Unit II

CHAPTER 2

Authentication

Syllabus Topic : Authentication

2.1 Authentication

Q. 2.1.1 Explain the terms authentication. (Ref. Sec. 2.1) **(5 Marks)**

- **Authentication** mechanism determines the user's identity before revealing the sensitive information. It is very crucial for the system or interfaces where the user's priority is to protect the confidential information. In the process, the user makes a provable claim about individual identity (his or her) or an entity's identity.
- The credentials or claim could be a username, password, fingerprint etc. The authentication and non-repudiation, kind of issues are handled in the application layer. The inefficient authentication mechanism could significantly affect the availability of the service.

Example

- For example, there is a sender A sending an electronic document to the receiver B over the internet. How does the system will identify that the sender A has sent a message dedicated to the receiver B. An intruder C may intercept, modify and replay the document in order trick or steal the information this type of attack is called **fabrication**.
- In the given situation authentication mechanism ensures two things; first, it ensures that the sender and receiver are righteous people and it's known as **data-origin authentication**. Secondly, it ensures the security of the established connection between sender and receiver with the help of secret session key so that it could not be inferred and it is known as **peer entity authentication**.

2.1.1 Types of Authentication Methods

- Traditional authentication depends on the use of a password file, in which user IDs are stored together with hashes of the passwords associated with each user. When logging in, the password submitted by the user is hashed and compared to the value in the password file. If the two hashes match, the user is authenticated.
- This approach to authentication has several drawbacks, particularly for resources deployed across different systems. For one thing, attackers who are able to access to the password file for a system can use brute force attacks against the hashed passwords to extract the passwords. For another, this approach would require multiple authentications for modern applications that access resources across multiple systems.
- Password-based authentication weaknesses can be addressed to some extent with smarter user names and password rules like minimum length and stipulations for complexity, such as including capitals and symbols. However, password-based authentication and knowledge-based authentication are more vulnerable than systems that require multiple independent methods.

Other authentication methods include :

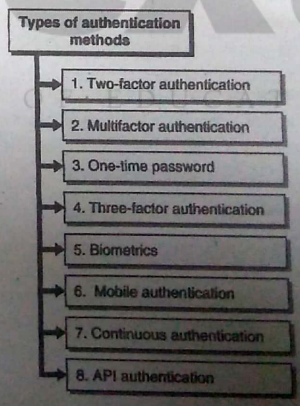

Fig. 2.1.1 : Types of authentication methods

➜ **1. Two-factor authentication**

Two-factor authentication adds an extra layer of protection to the process of authentication. 2FA requires that a user provide a second authentication factor in addition to the password. 2FA systems often require the user to enter a verification code received via text message on a preregistered mobile phone, or a code generated by an authentication application.

➜ **2. Multifactor authentication**

Multifactor authentication requires users to authenticate with more than one authentication factor, including a biometric factor like fingerprint or facial recognition, a possession factor like a security key fob or a token generated by an authenticator app.

➜ **3. One-time password**

A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user. This password is only valid for one login session or transaction, and is usually used for new users, or for users who lost their passwords and are given a one-time password to log in and change to a new password.

➜ **4. Three-factor authentication**

Three-factor authentication (3FA) is a type of MFA that uses three authentication factors, usually a knowledge factor (password) combined with a possession factor (security token) and inherence factor (biometric).

➜ **5. Biometrics**

While some authentication systems can depend solely on biometric identification, biometrics are usually used as a second or third authentication factor. The more common types of biometric authentication available include fingerprint scans, facial or retina scans and voice recognition.

➜ **6. Mobile authentication**

Mobile authentication is the process of verifying user via their devices or verifying the devices themselves. This lets users log into secure locations and resources from anywhere. The mobile authentication process involves multifactor authentication that can include one-time passwords, biometric authentication or QR code validation.

➜ **7. Continuous authentication**

With continuous authentication, instead of a user being either logged in or out, a company's application continually computes an "authentication score" that measures how sure it is that the account owner is the individual who's using the device.

➜ **8. API authentication**

- The standard methods of managing API authentication are : HTTP basic authentication; API keys and OAuth.
- In HTTP basic authentication, the server requests authentication information, i.e., a username and password, from a client. The client then passes the authentication information to the server in an authorization header.
- In the API key authentication method, a first-time user is assigned a unique generated value that indicates that the user is known. Then each time the user tries to enter the system again, his unique key is used to verify that he is the same user who entered the system previously.
- Open Authorization (OAuth) is an open standard for token-based authentication and authorization on the internet.
- OAuth allows a user's account information to be used by third-party services, such as Facebook, without exposing the user's password.
- OAuth acts as an intermediary on behalf of the user, providing the service with an access token that authorizes specific account information to be shared.

2.1.2 User Authentication Vs. Machine Authentication

Machines also need to authorize their automated actions within a network. Online backup services, patching and updating systems and remote monitoring systems, such as those used in telemedicine and smart grid technologies, all need to securely authenticate to verify that it is the authorized system involved in any interaction and not a hacker.

2.1.3 Additional Uses for Authentication

Computer establishing a secure channel for network communication. Examples of these are SSH and IPSec.

2.1.3.1 SSH

Secure SHell (SSH) is available for most versions of Unix as well as for Windows systems. The SSH protocol is used for secure remote login from one computer to another. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. It is a secure alternative to the non-protected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP).

2.1.3.2 IPSec

- IPSec is one of the new buzz words these days in the networking security area. It's becoming very popular and also a standard in most operating systems. Windows 2000 fully supports IPSec and that's most probably where you are likely to find it.
- Routers these days also support IPSec to establish secure links and to ensure that no-one can view or read the data they are exchanging.
- When the original IP (Internet Protocol) specification was created, it didn't really include much of a security mechanism to protect it from potential hackers. There were 2 reasons they didn't give IP some kind of security.
- First was because back then (we are talking around 30 years ago) most people thought that users and administrators would continue to behave fairly well and not make any serious attempts to compromise other people's traffic. Second reason was because the cryptographic technology needed to provide adequate security simply wasn't widely available and in most cases not even known about!

Syllabus Topic : Authorization

2.2 Authorization

Q. 2.2.1 Explain the term authorization. (Ref. Sec. 2.2) **(5 Marks)**

Authorization technique is used to determine the permissions that are granted to an authenticated user. In simple words, it checks whether the user is permitted to access the particular resources or not. Authorization occurs after authentication, where the user's identity is assured prior then the access list for the user is determined by looking up the entries stored in the tables and databases.

Example

- For example, a user X wants to access a particular file from the server. The user will send a request to the server. The server will verify the user identity. Then, it finds the corresponding privileges the authenticated user have or whether he/she is allowed to access that particular file or not. In the following case, the access rights could include viewing, modifying or deleting the file if the user has authority to perform the following operations.
- The authentication and authorization are used in respect of information security which enables the security on an automated information system. The terminologies are

interchangeably used but are distinct. The identity of a person is assured by authentication. On the other hand, authorization checks the access list that the authenticated person has. In other words, the authorization includes the permissions that a person has given.

