Die grundlegende Idee des Kerberos Protokolls - In Theorie und Spiel

Dieser Vortrag ist eine kleine Einführung in das Kerberos Protokoll. Kerberos wurde zu Beginn des Computer-Zeitalters am MIT entwickelt, aber erst Ende der 80-er entwich es zum ersten mal in der (Labor-)Version 4. Heute liegt es in der Version 5 vor und wird mit kleinen Variationen in verschiedenen Produkten wie z.B „Active Directory“ verwendet. Kerberos, dient dazu jeweils zwei Partner über ein unsicheres öffentliches Computer-Netzwerkes wechselseitig zu Authentisieren.
Damit ein Prinzipal (zumeist ein Mensch) Dienstleistungen von bisher unbekannten Anbietern (i.A.Maschinen) beziehen kann wird der Kerberosserver als „trusted third party“ (vertrauenswürdiger gemeinsamer Bekannte) benutzt.
Die Client-Maschine selbst muss dazu lediglich ein Stück Software und Netzzugang besitzen – nichts weiter. Das bedeutet, dass die vom Mensch als Kerberos-Client benutze konkrete Maschine kein eminenter Teil der Kerberos-Authentisierung an sich ist. Der Benutzer kann Kerberos auch auf einer neu installierten Maschine problemlos benutzen, ohne dass zuvor ein zentraler Administrator irgendwelche mystischen Initialisierungsriten zelebrieren muss.
Abgesehen davon ist es natürlich immer wichtig, dass ein Anwender von der Integrität einer Client-Maschine überzeugt sein sollte.
Nach erfolgreicher Authentisierung erhält der Benutzer eine zeitlich begrenzte Zugriffsberechtigung, ein sogenanntes „Ticket“ . Die Zeitliche Limitierung ist wichtig, da nur so sichergestellt werden kann, dass eine entzogene Berechtigung auch in definiert endlicher Zeit wirksam wird.
Berechtigte Benutzer können sich gegen Ende der Gültigkeit , welche für gewöhnlich zwischen 8 und 25 Stunden liegt, in neues Ticket besorgen.
Eine weitere wichtige Eigenschaft des Kerberos ist die Wechselseitigkeit der Authentisierung.
Um es auf den Punkt zu bringen: Nicht nur die Bank hat ein Interesse daran festzustellen wer vor dem Geldautomaten steht, nein, auch der Bankkunde sollte ein Interesse daran haben, sicherzustellen, dass der gerade benutze Automat auch wirklich zu der Bank gehört.

Die *„Autorisierung“* ist nicht Gegenstand des Kerberos-Protokolls.
Die *„Authentisierung“* stellt lediglich sicher, dass der Dienstsuchende auch der ist, der er behauptet zu sein. Die Autorisierung hingegen bestimmt danach, ob der (authentisierte) Anwender auch erhält, was er begehrt.
Um im Beispiel zu bleiben – Sicherzustellen, dass sich wirklich der zur Karte gehörende Kunde vor dem Terminal befindet ist Authentisierung, ob dieser Kunde tatsächlich den avisierten Betrag abheben kann oder darf ist die Frage der Autorisierung.

Im Vortrag werden die wichtigsten Begriffe aus diesem Umfeld geklärt und auf das grundlegende Kerberos-Protokoll eingegangen. Danach wird die Notwendigkeit des vollständigen KGS / TGT und der Preauthentication dargestellt.

Am Ende des Vortrages steht eine Frage , welche zeigen kann, ob das Wesen dieser Authentisierung verstanden wurde.

Bei Bedarf kann nach dem Vortrag im kleinen Kreis das Kerberos-Kern-Protokoll „händisch“ durchgespielt werden.

Mathias Feiler , Administrator am KIM-Hohenheim