Kerberos

Folien unter

http://www.tu-berlin.de/zrz/mitarbeiter/stsc4000/tubIT_Kerberos_Infrastruktur.pdf

Authentication of Unknown Entities on an Insecure Network of Untrusted Workstations

B. Clifford Neumann, Jennifer G. Steiner

Authentisierung unbekannter Einheiten in einem unsicheren Netzwerk von nicht vertrauenswürdigen Rechnern

Agenda

- Motivation
- Was ist Kerberos
- Definition der Komponenten
- tubIT Kerberos Infrastruktur
- Praktisches Beispiel

Anforderungen

Um die Sicherheit der Authentisierung gegenüber den bisherigen Verfahren zu erhöhen, wird gefordert:

1. keine Übertragung von Passwörtern über das Netz
2. wechselseitige Authentisierung zwischen Klienten und Serviceprovidern (Diensten bzw. Servern)
3. „fälschungssicherer“ Identitätsnachweis
4. Verschlüsselung der Verbindung zwischen Client und Service muss möglich sein

Weitere Anforderungen

- Single Password
  - an allen angeschlossenen Systemen kann das gleiche Passwort verwendet werden
- Single Sign On
  - nur zu Beginn einer Sitzung authentisieren
- Zentrale „**Self-Care**“ Schnittstelle für Nutzer
  u.a. zum ändern des Passwortes
- **Administrative Schnittstelle**, z.B. zum Sperren von Usern oder zum Rücksetzen von Passwörtern

Kerberos als Authentisierungsservice

- tubIT baut eine **Authentisierungs- und Autorisierungsinfrastruktur (AAI)** auf
- Kerberos ist wichtiger Bestandteil dieser Infrastruktur
- „Bereiche“ der TU können diese AAI nutzen!

Was ist Kerberos?

- am MIT im Rahmen des Athena-Projekts von Steve Miller und Clifford Neuman entwickelt
- basiert auf dem Needham-Schroeder-Protokoll zur Authentifizierung
- aktuelle Version 5, definiert im RFC 4120 (2005)
- US Exportbeschränkungen führten zur Entwicklung einer weiteren Implementation: *Heimdal*
- tubIT setzt auf seinen Servern die **MIT-Kerberos** Pakete der Debian Distribution Etch ein
- Aktuelle Version: ***1.4.4-7etch1***

Realm

- administrativer Bereich zur Verwaltung von Identitäten, z.B. Benutzerkennungen
- der Name des Realm ist Case Sensitive,
  wird per Übereinkunft in Großbuchstaben notiert
- jeder Realm hat einen eindeutigen Namen,
  meist angelehnt an DNS-Domainnamen
  Realm der TU: **TU-BERLIN.DE**
- über Vertrauensstellungen können Dienste eines anderen Realms genutzt werden:

  TU-BERLIN.DE <-> WIN.TU-BERLIN.DE

Principal

- bezeichnet eine zu authentisierende Entität eines Realm
- muss innerhalb des Realms eindeutig sein
- setzt sich zusammen aus:
  component[/component]...@<REALM>
- wird zusammen mit den Keys bei der Freischaltung eines tubIT-Accounts in der Realm-Datenbank angelegt

Principal

- für Personen: *name[/instance]@<REALM>*
  - *stsc4000@TU-BERLIN.DE*
  - *stsc4000/admin@TU-BERLIN.DE*
  - Wobei *name* von der tubIT Benutzerverwaltung erzeugt wird
- für Hosts: *host/<hostname>@<REALM>*
  - *host/mailbox.tu-berlin.de@TU-BERLIN.DE*
- für Services: *<servicename>/<hostname>@<REALM>*
  - *imap/mailbox.tu-berlin.de@TU-BERLIN.DE*

Ticket

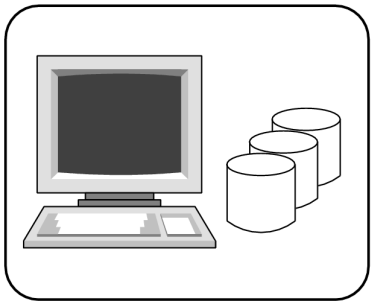
- wird vom Client beim KDC für einen bestimmten Dienst angefordert
- fälschungssicherer befristeter Nachweis der Identität eines Principals
- gegenseitige Authentisierung von Benutzer und Dienst (Mutual Authentication)
- enthält u.a. SessionKey, UserPrincipal und Lebensdauer
- wird in einem lokalen Ticketcache befristet gespeichert
- wird vor der Authentisierung um Zeitstempel (Authenticator) ergänzt

