Chapter Six

IntroductiontoDBSecurityIssues

DiscretionaryAccessControlBasedonGranting

/RevokingofPrivileges

MandatoryAccessControlforMultilevelSecurity

StatisticalDBSecurity

Database Security and Authorization

Introduction to DB Security

DatabaseSecurity-themechanismsthatprotectthedatabaseagainst

intentionaloraccidentalthreats.

Databasesecurityencompasseshardware,software,peopleanddata.

DatabaseManagementSystemssupportingmulti-userdatabasesystemmust

provideadatabasesecurityandauthorizationsubsystemtoenforcelimitson

individualandgroupaccessrightsandprivileges.

DatabaseSecurity:referstothecollectivemeasuresusedtoprotect

andsecureadatabaseordatabasemanagementsoftwarefromillegitimateuse

andmaliciousthreatsandattacks.

Databasesecurity:isthetechniquethatprotectsandsecuresthedatabase

againstintentionaloraccidentalthreats.

Introduction to DB Security…

Agooddatabasesecuritymanagementsystemhasthefollowing

majorcharacteristics:

DataIndependence:-thecapacitytochangetheschemaatonelevel

ofadatabasesystemwithouthavingtochangetheschemaatthenext

higherlevel

Minimalredundancy:-minimizesimilarvaluesthatoccurredmore

thanonce

Dataconsistency:-Dataconsistencymeansthateachuserseesa

consistentviewofthedata,includingvisiblechangesmadebythe

user'sowntransactionsandtransactionsofotherusers.

Introduction to DB Security…

Dataintegrity:-referstotheoverallcompleteness,accuracyand

consistencyofdata.

Privacy:-signifiesthatanunauthorizedusercannotdisclosedata

Integrity:-ensuresthatanunauthorizedusercannotmodifydata

Availability:-ensuresthatdatabemadeavailabletotheauthorized

userunfailingly

Copyright:-ensuresthenativerightsofindividualsasacreatorof

information.

Validity:-ensuresactivitiestobeaccountablebylaw.

Introduction to DB Security….

Databasesecurityandintegritydealsaboutprotectingthedatabase

frombeinginconsistentandbeingdisrupted,alsocallitdatabase

misuse.

DatabasemisusecouldbeIntentionalorAccidental,whereaccidental

misuseiseasiertocopewiththanintentionalmisuse.

Introduction to DB Security…

Accidentalinconsistencycouldoccurdueto:

Systemcrashduringtransactionprocessing

Anomaliesduetoconcurrentaccess

Anomaliesduetoredundancy

Logicalerrors

Intentionalmisusecouldbe:

Unauthorizedreadingofdata

Unauthorizedmodificationofdata

Unauthorizeddestructionofdataetc.

We consider database security about the following situations:

Theft and fraudulent

Loss of confidentiality or secrecy

Loss of data privacy

Loss of data integrity

Loss of availability of data

A vulnerability is a weakness in design, implementation,

operation or internal control.

Cont…

Tosecureacomputersystem,itisimportanttounderstandtheattacks

thatcanbemadeagainstit,andthesethreatscantypicallybeclassified

intooneofthesecategoriesbelow:

1.Backdoor:Abackdoorinacomputersystem,acryptosystemoran

algorithm,isanysecretmethodofbypassingnormalauthenticationor

securitycontrols.

2.Denial-of-serviceattack(DoS):DOSisacyber-attackinwhichthe

perpetrator(criminal)seekstomakeamachineornetworkresource

unavailabletoitsintendedusersbytemporarilyorindefinitely

disruptingservicesofahostconnectedtotheinternet.

Cont….

3.Eavesdropping:istheunauthorizedreal-timeinterceptionofa

privatecommunication,suchasaphonecall,instantmessage,

videoconferenceorfaxtransmission.

Thetermeavesdropderivesfromthepracticeofactuallystanding

undertheeavesofahouse,listeningtoconversationsinside.

4.Phishing:istheattempttoacquiresensitiveinformationsuchas

usernames,passwords,andcreditcarddetailsdirectlyfromusersby

deceiving(misleading)theusers.

Levels of Security Measures

Securitymeasurescanbeimplementedatseverallevelsandfor

differentcomponentsofthesystem.Theselevelsare:

PhysicalLevel:concernedwithsecuringthesitecontainingthe

computersystem.

Thebackupsystemsshouldalsobephysicallyprotectedfromaccess

exceptforauthorizedusers.

