Kerberos

Proseminar Grundlagen kryptographischer Protokolle

09. Juni 2009

Korbinian Riepl

Gliederung

- Was ist Kerberos?
- Ziele von Kerberos
- Entstehung
- Kerberos 4
- Probleme in Kerberos 4 und deren Lösung in Kerberos 5
- Schwachstellen von Kerberos
- Vorteile von Kerberos

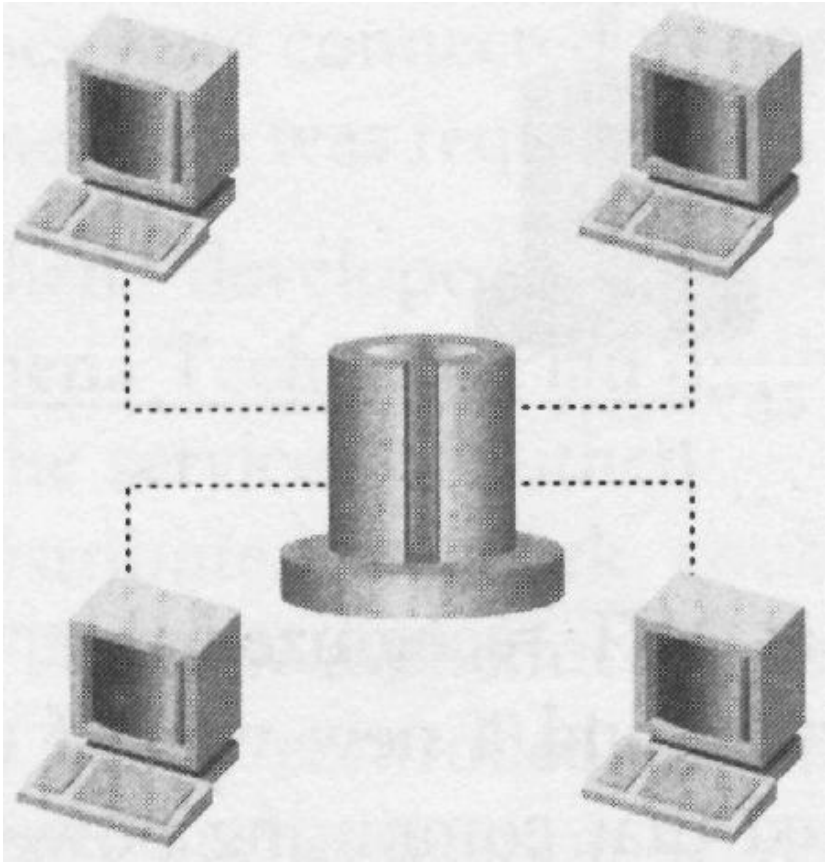
Was ist Kerberos?

- Lat. „Cerberus“: In griechischer Mythologie mehrköpfiger Hund, der Eingang zur Unterwelt bewacht
- Kerberos ist ein
  - **sicherer** und
  - **beiderseitiger** Authentifizierungsprotokoll und -service, bei dem nur
  - **eine Anmeldung** benötigt wird und der über einen
  - **vertrauenswürdigen Dritten** abgewickelt wird.
- Achtung: nur Authentifizierung, keine Autorisierung!

