Konzepte von Betriebssystemkomponenten
Schwerpunkt Authentifizierung

Das Kerberos-Protokoll

Referent: Guido Söldner

Überblick über Kerberos

- Network Authentication Protocol
- Am MIT Mitte der 80er Jahre entwickelt (Projekt Athena)
- Sowohl als Open Source als auch in kommerzieller Software verfügbar

Motivation

- Gefahren nicht nur außerhalb des Netzwerkes, sondern auch innerhalb
- Ressourcen müssen vor unberechtigten Zugriff geschützt werden

Kerberos

- Vertrauenswürdiger 3rd party Authentifizierungsdienst
- Annahme, dass Netzwerkverbindung unsicher ist
- Jeder Client muss seine Identität beweisen
- Wiederholtes Eingeben des Passwortes für verschiedene Services nicht nötig

Kerberos Design

- User muss beim Einloggen einmalig seine Authentizität beweisen
- Passwörter werden nicht als Klartext, sondern als Chiffretext über das Netzwerk versendet
- Verschlüsselt wird mit DES, in Kerberos V5 gibt es auch andere Verschlüsselungsmöglichkeiten
- Jeder Benutzer und Service hat ein eigenes Passwort
- Die einzige Instanz die alle Passwörter kennt, ist Authentication Server (AS)

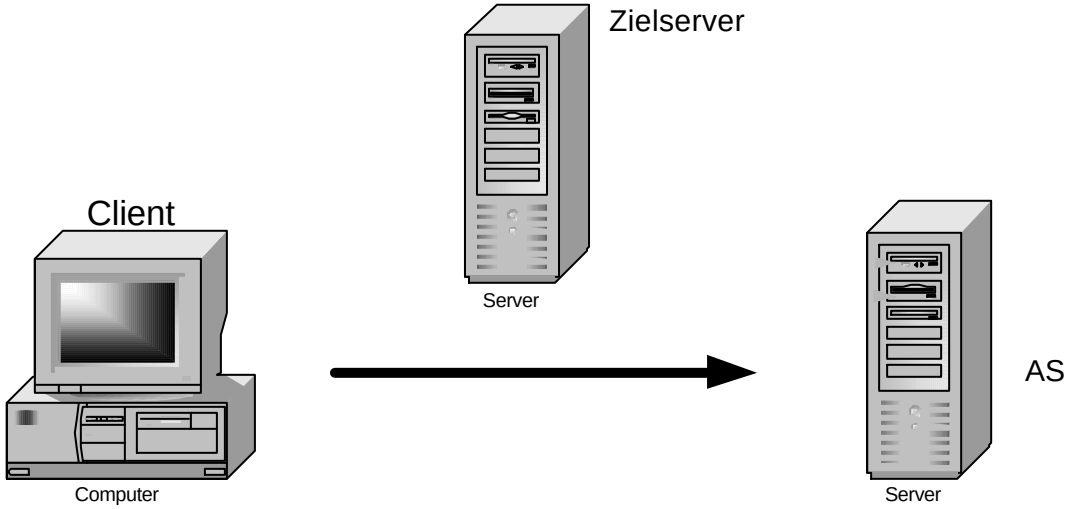
Grundbegriffe

- Principal: Eindeutig benannter Benutzer, Client oder Server, der an einer Netzwerkkommunikation teilnimmt
- Session Key: Temporärer Codierungsschlüssel, der zwischen zwei Principals benutzt wird. Er ist nur diesen bekannt und wird immer verschlüsselt versendet.
- Secret Key: Codierungsschlüssel zwischen dem Kerberosdienst und einem Principal
- Authentication Server (AS): erteilt Ticket Granting Ticket, mit dem sich der Client am Ticket Granting Service anmelden kann

Grundbegriffe (2)

- TicketGrantingService (TGS) : Stellt einem Client Tickets aus, die Kommunikation mit dem Zielserver ermöglichen
- Key Distribution Center (KDC): umfasst TGS und AS

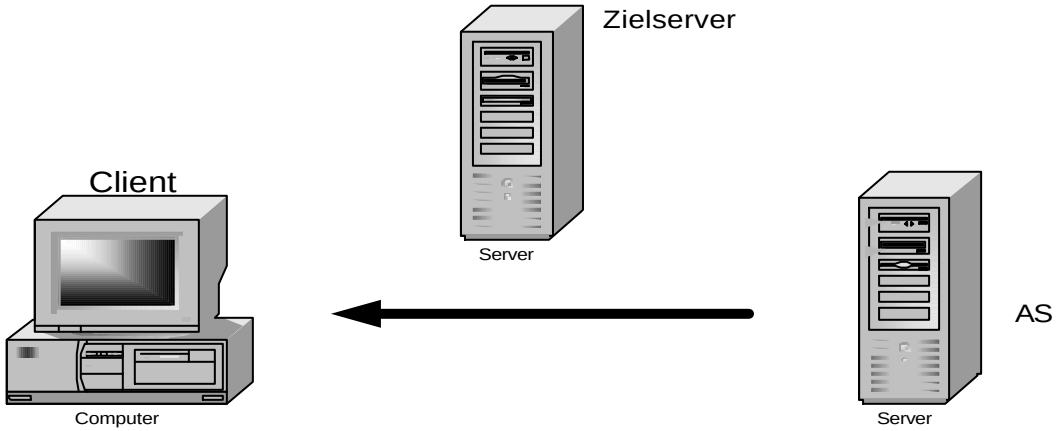
Funktionsweise von Kerberos (1)



