Toilet Paper #70

Single Sign-On with Kerberos

By Hannes Lerchl

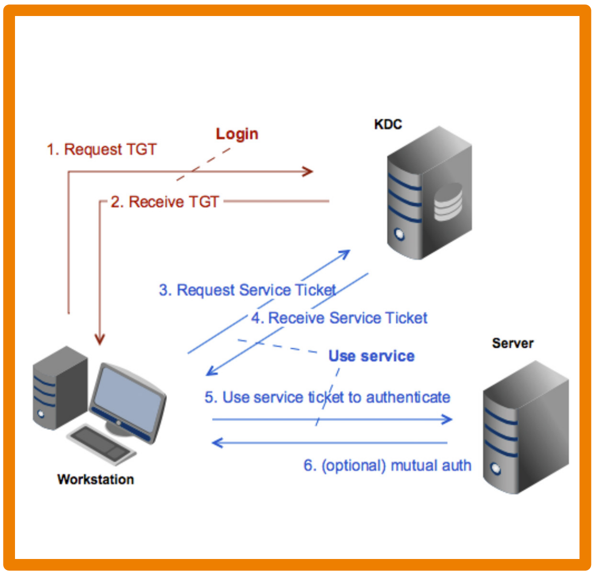
✖ Problem

To handle different users and their permissions, the concept of an "account" is firmly established in computer systems. In most cases, this account is linked to a password that (hopefully) only the user knows. You have such an account for quite a few systems. The problem that arises especially in company networks (or similar ones) is the balancing act between "convenience" and security.

✔ Solution

In the late 1980s / early 1990s (*1), the Kerberos network protocol was developed (*2) in response to this problem. Since Windows 2000, Kerberos has been the standard protocol for authentication in Windows domains. This protocol is used for the cryptographically secured exchange of "authentication tickets" and has some very nice features:

- At first, the user (more precisely: his OS) obtains a *ticket-granting ticket*(TGT). This is usually valid for 10 hours.
- This TGT can be used to request tickets for specific services, with which you can then identify to the corresponding servers.
- The TGT can also be used to negotiate session keys.
- The protocol is designed for the use in "insecure networks".
- It is safe against unauthorized reading and replay attacks.
- Not only the client, but also the server must identify itself (if required by the client).
- There is only one central location where the password is stored (the KDC, in Windows PDC networks); this is the only location all participants in the domain (the "realm") (have to) trust.
- All servers in this realm do not have to take care of user administration or password security.
- The password never "travels" unsecured through the network.
- The user logs in once; from then, the network "knows" the user.


1. Request TGT
Login
KDC
2. Receive TGT
3. Request Service Ticket
4. Receive Service Ticket
Server
Use service
5. Use service ticket to authenticate
6. (optional) mutual auth
Workstation

The problem is that not all services use Kerberos authentication. This applies in particular to web applications. But since Apache and Firefox / Safari / Chrome can authenticate using Kerberos, these services can often be "upgraded".

➔ Example

In a Windows network, users typically use Kerberos for authenticating to the following services:

- cifs – Windows network shares; commonly called "network drive" or "project drive"
- ldap – Next to Kerberos, the second important pillar of Active Directory; contains network-global configurations
- http – Exchange can use Kerberos for its http based parts

Other examples of Kerberos-enabled services include NFSv4, ssh, HTTP (e.g. Apache with mod_auth_kerb), xmpp (aka jabber), ftp (e.g. vsftpd), cups (Apple's printing system).

✚ Further aspects

- Different Kerberos realms ("domains") can build trust relationships. Uni- or bidirectional.
- DNS and NTP (clock synchronization) must be in use correctly for Kerberos to work reliably.
- For Unix-like operating systems (e.g. Linux, Mac OS X), the command "klist" displays the tickets currently used. “kinit” requests a new TGT; potentially from other realms (unfortunately, only one TGT can be in use at the same time).
- By the way: "Kerberos" (or Cerberus) is in Greek mythology the three-headed dog guarding the entrance to Hades.

(*1) See specification in RFC 1510 and RFC 4120.
(*2) Using Unix computers during the Athena project, which also produced the X Window System.