

# FACHHOCHSCHULE WEDEL

- University of Applied Sciences -

## SEMINAR

Thema:

### **Kerberos: The Network Authentication Protocol**

Stefan Roggensack, B. Sc.  
E-Mail: [inf6509@fh-wedel.de](mailto:inf6509@fh-wedel.de)

Abgegeben am: 4. Dezember 2008

Dozenten: Prof. Dr. Uwe Schmidt  
Prof. Dr. Ulrich Hoffmann

# Inhaltsverzeichnis

|                                                              |            |
|--------------------------------------------------------------|------------|
| <b>Abbildungsverzeichnis</b>                                 | <b>III</b> |
| <b>1 Vorbemerkungen</b>                                      | <b>1</b>   |
| 1.1 Allgemeines . . . . .                                    | 1          |
| 1.2 Anwendung . . . . .                                      | 2          |
| 1.3 Symmetrische und asymmetrische Verschlüsselung . . . . . | 2          |
| 1.4 Notation . . . . .                                       | 4          |
| <b>2 Protokollgrundlagen</b>                                 | <b>5</b>   |
| 2.1 Symmetrisches Needham-Schroeder-Protokoll . . . . .      | 5          |
| 2.2 Replay-Angriff nach Denning und Sacco . . . . .          | 6          |
| <b>3 Kerberos</b>                                            | <b>8</b>   |
| 3.1 Protokoll . . . . .                                      | 8          |
| 3.2 Schlüsselgenerierung . . . . .                           | 13         |
| 3.3 ASN.1 . . . . .                                          | 14         |
| 3.4 Delegation . . . . .                                     | 14         |
| <b>4 Kerberos mit Smartcards</b>                             | <b>16</b>  |
| 4.1 PKINIT . . . . .                                         | 16         |
| 4.2 Schwachstelle . . . . .                                  | 16         |
| <b>5 Fazit</b>                                               | <b>19</b>  |
| <b>A Kerberos String to Key Function in Python</b>           | <b>20</b>  |
| <b>B Abkürzungen</b>                                         | <b>35</b>  |
| <b>C Literaturverzeichnis</b>                                | <b>36</b>  |

## Abbildungsverzeichnis

|   |                                                                     |    |
|---|---------------------------------------------------------------------|----|
| 1 | Darstellung der symmetrischen Verschlüsselung . . . . .             | 3  |
| 2 | Darstellung der asymmetrischen Verschlüsselung . . . . .            | 4  |
| 3 | Einfache Authentifizierung im Kerberos-Protokoll . . . . .          | 8  |
| 4 | Wireshark-Analyse des KRB-AS-REQ Paketes . . . . .                  | 10 |
| 5 | Wirshark-Analyse des KRB-AS-REP Paketes . . . . .                   | 11 |
| 6 | Authentifizierung im Kerberos-Protokoll . . . . .                   | 12 |
| 7 | Aufbau zu einem Server, wenn ein TGT bereits vorhanden ist. . . . . | 12 |
| 8 | Abhören der Kerberospakete . . . . .                                | 17 |
| 9 | Vortäuschen einer Serveridentität . . . . .                         | 18 |

# 1 Vorbemerkungen

Diese Seminararbeit im Rahmen des Informatik-Seminars WS2008/09 mit dem Thema „Linux und Netzwerke, Softwareentwicklung mit Eclipse“ behandelt das Protokoll Kerberos. Kerberos sorgt für die Authentifizierung eines Kommunikationspartners und erlaubt es einen Schlüssel für eine weitere sichere Kommunikation auszutauschen.

In dieser Arbeit werden zuerst kurz beschrieben was unter symmetrischer und asymmetrischer Verschlüsselung verstanden wird und wie Kryptographische Protokolle notiert werden. Folgend wird das Protokoll auf dem Kerberos basiert, das Needham-Schroeder-Protokoll, und die Erweiterung durch Denning und Sacco näher beschrieben. Danach wird auf das Kerberosprotokoll und einige technischen Details eingegangen. Zum Ende wird noch Kerberos mit Smartcards beschrieben.

## 1.1 Allgemeines

Der Name Kerberos leitet sich aus der *griechischen Mythologie* ab. Kerberos ist der mehrköpfige Höllenhund, welcher den Eingang zur Unterwelt bewacht. Ihn zu besiegen ist die letzte und schwierigste Aufgabe des Helden Herkules.

Das Protokoll wurde im Rahmen des „*Project Athena*“ ab Anfang der 80er Jahre entwickelt. „Project Athena“ war ein Projekt des Massachusetts Institute of Technology (MIT) in Cambridge. In Zusammenarbeit mit IBM und DEC sollte Strategien und Software für das Computernetz des MIT entwickelt werden. (vgl. [Gar03, S. 3ff])

Das Kerberos Protokoll nutzt *symmetrische Verschlüsselung*, „da in den USA zur Zeit der Entwicklung von Kerberos die Public-Key Verschlüsselung noch unter patentrechtlichen Beschränkungen lag.“[Eck01, S. 504] Das Protokoll basiert auf dem theoretischen symmetrischen Needham-Schroeder-Protokoll mit den Veränderungen von Denning und Sacco. (vgl. [RFC4120, S. 5])

Die ersten drei Versionen von Kerberos wurden nur für Testzwecke innerhalb des MIT genutzt. Erst Version 4 und 5 wurden weltweit in Computernetzen eingesetzt. Version 4 wurde am 24. Januar 1989 veröffentlicht. (vgl. [Gar03, S. 7]) Das MIT hat das Ende von Kerberos 4 angekündigt.<sup>1</sup> Diese Seminararbeit legt daher den Schwerpunkt auf Kerberos 5. Für eine Liste der Änderungen zwischen Version 4 und 5 sei auf [KNT91] verwiesen.