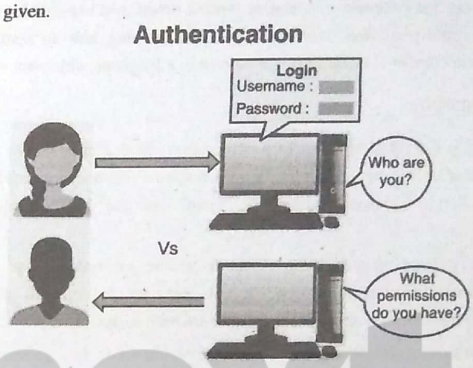

Fig. 2.2.1

Syllabus Topic : Encryption

2.3 Encryption

Q. 2.3.1 Write a short note on encryption. (Ref. Secs. 2.3 and 2.3.1) **(5 Marks)**

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Syllabus Topic : A Brief History of Encryption

2.3.1 A Brief History of Encryption

Q. 2.3.2 Write a short note on encryption. (Ref. Secs. 2.3 and 2.3.1) **(5 Marks)**

- Once upon a time, when technology was not that developed, securing a data was not hard. Few people were literate, the use of written language alone often sufficed to keep information from becoming general knowledge.
- To keep secrets, the information is simply written down, and kept hidden from those few people who could read, and prevent others from learning how to read. Decoding the meaning of a document is difficult if it is written in a language which not used in general.

2.3.2 Cryptography

- Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing".
- In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher.
- These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

2.3.2.1 Cryptography Techniques

- Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.
- However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives :

1. **Confidentiality :** The information cannot be understood by anyone for whom it was unintended.
2. **Integrity :** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
3. **Non-repudiation :** The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

4. **Authentication :** The sender and receiver can confirm each other's identity and the origin/destination of the information.

- Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

Syllabus Topic : Symmetric-Key Cryptography

2.3.2.2 Symmetric-Key Encryption(Cryptography)

Q. 2.3.3 Explain Symmetric Key Cryptography. (Ref. Sec. 2.3.2.2) **(5 Marks)**

- In **symmetric-key encryption**, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message.
- Think of it like this : You create a coded message to send to a friend in which each letter is substituted with the letter that is two down from it in the alphabet. So "A" becomes "C", and "B" becomes "D". You have already told a trusted friend that the code is "Shift by 2". Your friend gets the message and decodes it. Anyone else who sees the message will see senseless message.
- The same goes for computers, but, of course, the keys are usually much longer. The first major symmetric algorithm developed for computers in the United States was the Data Encryption Standard (DES), approved for use in the 1970s. The DES uses a 56-bit key.
- Because computers have become increasingly faster since the 70s, security experts no longer consider DES secure - although a 56-bit key offers more than 70 quadrillion possible combinations (70,000,000,000,000,000), an attack of brute force (simply trying every possible combination in order to find the right key) could easily decipher encrypted data in a short while.
- DES has since been replaced by the Advanced Encryption Standard (AES), which uses 128-, 192- or 256-bit keys. Most people believe that AES will be a sufficient encryption

standard for a long time coming: A 128-bit key, for instance, can have more th 300,000,000,000,000,000,000,000,000,000,000,000 key combinations.

Syllabus Topic : Public Key Cryptography

2.3.2.3 Public Key Cryptography

Q. 2.3.4 Explain Public Key Cryptography. (Ref. Sec. 2.3.2.3) **(5 Marks)**

- Unlike symmetric key cryptography, we do not find historical use of public-k cryptography. It is a relatively new concept.
- Symmetric cryptography was well suited for organizations such as governments, militar and big financial corporations were involved in the classified communication.
- With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be not practical due to challenges it faced for key management. This gave rise to the public ke cryptosystems.
- The process of encryption and decryption is depicted in the following illustration :

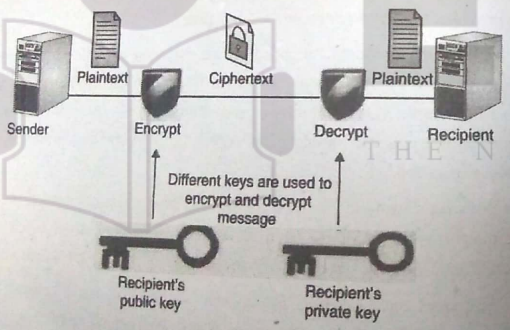

Fig. 2.3.1

The most important properties of public key encryption scheme are

- Different keys are used for encryption and decryption. This is a property which set this scheme different than symmetric encryption scheme.
- Each receiver possesses a unique decryption key, generally referred to as his private key.

- Receiver needs to publish an encryption key, referred to as his public key.
- Some assurance of the authenticity of a public key is needed in this scheme to avoid spoofing by adversary as the receiver. Generally, this type of cryptosystem involves trusted third party which certifies that a particular public key belongs to a specific person or entity only.
- Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.
- Though private and public keys are related mathematically, it is not be feasible to calculate the private key from the public key. In fact, intelligent part of any public-key cryptosystem is in designing a relationship between two keys.

Syllabus Topic : Public Key Infrastructure

2.3.2.4 Public Key Infrastructure

Q. 2.3.5 Explain Public Key Infrastructure. (Ref. Sec. 2.3.2.4) **(5 Marks)**

- The public key infrastructure concept has evolved to help address this problem and others. A Public Key Infrastructure (PKI) consists of software and hardware elements that a trusted third party can use to establish the integrity and ownership of a public key.
- The trusted party, called a Certification Authority (CA), typically accomplishes this by issuing signed (encrypted) binary certificates that affirm the identity of the certificate subject and bind that identity to the public key contained in the certificate.
- The CA signs the certificate by using its private key. It issues the corresponding public key to all interested parties in a self-signed CA certificate. When a CA is used, the preceding example can be modified in the following manner:
  1. Assume that the CA has issued a signed digital certificate that contains its public key. The CA self-signs this certificate by using the private key that corresponds to the public key in the certificate.
  2. Alice and Bob agree to use the CA to verify their identities.
  3. Alice requests a public key certificate from the CA.
  4. The CA verifies her identity, computes a hash of the content that will make up her certificate, signs the hash by using the private key that corresponds to the public key in the published CA certificate, creates a new certificate by concatenating the certificate content and the signed hash, and makes the new certificate publicly available.

5. Bob retrieves the certificate, decrypts the signed hash by using the public key of the CA, computes a new hash of the certificate content, and compares the two hashes. If the hashes match, the signature is verified and Bob can assume that the public key in the certificate does indeed belong to Alice.
6. Bob uses Alice's verified public key to encrypt a message to her.
7. Alice uses her private key to decrypt the message from Bob.

- In summary, the certificate signing process enables Bob to verify that the public key was not tampered with or corrupted during transit.
- Before issuing a certificate, the CA hashes the contents, signs (encrypts) the hash by using its own private key, and includes the encrypted hash in the issued certificate.
- Bob verifies the certificate contents by decrypting the hash with the CA public key, performing a separate hash of the certificate contents, and comparing the two hashes. If they match, Bob can be reasonably certain that the certificate and the public key it contains have not been altered.

