Web Security Concepts

MCS-051 Block - 3

Web Security

- Web Security is defined as technological and managerial procedures applied to computer systems to ensure the integrity, availability and confidentiality of information.
- Web security is divided into two categories :

1. Computer security
2. Network security

Computer Security :

- It is the process of securing a single, standalone computer.
- It is the technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of the data managed by the computer.

Network Security :

- It is the process of securing an entire network of computers.
- It is the protection of network and their services from unauthorised modification destruction, or disclosure.

Web Services

- Web Services is a software system designed to support interoperable machine-to-machine interaction over the network.
- It has an interface, which is described in a machine-processable format such as WSDL.
- Other systems interact with the web service in a manner prescribed by its messages using messages.
- These messages are conveyed using HTTP, and comprise XML in conjunction with other web-related standards.
- Software applications written in various programming languages and running on various platforms, can use web services to exchange data over computer networks .
- This interoperability is due to the use of open standards.

Advantages of web services :

- It provides interoperability between various software applications running on different platforms/ operating system.
- It uses open standards and protocols.
- Using HTTP, web services can work through many common firewall security measures without having to make changes to the firewall filtering rules.
- It allow software and services from different companies and locations to be combined easily to provide an integrated service.
- It allows the reuse of services and components within an infrastructure.
- Web services are loosely coupled- facilitating a distributed approach to application integration.

WS-Security

- WS-Security is a communication protocol that provides means for applying security to Web Services .
- It was developed by IBM, Microsoft and VeriSign.
- It is also called WSS.
- It consists of specifications on how integrity and confidentiality can be enforced.

Web Security Concepts

- Basic concepts related to web security are :

1. Integrity
2. Confidentiality
3. Availability
4. Authenticity
5. Authorisation
6. Assurance

1. Integrity :

Integrity is an organizations important security objective. Integrity is important for critical safety and financial data used in activities like air traffic control, financial counting and electronic fund transfers.

- Integrity has two facets :

1. Data integrity
2. System integrity

Data integrity :

- This property ensures that data has not been altered in an unauthorised manner while in storage, during processing or while in transit. It assures that data can only be accessed and altered by those authorised to do so. Integrity is ensured by a number known as a Message Integrity Code (MIC) or Message Authentication Code (MAC).

System Integrity :

- This property ensures that a system has performed the intended function in an unimpaired manner, free from unauthorised manipulation.

2. Confidentiality :

- It is the property that private or confidential information should not be disclosed to unauthorised individuals.
- Confidentiality applies to data in storage, during process and while in transit.
- It is used for research data, medical records, insurance records, new product specifications etc..

3. Availability

- It is a property that assures that systems work promptly and service is not denied to authorised users.
- Objective of availability property is :

1) Intentional or accidental attempts to either :

- Perform unauthorised deletion of data or
- Otherwise cause a denial of service or data.

2) Attempts to use system or data for unauthorised purposes

Availability is to make information available to those who need it and who can be trusted with it . To do this organizations use two ways :

i. Authentication

ii. Authorization

i. Authentication :

- It is proving that a user is whom she claims to be.
- This may be using :

* Something the user knows: password

* Something the user has : smart card

* Something that proves users identity : fingerprint

ii. Authorization :

- It is the act of determining whether a particular user has the right to perform some activity like reading a file.
- Before performing some activity they are authorised to perform, users must be authenticated.