Ziele von Kerberos

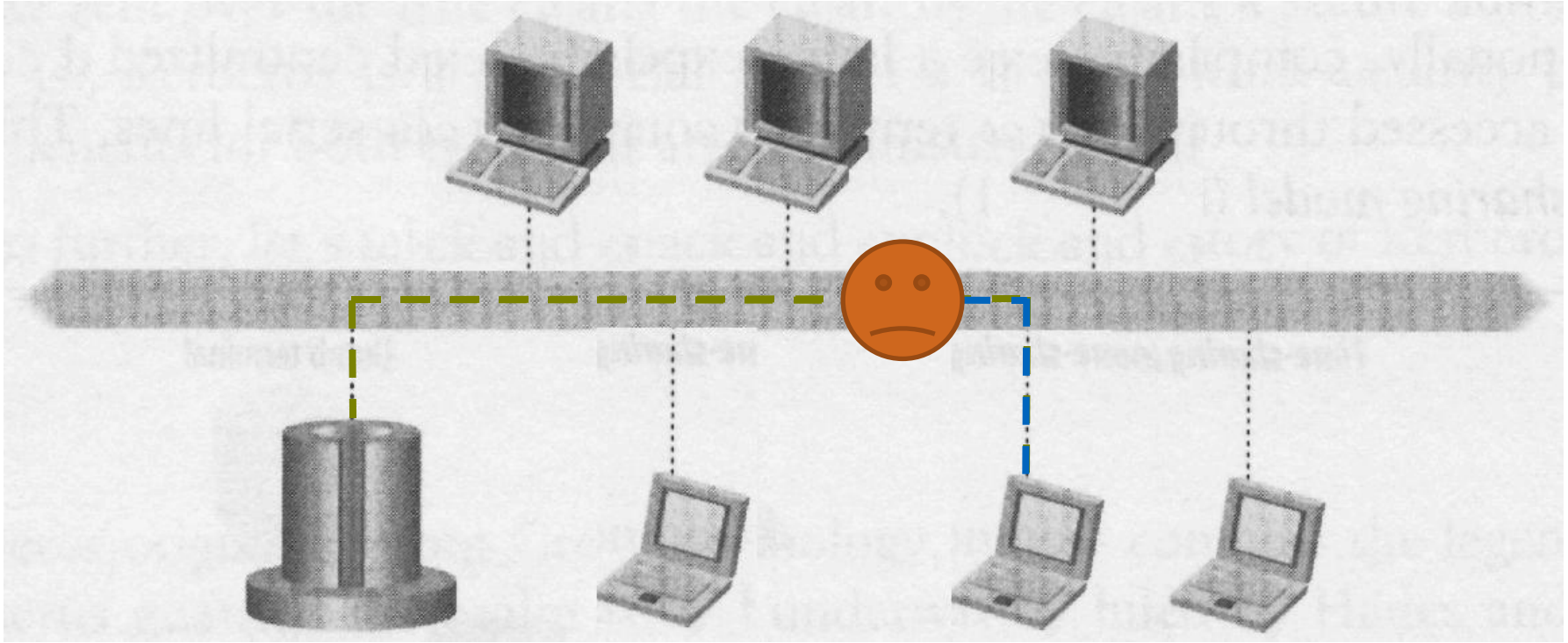
- Sicherheit und Schutz vor Angriffen
  - Authentifizierung und Austausch von Sitzungsschlüsseln
  - Schutz vor z.B. Man-in-the-Middle-Attacks
- Single-Sign-On: Nur eine Anmeldung nötig

Entstehung: Früher



Quelle: [Q2], Seite 3

Entstehung: Später

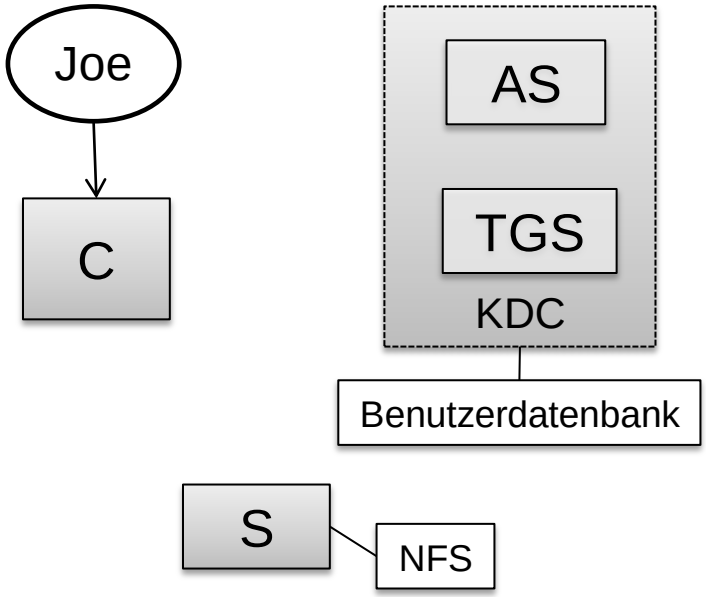


Quelle: [Q2], Seite 4

➔ Gründung des ATHENA-Projektes 1983 am MIT

Kerberos 4: Beteiligte

- Client C mit Benutzer Joe
- Server S mit Dienst, z.B. NFS
- Ticket Granting Server (TGS): Ausstellung von Tickets
- Authentification Server (AS): Ausstellung des Ticket Granting Tickets (TGT)
- AS und TGS bilden das Key Distribution Center (KDC), welches über eine Benutzerdatenbank verfügt, in der u.a. alle Benutzerschlüssel ($K_{Benutzer}$) gespeichert sind.