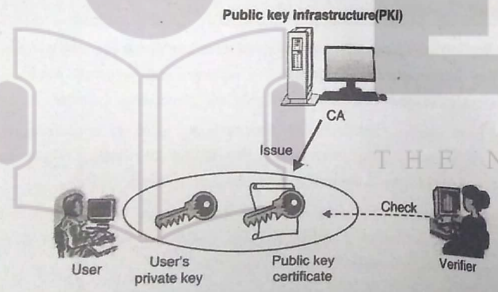

Fig. 2.3.2

Syllabus Topic : Storage Security : Storage Security Evolution

2.4 Storage Security

2.4.1 Evolution of Storage Security

Q. 2.4.1 Write a short note on storage security evolution. (Ref. Sec. 2.4.1) (5 Marks)

- In terms of data storage, the first generation was floppy disk drives. For long, floppy diskettes had dominated but now technology has unveiled flash disks. Compare to portable storage devices floppy disks were hard to secure.
- They were easily lost, or the data on them became corrupted. They could be used to propagate malware, either through files on the disk or through active code like the "girlfriend exploit" (named for the infamous practice of breaking into a network by giving a disk containing exploit software to a significant other who works there, and instructing her to run the program).
- The use of floppy disks was largely phased out by the late 2000s. Now a days, almost no new computers include floppy drives.
- The next generation of storage devices, Compact Discs (CDs) and Digital Video Discs (DVDs). Unlike other, these are more volatile storage media, these optical data storage devices seem like they will last forever if handled properly.
- While optical discs are great for reliability and availability of data, their longevity may cause an issue. If a private or confidential data is stored on a CD or DVD and then disc is misplaced, it might be discovered by an intruder in the future.
- Flash drives (USB sticks and the like) have exploded in popularity over the past few years. These devices have become so cheap and prevalent that they have practically supplanted optical storage devices. Data can be store in such drives by simply copy pasting.
- Flash drives are prone to both malware and girlfriend exploits, in the same way floppies were. Also, these are prone to "autorun" (automatic execution of any code that is on the device, immediately upon connecting it).
- Flash drives are a significant source of malware infections in many environments. In addition, they make data theft remarkably easy with their small size, portability, and compatibility with every major computing platform.
- Portable hard drives, like flash drives, are cheap and plentiful. With their large storage capacities, they carry all the same threats. In fact, portable USB hard drives have so much capacity that they can be used to steal all the data in many organizations.
- Portable hard drives have made it so easy to bulk-download huge amounts of data like fishing with a huge net that data thieves are sure to find valuable intellectual property strewn among the files they collect. Even modern smart phones, cameras, and tablets contain large amounts of flash memory and are accessible via USB, allowing data thieves to copy files unnoticeable.

- The newest form of portable storage is the Solid-State Drive (SSD). SSD devices combine the best features of flash drives and portable hard drives, and as their prices drop in relation to demand, we can expect them to become increasingly ubiquitous.
- And, like flash drives and portable hard drives, SSDs facilitate bulk data theft. The security practitioner now also has to contend with smart phones and mobile devices, which have significant amounts of onboard storage. Now a days, it's easy to store and hide private data on smart phones. These devices pose a significant risk to an organization's data because any stolen data hiding on them can be hard to detect.
- All of the storage devices mentioned are considered to be unmanaged if no protection mechanisms are applied on data stored on them. The best protections for (and against) them are encryption and access control. Encrypting confidential data can stop, or discourage, data theft.
- Information rights management can protect confidential documents such that, even if they are stolen, they can't be opened by unauthorized users. In addition, USB device control software can block access to the USB ports on computers where it's installed, and it can allow or block various activities such as copying to or from USB devices, based on the type of document.
- Ultimately, unmanaged storage devices are hard to secure and hard to control. That's why organizations have turned to managed storage, which allows their data to be accessed in secure, controlled ways. With managed storage, organization scan block USB storage devices and drive users toward the managed storage instead.

Syllabus Topic : Modern Storage Security

2.4.2 Modern Storage Security

Q. 2.4.2 Write a short note on modern storage security. (Ref. Sec. 2.4.2) (5 Marks)

- Growing cyber threats are driving the need for a new best practice for data storage security and management. Modern storage solutions have moved away from the endpoint computers to the network.
- Network-Attached Storage (NAS) and Storage Area Networks (SANs) consist of large hard drive arrays with a controller that serves up their contents on the network. NAS can

be accessed by most computers and other devices on the network, while a SAN is typically used by servers.

- These storage systems have many built-in security capabilities to choose from. Based on the security requirements of the environment, these security settings can be configured to meet the objectives of the security policy. Today's storage environments are complex. In fact, modern storage environments can be considered as separate IT infrastructures of their own. Many organizations are now dividing their IT organizations along the lines of networks, servers, and storage.

Syllabus Topic : Risk Remediation

2.4.3 Risk Remediation

Q. 2.4.3 Write a short note on risk remediation. (Ref. Sec. 2.4.3) (5 Marks)

- There are several risks associated with data storage. These risks are categorized according to the classic CIA triad of Confidentiality, Integrity, and Availability. For each identified risk, where possible, security controls consistent with the "three Ds" of security; defense, detection, and deterrence.
- They are applied in an effort to mitigate the risk using the principle of layered security (also known as defense-in-depth). What's left after those controls are applied to mitigate the risks is then identified as residual risks.

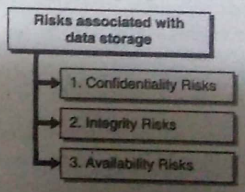

Fig. 2.4.1 : Risks associated with data storage

2.4.3.1 Confidentiality Risks

Q. 2.4.4 Explain risk remediation for confidential risk. (Ref. Sec. 2.4.3.1) (5 Marks)

Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to unauthorized ones. Confidentiality risks

information, it is important to make the information available in a controlled fashion to those who need it, without exposing it to unauthorized parties.

Data leakage, theft, exposure, forwarding

Data leakage is the risk of loss of information, such as confidential data and intellectual property, through intentional or unintentional means. There are four major threat vectors for data leakage: theft by outsiders, malicious sabotage by insiders (including unauthorized data printing, copying, or forwarding), inadvertent misuse by authorized users, and mistakes created by unclear policies.

- **Defense :** Employ software controls to block inappropriate data access using a Data Loss Prevention (DLP) solution and/or an Information Rights Management (IRM) solution.
- **Detection :** Use watermarking and data classification labelling along with monitoring software to track data flow.
- **Deterrence :** Establish security policies that assign serious consequences to employees who leak data, and include clear language in contracts with service providers specifying how data privacy is to be protected and maintained, and what the penalties are for failure to protect and maintain it.
- **Residual risks :** Data persistence within the storage environment can expose data after it is no longer needed, especially if the storage is hosted on a vendorprovidedservice that dynamically moves data around in an untraceable manner.

Administrative access that allows system administrators full access to all files, folders, and directories, as well as the underlying storage infrastructure itself, can expose private data to administrators.

Espionage, packet sniffing, packet replay

Espionage refers to the unauthorized interception of network traffic for the purpose of gaining information intentionally. Using tools to capture network packets is called packet sniffing, and using tools to reproduce traffic and data that was previously sent on a network is called packet replay. The user specifies which packets to capture based on the filter parameters. Packet captures can be continuous or stop capture after a certain number of frames, bytes, or time

- **Defense :** Use of firewall to filter the packet. Encrypt data at rest as well as in transit through the use of modern, robust encryption technologies for file encryption, as well as network encryption between servers and over the Internet.

- **Detection :** An Information Rights Management (IRM) solution can keep track of data access, which can provide the ability to detect inappropriate access attempts. In addition, an Intrusion Detection System (IDS) can help identify anomalous behaviour on the network that may indicate unauthorized access.
- **Deterrence :** In storage environments that are hosted by a third party, employ contract language that makes the service provider liable for damages resulting from unauthorized access.
- **Residual risk :** Data can be stolen from the network through tools that take advantage of network topologies, network weaknesses, compromised servers and network equipment, and direct access to network devices. Sometimes, a legitimate packet may consist malicious data.

Inappropriate administrator access

An unauthorized access to system may cause threat to confidentiality. If users are given privilege levels usually reserved for system administrators, that provide full access to a system and all data that system has access to, they will be able to view data or make changes without being properly restricted through the system's authorization processes. Administrators have the authority to bypass all security controls, and this can be used to intentionally or mistakenly compromise private data.

