3 Kerberos aus Anwendersicht
3.1 Die Beispielumgebung
3.2 Lokale Anmeldung
3.3 Der Credential Cache
3.4 Anmeldung an Netzwerkdiensten
3.5 Delegation
3.6 Eine Demo-Webseite
3.7 Umgang mit dem Credential Cache
3.8 Zusammenfassung

4 Sicherheit und Kryptografie
4.1 Sicherheitsüberlegungen
4.1.1 Allgemeine Sicherheitsanforderungen
4.1.2 Die beteiligten Systemkomponenten
4.1.3 Anforderungen an Kerberos
4.2 Kryptografie in der Netzwerksicherheit
4.2.1 Vertraulichkeit
4.2.2 Integrität
4.2.3 Authentisierung
4.2.4 Passwörter, Schlüssel und Schlüsselaustausch
4.2.5 Zusammenfassung

5 Wie funktioniert Kerberos V5?
5.1 Das Funktionsprinzip im Überblick
5.1.1 Voraussetzungen
5.1.2 Das einstufige Kerberos-Verfahren
5.1.3 Diskussion
5.1.4 Das zweistufige Kerberos-Verfahren
5.1.5 Zusammenfassung
5.2 Das Funktionsprinzip im Detail
5.2.1 Die KDC-Datenbank
5.2.2 Der Authentication Service (AS)
5.2.3 Zugriff auf kerberisierte Dienste
5.2.4 Der Ticket-Granting Service (TGS)
5.3 Zusammenfassung

6 Kerberos für Fortgeschrittene
6.1 KDC-Optionen
6.1.1 Optionen für Ticket Renewing
6.1.2 Optionen für Ticket Postdating

6.1.3 Optionen für die Kerberos-Delegation
6.1.4 Sonstige Optionen
6.2 Ticket Flags
6.2.1 Flags für Ticket Renewing
6.2.2 Flags für Ticket Postdating
6.2.3 Flags für die Kerberos-Delegation
6.2.4 Sonstige Flags
6.3 AP-Optionen
6.4 Tickets automatisiert erneuern
6.5 Tickets für die Zukunft
6.6 Delegation zum Ersten
6.6.1 Ticket Forwarding
6.6.2 Ticket Proxying
6.7 Authentisierung zwischen Realms
6.7.1 Grundsätzliches zu Vertrauensstellung
6.7.2 Zwei Realms
6.7.3 Mehr als zwei Realms
6.8 Namenskanonisierung und Referrals
6.8.1 Kanonisierung der Client-Principal-Namen
6.8.2 Kanonisierung der Dienste-Principal-Namen
6.8.3 Verweise an entfernte Realms
6.9 User-to-User-Authentisierung
6.10 Kerberos und Autorisierungsdaten
6.11 Die S4U2Self-Erweiterung
6.12 Delegation zum Zweiten
6.12.1 Constrained Delegation
6.12.2 Protocol Transition
6.12.3 Diskussion
6.13 Initiale Authentisierung mit Zertifikaten
6.13.1 Eine Lösung für die Passwort-Problematik
6.13.2 Das Funktionsprinzip von PKINIT
6.13.3 Anonymes PKINIT
6.13.4 PKINIT Freshness Extension
6.13.5 Fazit
6.14 FAST: zusätzlicher Schutz für KDC-Austausch
6.15 Kerberos über HTTPS
6.16 Initiale Authentisierung mit zweitem Faktor

II Zentrale Infrastrukturen

7 Grundlegende Infrastruktur
7.1 Überblick
7.2 Software, Systemdienste und lokale Firewall
7.3 DNS-Namensauflösung mit BIND
7.3.1 BIND installieren
7.3.2 Zonen einrichten
7.3.3 Starten und Testen
7.3.4 Subdomänen
7.4 Zeitsynchronisation mit NTP
7.5 Certificate Authority (CA) mit OpenSSL
7.5.1 Einrichtung der CA
7.5.2 Einen Zertifikatsrequest erzeugen
7.5.3 Das Zertifikat unterschreiben
7.6 Verzeichnisdienst mit OpenLDAP
7.6.1 Installation und Grundkonfiguration
7.6.2 Schemadefinition
7.6.3 Datenbank für dc=example,dc=com konfigurieren
7.6.4 Datenbank für dc=example,dc=com befüllen
7.6.5 Ein erster Test
7.6.6 Sicherheit

