ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

Ειδικά Θέματα Βάσεων Δεδομένων

Ενότητα 8: Ασφάλεια ΒΔ

Δρ. Τσιμπίρης Αλκιβιάδης

Τμήμα Μηχανικών Πληροφορικής ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

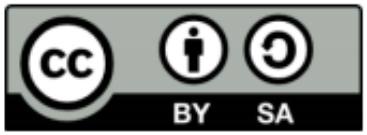
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.

- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ενότητα 8

Ασφάλεια ΒΔ

Δρ. Τσιμπίρης Αλκιβιάδης

Περιεχόμενα ενότητας

- **Ασφάλεια(Security)**
- **Ακεραιότητα (integrity)**
- **Εξέταση προβλημάτων ασφαλείας**
- **Πολιτική Ασφάλειας**
- **Μηχανισμοί Ασφάλειας**
- **Έλεγχος Προσπέλασης**
- **Επιλεκτικός Έλεγχος Προσπέλασης**
- **Εντολές GRANT και REVOKE**
- **Υποχρεωτικός ή Κανονιστικός Έλεγχος Προσπέλασης**
- **Κλάσεις Ασφαλείας(Security Classes)**

Σκοποί ενότητας

Σε αυτήν την ενότητα γίνεται αναφορά στην ασφάλεια και στην προστασία των δεδομένων από την γνωστοποίηση την αλλοίωση ή την καταστροφή τους από μη εξουσιοδοτημένα άτομα. Επίσης παρουσιάζονται πολιτικές και μηχανισμοί ασφαλείας καθώς και η υλοποίηση τους με εντολές SQL δίνοντας δικαιώματα, προνόμια ή ρόλους ασφαλείας στους χρήστες.

Ασφάλεια(Security)

Οι τεχνικές ασφαλείας μας **εξασφαλίζουν** προστασία από μη εξουσιοδοτημένα άτομα.

Προστασία των δεδομένων από ανεπιθύμητες ενέργειες όπως:

- Διαγραφή
- Μετατροπή
- Υποκλοπή

Ακεραιότητα (integrity)

- Η ακεραιότητα αφορά την διατήρηση της **εγκυρότητας** των δεδομένων
- Οι τεχνικές ακεραιότητας έχουν ως στόχο να **αποτρέψουν** τις ακούσιες αλλαγές στα δεδομένα και να τα κρατήσουν με ακρίβεια όπως καταχωρήθηκαν

Εξέταση προβλημάτων ασφαλείας

- **Νομικά**, **Κοινωνικά**, **Ηθικά**
- **Φυσικά**: (κλείδωμα, συναγερμός, βιομετρικός έλεγχος)
- **Πολιτικά**: σε ποιόν και τι επιτρέπεται
- **Λειτουργικά**: (κωδικοί, πόσο συχνά αλλάζουν)
- **Έλεγχοι μέσω υλικού**: (κλειδιά προστασίας μνήμης, προνόμια)
- **Ασφάλεια μέσω λειτουργικού συστήματος:** (άδειες χρήσης, σβήσιμο περιεχομένων μνήμης, προσωρινά αρχεία)

Ορολογία

Ακεραιότητα(Integrity)

- Οι χρήστες δεν θα έπρεπε να τροποποιούν τα δεδομένα που δεν έχουν εξουσιοδότηση
- **π.χ.,** Ένας υπάλληλος δεν μπορεί να αλλάξει τον μισθό του

Διαθεσιμότητα(Availability)

- Οι χρήστες θα πρέπει να δουν και να αλλάξουν μόνο πράγματα που τους επιτρέπεται
- **π.χ.,** Ένας υπάλληλος θα μπορεί να αλλάξει την λίστα καταγραφής εμπορευμάτων

Μυστικότητα(Secrecy)

- Οι χρήστες θα πρέπει να δουν μόνο ότι πρέπει
- **π.χ.,** Ένας υπάλληλος δεν μπορεί να δει τους μισθούς άλλων υπαλλήλων

Ορολογία

Πολιτική ασφαλείας(Security Policy)

- Μια δήλωση που καθορίζει ποιος έχει τη δικαιοδοσία να κάνει τι

Μηχανισμός ασφαλείας(Security Mechanism)