Client-Anforderung:

- Loginname
- Name des gewünschten Service

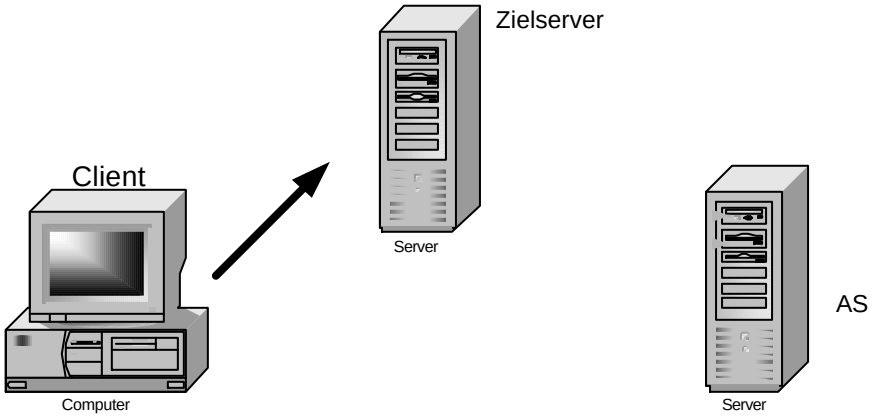
Funktionsweise von Kerberos(2)



AS-Antwort

- Paket 1: Session Key und Name des zu kontaktierenden Servers, verschlüsselt mit Secret Key des Benutzers
- Paket 2: Session Key und Name des Benutzers, verschlüsselt mit Secret Key des Servers

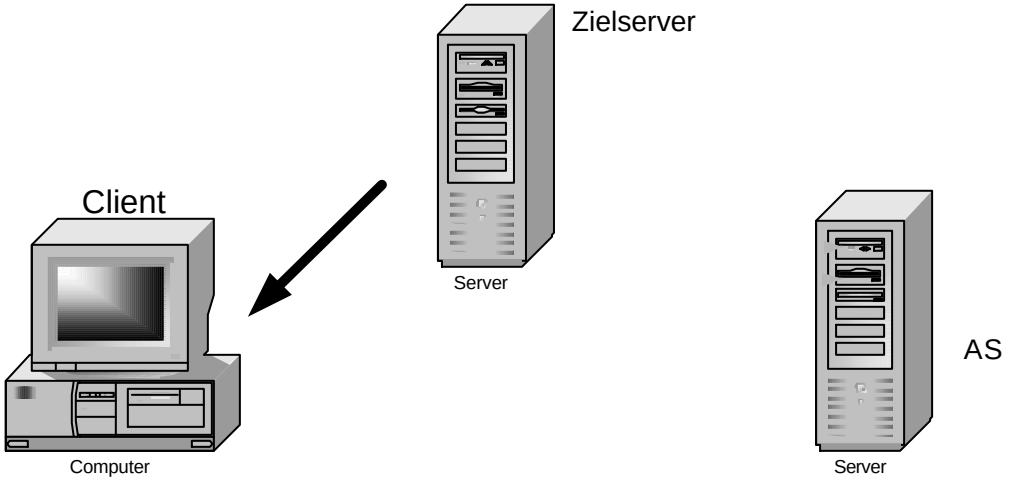
Funktionsweise von Kerberos (3)



Client-Anforderung:

- Paket 2: wird ungeöffnet weitergegeben
- Paket 3: enthält TimeStamp, verschlüsselt mit Session Key

Funktionsweise von Kerberos (4)