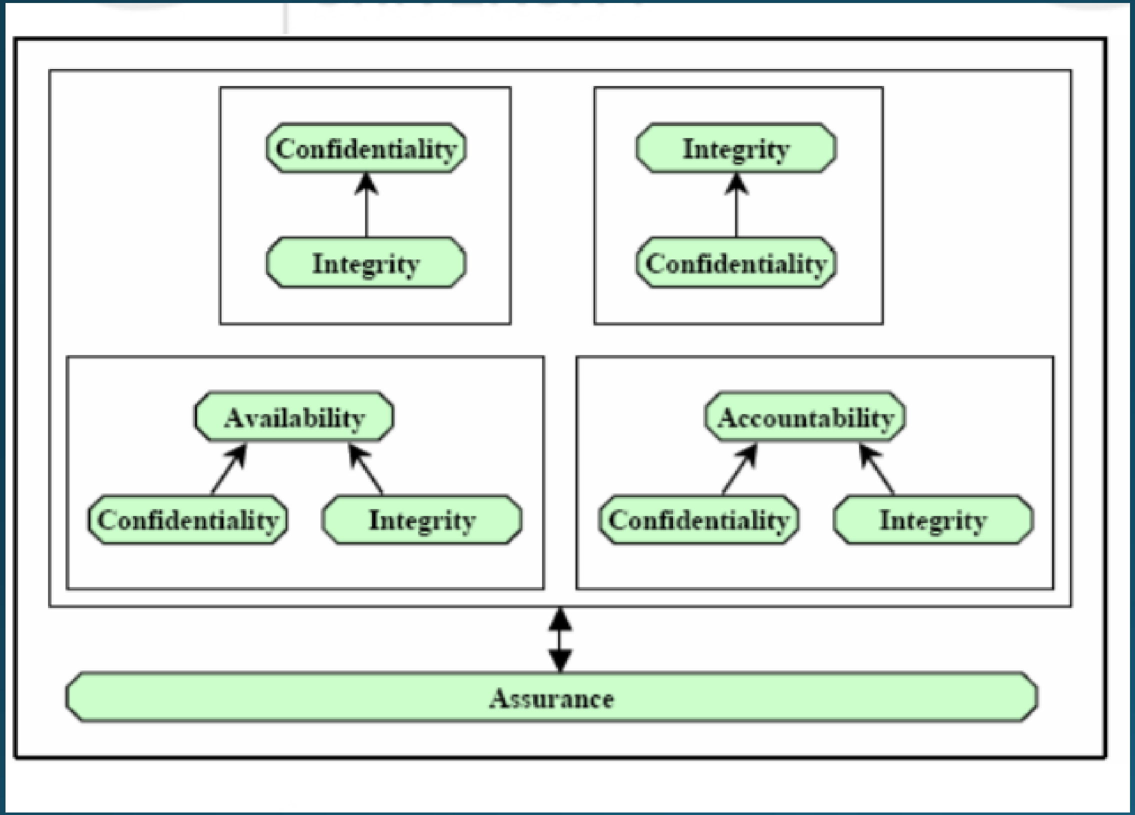
Accountability :

- It is the requirement that actions of an entity may be traced uniquely to that entity.
- Accountability is an organizational policy requirement and directly supports repudiation, deterrence, fault isolation, intrusion detection and prevention.

Assurance :

- It ensures that the security measures , both technical and operational, work as intended to protect the system and the information it processes.

Dependency between the basic concepts



SSL and TLS

- SSL stands for Secure Socket Layer.
- TLS stands for Transport Layer Security.
- SSL was developed by Netscape Corporation in 1994.
- TLS is a successor of SSL.
- Both SSL and TLS are cryptographic protocols. They provide security for communication over the internet (eg. email, internet faxing).

SSL- Secure Socket Layer

- SSL provides endpoint authentication and communication privacy over the Internet using cryptography.
- Typically, only server is authenticated while the client is unauthenticated. In order to have mutual authentication, public key infrastructure (PKI) is required to clients.
- The client/server applications communicate in a designed way to prevent :

* Eavesdropping

* Tampering

* Message forgery

- Tampering may be like :
- Tampering (sports) : the practice of professional sports teams negotiating with athletes of other teams. (illegal)
- Temper evident : A process or device that makes unauthorised access to a protected object easily detected.
- Temper proofing : A methodology used to hinder, deter or detect unauthorised access to a device or circumvention of a security system.

Message Forgery :

Message forgery is the sending of a message to deceive the recipient of whom the real ender is.

