

Konzepte von Betriebssystem-Komponenten Schwerpunkt Authentifizierung

Das Kerberos-Protokoll

Guido Söldner
guido@netlogix.de

1. Überblick über das Kerberos-Protokoll

Ein Standardvorgang in der Computersicherheit besteht darin, dass Server die Identität der Benutzer prüfen, die ihre Dienste nutzen wollen. Die Identität wird bestätigt, indem der Benutzer das Passwort für ein bestehendes Benutzerkonto eingibt. Da aber für die Nutzung von verschiedenen Diensten die wiederholte Eingabe des Passwortes nötig ist, ist diese Lösung nicht ganz zufrieden stellend. Zudem weiß der Benutzer nicht, auf welche Art und Weise und mit welcher Sicherheit das Passwort übermittelt wird.

Zur Lösung dieses Problem wurde am Massachusetts Institute of Technology das Kerberos-Protokoll entwickelt. Es ermöglicht dem Benutzer, mit einer einzigen Anmeldung auf alle Ressourcen im Netzwerk zuzugreifen. Dies funktioniert, indem sich der Benutzer vor dem eigentlichen Verbindungsaufbau zu einem Server an den Kerberos-Dienst, genannt Kerberos Key Distribution Center wendet. Von diesem erhält er ein Ticket für den Zielservers. Der Zielservers akzeptiert das Ticket als Beweis für die Authentizität des Benutzers.

2. Kerberos-Protokollbegriffe

Zum besseren Verständnis des Kerberos-Protokolls werden die nachfolgenden Begriffe erwähnt, mit denen unterschiedliche Kerberos-Komponenten beschrieben werden[2].

Principal:

Eindeutig bestimmter Nutzer, Client oder Server, der an einer Netzwerkkommunikation teilnimmt.

Session Key:

Ein Session Key ist ein temporärer Codierungsschlüssel der zwischen zwei Principals benutzt wird. Er ist nur diesen beiden bekannt und wird immer verschlüsselt versendet.

Secret Key :

Der Secret Key ist ein Codierungsschlüssel für die Kommunikation zwischen dem Kerberosdienst und einem Principal. Bei einem Benutzer besteht der Schlüssel aus dem Passwort, bei dem Server

aus Zufallszahlen. Die Secret Keys müssen beim Kerberos-Dienst gespeichert sein, damit dieser chiffriert senden kann.

Authentication Server

Der Authentication Server erteilt das TicketGranting Ticket (TGT). Mit diesem ist es dem Client möglich, sich am TicketGrantingService anzumelden.

TicketGrantingService (TGS)

Stellt dem Principal Tickets aus, die dem Client die Kommunikation mit dem Zielservice ermöglicht.

Key Distribution Center

Das Key Distribution Center (KDC) umfasst zwei Funktionen:

Den Authentication Server (AS) und den TicketGranting Service (TGS). Bevor ein Principal den TGS nutzen kann braucht es ein Ticket vom AS, nämlich das TGT.

3. Funktionsweise von Kerberos

3.1 Basisauthentifizierungsprozess

Um die prinzipielle Funktionsweise von Kerberos zu erläutern, soll ein Vergleich aus dem täglichen Leben hergenommen werden. Um unsere Identität zu beweisen, haben wir einen Ausweis. Auf diesem sind eine Reihe von Merkmalen, wie Bild, Größe, Geburtsdatum, usw. aufgelistet, mit denen wir überall zweifelsfrei identifiziert werden können. Wichtig ist, dass es nur eine Instanz gibt, die dieses Dokument ausstellen darf.

Dieses Konzept kann auch auf die Computerwelt übertragen werden und wird mit Kerberos realisiert. Wir erhalten von einer zentralen Instanz ein Ticket, mit dem wir unsere Authentizität beweisen können. Diese Instanz heißt Authentication Server (AS). Mit diesem Ticket können wir uns an dem gewünschten Server identifizieren und somit Zutritt zu den gewünschten Diensten erlangen.

