Assignment 7
Gunnar Yonker

1.

(1)

SSO vs Kerberos

Similarities:

- They both utilize encryption techniques to protect the user's credentials during transmissions.
- They both use tickets to authenticate users.
- They both are authentication and authorization schemes to authenticate users and then grant the user access to further resources.

Differences:

- SSO is a web-based authentication scheme that lets the user access multiple different applications with one set of credentials.
- Kerberos is a network-based authentication scheme that is mostly used in Windows environments.
- SSO uses central authentication to authenticate users.
- Kerberos uses distributed authentication where each computer on the network acts as a Kerberos client and server.
- SSO supports authentication protocols such as OAuth and SAML, Kerberos uses its own protocol.

(2)

i. An example of where you could use federated identity management for you to use Organization A to authenticate and then use Organization B's services. The employee for Organization A would use their authentication with Organization A to authenticate with Organization B.

User(Organization A) → Service Provider(Organization B) → Identity Provider(Organization A)

Token Issued from Identity Provider to Service Provider

Identity Provider(Organization A) → Service Provider(Organization B) → User(Organization A) Access Granted

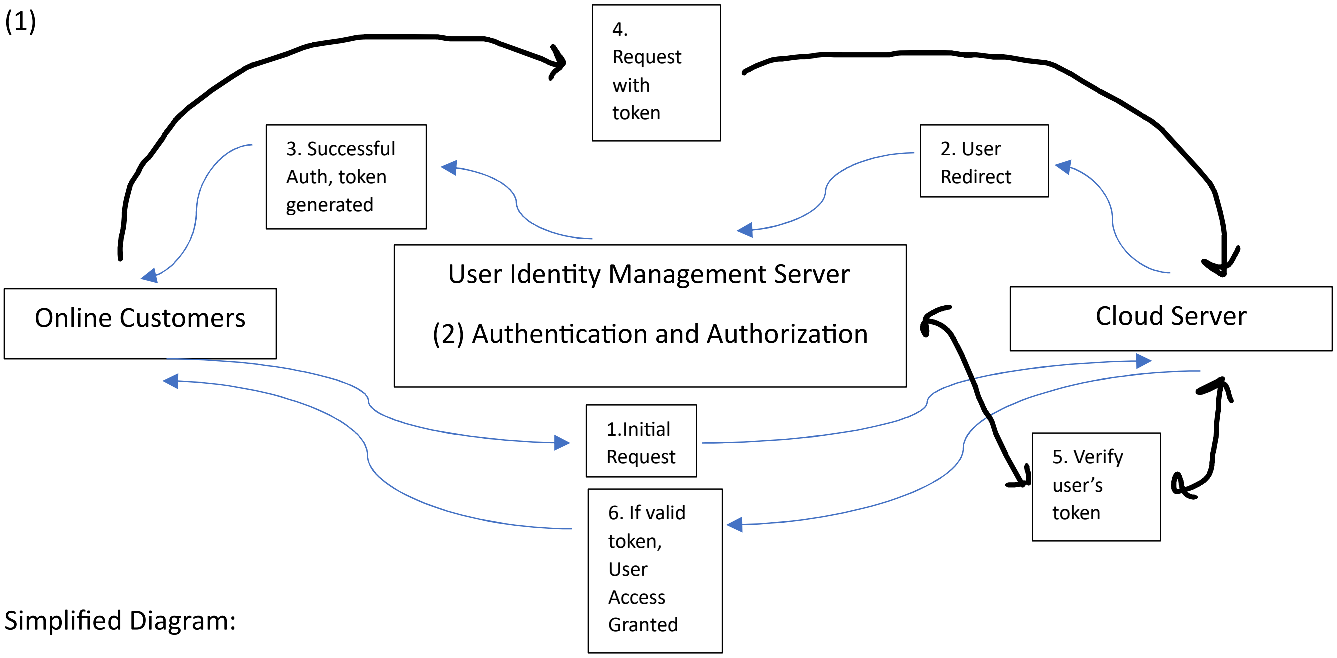
This is an example of how the flow of information would look. User from Organization A would use their login credentials on the Organization B login page. The service provider for Organization B would then redirect the user to the identity provider for Organization A for authentication. Once the identity provider has a successful authentication then a token is issued to the service provider of Organization B who would then grant the user of Organization A access to the intended services.

ii.

