Unit-V

Database Security

1) Introduction to Database security issues:

Database security is a broad

1.1) Types of security: are that address many issues.

→ various legal and ethical issues regarding the right to access certain information.

Eg: some information may be deemed to be private and cannot be accessed legally by unauthorized organizations or persons. In the united states, there are numerous laws governing privacy of information.

→ Policy issues at the governmental, institutional, or corporate level regarding what kinds of information should not be made publicly available.

Eg: credit ratings and personal medical records.

→ System related issues such as system levels at which various security functions should be enforced.

Eg: whether a security function should be handled at the physical hardware level, the operating system level or the DBMS level.

→ The need in some organizations to identify multiple security levels and to categorize the data and users based on these classifications.

Eg: top secret, secret, confidential and unclassified.

What Does Database Security Mean?

→ Database security refers to the collective measures used to protect and secure a db or database management software from illegitimate use and malicious cyber threats and attacks.

Threats to Databases: Threats to databases can result in the loss or degradation of some or all of the following accepted security goals:

1) Integrity.
2) availability.
3) Confidentiality.

Loss of integrity: Database integrity refers to the requirement that information be protected from improper modification.

(Improper modification of information)

→ Modification of data includes creating, inserting, and updating data, changing the status of data and deleting data.

→ Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts.

→ If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud or erroneous decisions.

→ Loss of availability: Database availability refers to making objects available to a human user or program who/which has a legitimate right to those data objects.

→ Loss of availability occurs when the user or program cannot access data objects.

→ Loss of confidentiality: Database confidentiality refers to the protection of data from unauthorized disclosure.

→ The impact of unauthorized disclosure of confidential information can range from violation of the Data Privacy Act to the jeopardization (risk) of national security. This could result in loss of public confidence, embarrassment or legal action against the organization.

Not an isolated concern (DB security):

When considering the threats facing databases, it is important to remember that the database management system alone cannot be responsible for maintaining the confidentiality, integrity, and availability of the data.

→ The database works as parts of a n/w of services including appln's, web servers, firewalls, SSL terminators and security monitoring systems.

To protect databases against the threats discussed above 4 kinds of control measures are implemented

1) Access Control
2) Inference Control
3) Flow control
4) Encryption.

Two types of security mechanisms are

1) Discretionary security mechanism
2) Mandatory security mechanism

Discretionary security mechanism: These are used to grant privileges to users, including the capability to access specific data files, records or fields in a specified mode.
(Such as read, insert, delete or update)

Mandatory security mechanism: These are used to enforce multilevel security by classifying the data and users into various security classes then implementing the appropriate security Policy of the organization.

Eg: A typical security policy is to permit users at a certain classification (or clearance) level to see only the data items classified at the user's own (or lower) classification level.

Role-based security:- An extension of mandatory security is role-based security, which enforces policies and privileges based on the concept of organizational roles.

→ 1.2) Control Measures: Access control is handled by creating user accounts and passwords to control the login process by the DBMS.

Inference control (statistical database security)
Must ensure information about individuals cannot be accessed.

Flow control:- which prevents information from flowing in such a way that it reaches unauthorized users.

Convert channels: are pathways on which information flows implicitly in ways that violate the security policy of an organization.

Data encryption: which is used to protect sensitive data (such as credit card numbers) that is transmitted via some type of communications n/w.

3) Database security and the DBA

The DBA's responsibilities include granting privileges to users who need to use the system and classifying users and data in accordance with the policy of the organization.

→ The DBA has a DBA account in the DBMS, sometimes called a system or superuser account, which provides powerful capabilities that are not made available to regular db accounts and users.

DBA - Privileged Commands (actions)

1. Account creation: This action creates a new account and password for a user or a group of users to enable access to the DBMS.

2. Privilege granting: This action permits the DBA to grant certain privileges to certain accounts.

3. Privilege revocation: This action permits the DBA to revoke (cancel) certain privileges that were previously given to certain accounts.

4. Security level assignment: This action consists of assigning user accounts to the appropriate security clearance level.

→ The DBA is responsible for the overall security of the database system.

Action 1 in the preceding list is used to control access to the DBMS as a whole, where as actions 2 and 3 are used to control discretionary database authorization and action 4 is used to control mandatory authorization.

Access control, User Accounts and database Audits

→ Whenever a person or a group of persons needs to access a database systems, the individual or group must first apply for a user account.