8 Das Key Distribution Center von MIT Kerberos
8.1 Übersicht
8.2 Softwareinstallation
8.3 Konfiguration
8.3.1 Der Master Key der KDC-Datenbank
8.3.2 Zeitangaben bei MIT Kerberos
8.3.3 Verschlüsselungstypen
8.3.4 Die Datei kdc.conf
8.4 Initialisierung der KDC-Datenbank
8.4.1 Die Datenbank mit kdb5_util initialisieren
8.4.2 Die initiale Datenbank
8.4.3 Mit kadmin.local weitere Principals anlegen
8.4.4 Master Key in Stash-Datei ablegen
8.5 Ein erster Test

9 Die Administration von MIT Kerberos
9.1 Der Kadmin-Dienst
9.2 Administrative Zugriffe kontrollieren
9.3 Der Kpasswd-Dienst

9.4 Starten der administrativen Dienste
9.5 Principals verwalten
9.5.1 Passwortrichtlinien
9.5.2 Lockout Policies
9.5.3 Principal-Eigenschaften
9.5.4 Principals für Anwender:innen anlegen
9.5.5 Principals für Dienste anlegen
9.5.6 Verschlüsselungstypen der Principals verwalten
9.6 Keytabs verwalten
9.6.1 Keytabs mit kadmin verwalten
9.6.2 Keytabs mit ktutil verwalten
9.7 Service Keys ändern

10 Die Clientkommandos von MIT Kerberos
10.1 Installation und Konfiguration
10.2 Die Kommandos kinit und klist
10.2.1 Tickets holen
10.2.2 Den Credential Cache auswählen
10.2.3 Ticket-Eigenschaften anzeigen und beeinflussen
10.2.4 Protokollrequests beeinflussen
10.2.5 Sonstige Kommandozeilenoptionen
10.2.6 Service Tickets holen
10.2.7 Mit Keytabs arbeiten
10.3 Das Kommando kvno
10.4 Das Kommando kpasswd
10.5 Das Kommando kdestroy
10.6 Die Kommandos k5start und krenew
10.6.1 krenew
10.6.2 k5start

11 Die Konfiguration der MIT Libraries
11.1 Die Datei krb5.conf
11.1.1 Die Struktur der krb5.conf
11.1.2 Konfigurationsabschnitte
11.1.3 Parameter im Abschnitt [libdefaults]
11.1.4 Parameter im Abschnitt [realms]
11.1.5 Parameter im Abschnitt [domain_realm]
11.1.6 Parameter im Abschnitt [appdefaults]
11.1.7 Die krb5.conf für den Realm EXAMPLE.COM
11.2 Konfiguration über DNS

11.2.1 SRV Records
11.2.2 TXT Records
11.3 Konfiguration mit Umgebungsvariablen

12 Ausfallsicherheit für MIT Kerberos
12.1 Backup der KDC-Datenbank
12.2 Wiederherstellung der KDC-Datenbank
12.3 Replikation der KDC-Datenbank
12.3.1 Möglichkeiten der Kerberos-Replikation
12.3.2 Sicherheit der Replikation
12.4 Replikation bei MIT Kerberos
12.4.1 Ein Replica KDC einrichten
12.4.2 Schritte auf dem Master KDC
12.4.3 Das Replica KDC starten
12.4.4 Das Replica KDC bekannt machen
12.4.5 Regelmäßig replizieren

13 Ein LDAP-Backend für die MIT-Datenbank
13.1 Überblick
13.1.1 Erweiterte Funktionalitäten
13.1.2 Vorgehensweise
13.1.3 Sicherheit
13.2 Software, Schema und Konfiguration des LDAP-Servers
13.2.1 Software installieren
13.2.2 Das Schema erweitern
13.3 Das KDC auf LDAP umstellen
13.3.1 Vorbereitungen
13.3.2 Konfiguration
13.3.3 Die KDC-Datenbank im LDAP initialisieren
13.3.4 Den Realm einrichten
13.4 Existierende Nutzerobjekte
13.5 Principal-Aliase
13.5.1 Client-Aliase
13.5.2 Dienste-Aliase
13.6 Ausfallsicherheit mit LDAP
13.6.1 OpenLDAP auf kdc01 vorbereiten
13.6.2 LDAP-Server auf kdc02 einrichten
13.6.3 Ausfallsicherheit für das KDC
13.6.4 Die Clientkonfiguration anpassen