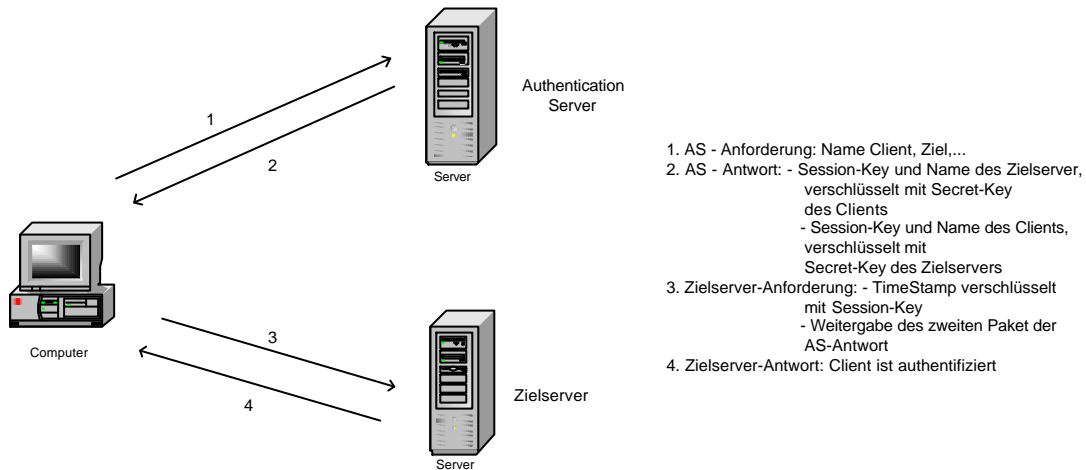
Der Authentifizierungsprozess läuft nun wie folgt ab: [7]

1. Um ein Ticket zu erhalten, meldet sich der Benutzer bei dem AS. Er teilt ihm mit wer er ist und welchen Dienst er nutzen will.
2. Der AS nimmt nun diese Anfrage entgegen und schickt dem Benutzer zwei Pakete zurück. Im ersten Paket sind der Session Key und der Name des zu kontaktierenden Servers enthalten. Dieses Paket ist mit dem Secret Key des Benutzers chiffriert. So kann sichergestellt werden, dass es auch nur der wirkliche Benutzer entschlüsseln kann. Das zweite Paket enthält auch den Session Key und zuzüglich den Namen des Benutzers. Allerdings wird es mit dem Secret Key des Zielservers chiffriert. Somit kann der Benutzer dieses zweite Paket nicht öffnen. Aus Sicherheitsgründen hat der Session Key nur eine Lebensdauer von acht Stunden. Dann muss er wieder erneuert werden.
3. Der Client öffnet nun das erste Paket und entnimmt daraus den Sitzungsschlüssel. Nun versucht der Client die Verbindung mit dem Zielservice herzustellen. Er chiffriert mit dem Session Key ein drittes Paket, in dem er die aktuelle Uhrzeit schreibt. Das zweite erhaltene Paket, wird an den Zielservice weitergereicht. Der TimeStamp in Paket 3 soll verhindern, dass später jemand die Pakete einfach kopiert. Da es in Rechnernetzen immer schwierig ist, dass alle Uhren synchron laufen, ist eine geringfügige Zeitspanne zwischen der momentan

- Zeit und dem Timestamp im Paket zulässig¹. Zusätzlich merkt sich der Service, welche Timestamps zu ihm gesendet wurden, so dass ein Wiederversenden kaum möglich ist.
4. Nach Erhalt der beiden Pakete hat der Zielsever die Authentizität des Benutzers erkannt. Jetzt kann die eigentliche Kommunikation zwischen den beiden Principals beginnen.

In Kerberosprache bezeichnet man das zweite Paket auch als Ticket, und das dritte Paket als Authenticator.

Folgende Abbildung illustriert noch mal die Kerberos-Anmeldeprozedur:

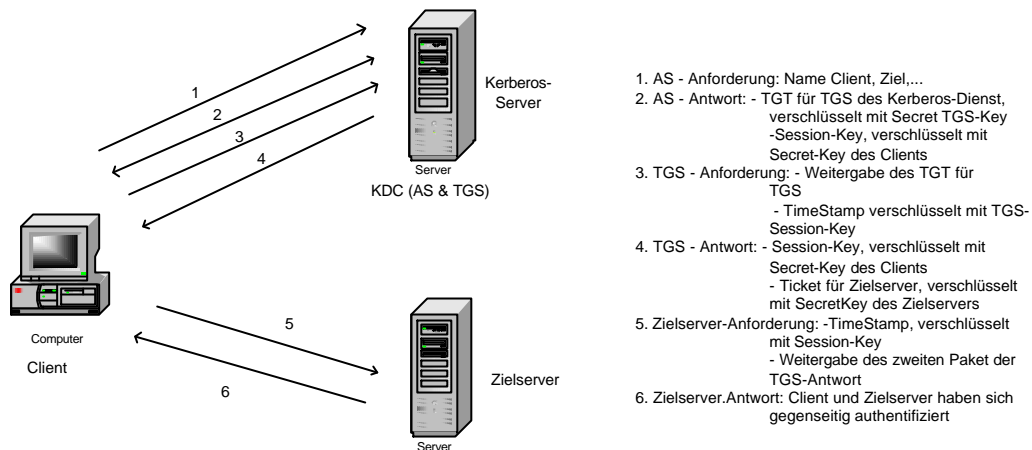


3.2 Erweiterter Authentifizierungsprozess

Leider ist es bis jetzt so, dass der Benutzer sich für jeden Dienst mit dem er kommuniziert, ein eigenes Ticket besorgen muss. Da es aber auf Dauer zu anstrengend ist, für jede Handlung ein Passwort einzugeben, ist in Kerberos noch das Konzept des TicketGrantingServers (TGS) enthalten. Dieser bildet zusammen mit dem AS das Key Distribution Center (KDC). Bevor nun ein Principal den TGS kontaktiert muss er sich vom AS ein Ticket für dessen Nutzen erteilen lassen. Dieses Ticket hat den Namen TicketGranting Ticket (TGT). Nachdem der Benutzer das TGT erhalten hat, wendet er sich zukünftig nicht mehr an den AS, sondern nur noch an den TGS. Die Antwort vom TGS ist nicht mehr mit dem Benutzerpasswort verschlüsselt, sondern mit dem Sitzungsschlüssel, das der AS erteilt hat. Die Antwort enthält dann einen weiteren Sitzungsschlüssel. Dieser wird dann für die tatsächliche Kommunikation mit dem Zielsever benutzt. Der Rest der Kommunikation erfolgt wie oben beschrieben.[6]

Nachfolgend ist noch mal der ganze Authentifizierungsprozess illustriert:

¹ In der Regel sind dies fünf Minuten.



3.3 Bereichsübergreifende Authentifizierung

Wenn nun das Netzwerk eine gewisse Größe erreicht hat, wird man schnell merken, dass ein Kerberosserver nicht ausreicht. Daher kann das Netzwerk in Bereiche aufgeteilt werden[6]. Jeder Bereich hat seinen eigenen AS und TGS. Will man nun auf einen Server in einem anderen Bereich zugreifen, ist es nötig, sich vom lokalen Authentication Server ein Ticket für den Zielbereich zu holen. Damit meldet er sich beim AS im Zielbereich an. Der Remote-AS erkennt², dass das Ticket in einem anderen Bereich ausgestellt wurde und übergibt dem Client ein Ticket und ein Session Key.

4.0 Gefahren und verwendete Kryptographie von Kerberos

Das Ticket nimmt im Kerberos-Protokoll eine zentrale Stellung ein, es ist der Schlüssel zur Nutzung der Netzwerkservices. Daher muss es auch besonders gesichert sein. Das geschieht durch das Benutzerpasswort, das niemand anderer wissen darf. Kerberos setzt voraus, dass dieses Passwort sicher ist. Lässt ein Benutzer das Passwort aus oder nimmt nur ein einfaches, kann ein Angreifer leicht mit einem „Dictionary-Attack“ Erfolg haben. Ein weiterer kritischer Punkt sind die Arbeitsstationen. Sind sie unsicher, sind z.B. Trojaner installiert ist Kerberos unsicher. Dagegen darf die Netzwerkverbindung unsicher sein, da ja Kerberos kryptographische Verschlüsselung benutzt. Im Moment sind dies aus Performance-Gründen symmetrische Verfahren wie DES. Aber da gerade asymmetrische Verfahren wie RSA für Authentifizierung gut geeignet sind, ist deren Implementierung gerade in Arbeit.[6]

² Um die Authentizität des Tickets anzuerkennen, ist es nötig, dass sich die verschiedenen AS einen gemeinsamen Schlüssel, den so genannten Cross-Realm Key teilen.

Literatur

- [1] Computer Networks, Andrew S. Tanenbaum, Prentice Hall, 1996
- [2] Microsoft Windows 2000 Server, Microsoft Press, 2000
- [3] <http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>
- [4] <http://www.ietf.org/rfc/rfc1510.txt>
- [5] <http://web.mit.edu/kerberos/www/>
- [6] Kerberos: An Authentication Service for Computer Network, B. Clifford Neumann and Theodore Ts'o , September 1994
<http://www.isi.edu/~brian/security/kerberos.html>
- [7] The Moron's Guide to Kerberos, Version 1.2.2
<http://www.isi.edu/~brian/security/kerberos.html>