Sagar Jadav

4020 - A

Information Security

Assignment Submission

MSc. [CA & IT]

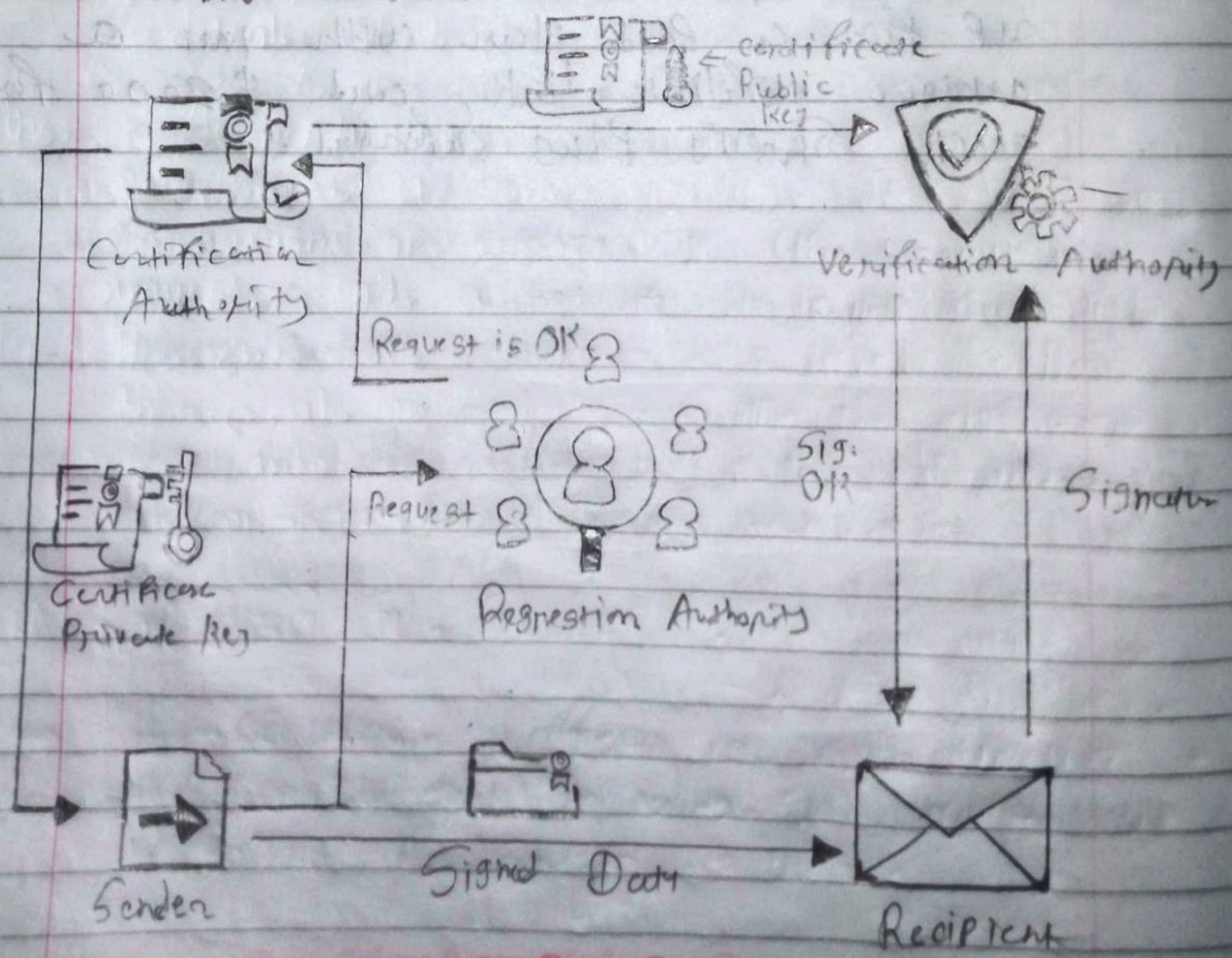
4020
Sagar
Singh

Information Security

Q.1 What is digital certificate ?
Explain Public Key infrastructure.