→ The DBA will then create a new account number and password for the user if there is a legitimate need to access the db.

→ The user must log in to the DBMS by entering the account no and password whenever database access is needed. The DBMS checks that the account number and password are valid; if they are, the user is permitted to use the DBMS and access the db.

→ The db system must also keep track of all operations on the db that are applied by a certain user throughout each login session, which consists of the sequence of db interactions that a user performs from the time of logging in to the time of logging off.

→ To keep a record of all updates applied to the db and particular users who applied each update, we can modify the system log.

→ Systemlog includes an entry for each operation applied to the database that may be required for recovery from a transaction failure or system crash.

→ If any tampering with database is suspected, a database audit is performed, which consists of reviewing the log to examine all accesses and operations applied to the db during a certain period of.

→ Database audits are particully important for sensitive databases that can be updated by many transactions and users, such as a banking database that can be updated by thousands of bank tellers.

→ A database log that is used mainly for security purposes serves as an audit trail.

45) Sensitive data and types of disclosures

Sensitivity of data is a measure of the importance assigned to the data by its owner for the purpose of denoting its need for protection.

several factors can cause data to be classified as sensitive:

1) Inherently Sensitive: The value of the data itself may be so revealing or confidential that it becomes sensitive. Eg A Person's salary or who a Patient has HIV/AIDS.

2) From a Sensitive Source: The source of the day data may indicate a need for secrecy. Eg An informer whose identity must kept secret.

3) Declared sensitive: The owner of the data may have explicitly declared it as sensitive.

4) A sensitive attribute or sensitive record: The particular attribute or record may have been declared sensitive.
Eg Salary attribute of an employee or the salary history record in a personnel db.

5) Sensitive in relation to previously disclosed data: Some data may not be sensitive by itself but will became sensitive in the presence of some other data.
Eg: Exact latitude and longitude information for location where some previously recorded event was later deemed sensitive.

Factors in deciding whether it is safe to reveal the data are:

1) Data availability: If a user updating a field, then this field becomes inaccessible and other users should not be able to view this data. This blocking is only temporary and only to ensure that no user sees any inaccurate data. This is typically handled by the concurrency control mechanism.

2. Access acceptability: Data should only be revealed to authorized users. A database administrator may also deny access to user request even if the request does not directly access a sensitive data item, on the grounds that the requested data may reveal info about the sensitive data that the user is not authorized to have.

3. Authenticity assurance: Before granting access, certain external characteristics about the user may also be considered.

Eg: A user may only be permitted access during working hours. The system may track previous queries to ensure that a combination of queries does not reveal sensitive data.

Security vs Precision

Security: Means of ensuring that data is kept safe from corruption and that access to it is suitably controlled.

→ To provide security means to disclose only non sensitive data and to reject any query that references a sensitive field.

Precision: To protect all sensitive data while disclosing or making available as much nonsensitive data as possible.

1.6) Relationship between Information Security and Information Privacy.

Security in information technology refers to many aspects of protecting a system from unauthorized use, including authentication of users, information encryption, access control, firewall Policies, and intrusion detection.

Privacy is the ability of individuals to control the terms under which their personal information is acquired and used.

→ Security involves technology to ensure that information is appropriately protected.

→ Security is a required building block for Privacy.

2) Discretionary Access Control Based on Granting and Revoking Privileges

DAC: Two levels for assigning privileges to use a db system

1) Account level: At this level, the DBA specifies the particular privileges that each account holds independently of the relations in the database. Eg CREATE, DROP, ALTER, MODIFY, SELECT privileges. 2) not defined for SQL2 (schema or table)

2) The relation (or table) level: At this level, the DBA can control the privilege to access each individual relation or view in the db.

→ Defined for SQL2

→ SQL2 Commands Provide Privileges at the relation and attribute level only.

→ The granting and revoking of privileges generally follow an authorization model for discretionary privileges known as access matrix model, where the rows of Matrix M represents subjects (users, accounts, Programs) and the columns represent objects (relations, columns, views, operations).

→ Each position M(i,j) in the matrix represents the types of privileges (write, read, update) that subject i holds on object j.

. Each relation R assigned an owner account

. owner of a relation given all privileges on that relation.

. owner can grant privileges to other users on any owned relation.

