εργασίες εκείνες για τις οποίες έχει τα κατάλληλα δικαιώματα. Οι εργασίες αυτές επιλέγονται είτε από τον κατάλογο πλαισίου (menu bar) είτε από τα πλήκτρα (buttons) του πλαισίου.

6. ΠΑΡΑΔΕΙΓΜΑ ΕΙΣΑΓΩΓΗΣ ΚΑΙΝΟΥΡΓΙΟΥ ΧΡΗΣΤΗ

Στη συνέχεια περιγράφονται τα βασικά βήματα που πρέπει να γίνουν για να μπορεί ένας χρήστης να χρησιμοποιήσει την εφαρμογή.

1. Ο ΔΣ ανοίγει λογαριασμό στον χρήστη και τον τοποθετεί στην αντίστοιχη ομάδα.
2. Ο ΔΙ δηλώνει το χρήστη στην Ingres και τον τοποθετεί σε αντίστοιχη ομάδα ανάλογα με τα δικαιώματα που θέλει να του δώσει.
3. Ο ΔΙ εξουσιοδοτεί το χρήστη να μπορεί να χρησιμοποιήσει τη ΒΔ (db0) του ΥΔΡΟΣΚΟΠΙΟΥ.

Στο σημείο αυτό ο χρήστης μπορεί να χρησιμοποιήσει την εφαρμογή του ΥΔΡΟΣΚΟΠΙΟΥ.

Εάν ο χρήστης θέλει να έχει ειδικά δικαιώματα σαν απομακρυσμένος χρήστης στους άλλους κόμβους τότε πρέπει να στείλει γράμμα στον ΔΣ του απομακρυσμένου κόμβου μέσω ηλεκτρονικού ταχυδρομείου (e-mail) και να ζητήσει ξεχωριστό λογαριασμό. Εάν του εγκριθεί η αίτηση και ανοιχτεί λογαριασμός στο όνομά του τότε με το εργαλείο της Ingres netu μπορεί να εξουσιοδοτήσει τον εαυτό του να χρησιμοποιεί τον απομακρυσμένο λογαριασμό του.

7. ΧΡΕΩΣΗ ΥΔΡΟΣΚΟΠΙΟΥ

Η πολιτική του ΥΔΡΟΣΚΟΠΙΟΥ είναι να δημιουργηθεί ολοκληρωμένη παρακολούθηση των ενεργειών που κάνει ο χρήστης καθώς χρησιμοποιεί την εφαρμογή.

Στόχοι:

1. Χρέωση συνδρομής
2. Χρέωση χρόνου απασχόλησης
3. Χρέωση δεδομένων
4. Χρέωση αντιγραφής

Η παρούσα εργασία για τη χρέωση σκοπό έχει να επισημάνει τις ενέργειες του χρήστη παρά να καθορίσει το βάρος της μονάδας που θα χρεώνεται ο χρήστης της εφαρμογής.
Ακολουθεί παρουσίαση του τρόπου που αναπτύχτηκε η παρακολούθηση του χρήστη καθώς χρησιμοποιεί την εφαρμογή και τα διαθέσιμα στοιχεία με βάση τα οποία θα χρεώνεται ο χρήστης, σύμφωνα με την ισχύουσα πολιτική.

Όπως έχει αναφερθεί και στην ενότητα της ασφάλειας, όταν ο χρήστης ξεκινάει την εφαρμογή ρυθμίζονται ορισμένες παράμετροι. Μία από αυτές τις παραμέτρους είναι ο χρόνος εκκίνησης της εφαρμογής. Δηλαδή είναι γνωστό εκτός των άλλων το όνομα χρήστη, ομάδα χρήστη κλπ όπως και η ώρα που ξεκίνησε η εφαρμογή. Έτσι λοιπόν, καθώς ο χρήστης εγκαταλείπει την εφαρμογή υπάρχει μια διαδικασία που υπολογίζει την ώρα εξόδου του από το πρόγραμμα και τα αποθηκεύει σε ένα πίνακα μαζί με όλα τα στοιχεία που θα παρουσιαστούν παρακάτω το χρόνο που ο χρήστης χρησιμοποίησε την εφαρμογή. Με τον τρόπο αυτό η εφαρμογή γνωρίζει τον ολικό χρόνο απασχόλησης της εφαρμογής.