→ "A Digital Certificate is an electronic 'Password' that allows a Person, organization to exchange data securly over the Internet using the Public Key infrastructure (PKI). Digital Certificate is also known as a Public Key certificate or identity certificate."

Public Key Infrastructure



4020 Sagar
Jeh

Amreli Nag. Sah. Bank Ltd.
Date :
Page :

* Public Key Infrastructure:

* Identification / Authentication:

The Persons / entities with whom we are communication are really who they say they are.

* Confidentiality:

The information with the message or transaction is kept confidential. It may only be read & understood by the intended sender and receiver.

* Integrity:

The information ~~with~~ within the message or transaction is not tampered accidentally or deliberately with ~~xx~~ en route without all parties involved being aware of the tampering.

* Non-Repudiation:

The sender can't deny sending the message or transaction, and the receiver can't deny receiving it.

પરિવારની સેવા આપતી અમરેલી નાગરિક સહકારી બેંક

4020 Sagar

Amreli Nag. Sah. Bank Ltd.
Date :
Page :

* Access Control:

Access to the Protected information is only realized by the intended person or entity.

→ All of the above Security Properties can be achieved and implemented through the use of Public Key Infrastructure.

Q.2 What Authetication? Explain KERBEROS in detail.

Ans: Authentication is the Process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials Provided are compared to those on a file in a database of the authorized user's info. on a local operating System or within an authentication Server.

* KERBEROS :-

→ Kerberos Provides a centralized authentication Server whose function is to authenticate users to Servers and Servers to users.

૩૫ દિવસ અવિરત કામ કરતી ભારતની એકમાત્ર બેંક

4020 Sagar

→ In Kerberos Authetication Server and database is used for client authentication.

→ Kerberos runs as a third-Party trusted Server known as the Key Distribution Center (KDC). Each user and service on the network is a Principal.

- The main Components of Kerberos are:

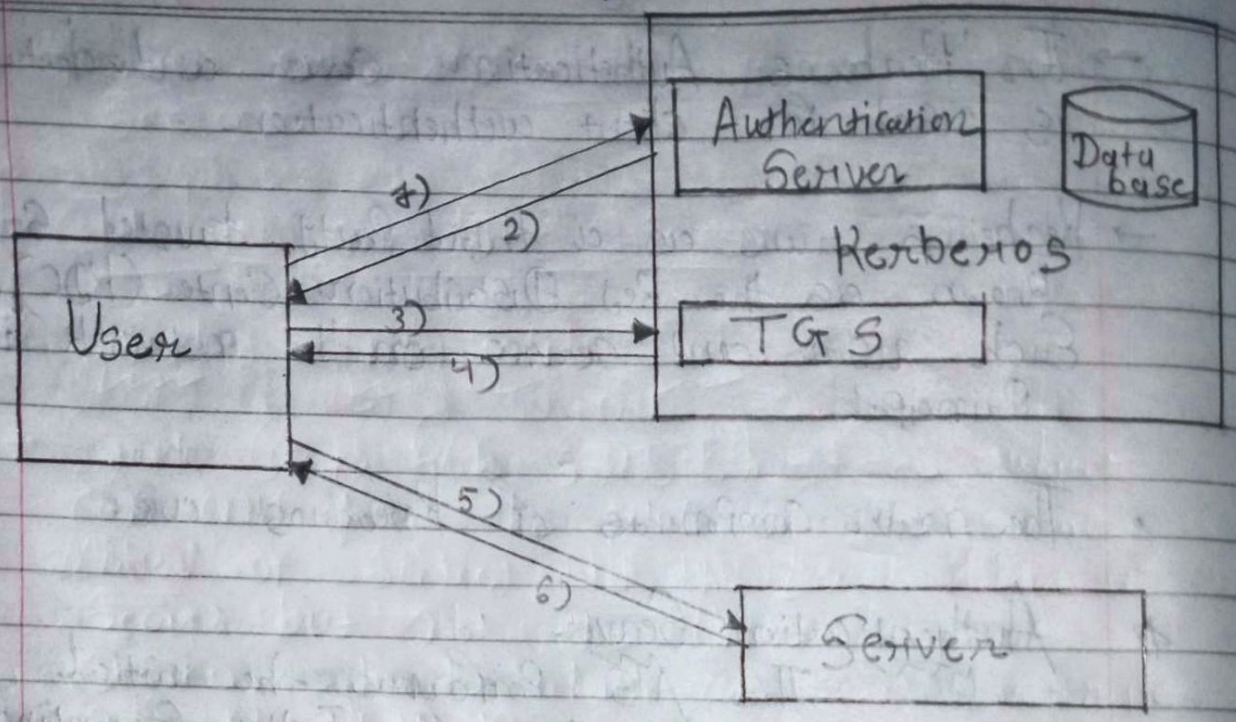
* Authentication Server :
The AS Performs the initial authentication & ticket for Ticket Granting Service.