1) SELECT (retrieval or read) Privilege on R: gives account retrieval privilege. In SQL, this gives the account the privilege to use the SELECT Statement to retrieve tuples from R.

2) Modification Privileges on R: This gives the account the capability to modify the tuples of R. In SQL, this includes three privileges UPDATE, DELETE and INSERT.

3) References Privilege on R: This gives the account the capability to reference a Relation R when specifying Integrity constraints.

Specifying Privileges through the use of views

The mechanism of views is an important discretionary authorization mechanism in its own right.

Eg: If the owner A of a relation R wants another account B to be able to retrieve only some fields of R, then A can create a view V of R includes only those attributes and then grant SELECT on V to B.

→ can define view with a query that selects only those tuples from R that A wants B to access.

Revocation and Propagation of Privileges

Revoking of Privileges

→ useful for granting a privilege temporarily

→ REVOKE command used to cancel a privilege

Propagation of Privileges using the GRANT OPTION

→ If GRANT OPTION is given, B can grant privilege to other accounts.

→ DBMS must keep track of how privileges were granted if DBMS allows propagation.

Simple GRANT Syntax:

```
GRANT priv_type [, priv_type]...
  ON object_type
  TO user [user]...
  [WITH GRANT OPTION]
```

An Example to illustrate Granting and Revoking of Privileges

Suppose that DBA creates four accounts — A_1, A_2, A_3 and A_4 and wants only A_1 to be able to create base relations.

```
GRANT CREATETAB TO A1;
```

The CREATETAB (create table) privilege gives account A_1 the capability to create new database tables and is hence an account Privilege.

→ A_1, A_2 and so forth may be individuals like John in IT department or mary in marketing but they may also be appln or programs that want to access database.

→ CREATE SCHEMA EXAMPLE AUTHORIZATION A1;

User account A1 can now create tables under the schema called EXAMPLE.

→ Suppose that A1 creates the two base relations EMPLOYEE and DEPARTMENT.

A1 is then the owner of these two relations and hence has all the relation privileges on each of them.

→ GRANT INSERT, DELETE ON EMPLOYEE, DEPARTMENT TO A2; (A1 to A2)

→ A2 was not given the WITH GRANT OPTION.

→ A2 cannot give privilege to other users.

→ A1 to A3

GRANT SELECT on Emp, Dept TO A3 WITH GRANT OPTION;

A3 given the WITH GRANT OPTION.

A3 can give privilege to other users.

→ A3 to A4

- GRANT SELECT on Emp TO A4;
- A4 cannot propagate the SELECT privilege.

- Suppose A1 decides to revoke the SELECT privilege from A3.
- REVOKE SELECT ON Emp FROM A3;
- DBMS revokes SELECT privilege on Emp from A3 but also A4 Because A3 no longer has that privilege.

→ Suppose A1 want to give back to A3 a limited capability on to SELECT on Emp

```
CREATE VIEW A3Emp AS
SELECT Name, Bdate, Address
FROM Emp
WHERE DNO=5;
GRANT SELECT on A3 Emp TO A3
WITH GRANT OPTION.
```

EMPLOYEE

Name	Ssn	Bdate	Address	Sex	Salary	Dno

DEPARTMENT

Dnumber	Dname	Mgr_ssn

→ Figure shows Schemas for the two relations EMPLOYEE and DEPARTMENT.

Specifying Limits on Propagation of Privileges

→ Horizontal Propagation

→ Vertical Propagation → It is more complicated.

Mandatory Access Control and Role Based Access Control for Multilevel Security

Mandatory access control is an additional security policy that classifies data and users based on security classes.

→ Typical security classes are
1) top secret (TS)
2) Secret (S)
3) Confidential (C)
4) unclassified (U) where TS is the highest level and U the lowest.

$TS \geq S \geq C \geq U$.

→ The commonly used model for multilevel security, known as the Bell-Lapadula model classifies each subject (user, account, program) and object (relation, tuple, column, view, operation) into one of the security classifications TS, S, C or U.

→ Simple security property

Subject S not allowed read access to object O unless class(S) ≥ class(O).

→ Star property (* - property)

. subject not allowed to write an object unless class(S) ≤ class(O)

. Prevent information from flowing from higher to lower classifications.

→ Attributes values and tuples considered as data objects.

Filtering & Polinstantiation

→ Sometimes it is necessary to store two or more tuples at different classification levels with the same apparent key.

