

Databases Illuminated

Chapter 9

Database Security

Privacy and Security

- **Database security**
 - protecting the database from unauthorized access, modification, or destruction
- **Privacy**
 - the right of individuals to have some control over information about themselves
 - protected by law in many countries
- Right to privacy can be protected by database security

Accidental Security Threats

- **User errors**
 - User unintentionally requests object or operation for which he/she should not be authorized
- **Communications system errors**
 - User sent a message that should be sent to another user
 - system connects a user to a session that belongs to another user with different access privileges
- **OS errors**
 - Accidentally overwrites files and destroys part of database
 - Fetches the wrong files and sends them to the user
 - Fails to erase files that should be erased

Deliberate Security Threats- Sources

- User intentionally gains unauthorized access and/or performs unauthorized operations on the database
- Disgruntled employee who is familiar with the organization's computer system seeks revenge
- Industrial spies seek information for competitors

Deliberate Security Threats- methods

- Wiretapping of communication lines
- Electronic eavesdropping-picking up electronic signals
- Reading display screens or printouts left unsupervised
- Impersonating authorized users or users with greater access
- Writing programs to bypass the DBMS and access database data directly
- Writing applications programs that perform unauthorized operations
- Deriving information about hidden data by clever querying
- Removing physical storage devices from the computer facility
- Making copies of stored files without going through the DBMS
- Bribing, blackmailing or influencing authorized users to obtain information or damage the database

Security Plan

- Should begin with physical security measures for the building-physical barriers, control access, require badges, sign-in etc.
- Should have more physical security for the computer facilities-e.g. locked door
- Additional security control for database

Authentication

- User **authentication** - verifying the identity of users
- Operating system uses user profiles, user ids, passwords, authentication procedures, badges, keys, or physical characteristics of the user
- Additional authentication can be required to access the database-additional user ID, PW

User Profiles

- System has a user profile for each id, giving information about the user
- Stored profiles should be kept secure, possibly in encrypted form
- Profile normally includes a password, allegedly known only to the user
- Passwords should be kept secret and changed frequently
- System should never display passwords at sign-in time

Other Authentication Procedures

- Password limitations-users write them down, choose words that are easy to guess, or share them
- Could require users to insert badges or keys to log on to a workstation
- Voice, fingerprints, retina scans, or other physical characteristics can be used
- Authentication procedure can be series of questions-takes longer and is more difficult to reproduce than PW
- Authentication can be required again at the database
- User should be required to produce an additional PW to access the database

Authorization

- DBMSs designed for multiple users have a security subsystem
- Provide for **authorization**-users are assigned rights to use database objects
- **Authorization language**-allows the DBA to write **authorization rules** specifying which users have what type of access to database objects

Access Control

- **Access control** covers the mechanisms for implementing authorizations
- **Access control matrix**
 - Planning tool to identify operations different users are permitted to perform on various database objects
 - List users in left column; objects on top row; write operations permitted at intersection
- DBA can delegate authorization powers to others-requires careful planning to avoid abuse

Security Mechanisms

- **Views**-simple method for access control
- **Security log**-journal for storing records of attempted security violations
- **Audit trail**-records all access to the database - requestor, operation performed, workstation used, time, data items and values involved
- **Triggers** can be used to set up an audit trail
- **Encryption** of database data also protects it

Encryption

- Uses a **cipher system** that consists of
 - **Encryption algorithm** that converts **plaintext** into **ciphertext**
 - **Uses encrypting key**
 - **Decryption algorithm** that reproduces plaintext from ciphertext
 - **Uses decryption key**
- Widely-used schemes for encryption
 - **Data Encryption Standard (DES)** and **Advanced Encryption Standard (AES)**
 - uses a standard algorithm, which is often hardware implemented
 - **Public key encryption**-uses a product of primes as a public key, and the prime factors of the product as a private key
 - Ex. **RSA**, named for its developers Rivest, Shamir and Adleman

DES and AES

- **Data Encryption Standard-DES** See Figure 9.4
 - National Bureau of Standards, 1977
 - Algorithm is public-can have hardware implementation
 - Key is private
 - Uses **symmetric** encryption-decryption key is the same as the encryption key and decryption algorithm is the inverse of encryption algorithm
 - Uses 56-bit key on 64-bit blocks of plaintext, producing 64-bit blocks of ciphertext
 - In each block, characters are substituted and rearranged according to the value of the key
 - Two major challenges with the DES system: key security and ease of cracking the code
- **Advanced Encryption Standard-AES**
 - Developed in 2000
 - symmetric scheme; more sophisticated than the DES scheme
 - three key sizes-128s,192, or 256 bits, depending on the level of security needed
 - Due to larger key sizes, cracking the scheme is more challenging

SQL Authorization Language

- GRANT statement used for authorization
- REVOKE statement used to retract authorization
- Privileges can be given to users directly
- Privileges can also be given to a role, and role given to users
- System keeps track of authorizations using a **grant diagram**, also called an **authorization graph**
- In Oracle, privileges include **object privileges** and **system privileges**
 - Granted using the authorization sublanguage or through the Oracle Security Manage

GRANT Statement

GRANT {ALL PRIVILEGES | *privilege-list*}

ON {*table-name*|*view-name*}

TO {PUBLIC | *user-list*|*role-list*} [WITH GRANT OPTION];

- privileges for base tables are SELECT, DELETE, INSERT, UPDATE or REFERENCES(*col-name*)
- For updatable views, privileges are SELECT, DELETE, INSERT and UPDATE
- To grant privileges to a user-Ex.