- **Defense :** Reduce the number of administrators for each function (servers, network, and storage) to as low a number as possible (definitely fewer than ten, and preferably fewer than five) and ensure that thorough background checks are used to screen personnel who have administrative access. A vendor security review should be performed to validate these practices before engaging any vendors.
- **Detection :** Review the provider's administrative access logs for its internal infrastructure on a monthly or quarterly basis. Review the provider's list of administrators on a biannual basis.
- **Deterrence :** Establish security policies especially for administrators, that assign serious consequences for inappropriate data access. In hosted environments, select only providers that have good system and network administration practices and make sure their practices are reviewed on a regular basis.
- **Residual risk :** Because administrators have full control, they can abuse their access privileges either intentionally or accidentally, resulting in compromise of personal information or service availability.

Storage persistence

Data remains on storage devices long after it is no longer needed, and even after it is deleted. Data that remains in storage after it is no longer needed, or that is deleted but not strongly overwritten, poses a risk of later discovery by unauthorized individuals.

- **Defense :** Maintain a U.S. Department of Defense (DoD)-level program of disk wiping or file shredding when disks are decommissioned or replaced, and after old data is archived.
- **Detection :** There isn't much that can be done to discover that your data persistsona disk that has been taken offline. Hence, the key is to prevent rather than detect.
- **Deterrence :** Establish data-wiping requirements before selecting a storage product and ensure that contract language clearly establishes these requirements.
- **Residual risk :** Data can remain on physical media long after it is thought to have been deleted. Sooner or later such can be leaked.

Storage platform attacks

Attacks against a SAN or storage infrastructure directly, including through the use of a storage system's management control, can provide access to private data, bypassing the controls built into an operating system because the operating system is out of the loop.

- **Defense :** Ensure that strong compartmentalization and Role-Based Access Control(RBAC) are implemented on the storage system. Ensure that access to the management interface of the storage system is not accessible from the common network.
- **Detection :** Implement an Intrusion Detection System (IDS) that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Also review storage system access control logs on a quarterly basis.
- **Deterrence :** Employ strong legal representation and project a strong commitment to identifying and prosecuting attackers.
- **Residual risk :** Data can be stolen directly from the SAN, and you may find out about it after the fact or not at all.

Misuse of data

People who have authorized access to data can do things with the data that they are not supposed to do. Examples are employees who leak information to competitors, developers who perform testing with production data, and employees who take data out of the controlled environment of the organization's network into their unprotected home environment.

- **Defense :** for employees, use security controls similar to those in private data networks. Block the ability to send e-mail attachments to external e-mail addresses.
- **Detection :** Use watermarking and data classification labelling along with monitoring software to track data flow. IRM can be used to perform these functions.
- **Deterrence :** Employ a strict security policy paired with an awareness program to deter people from extracting data from controlled environments and moving it to uncontrolled environments.
- **Residual risk :** People can find ways around controls and transfer data into uncontrolled environments, where it can be stolen or misused.

Fraud

A person who illegally or deceptively gains access to information they are not authorized to access commits fraud. Fraud may be perpetrated by outsiders but is usually committed by trusted employees or ex-employees.

- **Defense :** Use checks and balances along with separation of duties and approvals to reduce the dependence on single individuals for information access, so if somebody does perform a fraudulent action, it will be noticed. This can also be a deterrent action.
- **Detection :** Perform regular audits on computing system access and data usage, giving special attention to unauthorized access.
- **Deterrence :** Ensure that security policies include penalties for employees who access data they are not authorized for. Discontinue all the access rights when an employee leaves organization.
- **Residual risk :** Fraudulent data access can occur despite the controls that are designed to prevent it.

Hijacking

- Hijacking in the context of computing refers to the exploitation of a valid computer session (sometimes also called a session key) to gain unauthorized access to information or services in a computer system. In particular, it's the theft of a magic cookie used to authenticate a user to a remote server.
- For example, the HTTP cookies used to maintain a session on many web sites can be stolen using an intermediary computer or with access to the saved cookies on the victim's computer. If an attacker is able to steal the authentication cookie, they can make requests

themselves as if they were the genuine user, gaining access to privileged information or changing data.

- If this cookie is a persistent cookie, then the impersonation can continue for a considerable period of time. Any protocol in which state is maintained using a key passed between two parties is vulnerable, especially if it's not encrypted.
  - **Defense :** Look for solid identity management solutions that specifically address this risk using strong, difficult-to-guess session keys with encryption. Use good key management, key escrow, and key recovery practices as a customer so that employee departures do not result in the inability to manage your data.
  - **Detection :** Routinely monitor logs, looking for unexpected behavior.
  - **Deterrence :** Not much can be done to deter attackers from hijacking sessions, other than aggressive legal response.
  - **Residual risk :** Attackers can impersonate valid users or even use administrative credentials to lock you out or damage your infrastructure.

Phishing

Phishing is an attempt to trick a victim into disclosing personal information. The most common method of phishing is to send potential victims an e-mail message that appears to be from a legitimate organization and directs the recipients to log in and provide a username, password, credit card information, or other sensitive information.

- **Defense :** Employ anti-phishing technologies to block rogue web sites and detect false URLs. Use multifactor authentication for customer-facing systems to ensure that users are aware when they are redirected to fake copies of your web site. Send periodic informational updates and educational materials to customers explaining how the system works and how to avoid phishing attempts. Never send e-mails that include or request personal details, including ID or passwords.
- **Detection :** Use an application firewall to detect when remote web sites are trying to copy or emulate your web site.
- **Deterrence :** Maintain educational and awareness programs for individuals who use and store personal information of employees or customers.
- **Residual risk :** Employees can fall for phishing scams despite the best training and awareness programs, especially if those scams are sophisticated. This can result in data loss.

2.4.3.2 Integrity Risks

Q. 2.4.5 Explain risk remediation for integrity risk. (Ref. Sec. 2.4.3.2) **(5 Marks)**

Data integrity refers to the accuracy and consistency of data. Integrity risks affect both the validity of information and the assurance that the information is correct. Some government regulations are particularly concerned with ensuring that data is accurate. If information can be changed without warning, authorization, or an audit trail, its integrity cannot be guaranteed.

Malfunctions of computer and storage failures

Malfunctions of computer and storage failures can also corrupt data and damage the integrity of that data.

- **Defense :** Make sure the storage infrastructure you select has appropriate RAID redundancy built in and that archives of important data are part of the service. RAID (redundant array of independent disks); is a way of storing the same data in different places on multiple hard disks to protect data in the case of a drive failure.
- **Detection :** Employ integrity verification software that uses checksums or other means of data verification.
- **Deterrence :** Due to the nature of data, because there is no human element involved, there isn't much that can be done.
- **Residual risk :** Technology failures that damage data may result in operational or compliance risk.

Data Deletion and data loss

Data can be accidentally or intentionally destroyed due to computer system failures or mishandling. Such data may include financial, organizational, personal, and audit trail information.

- **Defense :** critical data must be redundantly stored and housed in more than one location.
- **Detection :** Maintain and review audit logs of data deletion.
- **Deterrence :** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.
- **Residual risk :** Once critical data is gone, if it can't be restored, it is gone forever.

Data Corruption and data tampering

Changes to data caused by malfunction in computer or storage systems, or by malicious individuals or malware, can damage the integrity of that data. Integrity can also be damaged by people who modify data with intent to defraud.