→ several tuples have the same key, but have different values for users at diff clearance levels. — Polyinstantiation

The apparent key of a multilevel relation is the set of attributes that would have formed the Primary key in a regular relation.

→ It is possible to store a single tuple in the at a higher classification level and Produce the corresponding tuples at a lower-level classification through a process known as

. filtering.

Example: A multilevel relation to illustrate multilevel security.

a) EMPLOYEE

Name	Salary	JobPerformance	TC
Smith U	40000 C	Fair S	S
Brown C	80000 S	Good C	S

a) The original EMPLOYEE tuples.

b) EMPLOYEE

Name	Salary	JobPerformance	TC
Smith U	40000 C	NULL C	C
Brown C	NULL C	Good C	C

b) Appearance of EMPLOYEE after filtering for classification C users.

c) EMPLOYEE

Name	Salary	JOB Performance	TC
Smith U	NULL C	NULL U	U

c) Appearance of EMPLOYEE after filtering for classification U users.

d) EMPLOYEE: Polyinstantiation of the Smith tuple.

Name	Salary	JOB Performance	TC
Smith U	40000 C	Fair S	S
Smith U	40000 C	Excellent C	C
Brown C	80000 S	Good C	S

Assume that the Name attributes is the apparent key. and consider the query SELECT * FROM EMPLOYEE.

→ A user with security clearance S would see the same relation shown in figure (a) since all tuple classifications are less than or equal to S.

→ A user with security clearance C would not be allowed to see the values for Salary of 'Brown' and Job_Performance of 'Smith', since they have higher classification.

→ The tuples would be filtered to appear as shown in figure (b) with Salary and Job_Performance appearing as null.

→ For a user with security clearance U, the filtering allows only name attribute of 'Smith' to appear, with all the other attributes appearing as null shown in figure (c)

```
UPDATE EMPLOYEE
SET Job_Performance = "Excellent"
WHERE Name = "Smith";
```

However the user should not be ~~highly secure system~~ allowed to overwrite the existing value of Job_Performance at the higher classification level. The solution is to create a polyinstantiation for the Smith tuple at the lower classification level; C shown in figure (d).

Comparing Discretionary Access control and Mandatory Access control.

→ DAC policies have a high degree of flexibility, which makes them suitable for a large variety of appⁿ domains.

→ The main drawback of DAC models is their vulnerability to malicious attacks.

→ Do not impose control on how information is propagated.

→ Mandatory policies ensure high degree of protection in a way, they prevent any illegal flow of information.

→ Mandatory policies are suitable for military and high-security types of appⁿs which require higher degree of protection.

→ The drawback of Mandator. policies are of being too rigid.

→ Prevent illegal information flow.

Role-Based Access control

Its basic notion is that privileges and other permissions are associated with organizational roles rather than individual users.

→ Individual users are then assigned to appropriate roles.

→ Roles can be created using the CREATEROLE and DESTROY ROLE commands.

→ can be used with traditional discretionary and mandatory access control.

→ Mutual exclusion of roles

↳ Boths roles cannot be used simultaneously.

→ Mutual exclusion of roles can be categorized into 2 types

1) authorization time exclusion (static)

2) runtime exclusion (dynamic)

Label-Based security and Row-level Access Control

Many mainstream RDBMS currently use the concept of row-level control, where sophisticated access control rules can be implemented by considering the data row by row.

→ In row-level access control, each data row is given a label, which is used to store information about data sensitivity.

→ used to prevent unauthorized users from viewing or altering certain data.

→ Provides finer granularity of data Security.

→ Label Security Policy: A Policy defined by an administrator is called label security Policy. Whenever data affected by the policy is accessed or queried through an appln, the Policy is automatically invoked.

→ When a Policy is implemented a new column is added to each row in the Schema.

→ The added column contains the label for each row that reflects the sensitivity of the row as per the policy.

→ The label Security requirements are applied on top of the DAC requirements for each user. Hence the user must satisfy the DAC requirements and then the label security requirement to access a row.

XML Access Control: With the world wide use of XML in commercial and scientific appln, efforts are under way to develop security standards.

→ Among those efforts are digital signatures and encryption standards for XML.

→ An XML digital sig Signature differs from other protocols for message signing, such as OpenPGP (Pretty Good Privacy).

→ OpenPGP is a confidentiality and authentication service that can be used for mail and file storage appln.