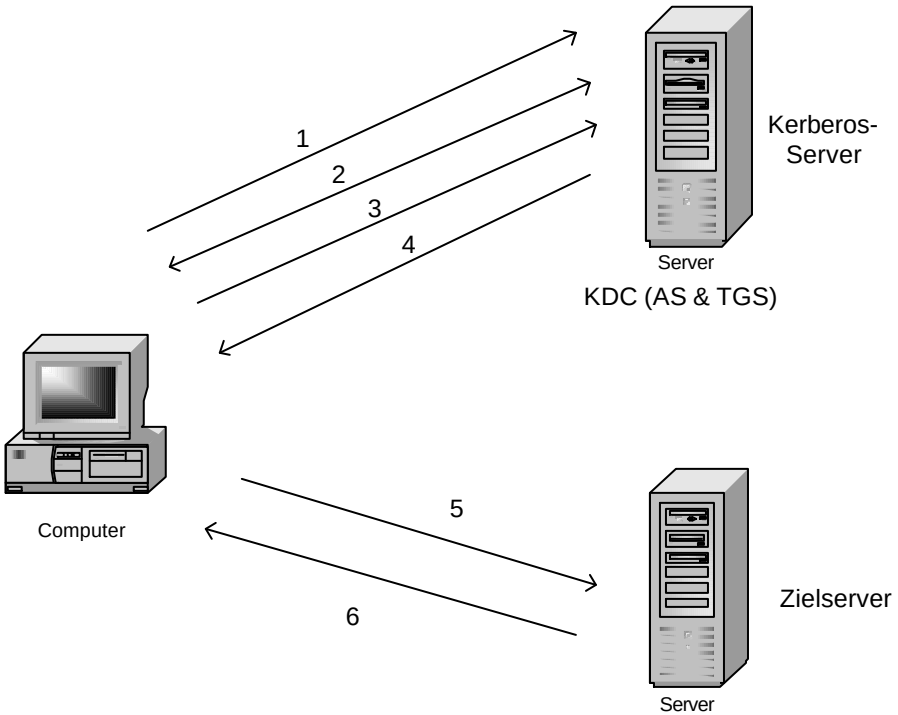
Zielserver-Antwort

- Client und Zielserver sind gegenseitig authentifiziert

Funktionsweise von Kerberos (5)

- Problem: für jeden Dienst eigenes Ticket
- Wiederholtes Eingeben des Passwortes lästig
- Passwort im Speicher zu halten ist gefährlich
- Ticket Granting Service zwischen Zielserver und AS, ermöglicht einmaliges Eingeben des Passwortes

Funktionsweise von Kerberos (6)



1. AS - Anforderung: Name Client, Ziel,...
2. AS - Antwort: - TGT für TGS des Kerberos-Dienst, verschlüsselt mit Secret TGS-Key
   -Session-Key, verschlüsselt mit Secret-Key des Clients
3. TGS - Anforderung: - Weitergabe des TGT für TGS
   - TimeStamp verschlüsselt mit TGS-Session-Key
4. TGS - Antwort: - Session-Key, verschlüsselt mit Secret-Key des Clients
   - Ticket für Zielserver, verschlüsselt mit SecretKey des Zielservers
5. Zielserver-Anforderung: -TimeStamp, verschlüsselt mit Session-Key
   - Weitergabe des zweiten Paket der TGS-Antwort
6. Zielserver.Antwort: Client und Zielserver haben sich gegenseitig authentifiziert

Bereichsübergreifende Authentifizierung

- Ab gewisser Größe oder Topologie des Netzwerkes: Aufteilung in mehrere Bereiche
- AS teilen sich einen gemeinsamen Schlüssel, mit dem sie über die Bereichsgrenzen hinweg kommunizieren

Schwachstellen und Lösungen

Ein gestohlenes TGT ermöglicht Zugriff auf Netzwerkservices.	Nur ein Problem bis Ticket in ein paar Stunden ausläuft
Dictionary Attack	TimeStamp erfordert es, Ticket in 5 min zu hacken
Schlecht, wenn AS kompromittiert	Physikalischer Schutz für den Server

Grenzen von Kerberos 4

- Papier von Bellovin und Merritt
- Einige dieser Grenzen beziehen sich auch auf Kerboros 5:
  - Authentikatoren verlassen sich auf synchronisierte und nicht kompromittierte Uhren. An einem kompromittierten Rechner kann die Uhrzeit geändert werden und damit kann leicht ein Replay durchgeführt werden
  - Password Guessing Angriffe können funktionieren. Angreifer könnten Tickets sammeln und sie ausprobieren ...
  - Verlass auf vertrauenswürdige Clients and Servers
  - Verlass auf die Vertrauenswürdigkeit des TGS und des Kerberos Servers

Verbesserungen in Kerberos 5

- Kein festes Kryptographieverfahren mehr (vorher nur DES)
  - Schlüssellänge kann variieren
- Key Salt Algorithmus benutzt den vollen Principalnamen
- Keine Protokollabhängigkeit mehr (vorher nur IP)
  - Adresse verknüpft mit Typ und Länge
- Ticket Lebenszeit
  - war 8 Bits (21 Stunden max)
  - Benutzt jetzt Start/End Zeiten
- Fowardable tickets

Grenzen beider Versionen

- Kein Schutz vor Systemsoftwaremodifikationen
- Alles muss kerberorisiert werden
- Kerberos Server muss funktionieren (single point of failure)
- Alle Passwörter sind mit den gleichen Schlüssel chiffriert, dem Kerberos Master Key

Literatur

- Kerberos official page (Definitionen, Sourches, Binaries) http://web.mit.edu/kerberos/www/index.html
- Kerberos: An Authentication Service for Computer Network , C. Neuman, T. Ts’o http://www.isi.edu/~brian/security/kerberos.html
- Applied Cryptography, Bruce Schneier
- Microsoft Windows 2000 Server, Microsoft Press