- **Defense :** Utilize version control software to maintain archive copies of important data before it is modified. Ensure that all data is protected by antivirus software. Maintain role-based access control over all data based on least privilege principles, pursuant to job function and need to know.
- **Detection :** Use integrity-checking software to monitor and report alterations to key data.
- **Deterrence :** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.
- **Residual risk :** Corrupted or damaged data can cause significant issues because valid, reliable data is the cornerstone of any computing system.

Accidental Modification

Perhaps the most common cause of data integrity loss, accidental modification occurs either when a user intentionally makes changes to data but makes the changes to the wrong data or when a user inputs data incorrectly.

- **Defense :** Utilize version control software to maintain archive copies of important data before it is modified. Maintain role-based access control over all data based on least privilege principles, pursuant to job function and need to know.
- **Detection :** Use integrity-checking software to monitor and report alterations to key data.
- **Deterrence :** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.
- **Residual risk :** Corrupted or damaged data can cause significant issues because valid, reliable data is the cornerstone of any computing system.

2.4.3.3 Availability Risks

Q. 2.4.6 Explain risk remediation for availability risk. (Ref. Sec. 2.4.3.3) **(5 Marks)**

High availability is a characteristic of a system, which aims to ensure an agreed level of operational performance (usually uptime). Availability means quality of being able to use or

operate. Availability risks are associated with vulnerabilities and threats pertaining to the reliability of services, given that we want the services that we use to be reliable, to pose a low risk, and to have a low incidence of outage.

Denial of Service

A Denial Of Service (DoS) attack or Distributed DoS (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. This type of attack commonly involves saturating the target machine with too many communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

- **Defense :** Select a storage platform that has solid protection against network attacks. Implement firewalls, an IPS, and network filtering at the perimeter of the storage network to block attacks.
- **Detection :** Monitor intrusion detection systems 24×7×365.
- **Deterrence :** Work with your legal department to ensure that attackers are found and prosecuted.
- **Residual risk :** Because most DoS and DDoS attacks make use of compromised systems across the globe, they can be hard to track, and because they flood system and network resources, they can get through an environment's defenses.

Outage

An outage is any unexpected downtime or unreachability of a computer system or network.

- **Defense :** The primary defense against any service outage is redundancy. Ensure that individual systems, devices, and network links are clustered or set up to use high availability. Outages are expensive, used to calculate the cost of downtime and use that to justify investment in the additional equipment needed for redundancy. Additionally, employ a solid disaster recovery plan to ensure that you are ready for extended outages, so that storage environments can be automatically switched to a different location during an outage.
- **Detection :** Employ monitoring tools to continuously monitor the availability and response time of the storage environment.
- **Deterrence :** Because outages generally occur as a result of software problems, little can be done to stop them from happening.

- **Residual risk :** Unforeseen outages can occur even when all devices and network paths are completely redundant, due to malfunctions or human error, so storage infrastructures may be down for as long as it takes to switch over to the disaster recovery environment.

Instability and Application Failure

Problems, such as bugs, in software or firmware can cause freezing, locking, or crashing of applications, making them unresponsive and resulting in loss of functionality or failure of an entire computer or network.

- **Defense :** Ensure that all software updates are applied to the infrastructure on a frequent basis. Updating latest path ensures that system is less vulnerable.
- **Detection :** Implement service monitoring to detect and alert when an application does not respond correctly.
- **Deterrence :** In contracts with storage suppliers, include clear language that specifies penalties and remuneration for instability issues.
- **Residual risk :** Because instability in applications and infrastructure generally occurs as a result of software problems, little can be done to stop them from happening.

Slowness

When the response time of a computer or network is considered unacceptably slow, its availability is affected.

- **Defense :** Using redundant storage system and network connections, set up the architecture so that application access will automatically switch to the fastest environment. Also ensure that you have implemented high-capacity services with demand-driven expansion of resources.
- **Detection :** Monitor response time of applications on a continuous basis and ensure that alerts have an out-of-band path to support staff so that response problems don't stop alerts from being delivered.
- **Deterrence :** Establish contract language with storage manufacturers that provides compensation for unacceptable response times.
- **Residual risk :** Slowness can persist despite best efforts, resulting in loss of efficiency and effective downtime.

High Availability Failure

A service that is supposed to fail over in the event of a problem with one device to other, functioning devices may not actually fail over properly. This can happen, for example, when a primary device slows down to the point where it becomes effectively unresponsive, but the HA software doesn't actually consider it to be "down".

- **Defense :** Monitor the health of secondary systems or all systems in an HA cluster.
- **Detection :** Perform periodic failover testing.
- **Deterrence :** Not much can be done to guarantee that systems will switch over when they are supposed to.
- **Residual risk :** Sometimes, a primary device slows down to the point that it becomes unresponsive for all practical purposes, but because it's not officially "down" according to its software, the backup system doesn't take over.

Backup failure

When backups aren't actually any good, either because the media is damaged or the backup data is corrupted or missing, data is lost.

- **Defense :** Leverage storage elasticity to avoid the use of traditional offline (tape or optical) backups.
- **Detection :** Frequently perform recovery testing to validate the resilience of data.
- **Deterrence :** Establish a data-loss clause in the contract with the storage manufacturer so that they have incentive to help with unforeseen loss of data.
- **Residual risk :** Backups fail, but multiple recovery paths can eliminate most of the risk.

The practice of backing up data has been around for a long time and, consequently, is one of the most reliable security practices. As long as data is appropriately replicated, it can live forever, so the majority of residual risk in this case would be due to substandard data replication practices or lack of attention to this matter.

Syllabus Topic : Best Practices

2.4.4 Best Practices

Q. 2.4.7 List and explain the best practices necessary for storage management. (Ref. Sec. 2.4.4) (5 Marks)

Growing cyber threats also increases risks to storage infrastructure and to the data that resides on it. Hence, new best practices for storage management are necessary. One of a new practice is the 3-2-1-1 rule. This policy is based on keeping three copies of data, on two types of media, storing one copy offsite, and storing one copy offline.

The following practices provide the best available mitigation.

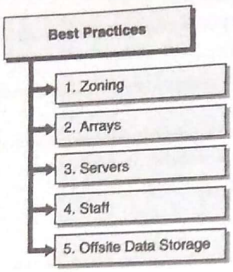

Fig. 2.4.2 : Best practices

2.4.4.1 Zoning

Port-based zoning improves security through control of the connections between hosts and the storage array. This method of zoning provides increased protection against a WWNs poof attack. With port zoning, even if a host system is introduced into the environment with a spoofed WWN, the host would need to also be in the port defined by the switch in order for its traffic to transmit to the storage array, because the zones are configured based on ports.

2.4.4.2 Arrays

Arrays have been developed over time to provide LUN masking as a form of protecting LUNs from access by unauthorized servers. The most likely cause of a LUN being accessed by an unauthorized system is accidental or intentional misconfiguration by a storage administrator. The best defense against this is to ensure that storage administrators are trustworthy and capable, and to control and limit the management of the storage array to a small number of highly trained, reliable administrators.

2.4.4.3 Servers

In order to fully secure a storage environment, the server environment must be properly controlled and monitored. Securing the storage infrastructure itself is not enough. Access to any server can significantly expose that server and the storage environment to harmful activity. It is important that servers be configured securely, and that the equipment is located in a secure facility with access control and monitoring.

Change management and activity monitoring, to track changes to the system and the

activities of administrators on the server, should be done with the security of the storage environment in mind. These steps need to be taken not only on the servers that are hosting the data but also on the management servers used to manage the arrays and switches.

