Q & A

- What are the steps involved in an authentication process?

- List three general approaches to dealing with replay attacks.
- **Simple replay: The opponent simply copies a message and replays it** later. **Repetition that can be logged: An opponent can replay a** timestamped message within the valid time window. **Repetition that cannot be detected: This situation could arise because the original** message could have been suppressed and thus did not arrive at its destination; only the replay message arrives. **Backward replay without modification: This is a replay back to the message sender.** This attack is possible if symmetric encryption is used and the sender cannot easily recognize the difference between messages sent and messages received on the basis of content.

- What is a suppress-replay attack?

1. Attach a sequence number to each message used in an authentication exchange. A new message is accepted only if its sequence number is in the proper order. **2.** Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgment, is close enough to A's knowledge of current time. This approach requires that clocks among the various participants be synchronized. **3.** Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value.

- What problem was Kerberos designed to address?

The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services.

- What are three threats associated with user authentication over a network or Internet?

1. A user may gain access to a particular workstation and pretend to be another user operating from that workstation. **2.** A user may alter

the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation. **3.** A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

- What four requirements were defined for Kerberos?

Secure: A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally, Kerberos should be strong enough that a potential opponent does not find it to be the weak link. **Reliable:** For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ a distributed server architecture, with one system able to back up another. **Transparent:** Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password. **Scalable:** The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

- **What entities constitute a full-service Kerberos environment?**

A full-service Kerberos environment consists of a Kerberos server, a number of clients, and a number of application servers.

- In the context of Kerberos, what is a realm?

A realm is an environment in which: **1.** The Kerberos server must have the user ID (UID) and hashed password of all participating users in its database. All users are registered with the Kerberos server. **2.** The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

- _____ protocols enable communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys.
-
- _____ in Greek mythology is a three headed dog with a serpent's tail that guards the entrance of Hades.
-
- There are four general means of authenticating a user's identity. They are: something the individual knows, something the individual possesses, something the individual is, and something the individual _____ .

- Mutual authentication
- Kerberos
- does

- To convince the server that a user is authentic, the authentication server creates a _____ that contains the user's ID and network address and the server's ID and sends it back to the client so they can continue the request for service.
-
- An authentication process consists of two steps: identification step and _____ step.
-
- _____ is a centralized, automated approach to provide enterprise wide access to resources by employees and other authorized individuals.

- ticket
- verification
- Identity management

- The first published report on Kerberos listed the following requirements: secure, reliable, scalable and _____ .
-
- Examples of something the individual possesses would include cryptographic keys, electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a _____ .
-
- The _____ is responsible for generating keys to be used for a short time over a connection between two parties and for distributing those keys using the master keys to protect the distribution.

- transparent
- token
- key distribution center (KDC)

- A _____ attack is where an opponent intercepts a message from the sender and replays it later when the timestamp in the message becomes current at the recipient's site.
-
- _____ is an authentication service developed as part of Project Athena at MIT.
-
- A solution, which eliminates the burden of each server having to confirm the identities of clients who request service, is to use an _____ that knows the passwords of all users and stores these in a centralized database and shares a unique secret key with each server.

- suppress-replay
- Kerberos
- authentication server (AS)

- The ticket granting ticket is encrypted with a secret key known only to the AS and the _____ .
-
- Intended to provide an integrity check as part of the encryption operation, encryption in Kerberos Version 4 makes use of a nonstandard mode of DES known as _____. It has been demonstrated that this mode is vulnerable to an attack involving the interchange of ciphertext blocks.

- ticket-granting server (TGS)
- propagating cipher block chaining (PCBC)