* Database :
The Authentication Server verifies access rights of users in database.

* Ticket Granting Server (TGS) :
The Ticket Granting Server issues the ticket for the Server.

Step 7: User logon & request services on host. Thus user req. for ticket granting-service.

4020 Sugar
Sep



Step:2 AS verifies user's access right using database & then gives ticket-granting-ticket & session key. Results are encrypted using Password of user.

Step:3 Decryption of msg. is done using the Password then send the ticket to Ticket Granting Server. The Ticket contain authentications like user name & network address.

Step:4 Ticket Granting Server decrypts the ticket send by User & Authenticator verifies the req. then creates the ticket for Req. Services from the Server.

4020 Sugar
fork

Step. 5: User send the Ticket and Authentication to the Server.

Step. 6: Server verifies the Tickets & authenticating then generate the access to the Service. After this User can access the Services.

Q.3 Diff. Types of Information Security Model.

Ans: These models are used for maintaining goals of security, i.e. Confidentiality, Integrity, & Availability. In Simple words, it details with CIA Triad maintenance.

- There are 3 main types of Classic Security Models.

(1) Bell - LaPadula :

→ This Model was invented by Scientists David Elliot Bell and Leonard J. LaPadula.

→ Thus this model is called the Bell-LaPadula Model. This is used to maintain the Confidentiality of Security.

→ Here, the classification of Subjects (Users) & Objects (Files) are Organized in a non-discretionary

સુમિત્ર-મડપી સેવા સામતી અમરેલી નાગરિક સહકારી બેંક

4020 Sugan
Sugan

fashion, with respect to different levels of secrecy.

→ It has mainly 3 Rules:

- Simple Confidentiality Rule:

→ Simple Conf. Rule states that the Subject can only Read the files on the same Level of Secrecy and the Lower Level of Secrecy but not the Upper Level of Secrecy, due to which we call this rule as No READ-UP.

- Star Confidentiality Rule:

→ This rule states that the subject can only write the files on the same Level of Secrecy & the Upper Level of Secrecy & the Upper Level of Secrecy but not the Lower Level of Secrecy, due to which we call this rule as NO WRITE-DOWN.

- Strong Star Confidentiality Rule:

→ Strong Star Confidentiality Rule is highly secured and strongest which states that the Subject can Read and write the files on the same Level of Secrecy only

૩૬૫ દિવસ અવિરત કામ કરતી ભારતની એકમાત્ર બેંક

4020 Sugar
fsk

and not the Upper Layer of Secrecy or the Lower Layer of Secrecy, due to which we call this rule as NO READ WRITE UP DOWN.

② Bibo :-

→ This Model invented by Scientist Kenneth. J. Bibo. This is used to maintain the Integrity of Security. Here, the classification of Subjects & Objects are organized in a non-discretionary fashion, with respect to diff. layers of Secrecy.

→ This works the exact reverse of the Bello-LaPadula Model.

* 3 Rules:

• Simple Integrity Rule:

Integrity Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO READ DOWN.

4020 Sugar
Sugar

Amreli Nag. Sah. Bank Ltd.
Date :
Page :

- **Star Integrity Rule:**

→ Star Integrity Rule states that the Subject can only Write the files on the Same Layer of Secrecy & the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as NO WRITE-UP

- **STRONG STAR INTEGRITY RULE.**

③ **Clarke Wilson Security Model :-**

→ This Model is a highly Secured model. It has the following entities.