2.4.4.4 Staff

- When hiring individuals to manage and secure the storage environment, the requisite skill set should include solid knowledge of storage security practices. Background and/or training in computer security methods should be considered an important requirement.
- Naturally, training and experience in managing storage arrays is also important, preferably with the product in use within your organization, rather than tasking an administrator of some other platform with managing the storage infrastructure. In addition, given the convergence of storage and networking that has resulted in the SAN, a background in networking can be very valuable.

2.4.4.5 Offsite Data Storage

- Storing data offsite (securely) is a critical aspect of any organization's business continuity process.
- Many vendors will pick up backup tapes and move them to a secured facility.
- Regular audits of these facilities should be done to ensure accountability for all data sent offsite. To protect the data, it should be encrypted whether on disk or tape. Any form of online data backup should be performed with an end-to-end encryption method.

Syllabus Topic : General Database Security Concepts, Understanding Database Security Layers

2.5 Database Security Concepts

2.5.1 Database Security Layers

Q. 2.5.1 Describe various database security layers. (Ref. Sec. 2.5.1) (5 Marks)

- Relational databases support a wide array of different types of applications and usage patents, and hence, they generally utilize security at multiple layers. Each layer of security is designed for a specific purpose and can be used to provide authorization rules. The different level of permissions can be given as follows and how they interact.

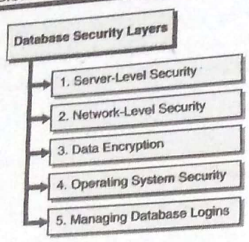

Fig. 2.5.1 : Database security layers

2.5.1.1 Server-Level Security

- When managing permissions for multiple logins, server roles can simplify your life significantly. In most places where permissions need to be handled, some kind of grouping does exist, for example Windows Groups.
- Their purpose is to allow you to define a permission set for example based on a job requirement. After that set is defined once, you can grant that entire set to one person just by adding their login to that group. When that person does not have this specific job requirement anymore, you can just remove their login from the group.
- This simplifies the administrators live significantly, particularly if a person is in multiple groups and is leaving only a few. If groups wouldn't exist, you would have to go through the list of all permissions and determine if each one is still necessary for any of that person's job requirements. With groups you just remove their login from the groups in question and the system handles the rest.

2.5.1.2 Network-Level Security

Generally, users access the database from remote location via internet. Databases system work with their respective operating system platforms to serve users with the data they need.

As an example, Microsoft's SQL Server database platform uses a default TCP port of 1433 for communications between clients and the database. If there is no need for users on certain subnets of a network, the user's network access to this TCP port can be blocked. Doing so can also prevent malicious users and code (such as viruses) from attacking this machine over the network.

2.5.1.3 Data Encryption

- Ensuring an authentication and authorization are not enough. Data must be kept confidential to avoid threats to data integrity. To ensuring the safety of database information in terms of confidentiality is to use encryption. Most modern databases support encrypted connections between the client and the server.
- Data encryption is one of the most important aspects of database security. With some database vendors, like Oracle, the encryption is stored outside of the database, and in the event of key loss the data within the table/column will also be lost.

2.5.1.4 Operating System Security

- Network configuration settings, file system permissions, authentication mechanisms, and operating system encryption features can all play a role in ensuring that databases remain secure. For this primary reason on most platforms, database security goes hand in hand with operating system security.
- For example, on Windows-based operating systems, only the NTFS file system offers any level of file system security (FAT and FAT32 partitions do not provide any file system security at all).One of the best practices of operating system security is to keep the system and applications up to date.
- To avoid system vulnerability, installing latest patches is important. A patch is a set of changes to a computer program or its supporting data designed to update, fix, or improve it. This includes fixing security vulnerabilities and other bugs and hence improve the usability or performance of operating system.

2.5.1.5 Managing Database Logins

- The first level of database security requires users to enter some authentication information before they can access a database. This is a convention used by most databases. This can be based on a standard username and password combination.
- Many relational database products that operate on Microsoft's Windows operating system platform can utilize the security features of a domain-based securitymodel.In addition, organizations are increasingly turning to biometric-based authentication (authentication through the use of fingerprint identification, retinal scans, and related methods), as well as smart-card and token-based authentication.

- Database administrators can take advantage of these mechanisms by relying on the operating system for identifying users. Therefore, integrated security is highly recommended, both for ease of use and for ease of management.
- Server logins can be granted permissions directly. A user may be given the permission to shut down or restart a database or the ability to create a new database on the server. Login-level permissions generally apply to the server as a whole and can be used to perform tasks related to backup and recovery, performance monitoring, and the creation and deletion of databases.

Syllabus Topic : Understanding Database-Level Security

2.5.2 Understanding Database-Level Security

Q. 2.5.2 Explain database-level security. (Ref. Sec. 2.5.2) **(5 Marks)**

- Database server systems are commonly used to host many different databases and applications and users should have different types of permissions based on their job functions.
- Once a legitimate user has connected to a server (through the use of a server login), the user will be given only the permissions that are granted to that login. This process of determining permissions is generally known as authorization. Following are some standard types of database-level permissions.
- The first type of database-level security is generally used to determine to which database(s)a user has access. Once a user has been granted permissions to access a database, further permissions must be assigned to determine which actions he or she can take within the database.
- Database administrators can specify whether or not certain databases can be accessed by a user login. For example, one login may be granted permissions to access only the Public Relationship database and not any system databases or databases used by other applications. Also, for that database user is only allow to read the data and not to modify or delete it.

2.5.2.1 Database Administration Security

- Maintenance of the server is an important task related to working with a relational database. Important tasks include creating databases, removing unneeded databases, managing disk space allocation, monitoring performance, and performing backup and

recovery operations. Database platforms allow the default systems administrator account to delegate permissions to other users, allowing them to perform these important operations.

- As an example, Microsoft's SQL Server platform provides built-in server-level roles, including Database Creators, Disk Administrators, Server Administrators, Security Administrators, and many others. The majority of database users will not require server-level permissions. Instead, they'll need permissions that are assigned at the level of the database.

2.5.2.2 Database Roles and Permissions

- Having a valid server login only allows a user the permission to connect to a server. In order to actually access a database, the user's login must be authorized to use it.
- The general process begins with specifying to which database(s) a login may connect. Then, permissions must be assigned within the database. The details here do vary between types of relational database platforms, but the overall concepts are the same. Generally, database administrators will create "groups" or "roles," and each of these will contain users.
- Specific permissions are assigned to the roles. This process is quite similar to the best practices that are suggested for most modern network operating systems. Additionally, some relational database platforms allow groups to be nested, thereby allowing you to create a hierarchy of permissions.
- For example, a database administrator might create a role that allows specific employee to insert and update data in a specific table. Users of this role might also be able to call certain stored procedures, views, and other database objects. Another role might be created for Managers of specific departments which provides the ability to delete any data that is entered by the employee and make other changes within the database.
- Through the use of roles, database administrators can easily control which users have which permissions. It is very important to properly design security based on the needs of database users. The key is to provide the least required permissions to avoid any security issues. This is especially important since, through the use of the SQL language, well-meaning users can accidentally delete or modify data when their permissions are too lax.

Following are the types of permissions that can be granted to users.