Key Distribution Center (KDC)

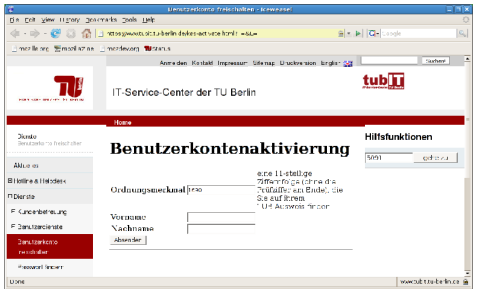
- Zentrale Komponente des Realm

  Server: **kerberos-1.tu-berlin.de**
- Besteht aus:
  - Principal-Datenbank
    - enthält **Principals** des Realm mit deren **Keys** und den entsprechenden Attributen
  - Authentication Server (AS)
    - erstellt das Ticket Granting Ticket (TGT)
  - Ticketgranting Server (TGS)
    - erstellt Service Tickets

Erzeugen eines Userprincipals:



Benutzerverwaltung



Self–Care–Interface

Principal wird erzeugt:
username@TU–BERLIN.DE

Windows Domäne

LDAP

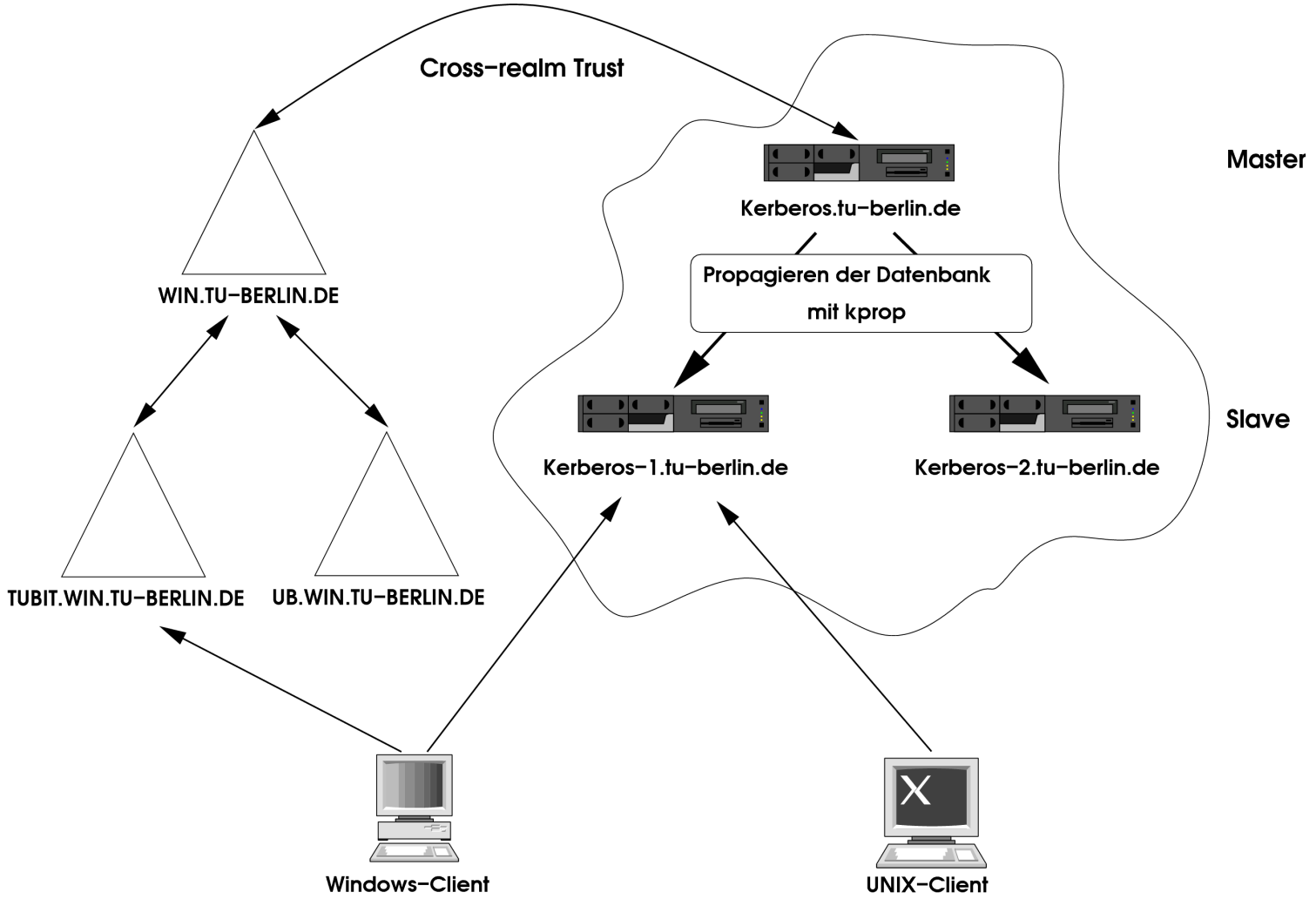
KDC

kerberos.tu–berlin.de

Auszug aus der Principal-Datenbank

Principal: stsc4000@TU-BERLIN.DE
Expiration date: [never]
Last password change: Thu Mar 22 21:45:34 GMT 2007
Password expiration date: [none]
Maximum ticket life: 0 days 10:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Thu Mar 22 21:45:34 GMT 2007 (root/admin@TU-BERLIN.DE)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 6
Key: vno 1, Triple DES cbc mode with HMAC/sha1, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Key: vno 1, DES cbc mode with RSA-MD5, Version 4
Key: vno 1, DES cbc mode with RSA-MD5, Version 5 - No Realm
Key: vno 1, DES cbc mode with RSA-MD5, Version 5 - Realm Only
Key: vno 1, DES cbc mode with RSA-MD5, AFS version 3
Attributes: REQUIRES_PRE_AUTH
Policy: [none]

Realm Infrastruktur



Was zu beachten ist

- **Pre-Authentication** wird zwingend gefordert und muss von den Clients unterstützt werden!
- **Änderung des Passwortes nur noch über das zentrale Web-Interface, d.h. lokale Möglichkeiten unterbinden**
- Service-Keys müssen auf sicherem Weg auf die Server gebracht werden