- **SUBJECT:** It is any user who is requesting for Data Items.
- **CONSTRAINED DATA ITEMS:** It can't be accessed directly by the Subject. These need to be accessed via Clarke Wilson Security Model
- **UNCONSTRAINED DATA ITEMS:** It can be accessed directly by the Subject.

4020 Sagar

Q.4. What is Tunneling ? Explain IP Sec.

→ "In the physical world, tunneling is a way to cross terrain or boundaries that could not normally be crossed."

→ Similarly, in networking, tunnels are a method for transporting data accrossed a network using protocols that are not supported by that network.

→ Tunneling works by encapsulation packets: wrapping packets inside of other packets.

→ Tunnelling is often used in virtual private networks. It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

IP Sec :

→ IP Sec is a suite of protocols and algorithms for securing data transmitted over the internet or any public network.

→ The internet Engineering Task Force, or IETF, developed the IPSec protocols

સુશિક્ષિત-ઝડપી સેવા આપતી અમરેલી નાગરિક સહકારી બેંક

4020 Sagar
Gup

in the mid-1990s to Provide Security at the IP layer through authentication and encryption of IP network Packets.

* The following are key IPsec Protocols :-

- **IP AH** :- AH is specified in RFC 4302. It Provides data integrity and transport Protection Services.
AH was designed to be inserted into an IP Packet to add authentication data and Protect the contents from modification.

- **IP ESP** :- Specified in RFC 4303, ESP Provides authentication, integrity and confidentiality through encryption of IP Packets.

- **IKE** :- Defined in RFC 7296, IKE is a Protocol that enables two system OR devices to establish a secure communication channel over an untrusted network.

- **Internet Security Association and Key Mgt. Protocol (ISAKMP)** :-

ISAKMP is specified as Part of the IKE Protocol and RFC 7296. It is a framework for key establishment, authentication

૩૫ દિવસ અવિરત કામ કરતી ભારતની એકમાત્ર બેંક

4020 Sagar
Sagar

and negotiation of an SA for a secure exchange of Packets of the IP layer.

→ There are five key steps involved with how IPsec works.

(1) Host Recognition:
(2) Negotiation, or IKE Phase 1
(3) IP Sec circuit, or IKE Phase 2
(4) IPSec transmission.
(5) IP Sec termination.

4020 Sugan
Sugu

Amreli Nag. Sah. Bank Ltd.
Date :
Page :

Q.5. Explain SSL Protocol in detail.

Ans: "Secure Sockets Layer is a security Protocol that Provides Privacy, authentication, & integrity to Internet Communication. SSL eventually envolved into Transport Layer Security (TLS).

→ SSL is an encryption-based internet Security Protocol. It was first developed by Netscape in 1995 for the Purpose of ensuring Privacy, authentication, and data integrity in Internet communication.

→ SSL is the Predecessor to the modern TLS encryption used today.

→ A Website that implements SSL has "HTTPS" in its URL instead of "HTTP".

- How does SSL work?

→ In order to Provide a high degree of Privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of chareters that is nearly impossible to decrypt.

૩૬૫ દિવસ અવિરત કામ કરતી ભારતની એકમાત્ર બેંક

4020 Sagar
Sagar

→ SSL initiates an authentication Process called a handshake between two Communicating devices to ensure that both devices are really who they claim to be.

→ SSL also digitally signs data in order to Provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

• **SSL Certificate :**

→ SSL can only be implemented by websites that have an SSL Certificate. An SSL Certificate is like an ID card or a badge that Proves Someone is who they Say they are. SSL Certi. are Stored and displayed on the Web by a website's or application's Server.

→ The Public key makes encryption Possible. A user's device views the Public key and Uses it to establish secure encryption keys with the web Server.

→ Certificate Authorities (CA) are responsible for issuing SSL Certificates.