- Προστατεύει αποτελεσματικά τα δεδομένα
- Μας επιτρέπει την εφαρμογή μιας συγκεκριμένης πολιτικής

Πολιτική Ασφάλειας (Security Policy)

Τα αποτελέσματα αυτών των αποφάσεων πολιτικής

- Πρέπει να **γνωστοποιηθούν** στο σύστημα (εντολές γραμμένες σε κάποια κατάλληλη γλώσσα ορισμών)
- Το σύστημα πρέπει να τα **θυμάται** (αποθήκευση στον κατάλογο με τη μορφή κανόνων ασφάλειας (security rule), που είναι γνωστοί και ως κανόνες εξουσιοδότησης (authorization)).

Πολιτική Ασφάλειας (Security Policy)

Για τα αποτελέσματα αυτών των αποφάσεων πολιτικής:

- Πρέπει να υπάρχει ένα μέσο για τον έλεγχο μιας δεδομένης αίτησης πρόσβασης με βάση τους ισχύοντες κανόνες ασφάλειας. (Με τον όρο "αίτηση πρόσβασης" εδώ εννοούμε γενικά το συνδυασμό αιτούμενη πράξη συν αιτούμενο αντικείμενο συν αιτών χρήστης.)
- Ο έλεγχος αυτός γίνεται από το υποσύστημα ασφάλειας του DBMS, που είναι γνωστό και ως **υποσύστημα εξουσιοδοτήσεων**

Πολιτική Ασφάλειας (Security Policy)

Το **DBMS** για να μπορεί να αποφασίζει ποιοι κανόνες ασφάλειας ισχύουν για μια δεδομένη αίτηση πρόσβασης:

- Πρέπει να έχει τη δυνατότητα να **αναγνωρίζει** την προέλευση αυτής της αίτησης — δηλαδή, τον αιτούντα χρήστη. Γι' αυτόν το λόγο, όταν οι χρήστες εισέρχονται (sign in) στο σύστημα, συνήθως απαιτείται να δίνουν όχι μόνο την ταυτότητα τους (user ID — για να δηλώσουν ποιοι είναι) αλλά και ένα συνθηματικό (password — για να αποδείξουν ότι είναι αυτοί που ισχυρίζονται ότι είναι). Το συνθηματικό υποτίθεται ότι είναι γνωστό **μόνο** στο **σύστημα** και στους **νόμιμους χρήστες** που έχουν τη συγκεκριμένη ταυτότητα χρήστη.

Μηχανισμοί Ασφαλείας ΣΔΒΔ

Επιλεκτικοί μηχανισμοί ασφάλειας ή **Περιπτωσιακός έλεγχος (Discretionary Access Control)**

- Κάθε χρήστης έχει διαφορετικά δικαιώματα πρόσβασης
  - **Προνόμια (Privileges)**
  - **Εξουσίες (Authorities)**

Υποχρεωτικοί μηχανισμόι ασφαλείας ή **Κανονιστικός έλεγχος(Mandatory Access Control - MAC)**

- Επιβολή πολλών επιπέδων - διαχωρισμός των χρηστών σε διάφορα επίπεδα (κλάσεις) ασφαλείας
- Κάθε αντικείμενο χαρακτηρίζεται με επίπεδο βαθμού ασφαλείας (classification) και κάθε χρήστης έχει ορισμένο επίπεδο δικαιοδοσίας (clearance). Μηχανισμοί ελέγχου άκαμπτοι.

Πολιτική Ασφάλειας (Security Policy)

Το **DBMS** για να μπορεί να αποφασίζει ποιοι κανόνες ασφάλειας ισχύουν για μια δεδομένη αίτηση πρόσβασης:

- Πρέπει να έχει τη δυνατότητα να **αναγνωρίζει** την προέλευση αυτής της αίτησης — δηλαδή, τον αιτούντα χρήστη. Γι' αυτόν το λόγο, όταν οι χρήστες εισέρχονται (sign in) στο σύστημα, συνήθως απαιτείται να δίνουν όχι μόνο την ταυτότητα τους (user ID — για να δηλώσουν ποιοι είναι) αλλά και ένα συνθηματικό (password — για να αποδείξουν ότι είναι αυτοί που ισχυρίζονται ότι είναι). Το συνθηματικό υποτίθεται ότι είναι γνωστό **μόνο** στο **σύστημα** και στους **νόμιμους χρήστες** που έχουν τη συγκεκριμένη ταυτότητα χρήστη.