---

<sup>1</sup>Die Ankündigung des MIT: Kerberos Version 4 End of Life Announcement

Die aktuelle Version 5 des Protokolls wird im [RFC4120] aus dem Juli 2005 definiert. Es handelt sich um einen Proposed Standard der Internet Engineering Task Force (IETF), welcher durch [RFC4537] und [RFC5021] leicht erweitert wurde. Das Protokoll ist in fast jeden größeren Computernetzwerk im Einsatz. Jedes Windows- und Applenetzwerk setzt standardmäßig auf Kerberos auf. Aber es wird auch in vielen Linux und Unix Umgebungen eingesetzt.

### 1.2 Anwendung

Kerberos wurde entwickelt um eine Anmeldung in einem Netzwerk zu ermöglichen. Auf klassischen Einzelrechnern lässt sich das Passwort mit einem Hashwert Vergleichen und die damit die Korrektheit überprüfen. In einem Netzwerk können solche Übertragungen abgehört werden. Es sollte daher ein Passwort nicht unverschlüsselt übertragen werden. Da sich ein Hashwert aufzeichnen und erneut senden lässt bietet es keine weitere Sicherheit. Daher ist es notwendig kryptographische Protokolle zu verwenden um einen Benutzer an einem Server anzumelden.

In Version 5 von Kerberos wurden außerdem die Funktionen für ein „Single-Sign-On“ erweitert. „Single-Sign-On“ ist ein Prinzip nachdem ein Benutzer eines Netzwerkes nur einmal sein Passwort eingeben muss und dann alle Dienste nutzen kann. Ein Szenario wäre die Anmeldung an einem beliebigen Arbeitsplatz im Netzwerk. Dann der Aufruf des Intranetportals der Firma. In dem Portal wird von dem Intranetserver auf die Datenbank des Customer Relationship Management (CRM) mit den entsprechenden Rechten des Nutzers zugegriffen und die Daten ins Portal integriert. Dabei ist es notwendig nur einmal das Passwort bei der Anmeldung an der Arbeitsstation einzugeben.

Außerdem lässt sich mit Kerberos nicht nur die Identität des Client, sondern auch die des Servers überprüft werden. So können Angreifer nicht die Identität eines Servers vortäuschen. Zur Authentisierung können viele Protokolle Kerberos nutzen, z. B. Secure Shell (SSH), Network File System (NFS) und Lightweight Directory Access Protocol (LDAP).

### 1.3 Symmetrische und asymmetrische Verschlüsselung

Eine *kryptographische Hashfunktion* ist wie „normale“ Hashfunktionen eine surjektive Abbildung. Zusätzlich wird noch gefordert, dass die Funktion unumkehrbar ist. Es sollten

also aus dem Hashwert keine Rückschlüsse auf die Eingabe möglich sein. Auch sollte eine kleine Änderung an der Eingabe, eine ganz andere Ausgabe erzeugen.

Bei Verschlüsselungsverfahren wird zwischen zwei Arten unterschieden.

Zum einen die *symmetrische Verschlüsselung*. Hier existiert ein Schlüssel mit dem der Text verschlüsselt wird und mit dem gleichen Schlüssel wird der Text auch wieder in den Klartext verwandelt. In Abbildung 1 wird die Verschlüsselung und Entschlüsselung dargestellt. Verbreitet Verfahren sind Data Encryption Standard (DES), Blowfish und Advanced Encryption Standard (AES).

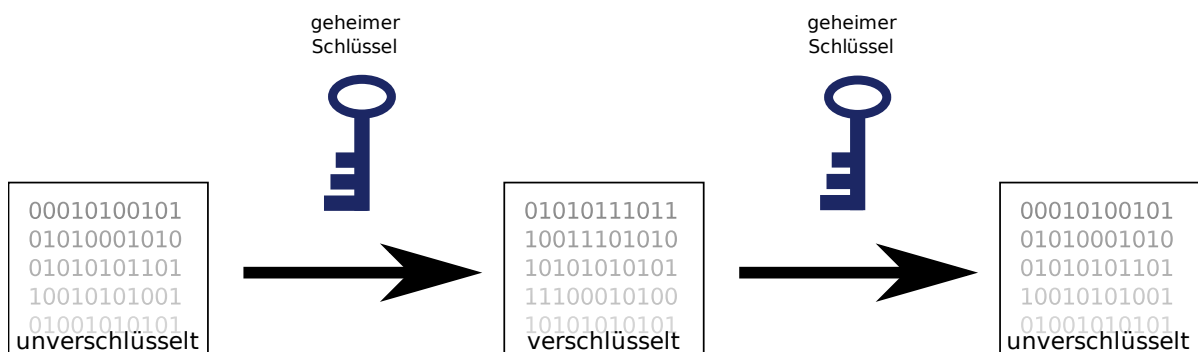


Abbildung 1: Darstellung der symmetrischen Verschlüsselung

Bei der *asymmetrischen Verschlüsselung* existiert ein Paar von einem privaten und einem öffentlichen Schlüssel. Jeder kann eine Nachricht an einen Empfänger mit dem öffentlichen Schlüssel chiffrieren. Denn Klartext kann nur der Empfänger, welcher im Besitz des privaten Schlüssel ist, wiederherstellen. Hierfür müssen die beiden Schlüssel in einem mathematischen Zusammenhang stehen. Dies ist oft das inverse Element in einer Gruppe  $\mathbb{N}_P$  mit der Primzahl  $P$ . In Abbildung 2 ist dies dargestellt. Verbreitete Verfahren sind RSA und Elgamal.