- Three basic phases are :

1. Peer negotiation for algorithm support,
2. Public key encryption –based key exchange and certificate-ased authentication
3. Symmetric cipher- based traffic encryption

In the first phase, the client and server negotiation uses cryptographic algorithms. Some of these are :

- For public key cryptography : RSA, Diffie-Hellman, DSA or Fortezza
- For symmetric ciphers :RC2, RC4,IDEA,DES, Triple DES or AES.
- For one-way hash function : MDS or SHA

Working of SSL

- SSL protocol exchanges records. Each record can be optionally compressed, encrypted and packed with a MAC (Message Authentication Code). Each record has a “content type” field. Content type field specifies which upper level protocol is being used.
- When the connection begins, the record level encapsulates another protocol, the handshake protocol.
- The client sends and receives several handshake structures:

○ It sends a ClientHello message that specifies the list of cipher suites, compression methods and the highest version it supports. It also sends random bytes that will be used later.

- Then it receives a ServerHello message which specifies the connection parameters.
- Once the connection parameters are known, client and server exchange certificates based on the selected public key cipher. Currently X.509 is used.
- The server can request a certificate from the client, so that the connection can be mutually authenticated.
- Client and server negotiate a common secret called "aster secret", the result of Diffie-Hellman exchange or simply encrypting a secret with a public key that is decrypted with the peer's private key. Other key data is derived from this master secret, which is passed through a carefully designed "Pseudo Random Function".

TLS/SSL security measures

- Numbers all the records and uses the sequence number in the MACs.
- Uses a message digest enhanced with a key.
- Protection against several known attacks.
- The message that ends the handshake ("Finished") sends a hash of all the exchanged data seen by both parties.
- The Pseudo Random Function divides the data into two halves and processes them with different hashing algorithms, namely MD5 and SHA, then XORs them together.

Public key cryptography:

- It is a form of cryptography that allows users to communicate securely without having prior access to a shared secret key.
- It uses a pair of cryptographic keys – namely public key and private key.
- Private key is kept secret, while the public key is widely distributed.

Different forms of public key cryptography :

- Public key encryption : keeps a message secret from anyone that does not possess a specific private key.
- Public key digital signature : it allows anyone to verify that a message was created with a specific private key.
- Key agreement : it allows two parties that may not initially share a secret key to agree on one.

HTTP Authentication

- A web client can authenticate a user to web server using one of the following mechanisms :

1. HTTP Basic Authentication
2. HTTP Digest Authentication
3. Form Based Authentication
4. HTTPS Client Authentication

HTTP Basic Authentication

- It is based on a username and password.
- It is the authentication mechanism defined in the HTTP/1.0 specification.
- A web server requests a web client to authenticate the user.
- As part of the request, the web server passes the realm (a string) in which the user is to be authenticated.
- The realm string of Basic Authentication does not have to reflect any particular security policy domain (confusingly also referred to as a realm).
- The web client obtains the username and the password from the user and transmits them to the web server.

- The web server then authenticates the user in the specified realm.
- Basic Authentication is not a secure authentication protocol. User passwords are sent in simple base64 encoding (not encrypted). The target server is not authenticated.
- Additional protection can alleviate some of these concerns: a secure transport mechanism (HTTPS), or security at the network level (such as the IPSEC protocol or VPN strategies) is applied in some deployment scenarios.

Example :

```
<web-app>
    <security-constraint>
        <web-resource-collection>
            <web-resource-name> User Auth</web-resource-name>
            <url-pattern>/auth/*</url-pattern>
            </web-resource-collection>
            <auth-constraint>
                <role-name>admin</role-name>
                <role-name>manager</role-name>
            </auth-constraint>
      </security-constrait>
      <login-config>
          <auth-method>BASIC</auth-method>
          <realm-name>User Auth</realm-name>
      </login-config>
    <security-role>
          <role-name>admin</role-name>
    </security-role>
    <security-role>
          <role-name>manager</role-name>
    </security-role>
</web-app>
```

HTTP Digest Authentication

- HTTP Digest Authentication authenticates a user based on a username and a password.
- The authentication is performed by transmitting the password in an encrypted form.
- It is more secure than Basic Authentication.
- Digest Authentication is not currently in widespread use.
- Advantage of Digest Authentication is that the cleartext password is protected in transmission. It cannot be determined from the digest that is submitted by the client to the server.
- It supports the concept of digesting user passwords.