2.5.2.3 Object-Level Security

- Relational databases support many different types of objects. Modern relational databases offer graphical methods for administering security. Tables, however, are the fundamental unit of data storage. Each table is generally designed to refer to some type of entity (such as a Book, an Author, a Publisher). Columns within these tables store details about each of these items (BookTitle or BookNumber are common examples).
- Permissions are granted to execute one or more of the most commonly used SQLcommands. These commands are
  - **SELECT :** Retrieves information from databases. SELECT statements can obtain and combine data from many different tables, and can also be used for performing complex aggregate calculations.
  - **INSERT :** Adds a new row to a table.
  - **UPDATE :** Changes the values in an existing row or rows.
  - **DELETE :** Deletes rows from a table.

The ANSI Standard SQL language provides for the ability to use three commands for administering permissions to tables and other database objects :

- **GRANT :** Specifies that a particular user or role will have access to performa specific action.
- **REVOKE :** Removes any current permissions settings for the specified users or roles.
- **DENY :** Prevents a user or role from performing a specific action.

A typical command might look as follows :

- Grant SELECT on Book Table to Publisher1
- Managing all of these levels of database security can cause significant work for a database administrator. It can take a lot of time and effort initially to implement database security based on business and technical requirements, and it can take even more time and effort to ensure that database permissions reflect changes in the needs of your users. Some application-level security mechanisms can be used to make the management of database permissions easier.

Syllabus Topic : Using Application Security

2.5.3 Using Application Security

Q. 2.5.3 Explain application security along with its limitations with respect to databases. (Ref. Sec. 2.5.3) **(5 Marks)**

- Studies indicate that most websites are secured at the network level while there may be security loopholes at the application level which may allow information access to unauthorized users. Software and hardware resources can be used to provide security to applications.
- In this way, attackers will not be able to get control over these applications and change them. XSS attacks, Cookie Poisoning, Hidden field manipulation, SQL injection attacks, DoS attacks, and Google Hacking are some examples of threats to application level security which resulting from the unauthorized usage of the applications.
- Application security allows you to limit the number of database accounts and thus, by limiting the number of actual accounts that have database access, limit your exposure to external hacking attempts.

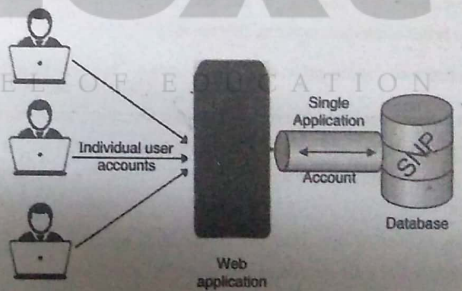

Fig. 2.5.2 : Application-level security for a database application

- Large and complex database applications often enforce their own security based on business rules that are stored and enforced within the application itself. For example, consider a common ordering system for an online mobile store that stores records of all its information in a relational database system, special databases contain important information such as inventory information, a brand details, and user information.

- Through the front-end web servers, the online store is accessible to anyone in the world at any time.
- However, there are various groups of users that require different permissions. Unregistered users can only view information about mobile, while registered users have much more access.
- Furthermore, the online mobile store's own staff might have access to view and modify information about mobile costs and selling prices.
- In such scenario, it would be difficult to implement and maintain all of the required security permissions at the database level. Instead, a commonly used approach would be to implement security-related rules within the web application logic.
- The web servers themselves would use only a single or relatively few database logins to access information stored in the database. From the viewpoint of the database, all data retrieval and modification requests coming from the web servers will be honoured.
- Common situation for multiple web applications is to access one or more relational databases. It's important to keep in mind that each application that requires access to your database should have a separate login.
- Apart from reducing the "sharing" of database authentication information, this will also allow you to better implement auditing functionality.

2.5.3.1 Limitations of Application-Level Security

- When implementing application level security, the first thing to be taken care is that you trust the application and its authors as by granting the "keys to the kingdom" to an application, it implicitly means that the application is trusted to manage all security for the entire system.
- However, any defects or vulnerabilities in the application could easily translate into a security breach where a user could access and modify without proper authorization. For this reason, it's important that applications that maintain their own security permissions are thoroughly tested.
- The second major concern related to application-level security is that it does not provide any type of protection for users that can bypass the application.

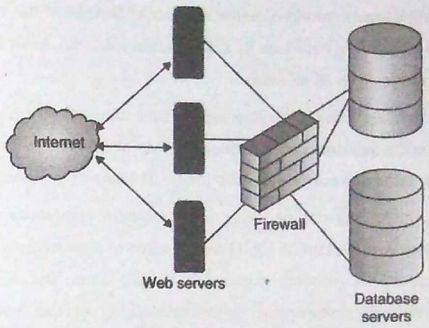

Fig. 2.5.3 : Securing Internet accessible database applications

Syllabus Topic : Database Backup and Recovery

2.5.4 Database Backup and Recovery

Q. 2.5.4 Explain database backup and recovery. (Ref. Sec. 2.5.4) (5 Marks)

2.5.4.1 Determining Backup Constraints

- Once you have a reasonable idea of what your organization needs to back up, it's time to think about ways in which you can implement a data protection strategy. It is of critical importance that you define your business requirements before you look at the technical requirements for any kind of data protection solution.
- In addition to these requirements, organisation might also have a preliminary budget limit that can serve as a guideline for evaluating solutions. An organisation should also need to have types of expertise in different aspects to implement a solution.

2.5.4.2 Determining Recovery Requirements

- The purpose of data protection is not to create backups. The real purpose is to provide the ability to recover information in case it is lost and make system available as quick as possible. A good practice is to begin designing a backup solution based on a recovery requirement.

- A database administrator should consider the cost of downtime, the value of the data, and the amount of acceptable data loss in a worst-case scenario. Also, keeping in mind the likelihood of certain types of disasters.
- When planners are evaluating business needs, they may forget to factor in the potential time for recovering information. The question they should ask is the following : "If we lose data due to failure or corruption, how long will it take to get it back?"
- In some cases, the answer will be based on the technical limitations of the hardware you select. For example, if backup of 13GB data is taken to tape media and then the database becomes corrupted, the recovery time might be two hours. But what if that's not fast enough? Suppose those systems must be available within half that time (one hour).
- In that case, an obvious choice is to find suitable backup hardware to meet these constraints. If budgetary considerations don't allow that, however, it's important to consider how long that business can *realistically* tolerate having certain information unavailable.

2.5.4.3 Types of Database Backups

Q. 2.5.5 Write a note on types of Database backups. (Ref. Sec. 2.5.4.3) (5 Marks)

- Taking a backup of large databases while considering its performance requirements can often constrain the operations that can be performed (and when they can be performed).
- For example, instead of backing up all of the data hourly, full backups can be taken once per week and smaller backups on other days. Although the terminology and features vary greatly between relational database platforms, the following types of backups are possible on most systems :

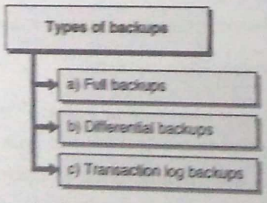

Fig. 2.5.3 : Types of backups

(a) Full backups

- This type of backup consists of making a complete copy of all of the data in a database. Generally, the process can be performed while a database is up and running.
- On modern hardware, the performance impact of full backups maybe almost negligible.
- Of course, it's recommended that database administrators test the performance impact of backups before implementing an overall schedule.
- Full backups are the basis for all other types of backups. If disk space constraints allow it, it is recommended to perform full backups frequently.

(b) Differential backups

- This type of backup consists of copying all of the data that has changed since the last full backup. Since differential backups contain only changes, the recovery process involves first restoring the latest full backup and then restoring the latest differential backup.
- Although the recovery process involves more steps (and is more time-consuming), the use of differential backups can greatly reduce the amount of disk storage space and backup time required to protect large databases.