Eine *digitale Signatur* ist die Benutzung der asymmetrischen Verschlüsselung in der anderen Richtung. Ein Hashwert des Texts wird mit dem privaten Schlüssel verschlüsselt. Jeder kann überprüfen ob der Text wirklich von der angegebenen Person ist indem er dem er die Signatur mit dem öffentlichen Schlüssel dechiffriert und mit dem Hashwert des Textes vergleicht.

Ein *Zertifikat* ist der öffentliche Schlüssel einer Person mit weiteren Daten, wie Name und Gültigkeitsdauer, welches von einer vertrauenswürdigen Instanz digital signiert wurde.

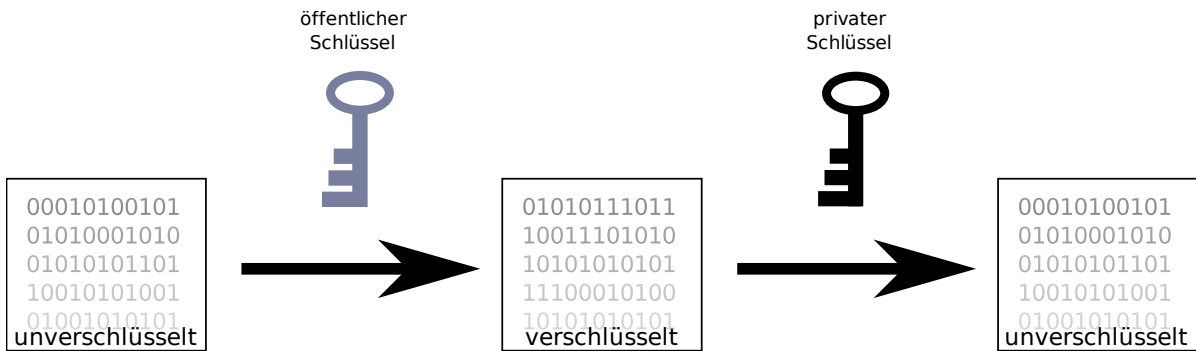


Abbildung 2: Darstellung der asymmetrischen Verschlüsselung

### 1.4 Notation

Für die Darstellung der kryptographischen Protokolle wird eine Notation ähnlich wie in den Veröffentlichungen [NS78], [DS81] und [NT94] benutzt.

Eine Nachricht ( $M$ ) von Alice ( $A$ ) zu Bob ( $B$ ) wird als  $A \rightarrow B : M$  geschrieben. Der geheime symmetrische Schlüssel von Alice wird als  $K_A$  geschrieben. Wenn eine Nachricht bestehend aus der Sequenz  $C, D$  mit  $K_A$  verschlüsselt ist wird  $\{C, D\}_{K_A}$  notiert.  $N_A$  bezeichnet eine Zufallszahl, welche anfangs nur  $A$  bekannt ist und wird als Nonce bezeichnet. Wenn der Angreifer Eve ( $X$ ) eine Nachricht im Namen von  $A$  sendet wird  $X_A \rightarrow B : M$  geschrieben.

Mit  $K_A$  wird ein symmetrischer Schlüssel bezeichnet. Der öffentliche Teil des asymmetrischen Schlüssels wird als  $k_A$  geschrieben und der private Teil als  $k_A^{-1}$ .

## 2 Protokollgrundlagen

Das Needham-Schroeder-Protokoll ist ein kryptographisches Protokoll, welches die Nutzer authentifiziert und einen Schlüssel sicher überträgt. Es wurde 1978 Roger Needham und Michael Schroeder veröffentlicht. (vgl. [NS78])

### 2.1 Symmetrisches Needham-Schroeder-Protokoll

In dem Protokoll gibt es drei Parteien:

- $A$  möchte eine Verbindung mit  $B$  aufbauen. (Client)
- $B$  wartet auf Verbindungen. (Server)
- Der Authentication Server ( $AS$ ).

Jeder Netzwerkteilnehmer hat einen geheimen Schlüssel  $K$ . Dieser ist jeweils nur dem Teilnehmer und dem Authentifikation-Server  $AS$  bekannt.

Folgende 5 Pakete werden bei dem Needham-Schroeder-Protokoll gesendet. Nach diesem 5 Paketen weiß  $A$  das es eine Verbindung mit  $B$  aufgebaut hat und  $B$  weiß das die Anfrage von  $A$  kommt. Außerdem ist der Sitzungsschlüssel nur  $A$ ,  $B$  und dem vertrauenswürdigen Server  $AS$  bekannt.

1.  $A \rightarrow AS : A, B, N_A$
2.  $AS \rightarrow A : \{N_A, B, K_s, \{K_s, A\}_{K_B}\}_{K_A}$
3.  $A \rightarrow B : \{K_s, A\}_{K_B}$
4.  $B \rightarrow A : \{N_B\}_{K_s}$
5.  $A \rightarrow B : \{f(N_B)\}_{K_s}$

$K_s$  bezeichnet einen zufälligen Sitzungsschlüssel.  $f(N_B)$  ist eine beliebige, vorher festgelegte Funktion ist die einen Wert in Abhängigkeit von  $N_B$  berechnet. Needham und Schroeder schlagen  $f(x) = x - 1$  vor. (vgl. [NS78, S. 995])

Die erste Nachricht signalisiert dem  $AS$ , dass  $A$  eine Verbindung mit  $B$  aufbauen will. In dem Paket ist eine zufällige Nouce enthalten. Der  $AS$  sucht sich denn die Schlüssel von  $A$  und  $B$  aus der Datenbank und generiert einen Sitzungsschlüssel. Der Schlüssel wird

zusammen mit der Zeichenkette „A“ mit dem Schlüssel von  $B$  verschlüsselt. Zusätzlich wird der Schlüssel und die Nouce mit dem Schlüssel von  $A$  verschlüsselt.