Access Control Policies for the Web and Mobile Applns

→ E-commerce environments require elaborate access control policies that go beyond traditional DBMSs.

→ Legal and financial consequences for unauthorized data breach

→ content-based access control
Takes protection object content into account.

→ Credential is a set of properties concerning a user that are relevant for security purposes.

Eg: By using credentials, one can simply formulate Policies such as only permanent staff with five or more service can access documents related to the sports

SQL Injection (SQLI)

SQL Injection is one of the most common threats to a database systems.

→ SQL injection is one of the most common web hacking techniques.

→ SQL injection is the placement of malicious code in SQL statements, via web page input.

Some of the frequent attacks on databases are:

Unauthorized Privilege escalation: This attack is characterized by an individual attempting to elevate his or her privilege by attacking vulnerable points in the database systems.

Privilege abuse: whereas unauthorized privilege escalation is done by an unauthorized user, this attack is performed by privilege user.

Eg: An administator who is allowed to change student information can use this privilege to update student grades without the instructor's permission.

Denial of service: DoS attack is an attempt to make resources unavailable to its intended users.

Eg Access to network applications or data is denied to intended users by overflowing the buffer or consuming resources.

Weak authentication: If the user authentication scheme is weak, an attacker can impersonate the identity of a legitimate user by obtaining her login credentials.

SQL Injection Methods

In an SQL Injection attack, the attacker injects a string input through the application, which changes or manipulates the SQL statement to the attacker's advantage.

Types of injection attacks

SQL Manipulation: A manipulation attack, which is the most common type of injection attack, changes an SQL commands in an appln.

Eg: By adding conditions to the WHERE clause of a query, or by expanding a query with additional query components using set operations such as UNION, INTERSECT, or MINUS.

other types of manipulation attacks are also possible.

Eg: Database Login (during)

SELECT * FROM users WHERE username = 'jake' and PASSWORD ="" 'jakespassword";

The attacker can try to change the SQL stmt by

SELECT * FROM users WHERE username = 'jake' and (PASSWORD = 'jakespassword or 'x' = 'x');

Code injection: This type of attack attempts to add additional SQL statements or commands to existing stmt by exploiting a computer bug, which is caused by processing invalid data.

→ The attacker can inject or introduce code into a computer program to change the course of execution.

→ Code injection is a popular technique for system hacking or cracking to gain information.

Function Call injection: In this kind of attack, a databe function or operating system function call is inserted into a vulnerable SQL statement to manipulate the data.

Eg: The dual table is used in the FROM clause of SQL. To get today's date

SELECT SYSDATE FROM dual;

to

SELECT TRANSLATE ('user input', 'from_string', 'to_string') FROM dual

Here TRANSLATE is used to replace a string of characters with another string of characters.

→ The TRANSLATE function above will replace the characters of the 'from_string' with the characters in the 'to_string' one by one. This means that the f will be replaced with the t, the r with the o, the o with the -, and so on.

Risks Associated with SQL Injection

1) Database fingerprinting: This attacker can determine the type of database being used in the backend so that he can use database-specific attacks that correspond to weakness in a particular DBMS.

Denial of Service: This attacker can flood the server with requests thus denying service to valid users or the attacker can delete some data.

Bypassing authentication: This is one of the most common risks in which the attacker can gain access to the database as an authorized user & perform all the desired tasks.

Identifying injectable parameters: In this type of attack the attacker gathers important info about the type of structure of the back-end db of a web appln.

Executing remote Commands: This provides attackers with a tool to execute arbitary Commands on the db.

Eg: Remote user can execute stored db Procedures & functions from a remote SQL Iteractive Interface.

Performing privilege escalation: This type of attack takes advantage of logical flaws within the db to upgrade the access level.

Protection Techniques against SQLI

protection against SQLI attacks can be achieved by applying certain Programming rules to web-accenible Procedures and functions

Bind variables (using Parameterized stmts): The use of bind variables (also known as Parameters) protects against injection attacks and also improves performance.

Eg using Java and JDBc

```
PreparedStatement stmt = Conn.PrepareStatement
("SELECT * FROM EMPLOYEES WHERE
EMPLOYEE_ID = ? AND PASSWORD = ? ");
stmt.setString (1, employee_id);
stmt.setString (2, Password);
```

Filtering Input (Input validation): This technique can be used to remove 'escape' characters from inputs by using the SQL Replace function.