C: Client
AS: Authentification Server
TGS: Ticket Granting Server
KDC: Key Distribution Center
S: Server, z.B. NFS

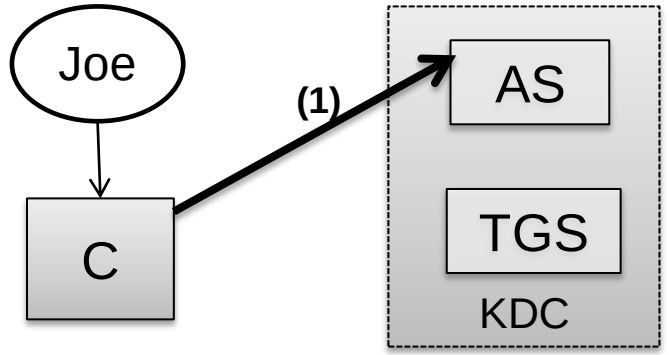
Kerberos 4: Schritt (1)

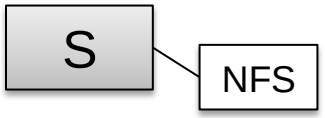
Client → AS: AS_REQ

$$\text{Joe, TGS, Nonce}_1$$

Identität des Clients

Identität des TGS, der für die Ausstellung der Tickets zuständig ist





<u>Authentifizierungsserver:</u>

- Verifikation der Existenz des Clients
- Generierung des Sitzungsschlüssels $K_{Joe,TGS}$

C: Client
AS: Authentification Server
TGS: Ticket Granting Server
KDC: Key Distribution Center
S: Server, z.B. NFS

Kerberos 4: Schritt (2)

AS → Client: AS_REP

$$\{K_{Joe,TGS}, Nonce_1\}^{K_{Joe}}, \{T_{Joe,TGS}\}^{K_{TGS}}$$

Sitzungsschlüssel für die Kommunikation des Clients mit dem TGS

Erkennung von Replays

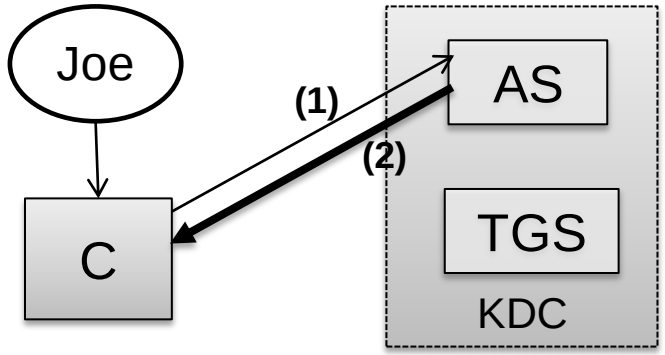
TGT
(Ticket Granting Ticket)

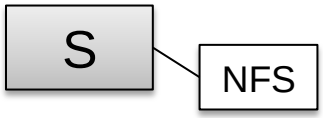
$$\{TGS, Joe, IP\text{-}Adresse_{Joe}, Zeitstempel, Laufzeit, K_{Joe,TGS}\}^{K_{TGS}}$$

Identität des TGS

Identität des Clients

Gültigkeitsdauer des TGT





C: Client
AS: Authentification Server
TGS: Ticket Granting Server
KDC: Key Distribution Center
S: Server, z.B. NFS

Kerberos 4: Schritt (3)