$A$  ist in der Lage den Schlüssel und den Nouce zu entschlüsseln. Der Teil der Nachricht, welche mit dem Schlüssel von  $B$  verschlüsselt ist kann  $A$  hingegen nicht lesen. Da nur  $A$  und  $AS$  den Schlüssel  $K_A$  kennen muss die Nachricht von  $AS$  kommen.  $A$  sendet nun an  $B$  den mit  $K_B$  verschlüsselten Teil weiter.

$B$  kann den Teil entschlüsseln und erhält so  $K_s$ . Da  $K_B$  nur  $B$  und  $AS$  bekannt sind muss die Nachricht von  $AS$  verschlüsselt worden sein. Da auch ein „A“ in dem Paket enthalten ist, kann  $B$  sich sicher sein das nur  $B$  und  $AS$   $K_s$  kennen.

Die Nachrichten 4 und 5 sind notwendig um sicherzustellen, dass Nachricht 3 nicht eine aufgezeichnete Nachricht ist, welche erneut von einem Angreifer gesendet wird (Replay).  $B$  verschlüsselt nun eine Nouce mit  $K_s$ . Und erhält eine Antwort die in Beziehung zu der Nouce steht, z. B.  $N_B - 1$ . Da nur  $A$  den Schlüssel  $K_s$  kennen kann, muss die Antwort von  $A$  sein.

## 2.2 Replay-Angriff nach Denning und Sacco

Dorothy E. Denning und Giovanni Maria Sacco haben 1981 ein Angriff beschrieben bei dem ein Angreifer eine fremde Identität annehmen, wenn er den Sitzungsschlüssel kompromittieren kann. Der Sitzungsschlüssel kann durch Brute-Force, Protokollfehler oder Einbruch in ein System in die Hände eines Angreifers kommen. (vgl. [DS81, S. 534])

Wenn er im Besitz des Sitzungsschlüssel, sendet er die Aufgezeichnete Nachricht 3 an  $B$  und kann die Nachricht 5 berechnen.

1.  $A \rightarrow AS : A, B, N_A$
2.  $AS \rightarrow A : \{N_A, B, K_s, \{K_s, A\}_{K_B}\}_{K_A}$
3.  $A \rightarrow B : \{K_s, A\}_{K_B}$
4.  $B \rightarrow A : \{N_{B_1}\}_{K_s}$
5.  $A \rightarrow B : \{f(N_{B_1})\}_{K_s}$
6.  $X_A \rightarrow B : \{K_s, A\}_{K_B}$
7.  $B \rightarrow X_A : \{N_{B_2}\}_{K_s}$

$$8. X_A \rightarrow B : \{f(N_{B_2})\}_{K_s}$$

Der Angreifer  $X$  gibt sich gegenüber  $B$  als  $A$  aus und sendet die aufgezeichnete Nachricht 3 erneut.  $B$  kann nicht unterscheiden ob es sich um eine alte Nachricht handelt und antwortet an  $A$  mit einer neuen Nouce. Da die Antwort von  $B$  auf dem Transport verloren gegangen sein kann, darf  $B$  auch nicht die bisherigen Nachrichten von  $A$  oder die dazugehörigen Sitzungsschlüssel speichern und vergleichen.

$X$  fängt die Nachricht an  $A$  ab und kann sie entschlüsseln, da ihm  $K_s$  bekannt ist. Der Angreifer kann nun die Antwort an  $B$  berechnen und verschlüsseln. Es hilft auch nicht für jeden Netzwerkteilnehmer eine eigene Funktion  $f(x)$  zu definieren, da das Funktionsaustauschproblem dasselbe wie das Schlüsselaustauschproblem ist. (vgl. [DS81, S. 534])

Nach diesen Paketen würde  $B$  glauben das er von  $A$  aufgerufen wird und nicht von  $X$ .  $X$  kann nun Operationen durchführen die eigentlich nur  $A$  darf.

Als Gegenmaßnahme empfehlen Denning und Sacco Zeitstempel in den Paketen zu nutzen. Dadurch lässt sich zusätzlich das Protokoll auf 3 Pakete verkürzen.  $B$  ist in der Lage zu erkennen, dass das Paket von  $A$  ein Replay ist und kann davon ausgehen eine neue Verbindung mit  $A$  zu haben.

$$1. A \rightarrow AS : A, B, N_A$$

$$2. AS \rightarrow A : \{N_A, B, K_s, \text{time}, \{K_s, A, \text{time}\}_{K_B}\}_{K_A}$$

$$3. A \rightarrow B : \{K_s, A, \text{time}\}_{K_B}$$

Da der Zeitstempel in dem durch den privaten Schlüssel von  $B$  geschützten Bereich enthalten ist, kann  $B$  erkennen wenn das Paket zu alt ist. So lassen sich Replay-Angriffe leicht erkennen. Wenn ein Paket empfangen wird dessen Zeitstempel älterer ist als eigentlich benötigt wird, soll es verworfen werden.

### 3 Kerberos

#### 3.1 Protokoll

Für das Kerberos-Protokoll werden drei Pakete benötigt. Das vierte ist optional für den Fall, dass auch der Server sich gegenüber dem Client authentifizieren soll. Da das dritte Paket schon einen Teil hat der durch  $K_s$  verschlüsselt ist und eine Sequenznummer enthält. Da  $K_s$  nur  $A$  und  $B$  bekannt ist kann nur  $B$  die Sequenznummer um eins erhöhen.