Διαχειριστής Συστημάτων

Ο διαχειριστής συστημάτων(system administrator) έχει λογαριασμό με αυξημένες αρμοδιότητες όπως:

- **Δημιουργία** λογαριασμού (έλεγχος προσπέλασης)
- **Εκχώρηση** προνομίων (επιλεκτική ασφάλεια)
- **Αφαίρεση** προνομίων (επιλεκτική ασφάλεια)
- **Καθορισμός** επιπέδου ασφαλείας (υποχρεωτική ασφάλεια)
- **Γνωστοποίηση** πολιτικής στο σύστημα με κανόνες ασφάλειας και εξουσιοδότησης(authorization)

Έλεγχος Προσπέλασης

- **Ίχνη ελέγχου**. (audit trail)
  - Εξακρίβωση αν τα πράγματα είναι υπό έλεγχο
  - Εντοπισμός ενόχου

- Ίχνος ελέγχου → Αρχείο ή Βάση Δεδομένων στην οποία καταγράφονται όλες οι πράξεις που γίνονται από τους χρήστες.
  - Αίτηση
  - Τερματικό
  - Χρήστης
  - Ημν/νία, ώρα
  - Σχέσεις, συστοιχίες, γνωρίσματα που επηρεάσθηκαν
  - Παλιές τιμές
  - Νέες τιμές

Επιλεκτικός ή Περιπτωσιακός έλεγχος προσπέλασης

Βασίζεται στην έννοια των δικαιωμάτων προσπέλασης ή προνομίων πάνω σε αντικείμενα όπως πίνακες(TABLES) ή όψεις(VIEWS)) και μηχανισμούς εκχώρησης και αφαίρεσης προνομίων στους χρήστες.

Επιλεκτικός Έλεγχος Προσπέλασης

Μοντέλο Πίνακα Προσπέλασης(Access Matrix Model)

- **M(i, j)** :
  - **i**: υποκείμενο (π.χ, χρήστης, λογαριασμός, πρόγραμμα)
  - **j**: αντικείμενο (σχέση, εγγραφή (πλειάδα), στήλη (γνώρισμα), όψη, πράξη)

- Αναπαριστά τον τύπο των προνομίων (εγγραφή, ανάγνωση, τροποποίηση) που έχει το υποκείμενο i στο αντικείμενο j

Επιλεκτικός Έλεγχος Προσπέλασης στην SQL

Μοντέλο Πίνακα Προσπέλασης(Access Matrix Model)

- **M(i, j)** :
  - **i**: υποκείμενο (π.χ, χρήστης, λογαριασμός, πρόγραμμα)
  - **j**: Στην SQL μόνο σχέση, όψη στήλη(γνώρισμα)

Επιλεκτικά επίπεδα δικαιωμάτων βάσει όψεων

Επίπεδο λογαριασμού

- Ορίζεται από αυτούς που υλοποιούν τις βάσεις δεδομένων
- Παραδείγματα:
  - CREATE SCHEMA
  - CREATE TABLE
  - CREATE VIEW
  - ALTER
  - DROP
  - MODIFY SELECT

Επίπεδο σχέσης

- Ορίζεται ως τμήμα της SQL
- Προσδιορίζουν για κάθε χρήστη τις σχέσεις στις οποίες μπορεί να εφαρμοστεί κάθε τύπος εντολής

Επιλεκτικός Έλεγχος Προσπέλασης

- Ο δημιουργός ενός πίνακα ή μιας όψης παίρνει αυτόματα όλα τα προνόμια σε αυτόν -- ιδιοκτήτης
- Το ΣΔΒΔ διατηρεί πληροφορία σχετικά με το ποιος παίρνει ή χάνει προνόμια και επιτρέπει μόνο αιτήσεις από χρήστες που έχουν τα απαραίτητα προνομία όταν γίνεται η αίτηση

Η εντολή GRANT

GRANT Privileges ON Object TO Users [WITH GRANT OPTION]

Επιτρέπονται τα παρακάτω **Privileges** :