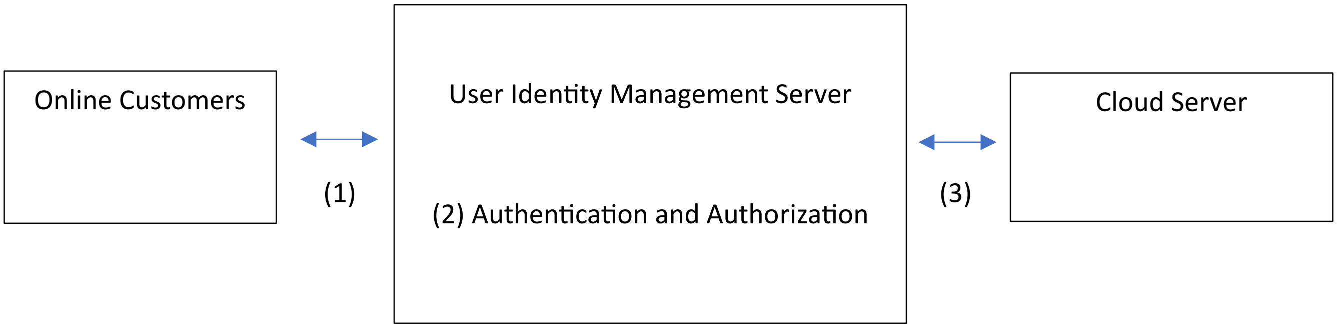
The common format of a token is in the form of a digital certificate that contains the information about the user's identity, access rights, and any other information that could be necessary. The token is then used to grant access to the user for what resources they are trying to access without needing to authenticate every time they are looking to use the resource. Tokens are encrypted using public key cryptography so that it can be ensured that the token has not been tampered or modified with during the transmission. Public key cryptography is used to encrypt and sign the token. The token's digital signature is signed with the Identity Provider's private key which can then be verified using the Identity Provider's public key. When the token reaches the Service Provider they can decrypt the token to then access the information contained in the token which is used to grant the user the appropriate access. Public key cryptography is used to ensure that the token is authentic and has not been tampered/modified during the transmission.

2.

(1)


4. Request with token
3. Successful Auth, token generated
2. User Redirect
Online Customers
User Identity Management Server
(2) Authentication and Authorization
Cloud Server
1.Initial Request
5. Verify user's token
6. If valid token, User Access Granted

Simplified Diagram:


Online Customers
(1)
User Identity Management Server
(2) Authentication and Authorization
(3)
Cloud Server

(2)

There needs to be secure communication between the online customers and the cloud server so that the shopping system is secure and can be trusted. The diagram above would be an example of how the online customers requests could be verified that they are coming from an authenticated and authorized user before reaching the cloud server. The user identity management server(2) would receive the requests(1) from the online customers to then authenticate and authorize them before sending it on to the cloud server(3). The flow of the interaction would go like this: The online customer would access the shopping site and this would send a request to the cloud server, the cloud server would then redirect that user to the user identity management server to be authenticated. The user would then enter their login credentials such as a username and password to the user identity management server which would verify the credentials and if successful generate a session token for the now authenticated user. The user identity management server would then send the session token back to the online customer who then sends the token along with their request to the cloud server. The cloud server then would verify the session token with the user identity management server to ensure that the user is authenticated and authorized to access the online shopping system. Once the token is validated then the cloud server would respond to the online customer's request, and they would be granted access to the shopping system.

(3)

For this system to defend against replay attacks, a secure authentication protocol will be used that includes the use of digital certificates. When the online customer connects to the user identity management server the server will send its certificate to the online customer. Then the online customer will verify the certificate and that it was issued by a trusted certificate authority, additionally it will be checked that it is valid and has not been revoked or expired. If the certificate is valid then the online customer will be able to establish a secure connection with the server. Additionally, to prevent the replay attack a nonce would be used in the authentication protocol. The nonce would be generated by the user identity management server and included in the authentication response sent back to the online customer. The online customer needs to include this nonce in any further requests to the cloud server so that the cloud server can verify that the nonce is valid with the identity manage server. This ensures that another user cannot reuse a valid session token of an online customer after they have ended their session.

3.

(1)

In IPSec, AH(Authentication Header) provides major security services such as data integrity, authentication, and anti-replay protection for IP packets. This can ensure that during a transmission of a packet that it is not tampered/modified and that the packet is being sent from a trusted source. AH does not offer encryption so the packet payload would be viewable if not encrypted by the sender, and if a third-party was listening and collected the packet.

ESP(Encapsulating Security Payload) also provides major security services such as data confidentiality, data integrity, authentication, and anti-replay protection for IP packets. ESP will encrypt the packet payload and if needed/wanted the packet header so that if a third-party was listening and collected the packet, they would be unable to read the payload unless it was decrypted. These security services help to ensure that the packet is not tampered/modified during the transmission and ensures that the packet is from a trusted source.

(2)

IKE Key Determination Algorithm Features:

Multiple Encryption Algorithms: This allows the peers to pick the algorithm best suited for their situation.

Assignment 7
Gunnar Yonker

Perfect Forward Secrecy(PFS): This is to ensure that if an attacker is able to obtain a secret key at a later time, they cannot decrypt any data that was sent before the key was obtained.

Mutual Authentication: Mutual authentication is ensured when using IKE between the two IPSec peers by using digital certificates or key that were previous shared/established.

Dynamic Key Refresh: This allows the users to periodically refresh the shared secret key so that if the key was compromised it would not be able to be used for the full communication because a new secret key could be used.

Replay Attack Protection: Replay attacks are protected against by the use of nonces that are exchanged between the users during the key exchange phase.

Key Exchange: A shared secret key is established between the two IPSec users, then secret key is then used to encrypt and decrypt any data transmitted between them keeping it secure.