Eg: The delimiter single quote (') can be replaced by two single quotes ('').

Function Security: Datab functions, both standard and custom, should be restricted, as they can be exploited in the SQL function injection attacks.

Introduction to Statistical Database Security

→ Statistical databases are used mainly to produce statistics about various populations.

→ The database may contain confidential data about individuals, this information should be protected from user accen.

→ users are permitted to retrieve statistical information about the populations, such as averages, sums, accounts, maximum, minimum and standard deviations.

PERSON

Name	Ssn	Income	Address	City	State	Zip	Sex	Last_degree

PERSON

The above example refers to the relation with the attributes Name, Ssn, Income, Address, City, State, Zip, sex and Last_degree.

→ A population is a set of tuples of a relation (table), that satisfy some selection condition. Hence each selection condition on the PERSON relation will specify a particular population of the PERSON tuples.

Ex: the condition Sex = 'M' specifies the male population, of

the condition ((Sex = 'F') and (Last_degree = 'M.S' OR Last_degree = 'Ph.D') specifies the female population that has an M.S or Ph.D. degree as their highest degree.

condition city = 'Houston' specifies the population that lives in Houston.

Statistical queries involve applying statistical functions to a population of tuples.

Ex: We may want to retrieve the no. of individuals in population or average income in the population.

→ statistical users are not allowed to retrieve individual data, such as the income of a specific person.

→ statistical database security techniques must prohibit the retrieval of individual data.

→ This can be achieved by prohibiting queries that retrieve attribute values and by allowing only queries that involves statistical aggregate functions such as COUNT, SUM, MIN, MAX, AVERAGE and STANDARD DEVIATION. Such queries are sometimes called statical database queries.

SELECT COUNT (*) FROM PERSON
WHERE <condition>;

→ Preventing the inference of individual information

Provide minimum threshold on number of tuples

Prohibit sequences of queries that refer to same population of tuples.

Introduce slight noise or inaccuracy.

- partition the database
  - store records in groups of minimum size.

Introduction of flow control

Flow control regulates the distribution of flow of information among accessible objects.

→ A flow between object x and object y occurs when a program reads values from x and writes values into y.

→ Flow controls check that information contained in some objects does not flow explicitly or implicitly into less protected objects. Thus user cannot get indirectly in y what he or she cannot get directly in x.

→ A flow policy specifies the channels along which information is allowed to move.

The simplest flow policy specifies just two classes of information - confidential (C) and nonconfidential (N) and allows all flows except those from class C to class N.

→ This policy can solve the confinement problem that arises when a service program handles data such as customer information, some of which may be confidential.

Ex: A income-tax computing service might be allowed to retain a customer's address and the bill for services rendered, but not a customer's income or deductions.

→ Convert channels: A convert channel allows a transfer of information that voilates the security or the policy.

→ specially, a convert channel allows information to pass from a higher classification level to a lower classification level through improper means.

2 types of convert channels are there

1) Timing channel: In this channel the information conveyed by the timing of events or processes.

2) Storage channel: - It does not require any temporal synchronization, in that information is conveyed by accessing system information or what is otherwise inaccessible to the user.

Encryption and public key Infrastructures

→ The previous methods of access and flow control despite being strong control measures may not able to protect databases from some threats.

→ Suppose we communicate data, but our data falls into the hands of a nonlegitimate user. In this situation, by using encryption we can disguise the message so that even if the transmission is diverted the message will not be revealed.

→ Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized persons.

→ • Ciphertext: Encrypted (enciphered) data

• Plaintext (or) cleartext: Intelligible data that has meaning and can be read or acted upon without the appln of decryption.

• Encryption: The process of transforming plaintext into ciphertext.

Decryption: The process of transforming ciphertext back into plaintext.

→ Encryption consists of applying an encryption algorithm to data using some specified encryption key.

→ The resulting data must be decrypted using decryption key to recover the original data.

The Data Encryption and Advanced Encryption Standards

→ The Data Encryption Standard (DES) is a system developed by the U.S government for use by the general PUBLIC.

→ It has been widely accepted as cryptographic Standard both in the united states and abroad.

→ DES can provide end-to-end encryption on the channel between sender A and receiver B.

→ DES algorithm derives is a careful and complex combination of two of the fundamental building blocks of encryption: Substitution and Permutation (transposition).