Εχει καθοριστεί να χρεώνονται μόνο δεδομένα και όχι γενικές ή διαχειριστικές πληροφορίες της ΒΔ που χρησιμοποιούνται στην εφαρμογή.
Αποθηκεύονται για κάθε χρήστη οι ακόλουθες πληροφορίες σχετικά με τα δεδομένα που επιλέγει:
1. Αριθμός γραμμών δεδομένων,
2. Τόπος αποθήκευσης των δεδομένων (τοπική ή κατανεμημένη ΒΔ),
3. Χρονική κλίμακα δεδομένων (υπερετήσια, ετήσια, μηνιαία, ημερήσια, ωριαία),
4. Προέλευση πρωτογενών δεδομένων (μετεωρολογικό όργανο με ανάγνωση, μετεωρολογικό καταγραφικό όργανο, σταθμήμετρο, σταθμηγράφος, ποιότητα νερού)
5. Τύπος επεξεργασίας δεδομένων (πρωτογενή δεδομένα, δευτερογενή δεδομένα, μέγιστα, ελάχιστα),
6. Ειδικές πληροφορίες (μητρώο σταθμού, ειδικές υδρογεωλογικές πληροφορίες, κατασκευαστικές πληροφορίες, λιθολογική τομή, δοκιμαστικές αντλήσεις, εικόνα bitmap),
7. Μέσο παράδοσης δεδομένων (οθόνη, ascii, bitmap).

Μία συνάρτηση συγκεντρώνει όλες τις παραπάνω πληροφορίες κάθε φορά που ο χρήστης πραγματοποιεί προσπέλαση δεδομένων στην ΒΔ.
Οταν ο χρήστης πρόκειται να εγκαταλείψει την εφαρμογή ο αριθμός που εκφράζει την ποσότητα των δεδομένων που έχουν προσπελαστεί, σύμφωνα με την κατηγορία που ανήκουν τα δεδομένα, αποθηκεύεται αθροιστικά σε ένα πίνακα στην ΒΔ.
Με αυτόν τον τρόπο ο χρήστης ανά πάσα στιγμή γνωρίζει τις ενέργειες που έκανε κατά τη χρήση της εφαρμογής.

Έτσι λοιπόν, υπάρχουν σταθερές οι συνιστώσες για τη χρέωση του χρήστη και σαν μεταβλητή είναι ο συντελεστής βάρους της κάθε συνιστώσας. Ο συντελεστής βάρους που μπορεί να πολλαπλασιαστεί με τη μονάδα χρέωσης και να είναι μεταβλητός ανάλογα με την πολιτική που θα ακολουθείται στην εκάστοτε χρονική περίοδο.

8. ΣΥΜΠΕΡΑΣΜΑΤΑ

Το λογισμικό που αναπτύχθηκε για την ασφάλεια του ΥΔΡΟΣΚΟΠΙΟΥ, το οποίο περιγράφεται στην παρούσα εργασία, επιτρέπει την ασφαλή χρήση του χωρίς να το περιπλέκει ή να επηρεάζει δυσμενώς τη λειτουργικότητα του. Το σύστημα παρακολούθησης των ενεργειών του χρήστη, που παρουσιάζεται στην παρούσα εργασία, μπορεί να αποτελέσει τη βάση για τη δίκαιη χρέωσή του.

9. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Κ. Πιπιλή & Ν. Παπακώστας, 1992, ΥΔΡΟΣΚΟΠΙΟ ΠΡΟΓΡΑΜΜΑ STRIDE ΕΛΛΑΣ, "Πρόταση για το Σχεδιασμό του Συστήματος Ασφάλειας και Χρέωσης".

2. Ingres, 1992, INGRES DBA Manual, INGRES Corporation, Alamenda California 1992.

3. Κ. Πιπιλή & Ν. Παπακώστας, 1992, ΥΔΡΟΣΚΟΠΙΟ ΠΡΟΓΡΑΜΜΑ STRIDE ΕΛΛΑΣ, "Επισκόπηση Επίσκεψης στις Η.Π.Α. και στον Καναδά: Αντίστοιχα Συστήματα, Εξοπλισμός, Λογισμικό και Δίκτυο".