(c) Transaction log backups

- Relational database systems are designed to support multiple concurrent updates to data.
- In order to manage contention and to ensure that all users see data that is consistent to a specific point in time, data modifications are first written to a transaction log file.
- Periodically, the transactions that have been logged are then committed to the actual database.
- Database administrators can choose to perform transaction log backups fairly frequently, since they only contain information about transactions that have occurred since the last backup.
- The major drawback to implementing transaction log backups is that, in order to recover a database, the last full (or differential) backup must be restored. Then, the unbroken chain of sequential transaction log files must be applied.
- Depending on the frequency of full backups, this might take a significant amount of time.
- However, transaction log backups also provide one extremely important feature that other backup types do not : point-in-time recovery.

- What this means is that, provided that backups have been implemented properly, database administrators can roll a database back to a specific point in time.
- For example, if it has been analysed that an incorrect or unauthorized database transaction was performed at 2:00 a.m. on Friday, the database can be restored to a point in time just before that transaction occurred. The end result is minimal data loss.

Syllabus Topic : Database Auditing and Monitoring

2.5.5 Database Auditing and Monitoring

Q. 2.5.6 What are database auditing and monitoring? (Ref. Sec. 2.5.5) (5 Marks)

- Often, users that are attempting to overstep their security permissions (or users that are unauthorized altogether) can be detected and dealt with before significant damage is done; or, once data has been tampered with, auditing can provide details about the extent of loss or data changes.
- There's another benefit to implementing auditing: when users know that certain actions are being tracked, they might be less likely to attempt to snoop around your databases. Thus, this technique can serve as a deterrent. Unfortunately, in many environments, auditing is overlooked.
- Though it won't necessarily prevent users from modifying information, auditing can bea very powerful security tool. Most relational databases provide the ability to track specific actions based on user roles or to track actions on specific database objects.
- For example, you might want to create an audit log entry whenever information in the Employee Salary table is updated, or you might choose to implement auditing of logins and certain actions to deter systems administrators (who might require full permissions on a database) from casually "snooping around" in a database.
- Perhaps one of the reasons that auditing is not often implemented is because it requires significant planning and management. Unlike some types of "set and forget" functions, it's important to strike a balance between technical requirements and capturing enough information to provide meaningful analysis.
- In many cases, auditing too much information can decrease system performance. Also, audit logs can take up significant disk space. Finally, few database administrators would enjoy the task of looking through thousands of audit log entries just to find a few items that may be of interest.

- Most relational database systems offer some level of auditing functionality. Even if one or more of the types of database you support does not include this feature, you can always implement your own.
- At a minimum, most database administrators should configure logging of both successful and failed database login attempts. Although this measure, by itself, will provide limited information, it will provide for some level of accountability. Of course, capturing data is only one part of overall auditing.

2.5.5.1 Reviewing Audit Logs

- In terms of security auditing is very useful, systems and database administrators should regularly review the data that has been collected. It is only through this activity that potential problems in security settings can be detected before they get worse.
- The challenge with reviewing audit logs is in determining what information is useful.
- Unfortunately, there's no simple method that will work for all situations. In some environments, administrator might want to perform "spot-checks" - that is, review access to particularly sensitive data or review the actions that have been taken by a specific user.
- In some case it's important to have triggers set on auditing tables to automatically alert someone when some threshold of a known event has happened, such as multiple user account password changes happening at the same time.
- Since activity logs can contain a lot of information, any methods for filtering the collected data can be helpful.

2.5.5.2 Database Monitoring

- Database auditing provide an excellent way to track detailed actions, but to get a quick snapshot of who's using the server and for what purpose a quick snapshot of current database activity can be taken or view any long-running transactions that are currently in process.
- Any potential misuse of the system can be quickly identified by establishing a performance and usage baseline. For example, using the Windows Performance Toolkit (WPT) that is part of Microsoft's server-side operating systems, many statistics related to database usage can be tracked.
- Also, an alerts can be configured to notify when performance or other statistics are "out of bounds," based on normal activity. All of these mechanisms can be helpful in monitoring the usage of database systems.

- Next, different application-level security are explained that can be used to maintain strict permissions while simplifying database administration.
- Another important aspect related tonsuring the security of database systems is implementing a data protection plan.
- Furthermore, Necessity of performing backups, how backups should be planned, and various backup operations that can be performed in relational databases. Finally, we looked at the importance of auditing and monitoring servers.

2.6 Exam Pack (Review Questions)

☞ **Syllabus Topic : Authentication**

Q. 1 Explain the terms authentication. (Refer Section 2.1) **(5 Marks)**

☞ **Syllabus Topic : Authorization**

Q. 2 Explain the terms authorization. (Refer Section 2.2) **(5 Marks)**

☞ **Syllabus Topic : Encryption, A Brief History of Encryption**

Q. 3 Write a short note on encryption. (Refer Sections 2.3 and 2.3.1) **(5 Marks)**

☞ **Syllabus Topic : Symmetric-Key Cryptography**

Q. 4 Explain Symmetric Key Cryptography. (Refer Section 2.3.2.2) **(5 Marks)**

☞ **Syllabus Topic : Public Key Cryptography**

Q. 5 Explain Public Key Cryptography. (Refer Section 2.3.2.3) **(5 Marks)**

☞ **Syllabus Topic : Public Key Infrastructure**

Q. 6 Explain Public Key Infrastructure. (Refer Section 2.3.2.4) **(5 Marks)**

☞ **Syllabus Topic : Storage Security : Storage Security Evolution**

Q. 7 Write a short note on storage security evolution. (Refer Section 2.4.1) **(5 Marks)**

☞ **Syllabus Topic : Modern Storage Security**

Q. 8 Write a short note on modern storage security. (Refer Section 2.4.2) **(5 Marks)**

☞ **Syllabus Topic : Risk Remediation**

Q. 9 Write a short note on risk remediation. (Refer Section 2.4.3) **(5 Marks)**

Q. 10 Explain risk remediation for confidential risk. (Refer Section 2.4.3.1) **(5 Marks)**

Q. 11 Explain risk remediation for integrity risk. (Refer Section 2.4.3.2) **(5 Marks)**

Q. 12 Explain risk remediation for availability risk. (Refer Section 2.4.3.3) **(5 Marks)**

☞ **Syllabus Topic : Best Practices**

Q. 13 List and explain the best practices necessary for storage management. (Refer Section 2.4.4) **(5 Marks)**

☞ **Syllabus Topic : General Database Security Concepts, Understanding Database Security Layers**

Q. 14 Describe various database security layers. (Refer Section 2.5.1) **(5 Marks)**

☞ **Syllabus Topic : Understanding Database-Level Security**

Q. 15 Explain database-level security. (Refer Section 2.5.2) **(5 Marks)**

☞ **Syllabus Topic : Using Application Security**

Q. 16 Explain application security along with its limitations with respect to databases. (Refer Section 2.5.3) **(5 Marks)**

☞ **Syllabus Topic : Database Backup and Recovery**

Q. 17 Explain database backup and recovery. (Refer Section 2.5.4) **(5 Marks)**

Q. 18 Write a note on types of Database backups. (Refer Section 2.5.4.3) **(5 Marks)**

☞ **Syllabus Topic : Database Auditing and Monitoring**

Q. 19 What are database auditing and monitoring? (Refer Section 2.5.5) **(5 Marks)**

Chapter Ends...

❑❑❑