→ The algorithm derives its strength from repeated appln of these two techniques for total no. of 16 cycles.

→ Plaintext (the original form of message) is encrypted as blocks of 64 bits.

→ Although key is 64 bits long, it effect the key can be any 56-bit no.

→ The NIST introduced the Advanced Encryption Standard (AES).

→ This algorithm has a block size of 128bits compared with DES's 56-block size, and can use keys of 128, 192 or 256 bits compared with DES's 56-bit key.

→ AES introduces more possible keys as compared with DES, and thus takes a much longer time to crack.

→ In present systems, AES is the default with large key lengths. It is also the standard for full drive encryption products, with both Apple FileVault and Microsoft BitLocker using 256-bit or 128 key bit keys.

→ Triple-DES is a fallback option if a legacy system cannot use modern encryption standard.

Symmentric key Algorithms

→ A Symmetric key is one key that is used for both encryption and decryption.

→ By using symmetric key, fast encryption and decryption is possible for routine data in db.

→ A Message encrypted with a secret key can be decrypted only with some secret key.

→ Algorithms used for symmetric key encryption are called secret key algorithms. Since secret key algorithms are mostly used for encrypting the content of a message, they are also called content-encryption algorithms.

→ Need for sharing the secret key - can apply some function to user-supplied password string at both send and receiver, this is called Password-based encryption algorithm.

Public (Asymmetric) Key Encryption

→ In 1976, Diffie and Hellman proposed a new kind of cryptosystem, which they called Public key encryption.

→ Public key algorithms are based on mathematical functions rather than operations on bit patterns.

→ They address one drawback of symmetric key encryption, namely that both senders and recipient must exchange the common key in a secure manner.

→ In Public key systems, two keys are used for encryption / decryption.

Digital Signatures

A digital signature is an example of using encryption techniques to provide authentication services in electronic Commerce appln's.

→ A digital signature consists of a string of symbols. If a person's digital signature were always the same for each message, it can easily copy the string of symbols. Thus signatures must be different for each use.

→ This can be achieved by making each digital signature a function of the message that is signing together with a timestamp.

→ Depends on secret number unique to the signer.

→ Public key techniques used to create digital signatures.

Digital Certificates

A digital certificate is used to combine the value of public key with identity of the person or service that holds the corresponding private key into digitally signed statement.

→ Certificates are issued and signed by certification authority (CA).

→ Entity receiving the certificate from a CA is the subject of that certificate. Instead of requiring each participant in an appln to authenticate each user, third party authentication relies on the use of digital certificates.

→ The digital certificate itself contains various types of information. Eg: both the certification authority and certificate owner information are included.

· The following list describes all the information included in the certificate

1. owner information – certificate owner information represented by unique identifier known as distinguished name (DN) of the owner. This includes the owner's name as well as the owner's organization and other information about the owner.
2) The certificate also includes the public key of the owner
3) The date of issue of the certificate is also included.
4. The validity period is specified by 'valid From' and 'valid to' dates, which are included in each certificate.
5) Issuer identifier information is included in the certificate.
6) Finally, the digital signature of the issuing CA for the certificate is included.

→ All the information listed is encoded through a message digest function, which creates the digital signature.

→ The digital signature basically certifies which that the association between the certificate owner and Public key is valid.

Privacy issues and Preservation

1) Growing challenge for database security.
2) Limit Performing large-scale mining and analysis.
3) central warehouses for vital information.
   - violating security could expose all data.
4) Distributed datamining algorithms.
5) Remove identity information in released data.
6) Inject noise into the data.
   - must be able to estimate errors introduced.

Challenges to Maintaining Database Security

1) Data Quality: Quality stamps that are posted on web sites.
   → Automatically repairing incorrect data.
2) Intellectual Property rights: watermarking techniques are used.
   → The main purpose of digital watermarking is to protect content from duplication and distribution by enabling Provable ownership of the content.
3) Database Survivability
   a) Confinement: Take immediate action to eliminate/reduce attacker's accey.
   b) Damage assessment: Determine the extent of Problem ~~to Prevent~~ including failed functions and corrupted data.
   c) Reconfiguration: Reconfigure to allow operation to continue in a degraded mode while recovery proceeds.
   d) Repair: Recover corrupted or lost data or reinstall failed system functions to reestablish a normal level of operation.
   e) Fault treatment: Identify the weakness and holes.