- This causes the stored version of the passwords to be encoded in a form that is not easily reversible.
- Digest authentication acts almost identically to basic authentication in that it triggers a login dialogue.
- The difference between basic and digest authentication is that on the network connection between the browser and the server, the password is encrypted, even on a non-SSL connection.
- In the server, the password can be stored in clear text or encrypted text, which is true for all login methods and is independent of the application development.

Example :

```
<web-app>
    <security-constraint>
        <web-resource-collection>
           <web-resource-name> User Auth</web-resource-name>
            <url-pattern>/auth/*</url-pattern>
            </web-resource-collection>
             <auth-constraint>
                 <role-name>admin</role-name>
                  <role-name>manager</role-name>
             </auth-constraint>
       </security-constrait>
```

```
<login-config>
                <auth-method>DIGEST</auth-method>
                 <realm-name>User Auth</realm-name>
        </login-config>
      <security-role>
                <role-name>admin</role-name>
       </security-role>
       <security-role>
                 <role-name>manager</role-name>
       </security-role>
</web-app>
```

Form Based Authentication

- The look and feel of the 'login screen' cannot be varied using the web browser's built-in authentication mechanisms.
- In form based authentication mechanism allows a developer to control the look and feel of the login screens.
- The web application deployment descriptor, contains entries for a login form and error page.
- The login form must contain fields for entering a username and password. These fields must be named as j_username and j_password respectively.

- When a user attempts to access a protected web resource, the container checks the user's authentication. If the user is authenticated and possesses authority to access the resource, the requested web resource is activated and a reference to it is returned. If the user is not authenticated, all of the following steps occur:

1. The login form associated with the security constraint is sent to the client and the URL path triggering the authentication is stored by the container.
2. The user is asked to fill out the form, including the username and password fields.
3. The client posts the form back to the server.
4. The container attempts to authenticate the user using the information from the form.
5. If authentication fails, the error page is returned using either a forward or a redirect, and the status code of the response is set to 200.
6. If authentication succeeds, the authenticated user's principal is checked to see if it is in an authorized role for accessing the resource.
7. If the user is authorized, the client is redirected to the resource using the stored URL path.

- The error page sent to a user that is not authenticated contains information about the failure.
- Form based authentication is less secure since the user password is transmitted as a plain text and the target server is not authenticated.
- Additional protection can alleviate some of these concerns: a secure transport mechanism (HTTPS), or security at the network level (such as the IPSEC protocol or VPN strategies) is applied in some deployment scenarios.
- Form based login and URL based session tracking are problematic to implement. Form based login should be used only when sessions are being maintained by cookies or by SSL session information.

Example :

```
<form method = ‘post’ action=‘j_security_check’>
         <input type=‘text’ name=‘j_username’>
         <input type=‘password’ name=‘j_password’>
</form>
<web-app>
   <security-constraint>
      <web-resource-collection>
        <web-resource-name> User Auth</web-resource-name>
        <url-pattern>/auth/*</url-pattern>
        </web-resource-collection>
         <auth-constraint>
            <role-name>admin</role-name>
        <role-name>manager</role-name>
    </auth-constraint>
</security-constrait>
<login-config>
            <auth-method>FORM</auth-method>
            <realm-name>User Auth</realm-name>
             <form-login-config>
                    <form-login-page>login.jsp</form-login-page>
                    <form-error-page>error.jsp</form-error-page>
              </form-login-config>
   </login-config>
```

```
    <security-role>
        <role-name>admin</role-name>
    </security-role>
    <security-role>
        <role-name>manager</role-name>
    </security-role>
</web-app>
```

HTTP Client Authentication

- End user authentication using HTTPS (compared over SSL) is a strong authentication mechanism.
- This mechanism requires the user to possess a Public Key Certificate(PKC).
- PKC are useful in e-commerce application and also for single-sign- on from within the browser.
- Client-certificate authentication is a more secure method of authentication when compared to BASIC or FORM authentication.
- It uses HTTP over SSL, in which the server and, optionally, the client authenticate one another with Public Key Certificates. Secure Sockets Layer (SSL) provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.