- Uhrzeit der teilnehmenden Rechner muss synchron sein
- Nicht ohne weiteres über Firewalls mit NAT einsetzbar (Lösung: Ticket ohne Client-Adresse beantragen!)
- Ausschließlich **Kerberos V** verwenden

Konfiguration eines Client am Beispiel von Debian Linux

- Installation der entsprechenden Kerberos-Pakete:

  apt-get install krb5-user

  apt-get install libpam-krb5

- lokale Benutzer anlegen
  adduser --disabel-password username
- oder LDAP-Sever nutzen
  apt-get install libnss_ldap

/etc/krb5.conf:

```
[libdefaults]
        default_realm = TU-BERLIN.DE
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true

[realms]
        TU-BERLIN.DE = {
                kdc = kerberos-1.tu-berlin.de
                kdc = kerberos-2.tu-berlin.de
                dns_lookup_kdc = false
                dns_lookup_realm = false
        }

 [domain_realm]
                tu-berlin.de = TU-BERLIN.DE
                .tu-berlin.de = TU-BERLIN.DE
```

PAM

- /etc/pam.d/common-auth

```
auth  sufficient  pam_krb5.so minimum_uid=1000
auth  required    pam_unix.so try_first_pass nullok_secure
```

- /etc/pam.d/common-account

```
account  required  pam_krb5.so minimum_uid=1000
account  required  pam_unix.so
```

- /etc/pam.d/common-session

```
session  optional  pam_krb5.so minimum_uid=1000
session  required  pam_unix.so
```

Fragen?

Ansprechpartner:

- Gerd Schering, schering@tubit.tu-berlin.de
  Tel.: 24383, Raum: E-N 007
  Struktur und Konzeption

- Klaus Lemkau, Klaus.Lemkau@TU-Berlin.DE
  Tel.: 24229, Raum E-N K
  Betrieb

- Stefan Schnieber, Stefan.Schnieber@TU-Berlin.DE
  Tel.: 24383, Raum: E-N 007
  Kerberos