Inotherwords,thesiteorsitescontainingthecomputersystemsmust

bephysicallysecuredagainstarmedorsneakyentrybyintruders.

Eg.Server

Cont…

OperatingSystem:concernedwiththeweaknessandstrengthofthe

operatingsystemsecurityondatafiles.

Itusesforprotectionofdatainprimaryandsecondarymemoryfrom

unauthorizedaccess.

ApplicationLevel:Sincealmostalldatabasesystemsallowremote

accessthroughterminalsornetworks,software-levelsecuritywiththe

networksoftwareisasimportantasphysicalsecurity,bothonthe

Internetandnetworksprivatetoanenterprise.

HumanLevel:concernedwithauthorizationofdatabaseusersforaccess

thecontentatdifferentlevelsandprivileges.

Cont…

DatabaseSystem:concernedwithdataaccesslimitenforcedbythe

databasesystem.Accesslimitlikepassword,isolatedtransactionandetc.

Somedatabasesystemusersmaybeauthorizedtoaccessonlyalimited

portionofthedatabase.Otherusersmaybeallowedtoissuesqueries,

butmaybeforbiddentomodifythedata.

Itistheresponsibilityofthedatabasesystemtoensurethatthese

authorizationrestrictionsarenotviolated.

Authentication

Authenticationistheprocessofcheckingwhethertheuseristheone

withtheprivilegefortheaccesslevel.

Allusersofthedatabasewillhavedifferentaccesslevelsand

permissionfordifferentdataobjects,and

Thus,thesystemwillcheckwhethertheuserwithaspecificusername

andpasswordistryingtousetheresource.

Istheprocessofcheckingtheusersarewhotheysaytheyare.

Eachuserisgivenauniqueidentifier,whichisusedbytheoperating

systemtodeterminewhotheyare

Authorization/Privilege:

Authorizationreferstotheprocessthatdeterminesthemodeinwhichaparticular(previously

authenticated)clientisallowedtoaccessaspecificresourcecontrolledbyaserver.

Thegrantingofarightorprivilegethatenablesasubjecttohavelegitimateaccesstoa

systemorasystem’sobject

Authorizationcontrolscanbebuiltintothesoftware,andgovernnotonlywhatsystemor

objectaspecifiedusercanaccess,butalsowhattheusermaydowithit

Authorizationcontrolsaresometimesreferredtoasaccesscontrols

Anydatabaseaccessrequestwillhavethefollowingthreemajorcomponents:

1.RequestedOperation:whatkindofoperationisrequestedbyaspecific

query?

2.RequestedObject:onwhichresourceordataofthedatabaseistheoperation

requiredtobeapplied?

3.RequestingUser:whoistheuserrequestingtheoperationonthespecified

object?

Cont…

Forms of user authorization

Userauthorizationonthedata/extension.Theseincludes:

1.ReadAuthorization:theuserwiththisprivilegeisallowedonlytoreadthe

contentofthedataobject.

2.InsertAuthorization:theuserwiththisprivilegeisallowedonlytoinsert

newrecordsoritemstothedataobject.

3.UpdateAuthorization:userswiththisprivilegeareallowedtomodify

contentofattributesbutarenotauthorizedtodeletetherecords.

4.DeleteAuthorization:userswiththisprivilegeareonlyallowedtodeletea

recordandnotanythingelse.

Note:Differentusers,dependingonthepoweroftheuser,canhaveoneorthe

combinationoftheaboveformsofauthorizationondifferentdataobjects.

Cont…

Userauthorizationonthedatabaseschema:

IndexAuthorization:dealswithpermissiontocreateaswellasdelete

anindextableforrelation.

ResourceAuthorization:dealswithpermissiontoadd/createanew

relationinthedatabase.

AlterationAuthorization:dealswithpermissiontoaddaswellasdelete

attribute.

DropAuthorization:dealswithpermissiontodeleteandexisting

relation.

Database Security and the DBA

Thedatabaseadministrator(DBA)isthecentralauthorityfor

managingadatabasesystem.

Wheneverapersonorgroupofpersonsneedtoaccessadatabase

system,theindividualorgroupmustfirstapplyforauseraccount.

TheDBAwillthencreateanewaccountidandpasswordforthe

userifhe/shebelievesthereisalegitimateneedtoaccessthe

database.

Access Protection, User Accounts

Role of DBA in Database Security

Thedatabaseadministratorisresponsibletomakethedatabasetobeas

secureaspossible.