4020 Sagar

Sagar

Amreli Nag. Sah. Bank Ltd.
Date :
Page :

* Types of SSL Certificates :

(1) Single-Domain
(2) Wild Card
(3) Multi-Domain
(4) Domain Validation
(5) Organization Validation
(6) Extended Validation..

→ Cloudflare offers free SSL Certi.. for any business. A website protected by Cloudflare can activate SSL with a few clicks. Websites may need to set up an SSL certificate on their origin server as well: this article has further instructions.

4020 Sagar

Q.6 Secure Electronic Transaction [SET] :-

Ans. → SET is a System which Ensures Security and integrity of electronic transaction done using Credit cards in a Scenario.

→ SET is not some System that enables Payment but it is a Security Protocol applied on those Payments.

→ It uses diff. encryption and hashing techniques to Secure Payments over internet done through Credit Cards.

- SET Protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which Provided its ~~Secure Trans~~ Secure Transaction Technology (STT) & Netscape which provided technology of Secure Socket Layer (SSL).

• Requirement in SET :-

→ It has to Provide mutual authentication i.e., Customer authentication by confirming if the customer is intended user or not and merchant authentication.

સુશ્રિત-ઝડપી સેવા આપતી અમરેલી નાગરિક સહકારી બેંક

4020 Sugar
Sugar

→ It has to keep the PI & OI confidential by appropriate encryptions.

→ It has to be resistive against messages modifications i.e, no changes should be allowed in the content being transmitted.

→ SET also needs to provide interoperability and make use of best security mechanisms.

- Participants in SET:

→ In the general scenerio of online transaction, SET includes similar participants:

(1) Card Holder => Customer
(2) Issuer => Customer financial institution
(3) Merchant
(4) Acquirer => Merchant financial
(5) Certificate Authority => Authority which follows certain standards & issues certificates (like X.509V3) to all other participants.

4020 Sagar

Sugr

Amreli Nag. Sah. Bank Ltd.
Date :
Page :

☆ SET functionalities :-

(1) Provide Authentication :-

(a) Merchant Authentication

(b) Customer / Cardholder Authentication

(2) Provide Message Confidentiality :-

(3) Provide Message Integrity :-

4020 Seagan
Sagar

Q.7. Explain Handling User Input in core defence mechansim in webapplication.

→ We can not guess user mind or methodology while inputting. So, we should use approach will "RKB" method which is "Reject Know Bad".

* Reject Known Bad :-

- This, method consists of a blacklist according to which characters are blocked. In general, this is regarded as the least effective approach to validating user input, for two main reasons.

- First, a vulnerability in a web application can be exploited using a wide variety of input, and Second, techniques for exploitation are at a constant change.

→ Black-list filters can be bypassed as:

(1) If SELECT is blocked, try SeLeCt
(2) If or 1 = 1 -- is blocked, try or 2 = 2 --

(3) If alert ('xss') is blocked, try Prompt ('xss')

4020 Sagar

→ Filters designed to block specific keywords can be bypassed by using nonstandard characters b/w expressions to disrupt the tokenizing performed by the application.

Ex:

SELECT /* foo */ username, Password /* foo */
FROM /* foo */ users

→ NULL byte bypassing example,
ex. %00 alert (1)

☆ Accepts Known Good (AKG):-

- This approach is reciprocal of "RKB" approach in which we can not reject the bad inputs. Instead, we can create a white-list. So, application can only accept only listed inputs and all other inputs are rejected by the applications.

- This is more secured than the reject bad known scheme.

☆ Sanitization:-

- In this approach data received must be sanitized. Malicious characters may be removed from the data, only safe characters are left,

સુરિયત-સરકારી સેવા આપતી અમરેલી નાગરિક સહકારી બેંક

4020 Sugar

Or they may be suitably encoded or "escaped" before further processing is performed.

- For ex. the usual defence against cross-site scripting attacks is to HTML-encode dangerous characters before these are embedded into pages of the application.

- But it may be bypassed if attacker understand the sanitization mechanism.

Multi-Step Verification:

- We all are using many secure services these days like gmail etc, which provides us two step or we can say multi-step verification. But all these verification is for user identification rather than data verification.

Semantic Checks:

Safe Data Handling: