Application Security :-

In today's IT world, it has become necessary to integrate an organisation's applications and those of its customer's and business partners. Web services offer a platform for integrating applications. One of the most important factors behind the adoption of web services is the ability of an enterprise to have access to real-time information concerning various departments, applications, platforms and systems. As business systems and applications within and across organisations get integrated, a number of security issues also arise.

Essentials for (Business) Applications Security

Following are some of the security issues that have to be addressed when any application is available to multiple users as a shared resource :

(1) ***Verification of users*** **:** Applications need to verify that only genuine users are trying to use them. The burden of proving identity (ID) rests with the users.

(2) ***Granting access to users*** **:** Once a user is authenticated, the application needs to determine if the identified user is allowed to access the requested functionality. The decision to grant access may depend on various criteria such as the action that is being requested, the resource on which the action is being requested, the groups to which the user belongs to and the roles that the user plays. The process of making this decision is known as "*authorization*".

(3) *Encryption of data* : This is done to keep the data confidential. For business transactions, data from application systems gets exchanged over the networks. Data stored by applications needs to be safeguarded from potential attacks. There is a possibility that unauthorized users can gain access to data that is being exchanged with legitimate users. The technique used to keep data confidential is called *encryption*. Without this technique e-commerce would have not succeeded as it is unsafe to transmit credit card information. The encrypted data can be understood only by the intended party and nobody else.

(4) *Guaranteeing data integrity and non-repudiation* : Keeping the data confidential which is stored in business applications is not sufficient. When the receiver gets a message, neither the sender nor the receiver should be able to deny the authenticity of the message, *i.e.*, *repudiate* it. Digital signature is a common technique which guarantees data integrity.

(5) *Safeguarding applications from attacks* : There are various types of threats and attacks that are common. Application have to be safeguarded from such attackes. This issue has been dealt in chapter 5 in detail.

(6) *Guarding privacy of applications* : From application perspective, there are two aspects of privacy :

- First is that of information generated from the applications and how it is used, distributed, shared or dispensed with third parties.
- Second is about how application services themselves expose the personal information of the users.

Various laws have been framed regarding data privacy. Service providers have to follow these privacy laws or business policies to guard the privacy of users.

We will be discussing these issues in this and subsequent two chapters in details.

3.2 DATABASE SECURITY

- A *database* can be defined as a collection of related or inter-dependent data elements.
- Alternatively, it can be viewed as a collection of information represented in coded data elements and specific relationships between those data elements.
- A database is usually intended to be shared across users, uses and applications.
- Databases are normally designed to provide a large user population with access to most of the data. The user can retrieve or update a small proportion of stored data. In most of the cases,users are unaware about the total volume or organization of data. Therefore, the user will access data in an indirect manner, formulating a query to which the retrieved data is an answer.
- Data in a database has to be protected from loss, unauthorized disclosure or modification.
- *Database security* is about allowing or disallowing user actions on the database and the objects within it. It is primarily concerned with the secrecy of data. In

the context of database security, "secrecy" means protecting a database from unauthorized access by users and software applications.

- When a database is created, it is assigned to an owner who executed the creation statement. Usually, only the owner or a super-user can do anything with the objects in that database. In order to allow other users to use the database, privileges are granted.
- Various secrecy-related problems in database systems are :
  (i) Improper release of information that is intentionally accessed by unauthorized users.
  (ii) Improper modification of data
  (iii) Denial of Service (DoS) threats.

3.3 DATABASE VULNERABILITIES

Following areas need attention when we think about database security :

(1) *Database server security* : Server security is the process of limiting actual access to the database itself. It is the most important aspect of security. Therefore, it should be carefully planned. The principle employed in server security is "you cannot access what you cannot see". It is essential to make the organizational database invisible to the would. There should not be any such thing as an anonymous connection to database access.

The database back-end should never be on the same machine as the web server. If the database is supplying information to a web server, then it should be configured to allow connections only from that web server.

(2) *Trusted IP addresses* : Just like other servers, the database server should also be configured to only allow trusted IP addresses. If it is a back-end for a web server, then only that web server's address should be allowed to access that database server. If the database server is supplying information to an internally developed application that is running on the internal network, then it should only answer to addresses from within the internal network.

It is not a good practice from the security viewpoint to host the web databases on the same server, where internal database information resides. Internal information should not be allowed to go out.

(3) *Securing database connections* : Now-a-days there are a number of dynamic applications which are available. We usually allow immediate unauthenticated updates to a database. This is a bad practice from the viewpoint of security. If users are allowed to make updates to a database via a web page, then security administrators must ensure that all such updates are validated. In this way we can ensure that all updates are warranted and safe.

(4) *Controlling table access* : Table access control is a difficult task in practice. Proper table access control requires the collaboration of both system administrator and database developer. This has some practical limitations also. Proper table structure and relational database structure and development are required for controlling table access.

(5) *Restricting database access* : Internet based databases are most frequently targeted by attacks. Ports assigned to web-enabled applications can be "listened to" by using "passive attack" methods. A simple method is available for protection against such attacks. These ports are normally assigned by default. We can change these ports so that Cyber crimals can no more listen to ports on which services are running.

(6) *Database encryption* : This is an essential step for database security and protection. If a database is contained in a computer system where the users have separate access to the operating system, an attacker may simply bypass the DBMS and access the data files directly. To overcome such circumstances, the database has to be encrypted to prevent such a direct attack.

(7) *User management* : Database administrators (DBAs) can perform special operations such as shutting down or starting up a database. As a security precaution, these operations should not be performed by normal database users. Some database systems (*e.g.*, Oracle) provide a more secure authentication scheme for DBA usernames. There are two types of user authentication schemes to authenticate DBAs :

(i) OS authentication

(ii) Password files

Applications should never connect to the database as its owner or a super-user. These users can execute any query at will. It is a good practice to create different database users for every aspect of an application with very limited rights to the database objects. Only the most required privileges should be granted and an interaction of the same user with the database in different use cases should be avoided. In this way if an intruder gains access to the database using applications credentials, they can only make minimal changes as granted by application.

3.4 E-MAIL SECURITY

- E-mail is one of the most widely used and regarded network services.
- It is an essential communications tool for many industries, Government and academic organizations.
- It is also popular and convenient medium for exchanging messages, data files, images and sound clips over computer networks and especially over the Internet.
- Sensitive information can be committed to an e-mail both inside and outside of the organization.
- Within and between organizations, e-mail can be an effective tool that helps to break down barriers to communication and promotes the free exchange of information and ideas.

However, message contents are not totally secure on e-mail. They may be inspected either in transit or by suitable privileged users on the destination system. More and more sophisticated attacks are being developed by rogue users. There is also a need to filter out malware and ensure that contents in the mail are suitable for the intended purpose. Mail systems available to public access can be vulnerable to misuse, unauthorized access and decline of service (DoS).

- Organizations and individual benefit when e-mails and mail systems are protected and are secure.

Objectives of E-mail Security

The main objectives of e-mail security are to ensure :

(1) *non-repudiation, that is, the sender cannot deny sending the message at a later date, and the receiver cannot deny receiving it;*

(2) *integrity of the message, i.e.,* messages are read only by their intended recipients;

(3) authentication of the source (*i.e.*, the sender or sender' network);

(4) verification of delivery;

(5) labeling of sensitive material;

(6) control of access (to e-mails).

3.4-1 SECURITY THREATS POSED BY E-MAILS TO INFORMATION SYSTEMS

Two principal components, *mail servers* and *mail clients,* support the e-mail processes.

- The *mail server* is the computer host that delivers, forwards and stores the mail.
- Users interface with the *mail client* software to read, compose, send and store e-mail messages.

Both mail servers and mail clients must be protected because they are vulnerable targets for attack by malicious intruders. After web servers, an organization's mail servers are typically the most frequent targets of attack. Both mail servers and public web servers communicate with unknown parties,who may or may not be trustworthy. Attackers have thorough understanding of the supporting computing and networking technologies. In this way they have been successful in exploiting weaknesses in mail servers and clients.

Mail servers and clients can be vulnerable to events such as :

(1) Denial of service (DoS) attacks that are directed to the mail server or its supporting network that can deny or hinder access to the mail server by valid users.

(2) Sensitive information on the mail server may be disclosed or changed in an unauthorized manner.

(3) Sensitive information that is transmitted unencrypted between a mail server and an e-mail client may be intercepted. For example, the e-mail software may default to sending user names, passwords and the e-mail message itself without the protection of encryption.

(4) Information within the e-mail message may be altered at some point between the sender and the recipient.

(5) A successful attack on a mail server can be used to gain an unauthorized access to resources else where in the organization's computer network, including user passwords and other computers on the network.

(6) A mail server that has been attacked can be used to attack another

- When we enhance the MIME to provide for security features, it is known as *Secure MIME (S/MIME)*.

3.6 INTERNET SECURITY

The Internet, e-mail and web are closely connected. However, the web is not the Internet. In a sense, the web runs using the communication infrastructure set by the Internet. The web is the collection of hypertext transfer protocol (HTTP) servers that hold and process the websites that we interact with. The Internet is the collection of physical devices and communications protocols used to navigate to and traverse to these websites and interact with them. Browsers can understand a lot of different protocols and have the capability to process many types of commands.

Internet is now widely used by business and government organizations as well as individuals. However, Internet and web are vulnerable to a variety of threats. Hence security of data in transit over the Internet becomes necessary because of growing data volume and importance. Various added security mechanisms are needed for this purpose. Following are some standards for Internet security :

(1) HTTP : TCP/IP is the protocol for the Internet and HTTP is the protocol for the web. HTTP is a stateless protocol, which means the client and the web server make and break a connection for each operation.

(2) Secure hypertext transfer protocol (S-HTTP) : This is an extension to the HTTP protocol to support sending data securely over the World Wide Web (WWW). The protocol was developed by enterprise integration technologies to keep data safe in a commercial transaction on the Internet. Not all web browsers and servers support S-HTTP. Thus, S-HTTP is HTTP with add-on security features. It was developed to provide a secure communication between a client and a server over the Internet. S-HTTP can also provide data integrity and sender authentication capabilities.

(3) HTTPS : Strictly speaking, this is not a separate protocol. It refers to the combination of a normal HTTP interaction over an encrypted secure sockets layer (SSL) or Transport Layer Security (TLS) transport mechanism. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks. There is a difference between S-HTTP and HTTPS. S-HTTP is a technology that protects each message that is sent between two computers. HTTPS protects the communication channel between two computers, message and all.

(4) Secure Socket Layer (SSL) : SSL is a certificate-based general purpose protocol. It was originally developed by Netscape for managing the encryption of information being transmitted over the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. It also provides data encryption, server authentication, message integrity and optional client authentication. SSL is a transport layer security service. It uses Transmission Control Protocol (TCP) to provide a reliable end-to-end service. SSL is build on top of TCP. In theory it can be used by all type of applications in a transparent manner. Just like S-HTTP, SSL keeps the communication path open until one of the parties requests to end the session. SSL protocol requires SSL-enabled server and browser. It should be noted that SSL will

provide security for the connection but does not provide security for the data once they are received. This means that the data are encrypted while they are being transmitted, but once they are received by a computer, they are no longer encrypted. (Refer to next article)

(5) MIME : This is a technical specification indicating how multimedia data and e-mail attachments are to be transferred. The Internet has mail standards that dictate how mail is to be formatted, encapsulated, transmitted and opened. If a message or document contains a multimedia attachment, MIME dictates how that portion of the message should be handled.

(6) S/MIME : It is a standard for encrypting and digitally signing e-mails that contain attachments and providing secure data transmissions. S/MIME extends the MIME standard by allowing for the encryption of e-mails and attachments. S/MIME provides confidentiality through the user's encryption algorithms and integrity through the user's hashing algorithms. Thus, we note that S/MIME is a standard for public-key encryption and signing of e-mail encapsulated in MIME.

(7) Secure Electronic Transaction (SET) : It is a security technology proposed by Visa and Master Card to allow for more secure credit card transaction possibilities than what is currently available. Although SET provides a very effective way of transmitting credit card information, users do not find it very efficient. SSL method is usually preferred over SET. We will discuss SET in detail in chapter 5.

to the nature of the data and the risks involved. Attention to security is also needed when data are to be destroyed.

Physical security, network security and security of computer systems and files—all need to be considered to ensure security of data and prevent unauthorised access, changes to data, disclosure or destruction of data.

Physical data security requires :

- controlling access to rooms and building where data, computers or media are held.
- logging the removal of, and access to, media or hardcopy material in store rooms.
- transporting sensitive data only under exceptional circumstances, even for repair purposes, *e.g.*, giving a failed hard drive containing sensitive data to a computer manufacturer may cause a breach of security.

Network Security means :

- not storing confidential data such as those containing personal information on servers or computers connected to an external network, particularly servers that host Internet services.
- firewall protection and security-related upgrades and patches to operating systems to avoid viruses and malicious code.

Security of computer systems and files may include :

- locking computer systems with a password and installing a firewall system.
- protecting servers by power surge protection systems through line-interactive uninterruptible power supply (UPS) systems.
- implementing password protection of, and controlled access to, data files, *e.g.*, no access, read only, read and write or administrator-only permission.
- controlling access to restricted materials with encryption
- imposing non-disclosure agreements for managers or users of confidential data.
- not sending personal or confidential data via e-mail or other file transfer means without first encrypting them.
- destroying data in a consistent manner when needed.
- remembering that file sharing services such as Google Docs or Dropbox may not be that secure.

3.8 DATA BACKUPS

- Making back-ups of files is an essential element of data management. Regular back-ups protect against accidental or malicious data loss and can be used to restore originals if there is loss of data.
- A data storage strategy is important because digital storage media are inherently unreliable and all file formats and physical storage media will ultimately become obsolete.

- Accidental or malicious loss of data can be due to :
  - hardware faults or failure
  - software or media faults
  - virus infection or malicious hacking
  - power failure
  - human errors by changing or deleting files

Choosing a precise back-up procedure to adopt depends on local circumstances (for example, power failure rate), the perceived value of the data and the levels of risk considered appropriate for the circumstances. Carrying out an informal risk analysis provides an indication of back-up needs.

Particular data files or the entire system backup

What will we need to restore in the event of data loss? If our organization can restore the system then we may wish to take responsibility only for our data files. If it cannot, we may wish to take full responsibility for our own 'system' back-ups. Portable computers or devices, non-network computers and home based computers mostly require entire system backups.

Where the data contains personal information, care should be taken to only create the minimal number of copies needed, *e.g.*, a master file and one back-up copy.

Organization's back-up policy

Most organizations have a back-up policy for data that are held on their network space. We should check with the organization about any strategies and policies in place. If we are not happy with the robustness of the solution we should maintain an independent back-up of critical files.

Backup Frequency

To reduce risk as far as possible, back-ups should be made after every change to data or at regular intervals. We can use an automated back-up process to backup frequently used and critical data files. Microsoft SyncToy is an easy-to-use method of synchronising files in different locations.

Media for Backup

The choice of media on which to store back-up files depends on the quantity of files, type of data, and the preferred method of backing up. Examples include recordable CD/DVD, networked hard drive, removable hard drive or magnetic tape. If we are backing up many small data files on a daily basis, copying them to a recordable CD is probably sufficient but if we are making back-ups of very large quantities of data from a networked hard drive, a removable hard drive or even magnetic tape is probably more convenient.

File Formats for Backup

Back-ups of master copies should ideally be in file formats that are suitable for long term digital preservation, that is open as opposed to proprietary formats.