1. KRB\_AS\_REQ:  $A \rightarrow AS : A, B, time, N_A$
2. KRB\_AS\_REP:  $AS \rightarrow A : \{K_s, time, N_A\}_{K_A}, \{K_s, A, time\}_{K_B}$
3. KRB\_AP\_REQ:  $A \rightarrow B : \{time, seqnumber\}_{K_s}, \{K_s, A, time\}_{K_B}$
4. KRB\_AP\_REP:  $B \rightarrow A : \{time, seqnumber + 1\}_{K_s}$  (optional)

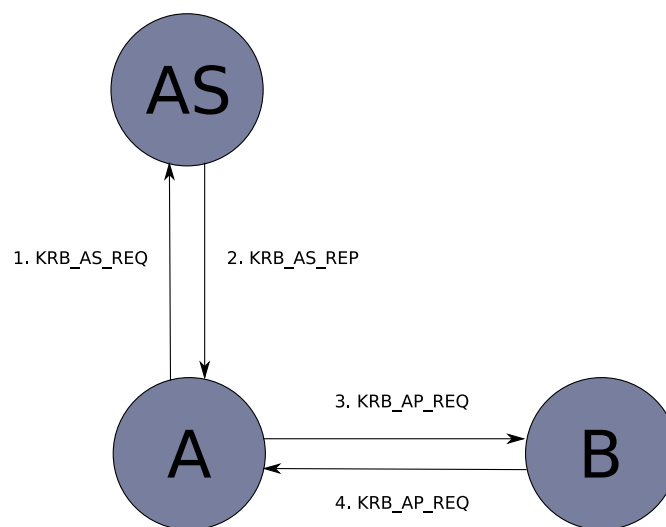


Abbildung 3: Einfache Authentifizierung im Kerberos-Protokoll (Nach [NT94, S. 35])

In Abbildung 3 ist eine vereinfachte Form von Kerberos dargestellt. Der Client möchte mit  $B$  eine Verbindung aufbauen und sendet dies mit einer Nounce und einem Zeitstempel an  $AS$ .

$AS$  erstellt den zufälligen, temporären Schlüssel  $K_s$ . Der Schlüssel wird zusammen mit der Zeichenkette „A“ und einem Zeitstempel mit dem Schlüssel von  $B$  verschlüsselt. Dieser Teil der Nachricht ist das sogenannte Ticket für  $B$ .  $A$  kann dieses Ticket nicht

entschlüsseln, da nur  $B$  und  $AS$  im besitzt von  $K_B$ , mit dem das Ticket verschlüsselt ist, sind. Zusätzlich wird mit dem Schlüssel von  $A$  die Nouce von  $A$ , ein Zeitstempel und  $K_s$  verschlüsselt.

$A$  kann nun sicher sein, dass die Nachricht von  $AS$  ist da nur  $AS$  seinen Schlüssel  $K_A$  kennt. Außerdem kann es sich nicht um eine aufgezeichnete Nachricht handeln, da  $A$  Zeitstempel und Nouce überprüft. Im Gegensatz zu dem Needham-Schroeder-Protokoll ist das Ticket nicht mit dem geheimen Schlüssel von  $A$  geschützt. Da aber in dem Ticket das „A“ enthalten ist, kann nur  $A$  damit zu  $B$  eine Verbindung aufbauen. Dadurch müssen weniger Daten verschlüsselt werden.

Nun baut  $A$  die Verbindung zu  $B$  auf. Hierfür sendet er das Ticket, welches er von  $AS$  erhalten hat unverändert an  $B$  weiter. Außerdem wird ein Teil der Nachricht mit dem Schlüssel  $K_s$  verschlüsselt. Dieser Teil enthält eine zufällige Startsequenznummer und ein Zeitstempel.

Wenn  $B$  dieses Paket erhält entschlüsselt er das Ticket mit seinem Schlüssel  $K_B$  und überprüft den Zeitstempel. Wenn das Paket zu alt ist wird es verworfen. So ist sichergestellt das es sich nicht um ein Replay handelt. Da nur  $AS$  das Ticket erstellt haben kann und es „A“ enthält, ist sicher, dass das Ticket von  $AS$  für  $A$  ausgestellt wurde. Außerdem kann  $K_s$  außer  $B$  nur  $A$  und  $AS$  bekannt sein.

Falls  $A$  sichergehen muss, dass die Verbindung erfolgreich aufgebaut wurde und die Identität von  $B$  überprüfen muss, wird eine 4 Nachricht von  $B$  versendet. In dieser wird die Sequenznummer um eins erhöht verschlüsselt mit  $K_s$  an  $A$  zurück geschickt. Dies ist vergleichbar mit der Funktion  $f(x)$  bei dem Needham-Schroeder-Protokoll in der Nachricht 5.

Alle Pakete enthalten Zeitstempel um Replay-Angriffe zu erschweren. Dies ist in den entschlüsselten Mittschnitten in Abbildung 4 und 5 zu sehen.

$A$  benötigt so für jeden Verbindungsaufbau zu einem Server  $K_A$ . So müsste man entweder  $K_A$  auf dem Rechner zwischenspeichern oder der Benutzer müsste jedes mal sein Passwort eingeben, damit  $K_A$  berechnet werden kann. Um dies zum umgehen wird eine Zwischenschicht eingezogen. Der Client fordert erstmal nur ein sogenanntes Ticket Granting Ticket (TGT) bei dem  $AS$  an. Mit diesem TGT kann der Client ein Ticket bei dem Ticket Granting Server (TGS) ein Ticket für einen konkreten Server anfordern.