Client → TGS: TGS_REQ

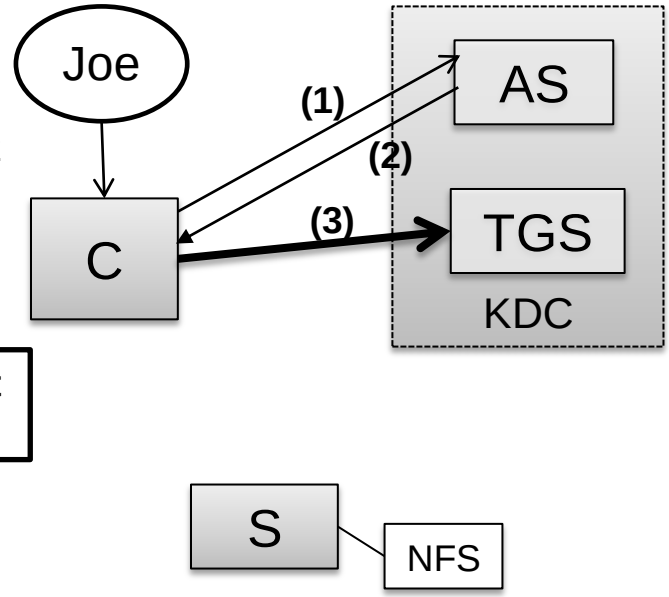
$\{A_{Joe}\}^{K_{Joe,TGS}}, \{T_{Joe,TGS}\}^{K_{TGS}}, NFS, Nonce_2$

Authentikator

TGT

Dienst, der genutzt werden soll

$\{Joe, IP\text{-}Adresse_{Joe}, Zeitstempel\}^{K_{Joe,TGS}}$



Ticket Granting Server:

- Verifizierung des Authentikators
- Generierung des Sitzungsschlüssels $K_{Joe,NFS}$

C: Client
AS: Authentification Server
TGS: Ticket Granting Server
KDC: Key Distribution Center
S: Server, z.B. NFS

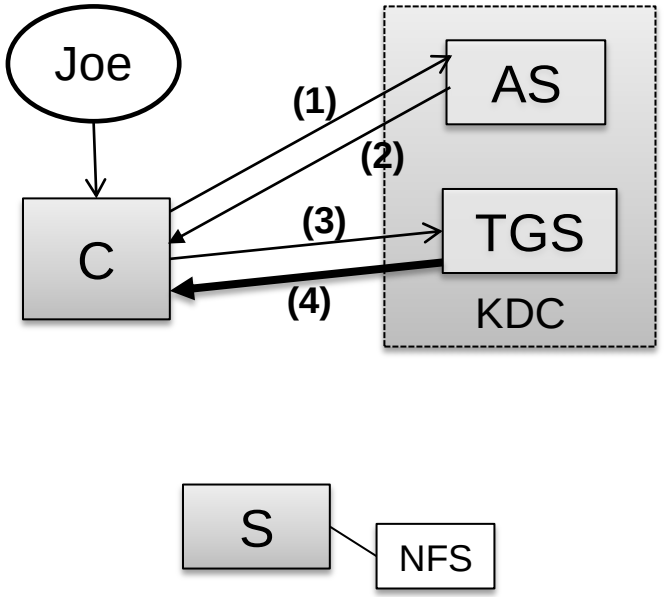
Kerberos 4: Schritt (4)

TGS → Client: TGS_REP

$$\{K_{Joe,NFS}, Nonce_2\}^{K_{Joe,TGS}}, \{T_{Joe,NFS}\}^{K_{NFS}}$$

Sitzungsschlüssel

Ticket für den Server, enthält u.a. Sitzungsschlüssel



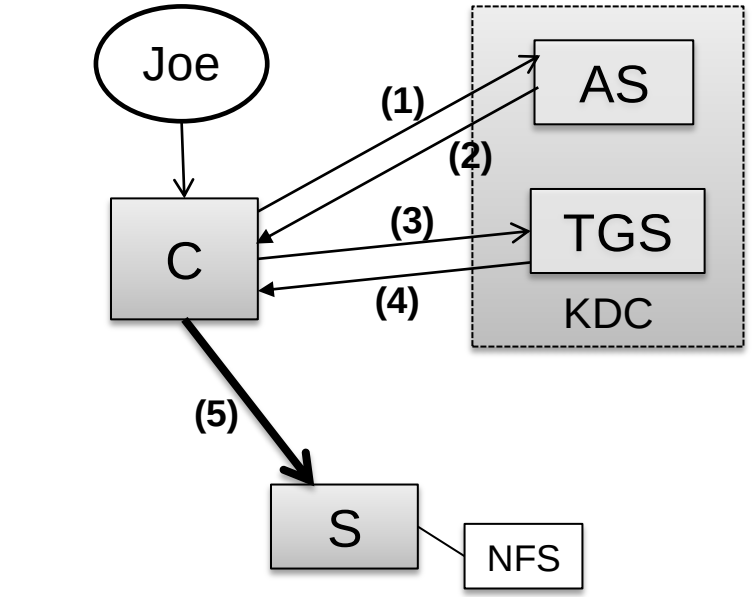
C: Client
AS: Authentification Server
TGS: Ticket Granting Server
KDC: Key Distribution Center
S: Server, z.B. NFS