ForthistheDBAshouldhavethemostpowerfulprivilegethanevery

otheruser.

TheDBAprovidescapabilityfordatabaseuserswhileaccessingthe

contentofthedatabase.

The major responsibilities of DBA in relation to authorization of

users are:

AccountCreation:involvescreatingdifferentaccountsfordifferentUSERS

aswellasUSERGROUPS.

SecurityLevelAssignment:involvesinassigningdifferentusersatdifferent

categoriesofaccesslevels.

PrivilegeGrant:involvesgivingdifferentlevelsofprivilegesfordifferent

usersandusergroups.

PrivilegeRevocation:involvesdenyingorcancelingpreviouslygranted

privilegesforusersduetovariousreasons.

AccountDeletion:involvesindeletinganexistingaccountofusersoruser

groups.Issimilarwithdenyingallprivilegesofusersonthedatabase.

ACCESS CONTROL

TherearetwotypesofDBsecuritytechniquesforexample:-

Discretionary security mechanism

Mandatory access control.

Themechanismsusedtograntandrevokeprivilegesinrelationaldatabasesystems

andinSQLreferredtoasdiscretionaryaccesscontrol.

Onotherround,themechanismsforenforcingmultiplelevelsofsecurity,whichisa

morerecentconcernindatabasesystemsecuritythatisknownasmandatoryaccess

control.

1.DISCRETIONARY ACCESSCONTROL

Isbasedontheconceptofaccessrights,orprivileges,andmechanismsforgiving

userssuchprivileges.

Aprivilegeallowsausertoaccesssomedataobjectinacertainmanner(e.g.,toread

ortomodify).

Cont…

Differentusershavedifferentaccessprivilegesontheobject(eithera

basetableoraview)ofthedatabase.

GRANTandREVOKEcommandsofdatamanipulationlanguage

correspondstograntandrevokeprivileges,respectively.

Discretionaryaccesscontrolmechanisms,Grantdifferentprivilegesto

differentusersandusergroupsonvariousdataobjectstoaccess

differentdataobjects.

Themodeoftheprivilegecouldbe:-Read,Insert,Delete,Updatefiles,

recordsorfields.

Itismoreflexible.

Cont…

Thesyntaxofthiscommandisasfollows:

GRANTprivilegesONobjectTOusers[WITHGRANTOPTION]

SELECT:Therighttoaccess(read)allcolumnsofthetablespecifiedastheobject,

includingcolumnsaddedlaterthroughALTERTABLEcommands.

INSERT(column-name):Therighttoinsertrowswith(non-nullornondefault)

valuesinthenamedcolumnofthetablenamedasobject.

Ifthisrightistobegrantedwithrespecttoallcolumns,includingcolumnsthatmight

beaddedlater,wecansimplyuseINSERT.

TheprivilegesUPDATE(column-name)andUPDATEcanalsobeused.

DELETE:Therighttodeleterowsfromthetablenamedasobject.

Objectcanbeabasetable,aview,orotherssupportedbySQL.

Privileges Using Views

GRANTcommandisusedforconferring(talking)theauthorizationtotheusers

whereas,

TheGRANTstatementisusedtogiveprivilegetousersorroles.

Note:ifthepermissionisgivenviathe[WITHGRANTOPTION],allusersintheTO

clausecanthemselvespassontheprivilegetootherusers.

Revokestatementisusedtowithdrawprivilegesfromauserwithoutdeletingthat

user.

Forexample:

TheownerofarelationmaywanttogranttheSELECTprivilegetoauserfora

specifictaskandthenrevokethatprivilegeoncethetaskiscompleted.

Hence,amechanismforrevokingprivilegesisneeded.

InSQL,aREVOKEcommandisincludedforthepurposeofcanceling

privileges.

EXAMPLE ONE

Examples:GRANTSELECTONstudenttou1

GRANTSELECT,INSERT,UPDATE(salary)ONemployeetou1

GRANTSELECTONstudenttou1WITHGRANTOPTION

Examples:REVOKEDELETEONemployeefromu1

REVOKEDELETE,INSERTONemployeefromu1

Note:-WITHGRANTOPTION:-Indicatesthattheabilitytograntthe

specifiedpermissionwillberevoked.

EXAMPLE TWO

Let user1 change department names.

GRANT UPDATE (d\_name) ON department TO user1;

Give Abeberead-only access to the sfname, smname, slnamecolumns of the

student table.