1. KRB\_AS\_REQ:  $A \rightarrow AS : A, TGS, time, N_A$
2. KRB\_AS\_REP:  $AS \rightarrow A : \{K_{s1}, time, N_A\}_{K_A}, \{K_{s1}, A, time\}_{K_{TGS}}$

### 3 Kerberos

```

▶ Frame 17 (285 bytes on wire, 285 bytes captured)
▶ Ethernet II, Src: CadmusCo_0d:d3:6e (08:00:27:0d:d3:6e), Dst: CadmusCo_72:ee:78 (08:00:27:72:ee:78)
▶ Internet Protocol, Src: 10.0.5.2 (10.0.5.2), Dst: 10.0.5.1 (10.0.5.1)
▶ User Datagram Protocol, Src Port: 60292 (60292), Dst Port: kerberos (88)
▼ Kerberos AS-REQ
  Pvno: 5
  MSG Type: AS-REQ (10)
  ▼ padata: PA-ENC-TIMESTAMP
    ▼ Type: PA-ENC-TIMESTAMP (2)
      ▼ Value: 3045A003020110A23E043C079781C233773AD160945A4A76... des3-cbc-sha1
        Encryption type: des3-cbc-sha1 (16)
        ▼ enc PA_ENC_TIMESTAMP: 079781C233773AD160945A4A765830D88C6D1009DD8DA05C...
          [Decrypted using: keytab principal client1@LAN]
          patimestamp: 2008-12-03 12:04:41 (UTC)
          pausec: 893364
    ▼ KDC_REQ_BODY
      Padding: 0
      ▶ KDCOptions: 50000010 (Forwardable, Proxyable, Renewable OK)
      ▶ Client Name (Principal): client1
      Realm: LAN
      ▶ Server Name (Unknown): krbtgt/LAN
      from: 2008-12-03 12:04:39 (UTC)
      till: 2008-12-04 12:04:39 (UTC)
      Nonce: 1228305879
      ▶ Encryption Types: aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 des3-cbc-sha1 rc4-hmac des-cbc-crc des-cbc-md5 des-cbc-md4

```

Abbildung 4: Wireshark-Analyse des KRB-AS-REQ Paketes

3. KRB\_TGS\_REQ:  $A \rightarrow TGS : \{time, seqnumber\}_{K_{s1}}, \{K_{s1}, A, time\}_{K_{TGS}}$
4. KRB\_TGS\_REP:  $TGS \rightarrow A : \{time, seqnumber + 1, K_{s2}\}_{K_{s1}}, \{K_{s2}, A, time\}_{K_B}$
5. KRB\_AP\_REQ:  $A \rightarrow B : \{time, seqnumber\}_{K_{s2}}, \{K_{s2}, A, time\}_{K_B}$
6. KRB\_AP\_REQ:  $B \rightarrow A : \{time, seqnumber + 1\}_{K_{s2}}$  (optional)

So werden weniger Pakete welche mit  $K_A$  verschlüsselt sind übertragen. Da bei vielen Angriffen auf kryptographische Verfahren viele Pakete benötigt werden, erschwert dies potentielle Angriffe.

In Normalfall sind AS und TGS auf dem gleichen Server und wird als Key Distribution Center (KDC) bezeichnet. Die Netzwerkteilnehmer werden als *Principal* bezeichnet. Jeder Principal gehört zu einem *Realm*. Ein Realm ist ein Kerberosnetz. Es ist aber auch möglich Kerberos über Realmgrenzen hinweg als authentifizierungs Protokoll zu verwenden. Um dies Schlüssel von Server für Dienste von denen der Nutzer zu unterscheiden haben die normalerweise die Form *host/<servername>@<realm>*. Um Administratorkonten von Benutzerkonten zu trennen, gibt es die Konvention diese in der Form *<name>/admin@<realm>* zu benennen.

### 3 Kerberos

```
▶ Frame 18 (591 bytes on wire, 591 bytes captured)
▶ Ethernet II, Src: CadmusCo_72:ee:78 (08:00:27:72:ee:78), Dst: CadmusCo_0d:d3:6e (08:00:27:0d:d3:6e)
▶ Internet Protocol, Src: 10.0.5.1 (10.0.5.1), Dst: 10.0.5.2 (10.0.5.2)
▶ User Datagram Protocol, Src Port: kerberos (88), Dst Port: 60292 (60292)
▼ Kerberos AS-REP
  Pvno: 5
  MSG Type: AS-REP (11)
  ▶ padata: PA-ENCTYPE-INFO2
    Client Realm: LAN
    ▶ Client Name (Principal): client1
    ▼ Ticket
      Tkt-vno: 5
      Realm: LAN
      ▶ Server Name (Unknown): krbtgt/LAN
      ▼ enc-part des3-cbc-shal
        Encryption type: des3-cbc-shal (16)
        Kvno: 4
        ▼ enc-part: 646FC3DBEC0354E0BF7E8878C91B82BD2BC66BF535C90D5D...
          [Decrypted using: keytab principal krbtgt/LAN@LAN]
          ▼ EncTicketPart
            Padding: 0
            ▶ Ticket Flags (Forwardable, Proxyable, Renewable, Initial, Pre-Auth)
            ▶ key des3-cbc-shal
              Client Realm: LAN
              ▶ Client Name (Principal): client1
              ▶ TransitedEncoding DOMAIN-X500-COMPRESS
              Authtime: 2008-12-03 12:04:41 (UTC)
              End time: 2008-12-03 22:04:41 (UTC)
              Renew-till: 2008-12-04 12:04:39 (UTC)
          ▼ enc-part des3-cbc-shal
            Encryption type: des3-cbc-shal (16)
            ▼ enc-part: 5A260224A001AA84C49F2265D5077C0F528591811FC2BF0D...
              [Decrypted using: keytab principal client1@LAN]
              ▼ EncKDCRepPart
                ▶ key des3-cbc-shal
                ▶ LastReqs:
                  Nonce: 1228305879
                  Padding: 0
                ▶ Ticket Flags (Forwardable, Proxyable, Renewable, Initial, Pre-Auth)
                  Authtime: 2008-12-03 12:04:41 (UTC)
                  End time: 2008-12-03 22:04:41 (UTC)
                  Renew-till: 2008-12-04 12:04:39 (UTC)
                  Realm: LAN
                ▶ Server Name (Unknown): krbtgt/LAN
```