GRANT SELECT ON Student TO U101 WITH GRANT OPTION;

- To create and use a role-Ex.
 - CREATE ROLE AdvisorRole;
 - Grant privileges to the role
 - GRANT SELECT ON Student TO AdvisorRole;
 - Assign a role to a user
 - GRANT AdvisorRole to U999;
 - To assign a role to another role
 - GRANT FacultyRole TO AdvisorRole;
 - Allows inheritance of role privileges

REVOKE

- REVOKE {ALL PRIVILEGES | *privilege-list*}
ON *object-list*
FROM {PUBLIC | *user-list* | *role-list*}
[CASCADE | RESTRICT];
- Ex:
 - REVOKE INSERT ON Student FROM U101;
- Can revoke just the grant option, without revoking the underlying privilege,
 - REVOKE GRANT OPTION FOR INSERT ON Student FROM U101;
- By default, revocations **cascade** or trigger other revocations, if the user has passed on the privileges that are revoked
- If RESTRICT is specified, any revocation that would cascade to others will not be performed

Statistical Databases

- Support statistical analysis on populations
- Data itself may contain facts about individuals, but is not meant to be retrieved on an individual basis
- Users are permitted to access statistical information-totals, counts, or averages, but not information about individuals

Statistical DB Security

- Need special precautions to ensure users are not able to deduce data about individuals
- Even if all queries must involve count, sum or average, user can use conditions in WHERE line to narrow the population down to one individual
- System can refuse any query for which only one record satisfies the predicate-not sufficient protection
- Can restrict queries
 - Require that the number of records satisfying the predicate be above some threshold
 - Require that the number of records satisfying a pair of queries simultaneously cannot exceed some limit
 - Can disallow sets of queries that repeatedly involve the same records

Need for DB Security on the Internet

- Messages transmitted in plaintext can be read by intruders using packet sniffing software
- Customers need assurance their credit card info is kept private when sent over the Internet
- Companies that allow web connections to their internal networks for access to their database need to protect it from attack
- Receivers and senders of messages need to be sure that the site they are communicating with is genuine and trustworthy

Techniques for Internet Security

- Firewalls
- Certifications authorities such as Verisign that issue digital certificates using SSL or S-HTTP
- SET for financial information
- Digital signatures

Firewalls

- A hardware/software barrier that protects an organization's intranet from unauthorized access
- Ensures that messages entering or leaving intranet meet the organization's standards
- May use a **proxy server** that intercepts all messages in both directions-hides the actual network address
- **Packet filter** examines each packet of information before it enters or leaves the intranet
- Gateway techniques can apply security mechanisms to applications or connections

Certification Authorities-SSL & S-HTTP

- **Verisign**-method of verifying that a site is genuine
- Uses public key encryption
- **Secure Sockets Layer (SSL)** protocol
 - site begins process by generating a public key and a private key, and sending a request to Verisign, along with the site's public key
 - Verisign issues an encrypted certificate to the site
 - Customer browser asks the site for its Verisign certificate; receives it in encrypted form
 - Browser decrypts the certificate using Verisign's public key, verifies that this is a Verisign certificate, and that the site's URL is the correct one
 - Certificate also contains the site's public key
 - Browser creates a session key, encrypts it using the site's public key from the certificate, and sends the session key to the site
 - Only the actual site can decrypt it using its private key
 - Browser and the site are the sole holders of the session key; they can exchange messages encrypted with it, using simpler protocol- DES or AES
- **Secure HTTP (S-HTTP)**, similar to SSL-guarantees security of individual messages rather than an entire session

SET

- **Secure Electronic Transaction (SET)** protocol
- Provides additional security for credit card info
- When customer is ready to transmit order info, browser sends the site most of the order information encoded with its public key
- Credit card information is encoded with the public key of the credit card company, so site cannot decode it directly
- Site sends credit card information directly to the card company site for approval and payment

Digital Signatures

- Double form of public key encryption
- Creates secure two-way communications that cannot be repudiated
- Users can verify the authenticity of the person they are communicating with, and prove that a message must have come from that person
- Sender encodes a message first with his or her own private key, and then with the public key of the receiver
- Receiver decrypts the message first using his or her private key, and then using the sender's public key
- Double encryption ensures that both parties are authentic, since neither one could have encoded or decoded the message without his or her private key
- Variation uses a Certification Authority, similar to SSL