- Public key certificate is like a digital equivalent of a passport. It is issued by a trusted organization, which is called a certificate authority (CA), and provides identification for the bearer.
- If you specify client-certificate authentication, the Web server will authenticate the client using the client's X.509 certificate, a public key certificate that conforms to a standard that is defined by X.509 Public Key Infrastructure (PKI).

Example :

```
<web-app>
   <security-constraint>
      <web-resource-collection>
        <web-resource-name> User Auth</web-resource-name>
        <url-pattern>/auth/*</url-pattern>
        </web-resource-collection>
         <auth-constraint>
            <role-name>admin</role-name>
            <role-name>manager</role-name>
         </auth-constraint>
     </security-constrait>
```

```
<login-config>
        <auth-method>CLIENT-CERT</auth-method>
        <realm-name>User Auth</realm-name>
    </login-config>
   <security-role>
        <role-name>admin</role-name>
   </security-role>
   <security-role>
         <role-name>manager</role-name>
   </security-role>
</web-app>
```

Check Your Progress Answers

Check your progress 1:

1. Compare and contrast Computer security and Network security.

Ans : Web Security is defined as technological and managerial procedures applied to computer systems to ensure the integrity, availability and confidentiality of information.

- Web security is divided into two categories :

1. Computer security
2. Network security

Computer Security :

- It is the process of securing a single, standalone computer.
- It is the technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of the data managed by the computer.

Network Security :

- It is the process of securing an entire network of computers.
- It is the protection of network and their services from unauthorised modification destruction, or disclosure.

2. Explain IP Protocol Suite.

Ans : A protocol is a set of rules that allows effective communication

The Internet protocol suite is the conceptual model and set of communications protocols used in the Internet and other computer networks. It is a set of different types of protocols used in different layers of network namely :-

- Physical layer
- Data link layer
- Network layer
- Transport layer
- Session layer
- Presentation layer
- Application layer

- The suite is sometimes just called TCP/IP, because those are the predominant protocols.

TCP : Transmission Control Protocol

IP : Internet Protocol

3. What is web security ? Explain with suitable examples.

Ans : Web Security is defined as technological and managerial procedures applied to computer systems to ensure the integrity, availability and confidentiality of information.

- Web security is divided into two categories :

1. Computer security
2. Network security

Computer Security :

- It is the process of securing a single, standalone computer.
- It is the technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of the data managed by the computer.

Network Security :

- It is the process of securing an entire network of computers.
- It is the protection of network and their services from unauthorised modification destruction, or disclosure.

Examples :

HTTPS : Hypertext Transfer Protocol Secure (**HTTPS**) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.

SSL stands for Secure Socket Layer/TLS : Transport Layer Security

SSL/TLS are cryptographic protocols designed to provide communication security over computer network.

IPSec : Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data sent over an Internet Protocol network.

Check your progress 2:

1. List the basic security concepts.

Ans : Basic security concepts are :

1. Integrity
2. Confidentiality
3. Availability
4. Authenticity

1. Authorisation
2. Assurance

2. What do you understand by information assurance?

Ans :It ensures that the security measures , both technical and operational, work as intended to protect the system and the information it processes. Information assurance includes protection of the integrity, availability, authenticity, non -repudiation and confidentiality of user data.

3. Compare and Contrast data security and system integrity.

Ans : Data integrity :

- This property ensures that data has not been altered in an unauthorised manner while in storage, during processing or while in transit. It assures that data can only be accessed and altered by those authorised to do so. Integrity is ensured by a number known as a Message Integrity Code (MIC) or Message Authentication Code (MAC).

System Integrity :

- This property ensures that a system has performed the intended function in an unimpaired manner, free from unauthorised manipulation.

Check your progress 3 :

1. Compare and contrast the authentication types (BASIC,DIGEST,FORM and CLIENT-CERT); describe how it works; and given a scenario, select an appropriate type.

Please check : HTTP Authentication.

Thank You!!

For reviews and more presentations comment below…