Abbildung 5: Wirshark-Analyse des KRB-AS-REP Paketes

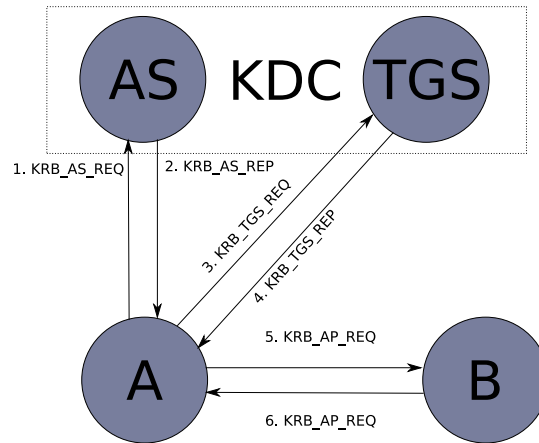


Abbildung 6: Authentifizierung im Kerberos-Protokoll (Nach [NT94, S. 37])

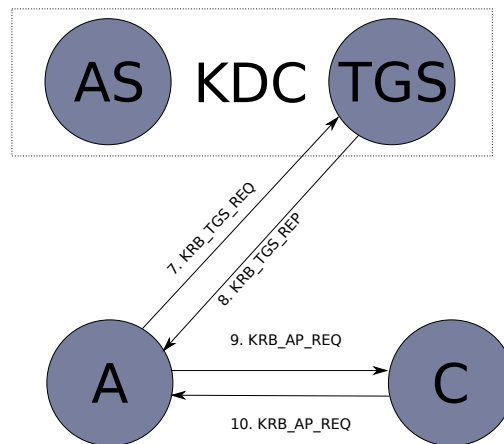


Abbildung 7: Aufbau zu einem Server, wenn ein TGT bereits vorhanden ist.

### 3.2 Schlüsselgenerierung

Im Normalfall geben Benutzer ein Passwort ein um sich an einem PC anzumelden. Für Kerberos werden, aber Schlüssel benötigt. Dafür werden kryptographische Hashfunktionen benutzt um einen Schlüssel für das gewählte Verschlüsselungsverfahren. Zum Teil wird noch ein Funktion n-fold benutzt um die Schlüssel besser über den Schlüsselraum zu verteilen.

Alle Kerberos StringToKey Funktionen haben nach [RFC3961, S. 5] drei Parameter. Ein Password-String, ein Salt-String und weitere Parameter als String. Für Triple-DES, sollten die Parameter leer sein. Der Salt ist eine Zeichenfolge um aus gleichen Passwörtern verschiedenen Schlüssel zu generieren. Dies ist im Normalfall der Name des Realm gefolgt vom Benutzernamen. So ist es nicht möglich eine vorberechnete Liste von Schlüsseln zu erzeugen. Der Salt wird einfach hinten an das Passwort angehängt.

Im nachfolgenden Codelisting ist die Kerberos String-To-Key-Funktion in Python zu sehen.

---

```
1 def krb5int_dk_string_to_key(password, salt, params):
2     if (params != ""):
3         raise Exception, "invalid params"
4     keybytes = 21
5     keylength = 24
6     foldkey = k5_des3_make_key(krb5_nfold(password + salt, keybytes)
7                               , keylength)
8     key = krb5_derive_key(foldkey, 'kerberos')
9     return key
```

---

Als erstes wird eine n-fold Funktion ausgeführt um eine Kette von 21 Byte zu bekommen. Diese Zeichen werden mit 3 Paritätsbits aufgefüllt, um die für einen Triple-DES-Schlüssel benötigen 24 Byte zu bekommen. Dieser Schlüssel wird genommen und damit das Wort „kerberos“ verschlüsselt. Das Ergebnis wird zugleich für die ersten 8 Byte des Schlüssels und als neuer Klartext für den nächsten Block benutzt.

Diese Funktion kann man als kryptographische Hashfunktion bezeichnen. Für die ganze Funktion ist der Quellcode im Anhang A zu sehen.

### 3.3 ASN.1

Die Pakete für Kerberos 5 sind in der Abstract Syntax Notation One (ASN.1) definiert. (vgl. [BMB<sup>+</sup>05, S. 417]) ASN.1 ist Teil des 7 Schichten OSI-Modells. Es ist der Standard für die 6. Schicht (Darstellung). Es definiert eine Syntax ähnlich wie die Backus-Naur-Form. So kann Kerberos auf allen Protokollen genutzt werden wo ASN.1 definiert ist. ASN.1 definiert eine Codierung, so dass Strings ohne Längenbeschränkungen übertragen werden können.

Folgendes Listing zeigt die Definition des *PrincipalName* in der [RFC4120].