- **SELECT**: Μπορεί να διαβάσει όλες τις στήλες (συμπεριλαμβανομένων αυτών που μπορεί να προστεθούν αργότερα με την εντολή ALTER TABLE).
- **INSERT**(column-name): Μπορεί να εισάγει πλειάδες με non-NULL ή non-default τιμές στη στήλη column-name.
  - **INSERT** σημαίνει το ίδιο για όλες τις στήλες.
- **DELETE**: Μπορεί να διαγράφει πλειάδες.
- **UPDATE(**column-name): Μπορεί να ενημερωνει πλειάδες.
- **REFERENCES** (column-name): Μπορεί να ορίσει ξένα κλειδιά (σε άλλους πίνακες) που αναφέρονται στην column-name.

Η εντολή GRANT

GRANT Privileges ON Object TO Users [WITH GRANT OPTION]

- Αν ένας χρήστης έχει ένα προνόμιο με το GRANT OPTION μπορεί να δώσει αυτό το προνόμιο σε άλλους χρήστες (μπορεί να δώσει ή να μη δώσει το GRANT OPTION).
- Αν και δεν έχουν ακόμα υλοποιηθεί υπάρχουν μηχανισμοί για τον περιορισμό της διάδοσης προνομίων
- Τα **CREATE, ALTER**, και **DROP** μπορεί να εκτελεστούν **μόνο** από τον ιδιοκτήτη.

Η εντολή GRANT : Παραδείγματα

- Ο χρήστης **Chara** να μπορεί να **κάνει ερωτήσεις** και να **εισάγει** πλειάδες στη σχέση **Vathmoi**.
  - **GRANT INSERT, SELECT ON Vathmoi TO maria**
- Ο χρήστης **Grammateia** να μπορεί να **διαγράφει** πλειάδες απο τη σχέση **Student** και μπορεί να **εξουσιοδοτήσει και άλλους** γιαυτό.
  - **GRANT DELETE ON Student TO Grammateia WITH GRANT OPTION**
- Ο χρήστης **Michaela** μπορεί να **τροποποιεί μόνο** το γνώρισμα **DIEYTHINSI** της σχέσης **Student**.
  - **GRANT UPDATE(DIEYTHINSI) ON Student TO elenh**

Η εντολή REVOKE

REVOKE Privilege ON Object FROM Users

- **Αφαίρεση** προνομίου από έναν χρήστη
- Παρόμοια με την εντολή **GRANT**
- Όταν **αφαιρεθεί** ένα προνόμιο από το χρήστη Χ **αφαιρείται και από όλους** τους χρήστες που πήραν αυτό το προνόμιο αποκλειστικά από αυτόν

Η εντολή REVOKE : Παραδείγματα

- Ο χρήστης **maria** να μην μπορεί να **κάνει ερωτήσεις** στη σχέση **Misthoi**.
  →**REVOKE SELECT ON Misthoi TO xara**
- Ο χρήστης **elenh** να μην μπορεί να **διαγράφει** πλειάδες απο τη σχέση **Misthoi**.
  →**REVOKE DELETE ON Misthoi TO elenh**

Όψεις(VIEWS)

- Οι όψεις μπορεί να χρησιμοποιηθούν για να δώσουν **μόνο** την απαραίτητη πληροφορία
- Οι όψεις μαζί με τις εντολές GRANT/REVOKE αποτελούν ένα πολύ ισχυρό εργαλείο για τον **έλεγχο προσπέλασης.**
- Ο δημιουργός μιας όψης έχει ένα προνόμιο πάνω στην όψη μόνο αν έχει το προνόμιο σε όλες τις σχέσεις που περιλαμβάνονται στον ορισμό της όψης
- Για την δημιουργία της όψης απαιτείται το προνόμιο **SELECT** σε όλες τις σχέσεις που περιλαμβάνονται στον ορισμό της όψης

Επιλεκτικός Έλεγχος Προσπέλασης

Πως μπορείτε να ορίσετε προνόμια στο επίπεδο του ενός γνωρίσματος μιας πλειάδαςQ:

- **SQL-92**: προνόμια σε authorization ids, που μπορεί να αναφέρονται σε ένα χρήστη ή σε μια ομάδα χρηστών
- **SQL-1999**: προνόμια σε ρόλους.
  - Στη συνέχεια μπορεί να ανατεθούν ρόλοι σε χρήστες ή σε άλλους ρόλους

Υποχρεωτικός ή Κανονιστικός Έλεγχος Προσπέλασης

Βασίζονται σε πολιτικές που ισχύουν για όλο το σύστημα και δεν μπορούν να τροποποιηθούν από συγκεκριμένους χρήστες.