GRANT SELECT (sfname, smname, slname) ON student TO Abebe;

Supposeyouwanttograntupdateandinsertprivilegeononlycertaincolumnsnoton

allthecolumnsthenincludethecolumnnamesingrantstatement.

Forexampleyouwanttograntupdateprivilegeonsfnamecolumnonlyandinsert

privilegeonsmnameandslnamecolumnsonly.

Thengivethefollowingstatement:

Grantupdate(sfname),insert(smname,slname)onstudenttoAbebe;

2.Mandatoryaccesscontrol

MACisbasedonsystemwidepoliciesthatcannotbechangedbyindividual

users.

Inthisapproach,eachdatabaseobjectisassignedasecurityclass,eachuseris

assignedclearanceforasecurityclass,andRulesareimposedonreadingand

writingofdatabaseobjectsbyusers.

TheDBMSdetermineswhetheragivenusercanreadorwriteagivenobject

basedoncertainrulesthatinvolvethesecurityleveloftheobjectandthe

clearanceoftheuser.

Onlyuserswhocanpasstheclearancelevelcanaccessthedataobject

Iscomparativelynot-flexible/rigid.

Cont…

Inmandatoryaccesscontrol,userworkincompanyandthecompany

decideshowdatashouldbeshared.

Hospitalownspatientrecordsandlimitstheirsharing.

DACtechniquesisanall-or-nothingmethod:

Ausereitherhasordoesnothaveacertainprivilege.

Inmanyapplications,additionalsecuritypolicyisneededthat

classifiesdataandusersbasedonsecurityclasses.

Typicalsecurityclassesaretopsecret(TS),secret(S),confidential

(C),andunclassified(U),whereTSisthehighestlevelandUthe

lowest:TS≥S≥C≥U

Comparing DAC and MAC

DACpoliciesarecharacterizedbyahighdegreeofflexibility,which

makesthemsuitableforalargevarietyofapplicationdomains.

ThemaindrawbackofDACmodelsistheirweaknesstomalicious

attacks,suchasTrojanhorsesembeddedinapplicationprograms.

Bycontrast,mandatorypoliciesensureahighdegreeofprotectionina

way,theypreventanyillegalflowofinformation.

Mandatorypolicieshavethedrawbackofbeingtoorigidandtheyare

onlyapplicableinlimitedenvironments.

In particular the DBA(Database administrator)deals with the following:

1.Creatingnewaccounts:Eachnewuserorgroupofusersmustbeassignedan

authorizationidandapassword.

Notethatapplicationprogramsthataccessthedatabasehavethesame

authorizationidastheuserexecutingtheprogram.

2.Privilegegranting:grantscertainprivilegestocertainaccounts

3.Privilegerevocation:revoke(cancel)certainprivilegesthatwerepreviouslygivento

certainaccounts.

4.Mandatorycontrolissues:IftheDBMSsupportsmandatorycontrol,theDBAmust

assignsecurityclassestoeachdatabaseobjectandassignsecurityclearancestoeach

authorizationidinaccordancewiththechosensecuritypolicy.

Note:-TheDBAisresponsiblefortheoverallsecurityofthedatabasesystem.

Statistical Database Security

Statisticaldatabasesareusedmainlytoproducestatisticsonvarious

populations.

Thedatabasemaycontainconfidentialdataonindividuals,which

shouldbeprotectedfromuseraccess.

Usersarepermittedtoretrievestatisticalinformationonthe

populations,suchasaverages,sums,counts,maximums,minimums,

andstandarddeviations.

Apopulationisasetofrowsofarelation(table)thatsatisfysome

selectioncondition.

Statisticalqueriesinvolveapplyingstatisticalfunctionstoa

populationofrows.

Cont…

Statisticaldatabasesecuritytechniquesmustdisallowtheretrievalof

individualdata.

Thiscanbeachievedbyeliminationofqueriesthatretrieveattribute

valuesandbyallowingonlyqueriesthatinvolvestatisticalaggregate

functionssuchas,SUM,MIN,MAX,Suchqueriesaresometimes

calledstatisticalqueries.

ItisDBMS’sresponsibilitytoensureconfidentialityofinformation

aboutindividuals,whilestillprovidingusefulstatisticalsummariesof

dataaboutthoseindividualstousers.

Provisionofprivacyprotectionofusersinastatisticaldatabaseis

paramount(vital).