KERBEROS AUTHENTICATION: WHAT IT IS AND HOW IT WORKS

What is Kerberos

Every time users log into a service by providing their credentials, they are potentially exposed to attacks, especially if they're using unsafe network protocols. For instance, an attacker could use a simple packet sniffer to recover your user id and password especially if they're not encrypted.

What does this mean? Every time I provide my credentials to a service, should I be afraid that they could be stolen? Potentially—however, there are many precautions that we should consider when accessing a service over the internet like:

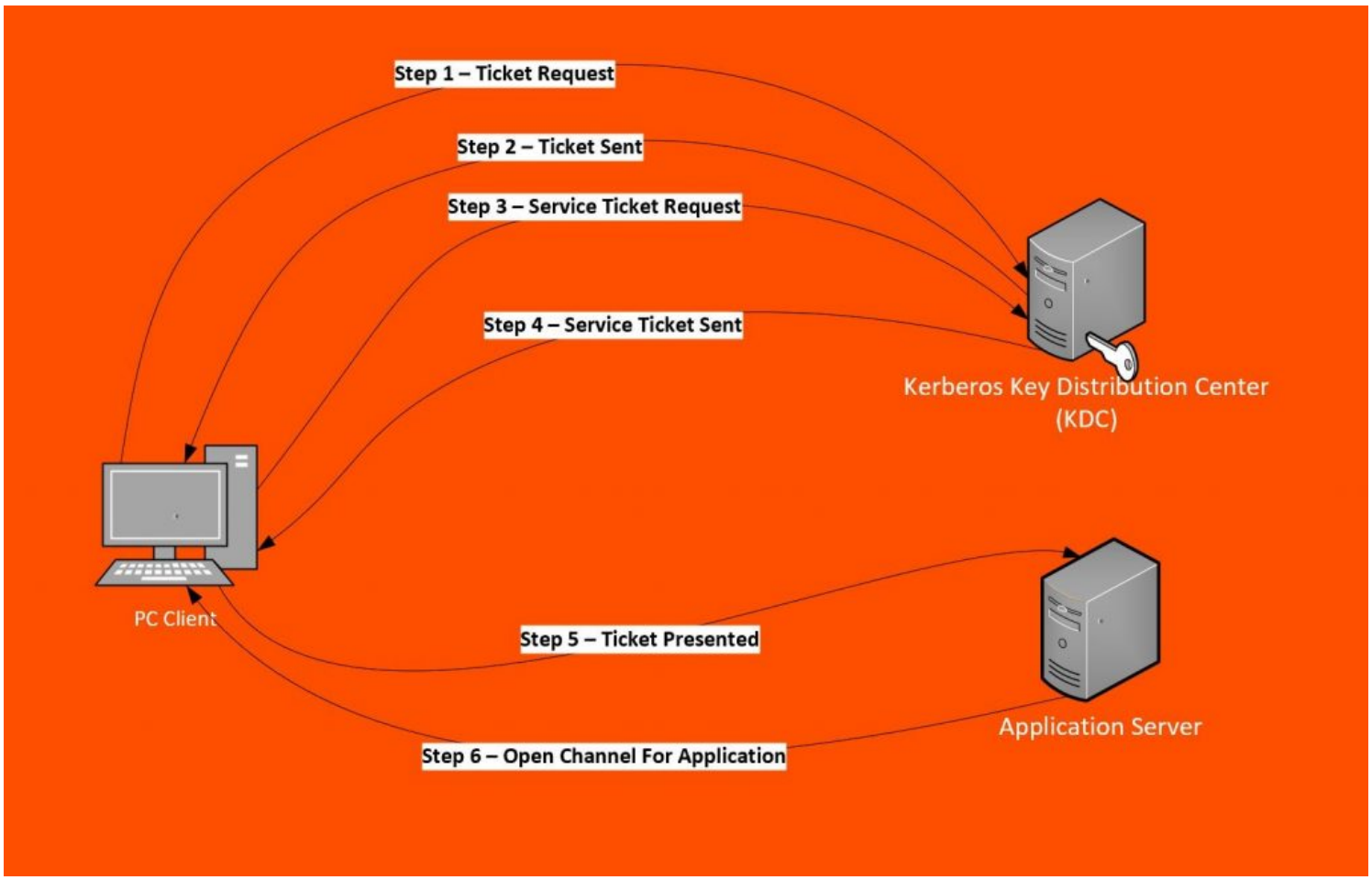
- Always using certified websites having https in their web address,
- Using CSRF protection,
- Disallowing framing, or
- Logging out from applications.

