Toilet Paper #70

Single Sign-On mit Kerberos

Von Hannes Lerchl

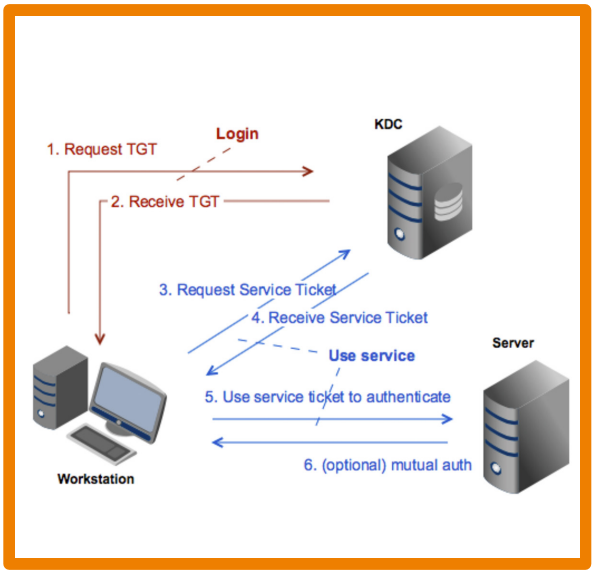
✖ Problem

Um verschiedene Benutzer und deren Berechtigungen zu handhaben, ist in Computersystemen das Konzept vom "Account" fest verankert. In den meisten Fällen ist dieser Account mit einem Passwort gekoppelt, das (hoffentlich) nur der entsprechende Nutzer kennt. So einen Account hat man heutzutage für ziemlich viele Systeme. Das Problem, das dadurch insbesondere in Firmennetzwerken (oder dergleichen) entsteht, ist der Spagat zwischen "Bequemlichkeit" und Sicherheit.

✔ Lösung

Ende der 1980er/Anfang der 1990er Jahre[1] wurde als Antwort auf dieses Problem das Kerberos-Netzwerk-Protokoll entwickelt[2]. Seit Windows 2000 ist Kerberos das Standard-Protokoll für Authentifizierung in Windows-Domänen. Dieses Protokoll dient dem kryptographisch gesicherten Austausch von "Berechtigungs-Tickets" und hat ein paar sehr nette Eigenschaften:

- Zu Beginn besorgt sich der Nutzer (genauer: sein OS) ein *Ticket-Granting-Ticket* (TGT). Dieses ist üblicherweise 10 Stunden lang gültig.
- Dieses TGT kann verwendet werden, um Tickets für spezifische Dienste anzufordern, mit denen man sich dann gegenüber den entsprechenden Servern ausweist.
- Das TGT kann auch verwendet werden, um Session-Keys auszuhandeln.
- Das Protokoll ist entworfen für Benutzung in "unsicheren Netzwerken".
- Es ist sicher gegen Mitlesen und Replay-Attacken.
- Nicht nur der Client, auch der Server muss sich ausweisen (wenn vom Client gefordert).
- Es gibt nur einen einzigen zentralen Ort, an dem das Passwort gespeichert wird (der KDC; in Windows-Netzwerken der PDC); dieser Rechner ist der einzige, dem alle Teilnehmer in der Domäne (dem "Realm") vertrauen (müssen).
- Sämtliche Server in diesem Realm müssen sich nicht um User-Verwaltung und Passwort-Sicherheit kümmern.
- Das Passwort wandert niemals ungesichert übers Netzwerk.
- Der Nutzer loggt sich einmal ein; ab dann "kennt" ihn das Netzwerk.



Der Pferdefuß an der Sache ist, dass nicht alle Dienste eine Kerberos-Authentifizierung verwenden. Insbesondere Web-Anwendungen haben hier Berührungsängste. Apache und Firefox/Safari/Chrome beherrschen eine Authentifizierung über Kerberos; insofern können diese Dienste oft "nachgerüstet" werden.

➔ Beispiel

In einem Windows-Netzwerk authentifizieren sich Nutzer üblicherweise an folgenden Diensten über Kerberos:

- cifs – Windows-Netzwerk-Freigaben; vulgo "Netzlaufwerk" oder "Projektlaufwerk"
- ldap – Neben Kerberos die zweite wichtige Säule des Active Directory; enthält Netzwerk-globale Konfigurationen
- http – Exchange kann Kerberos für seine http-Anteile nutzen

Weitere Beispiele für Kerberos-fähige Dienste sind NFSv4, ssh, HTTP (e.g. Apache mit mod_auth_kerb), xmpp (aka jabber), ftp (e.g. vsftpd), cups (Apples printing system).

✚ Weiterführende Aspekte

- Verschiedene Kerberos-Realms ("Domänen") können Vertrauens-Verhältnisse aufbauen. Uni- oder Bidirektional.
- Damit Kerberos zuverlässig funktioniert, müssen DNS und NTP (Uhrzeit-Synchronisierung) korrekt in Benutzung sein.
- Für unixoide Systeme (z.B. Linux, Mac OS X) zeigt der Befehl klist die aktuell verwendeten Tickets an. kinit fordert ein neues TGT an; möglicherweise von anderen Realms (leider darf zeitgleich immer nur ein TGT in Benutzung sein).
- Apropos: "Kerberos" (oder Cerberus) ist in der griechischen Mythologie der dreiköpfige Hund, der den Eingang zum Hades bewacht.

(*1) Spezifikation siehe RFC 1510 bzw. RFC 4120.
(*2) Auf Unix-Rechnern im Rahmen des Project Athena, welches ebenso das X Window System hervorbrachte.