Kerberos 4: Schritt (5)

Client → NFS: NFS_REQ

$$\{A_{Joe}\}^{K_{Joe,NFS}}, \{T_{Joe,NFS}\}^{K_{NFS}}$$

Authentikator



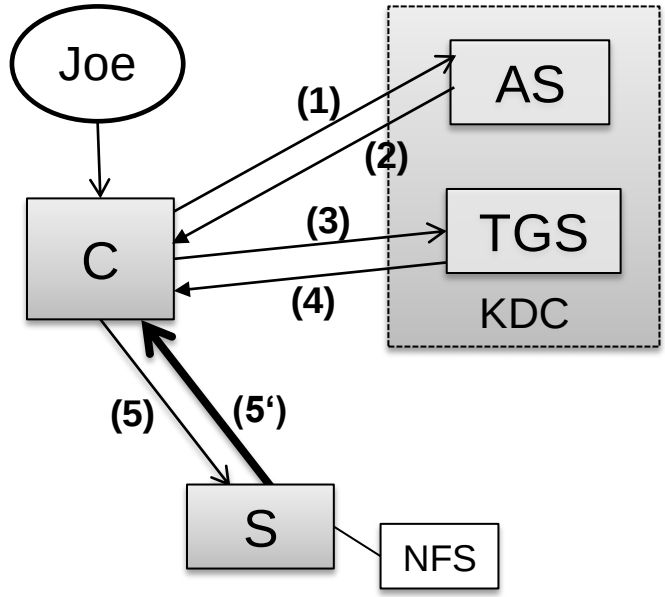
C: Client
AS: Authentification Server
TGS: Ticket Granting Server
KDC: Key Distribution Center
S: Server, z.B. NFS

Kerberos 4: optionaler Schritt (5‘)

NFS → Client: NFS_REP

$$\{A_{Joe}{}^{*}\}^{K_{Joe,NFS}}$$

Authentikator mit um 1 erhöhten Zeitstempel



C: Client
AS: Authentification Server
TGS: Ticket Granting Server
KDC: Key Distribution Center
S: Server, z.B. NFS

Probleme in Kerberos 4 und Lösung in Kerberos 5

- Offline-Attacke auf TGT nach Schritt (1) möglich
  - ✓ Client muss im Schritt (1) gehaschtes Passwort korrekt übermitteln, um TGT zu bekommen.
- Kein Forwarding möglich: Für Tickets, die nicht im Zuständigkeitsbereich des eigenen TGS liegen, muss das Passwort im Klartext übertragen werden.
  - ✓ Es gibt eine Hierarchie von KDCs, die untereinander das Forwarding ermöglichen.
- DES als Verschlüsselungsmethode vorgeschrieben
  - ✓ Es können verschiedene (sicherere) Verschlüsselungsmethoden zwischen Server und Clients verwendet werden.
- Keine Möglichkeit, im Auftrag Dritter tätig zu sein
  - ✓ Unterstützung des Delegationsprinzips

Schwachstellen von Kerberos

- Standardmäßig: Ablegung der Tickets im /tmp-Verzeichnis
- Passwörter als Basis
- KDC verschlüsselt alle Benutzerpasswörter mit gleichem Serverpasswort
- Problem der Synchronisierung der Zeit
- Sitzungsschlüssel können während der Laufzeit für jede Verbindung mit dem Server verwendet werden
- In Kerberos 5: Maximale Laufzeit der Tickets bis zum Jahr 9999

Vorteile von Kerberos

Trotzdem: hoher Sicherheitsgewinn durch:

- Authentifizierter Zugriff
- Keine Übertragung des Passworts im Klartext
- Single Sign-On ➔ Benutzer wählen sichereres Passwort

Literatur

[Q1] „IT-Sicherheit“ von Claudia Eckert, Oldenburg-Verlag, Seiten 498 bis 508

[Q2] „Kerberos – The Definitive Guide“ von Jason Garman, Verlag O‘Reilly, Seiten 1 bis 36

[Q3] http://de.wikipedia.org/wiki/Kerberos_(Informatik), aufgerufen am 14.04.2009