Incremental or Differential Back-ups

Incremental back-ups consist of first making a copy of all relevant files, often the

complete contents of a PC, then making incremental back-ups of the files which have altered since the last back-up. Removable media (CD/DVD) are recommended for this procedure.

For differential back-ups, a complete back-up is made first, and then back-ups are made of files changed or created since the first full back-up and not just since the last partial back-up. Fixed media, such as hard drives, are recommended for this method.

Whichever method is used, it is best not to overwrite old back-ups with new ones.

Storing the Backups

Depending on the form of back-up and the risks associated with data loss, it is most convenient to keep back-up files on a networked hard drive. For critical data, which are not available elsewhere, it is recommended that we adopt offline storage on recordable CD/DVD, removable hard drive or magnetic tape. Physical media can be safely stored in another location. Most manufacturers provide recommendations for the best storage conditions of physical media.

Validation of Back-ups Copies

It is important that we verify and validate back-up files regularly by fully restoring them to another location and comparing them with the original. Back-up copies can be checked for completeness and integrity, for example, by checking the MD5 checksum value, file size and date.

Organisation of Backups

If we are making our own back-ups on removable media, we have to make sure they are well labelled and well organised. Without some management, achieving the ultimate aim of restoring lost data may prove difficult.

3.9 ARCHIVAL DATA STORAGE

A data storage strategy is important because digital storage media are inherently unreliable and all file formats and physical storage media will ultimately become obsolete. Media currently available for storing data files are optical media - CDs and DVDs - and magnetic media - hard drives and tapes.

Data or File Formats for Storing Data

Best formats are generally non-proprietary formats or formats based on open standards. They meet long-term readability requirements for various data types. However, some proprietary formats, like Microsoft's Rich Text Format and Excel, are widely used and likely to be accessible for a reasonable time after any version has become obsolete. These formats are highly recommended for general use in any data storage environment.

A file extension does not necessarily refer to the file type, so a file with the extension .doc was not necessarily created with MS Word software, nor will it necessarily open successfully in that software.

Table (I) shows the generally accepted file formats for archival data storage.

Physical Conditions Needed for Storing Data

Areas and rooms designated for storage of digital or non-digital data sho ...e suitable for the purpose for which they are being used. Data should be well-organised, clearly labelled, easily located and physically accessible. The storage rooms should be structurally sound and free from the risk of flood and as far as possible from the risk of fire. The conditions under which data are stored significantly affect their longevity.

Optical media are vulnerable to poor handling, changes in temperature, changes in relative humidity, air quality and lighting conditions. Magnetic media, like hard drives, are equally sensitive to their physical environment. A personal computer is more likely to suffer from a fatal crash in a very hot office than in a temperature-controlled environment.

Printed materials and photographs are subject to degradation from sunlight and acid, *e.g.*, from sweat on skin in some kinds of paper. High quality media should be used for preparing paper-based materials for storage, or for copies of originals. Examples are using acid-free paper, folders and boxes and non-rust paperclips rather than staples.

Storing confidential data

Storage of data that are considered confidential or sensitive may need to be addressed during consent procedures, to inform the people to whom the data belong, how and why the data will be stored. The risks of identification of personal information are typically maintained through the anonymisation of data and the regulation of access through a dedicated rights management framework.

It is important to be aware of the risks of storing personal data. Legally, data which contain personal information must be treated with more care than data which do not. Personal information can be removed from data files and stored separately under more stringent security measures.

Signed consent forms or other non-digital records may contain identifying information and should be stored separately from data files, although an anonymous ID system can help link the two sets of materials together if required (*e.g.*, for re-contacting purposes).

3.10 SECURED DISPOSAL OF DATA

- After the completion of a project, data files which are not to be preserved need to be disposed of securely.
- Having a strategy for reliably erasing data files is an essential part of managing data security and is relevant at various stages in the data cycle.
- Note that deleting files and reformatting a hard drive will not prevent the possible recovery of data that have previously been on that hard drive.