To address potential insecurity when using authentication, new safe protocols have been created and one of them is Kerberos. Kerberos is the mythological three-headed Greek creature which is guarding the gates of underworld to prevent souls from escaping. With that as its inspiration, the Massachusetts Institute of Technology developed a protocol to protect its own projects in the late 1980s. The idea behind Kerberos is simple: authenticating users while avoiding sending passwords over the internet.

This protocol can be easily adopted even on insecure networks as it is based on a strong cryptography and it's developed on a client-server model. Enabling a service to use Kerberos authentication is referred to as making the service "Kerberos aware". This is actually possible for the majority of software.

How Kerberos Works

When authenticating, Kerberos uses symmetric encryption and a trusted third party which is called a Key Distribution Center (KDC). At the moment of the authentication, Kerberos stores a specific ticket for that session on the user's machine and any Kerberos aware service will look for this ticket instead of prompting the user to authenticate through a password.



Source: BMC Software

These are the steps in Kerberos Authentication:

1. PC Client logs on the domain. A Ticket-Granting Ticket (TGT) request is sent to a Kerberos KDC
2. The Kerberos KDC returns a TGT and a session key to the PC Client
3. A ticket request for the application server is sent to the Kerberos KDC. This request consists of the PC Client, TGT and an authenticator.
4. The Kerberos KDC returns a ticket and a session key to PC Client.
5. The ticket is sent to the application server. Upon receiving the ticket and the authenticator, the server can authenticate the PC Client.
6. The server replies to the PC Client with another authenticator. On receiving this authenticator, the PC Client can authenticate the server.

Kerberos integration is also supported by Remedy Single Sign On which is the main authentication module that is used for a great number of BMC products. In Remedy Single Sign On, it is possible to configure a Kerberos as the authentication service. In this case, Remedy Single Sign On validates the token that is sent from a client (e.g., a browser to give access to BMC Digital Workplace) together with a KDC and lets the user log into the application using her/his Windows credential.

Advantages and Disadvantages of Kerberos

Like many technical solutions, Kerberos has advantages as well as some weaknesses.

The principal advantages in adopting Kerberos as an authentication service are:

- Passwords are never sent across the network because only keys are sent in an encrypted form;
- Authentication is mutual, so client and server authenticate at the same steps and they are both sure they are communicating with the right counterpart;
- Authentications are reusable and do not expire;
- Kerberos is entirely based on open Internet standards and;
- Kerberos is adopted by a huge number of industries, so any new weaknesses in its security protocol or in underlying modules are quickly corrected.

The weaknesses of Kerberos are:

- If a non-authorized user has access to the Key Distribution Center, the whole authentication system is compromised.
- Kerberos can only be adopted by Kerberos aware applications. It could be a problem to rewrite the code for some applications in order to make them Kerberos aware.

Recommendations for Using Kerberos

When using Kerberos authentication in Remedy Single Sign On, you need to remember to enable Kerberos authentication for the browsers you're using. It is not always enabled by default. Here's how to do that for two commonly used web browsers.

For Internet Explorer:

1. On the Internet Options dialog box, select the Advanced tab.
2. Then, scroll down to the Security settings. Select the *Enable Integrated Windows Authentication* check box.
3. Click the OK button and then, restart the browser so that the settings take effect.

For Firefox:

1. Open Firefox and enter about:config in the address bar. Dismiss any warnings that appear.
2. In the Filter field, enter negotiate.
3. Double-click the network.negotiate-auth.trusted-uris preference. This preference lists the trusted sites for Kerberos authentication.
4. In the dialog box, enter the Remedy Single Sign On domain, such as rsso.bmc.com.
5. Click the OK button.

As you can see, Kerberos provides another way to authenticate that thwarts bad actors who hope to steal passwords. Even further, it can be effectively utilized with applications that are Kerberos aware.

While there are some downsides, it's another tool to make single-sign-on run smoothly while keeping passwords safe.

If you would like to utilize Kerberos with your BMC Remedy Single Sign On, please fill out our form and an expert will reach out to get you started.