Daniel Frey
CS 3910-001
Kerberos
4/7/19

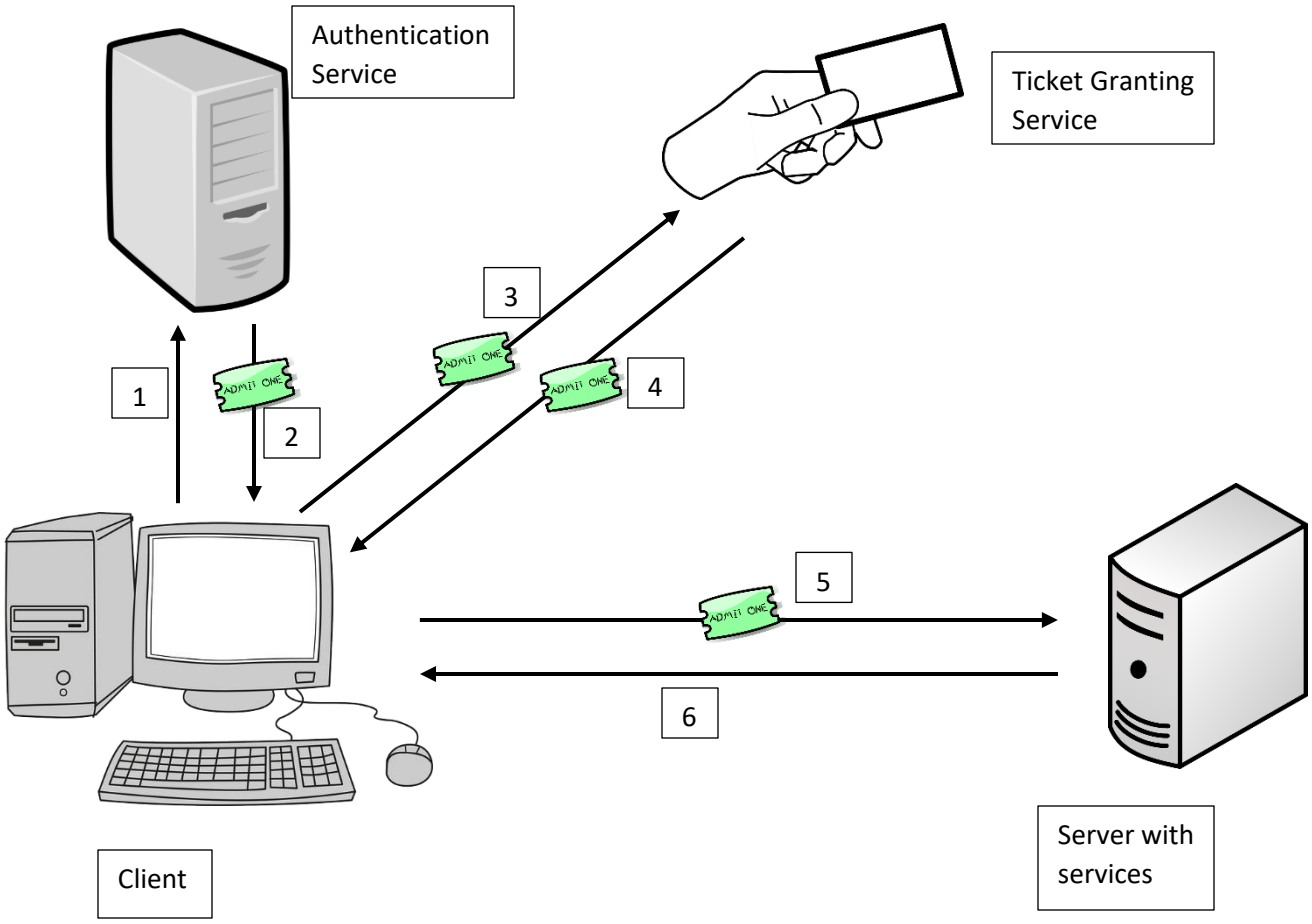
- **Explain in detail what Kerberos tries to solve.**
  Kerberos tries to solve the problem of authentication. It wants to prove you are who you say you are. The client must be who they say they are so that only they will have the appropriate permissions to access secured services. Information sent across networks should not be able to be intercepted and have the system tricked into thinking an "authenticated" user is using the system. Simply, Kerberos tries to address network security problems. It is a way to help secure information across insecure networks, and it is a way to authenticate users.

- **How does Kerberos solve the authentication issue?**
  Kerberos uses a ticket-granting service to assist in the authentication of a client. Your username will be used for Kerberos to look up your stored password. A ticket-granting ticket is built along with a session key. This information is encrypted with the password that Kerberos looked up. A packet is sent over the network and can only be decrypted by the user that knows their password. Once the packet is decrypted, the session key is obtained and can be used to create tickets to services. If the packet is not able to be successfully decrypted, then the user cannot be authenticated. Even if the packet is intercepted, the attacker cannot properly decrypt it to obtain the session key without the appropriate password. Tickets can then be granted with the proper session key to allow access to services on the server. The server must also prove it is the appropriate server by sending a packet to the client.

- **How is Kerberos used today and why is it important?**
  Kerberos is widely used today in many applications. One form is single sign-on. This allows users to be granted a ticket when they sign in so that they will not have to continually retype their password for every other service they wish to use. Kerberos is often used in sharing files, email, remote access, etc. Kerberos is important because it provides a way to keep communications secure with an authenticated user. It is a safeguard against hackers that might want to trick systems into thinking they are someone else that has approved access.

- **Explain why time is an important part of Kerberos.**
  Time is an important part of Kerberos because the tickets should only be valid for a certain amount of time so that they cannot be stolen by attackers. Timestamps are a part of the Kerberos protocol to briefly allow users to authenticate themselves and only themselves. Having inaccurate time could allow the system to be compromised since attackers could have more time to successfully complete their attacks.

- **Diagram Kerberos authentication process. Label key components.**



1. Client requests ticket from authentication service (AS).
2. AS sends an encrypted ticket-granting ticket (TGT) to client.
3. Client send TGT to ticket granting service (TGS) with request for specific access to service.
4. TGS sends client ticket for access to service.
5. Client sends service ticket to server.
6. Server sends client proof that it is the appropriate server.