- Σε κάθε αντικείμενο της ΒΔ ανατίθεται και μια ***κλάση ασφάλειας***.
- Σε κάθε υποκείμενο (χρήστη ή πρόγραμμα) ανατίθεται και ένα δικαίωμα για μια κλάση ασφάλειας
- Κανόνες βασιζόμενοι στις κλάσεις ασφάλειας και στα δικαιώματα καθορίζουν ποιος μπορεί να διαβάσει/γράψει ποια αντικείμενα

Τα περισσότερα εμπορικά συστήματα δεν υποστηρίζουν τον υποχρεωτικό έλεγχο πρόσβασης.

Υποχρεωτικός ή Κανονιστικός Έλεγχος Προσπέλασης

- Χρήστης i μπορεί να δει το αντικείμενο j εάν το επίπεδο δικαιοδοσίας του i είναι μεγαλύτερο ή ίσο του επίπεδου ασφαλείας του j.
- Χρήστης i μπορεί να τροποποιήσει το αντικείμενο j εάν το επίπεδο δικαιοδοσίας του i είναι μεγαλύτερο ή ίσο του επίπεδου ασφαλείας του j.
- Κάθε τι που γράφει ο χρήστης ι έχει επίπεδο ασφαλείας ίσο με το επίπεδο δικαιοδοσίας του ι

Υποχρεωτικός Έλεγχος Ασφαλείας
Κλάσεις Ασφαλείας(Security Classes)

Α -- **Βεβαιωμένη** προστασία.

- Μαθηματική απόδειξη ότι μηχανισμός ασφαλείας είναι συνεπής και επαρκής

Β -- **Δομημένη** προστασία

- **Β1** προστασία με ετικέτες (απόρρητο - εμπιστευτικό ..)
- **Β2** επιπλέον τυπική δήλωση πολιτικής, Β3 λογιστικός έλεγχος και υπεύθυνος διαχείρισης ασφαλείας.

Υποχρεωτικός Έλεγχος Ασφαλείας
Κλάσεις Ασφαλείας(Security Classes)

C -- **Περιπτωσιακή** προστασία

- **C1** -- Διαχωρισμός δεδομένων - χρηστών
- **C2** -- Διαδικασίες ελέγχου χρήστη, λογιστικού ελέγχου, απομόνωσης πόρων

D -- **Λιγότερο** ασφαλής

Υποχρεωτικός Έλεγχος Προσπέλασης

- **Αντικείμενα** (π.χ., πίνακες, όψεις, πλειάδες)
- **Υποκείμενα** (π.χ., χρήστες, προγράμματα)
- **Κλάσεις** ασφάλειας:
  - **Άκρως Απόρρητη** (TS)
  - **Απόρρητη** (S)
  - **Εμπιστευτική** (C)
  - **Αδιαβάθμητη** (U):
  - TS > S > C > U

Υποχρεωτικός Έλεγχος Προσπέλασης

- Χρήστες με S και TS μπορούν να δουν και τις δυο γραμμές
- Χρήστες με C βλέπουν μόνο $2^{η}$ γραμμή
- Χρήστες με U δε βλέπουν καμία

- Αν ένας χρήστης με C προσπαθήσει να εισάγει <101,Pasta,Blue,C>:
  - Αν επιτρέψουμε την εισαγωγή, παραβίαση του περιορισμού κλειδιού
  - Αν δεν τον επιτρέψουμε αποκαλύπτουμε ότι υπάρχει ένα άλλο αντικείμενο με κλειδί 101 και κλάση > C!
  - Η κλάση μέρος του κλειδιού.

- **Πρόβλημα**: **κανάλι διαρροής** (covert channel)
- **ΛΥΣΗ**: Δημιουργία **Πολλαπλών Στιγμιότυπων**