---

```
1 PrincipalName ::= SEQUENCE {
2     name-type      [0] Int32,
3     name-string    [1] SEQUENCE OF KerberosString
4 }
```

---

In einem Paket, der drunterliegenden Schicht, kann da zu Beispiel folgender Hex String auftreten: „3012a003020101a10b30091b07636c696556e7431“. Wenn man sich die Zeichen in einer ASCII-Representation anschaut erhält man den String: „0.....0...client1„. Mit einem ASN.1 decoder (z. B. pyasn1 für Python) lässt sich dies decodieren und lesen.

---

```
1 SEQUENCE {
2     [0] {
3         INTEGER 1
4     }
5     [2] {
6         [0] {KerberosString client1}
7     }
8 }
```

---

So kann bei der Protokolldefinition sich auf den Inhalt konzentriert werden. Auch ist ASN.1 auf vielen Arten von Netzwerken definiert. So ist Kerberos 5 nicht wie Kerberos 4 auf TCP-Netzwerke beschränkt.

### 3.4 Delegation

In verteilten Systemen besteht oft die Notwendigkeit, dass ein Server Daten andere Server für seine Aufgabe benötigt. Dabei sollte der Zugriff mit der Identität des Endnut-

zers und nicht der des Frontendservers durchgeführt werden. So werden die Daten des Backend nur an berechnigte Personen übermiltelt und in die Logdateien der Endbenutzer eingetragen welcher den Zugriff durchgeführt hat.

In dem Kerberos-Protokoll sind zwei Lösungsmöglichkeiten für das Problem vorgesehen. Zum einen lässt sich ein Ticket als PROXIABLE deklarieren. Wenn der empfangende Server bei KDC als berechnigt eingetragen ist, kann dieser bei dem KDC ein Ticket im Namen des Benutzers für den Backend Server beantragen. Dabei muss der Client die Identität des Backend Systems kenne. (vgl. [RM03, S. 251f])

Eine zweite Möglichkeit ist das Paket als FORWARDABLE zu markieren. Dann kann der Server sich ein TGT bei dem KDC holen und damit im Namen des Benutzers andere Systeme ansprechen. Dabei sollte die Konfiguration so eingeschränkt werden das nur Tickets für benötigte Server geholt werden können. (vgl. [RM03, S. 252])

## 4 Kerberos mit Smartcards

Die Benutzung von asymmetrischer Kryptographie in Form von X.509 Zertifikaten ist dort wo Sicherheit besonders wichtig ist verbreitet. (vgl. [RFC4556, S. 4]) Dafür werden in vielen Unternehmen Smartcards eingesetzt. Auf den Smartcards sind die privaten Schlüssel für eine asymmetrische Verschlüsselung gespeichert.

### 4.1 PKINIT

Da Kerberos aber in vielen Netzwerken eingesetzt wird, bestand der Wunsch Smartcards in die Kerberos Authentifizierung einzubinden. Kerberos arbeitet aber mit symmetrischer Kryptographie. Daher musste eine Erweiterung für Kerberos konzipiert werden.

Hierfür werden die ersten beiden Pakete verändert. Danach ist  $A$  wieder im Besitz eines TGT.

1. KRB\_AS\_REQ:  $A \rightarrow AS : A, TGS, Cert_A, \{time, N_A\}_{k_A^{-1}}$
2. KRB\_AS\_REP:  $AS \rightarrow A : \{Cert_{AS}, \{time, N_A, K_{s2}\}_{k_{AS}^{-1}}\}_{k_A}, A, \{K_{s1}, A, time\}_{K_{TGS}}, \{K_{s1}, TGS, time\}_{K_{s2}}$

Im ersten Paket wird die Zeit und ein Nouce mit dem privaten Schlüssel von  $A$  signiert. Damit kann  $AS$  überprüfen, ob die Nachricht wirklich von  $A$  kommt.

Der erste Teil der Antwort des  $AS$  wird mit dem öffentlichen Schlüssel von  $A$  verschlüsselt. Dies stellt sicher das nur  $A$  an den dort enthaltenen Schlüssel  $K_{s2}$  kommt. Der Teil ist zusätzlich von dem  $AS$  signiert worden um sicherzustellen das die Antwort wirklich von  $AS$  kommt. Der zweite Teil ist der TGT. Im letzten Teil der Nachricht ist der Sitzungsschlüssel des TGT mit dem Schlüssel  $K_{s2}$  verschlüsselt enthalten.

### 4.2 Schwachstelle

Im Jahre 2005 hat eine Gruppe Wissenschaftler um Iliano Cervesato eine Schwachstelle in PKINIT entdeckt. (vgl. [CJT<sup>+</sup>06]) Sie beschreiben ein Möglichkeit einen Man-in-the-Middle-Angriff durchzuführen. Als Vorbedingung muss der Angreifer sich selbst an dem Server anmelden dürfen.

1. KRB\_AS\_REQ:  $A \rightarrow X : A, B, Cert_A, \{time, N_A\}_{k_A^{-1}}$

2. KRB\_AS\_REQ:  $X_A \rightarrow AS : X, B, Cert_X, \{time, N_A\}_{k_X^{-1}}$
3. KRB\_AS\_REP:  $AS \rightarrow X : \{Cert_{AS}, \{time, N_A, K_{s2}\}_{k_{AS}^{-1}}\}_{k_X}, X, \{K_{s1}, X, time\}_{K_{TGS}}, \{K_{s1}, TGS, time\}_{K_{s2}}$
4. KRB\_AS\_REP:  $X_{AS} \rightarrow A : \{Cert_{AS}, \{time, N_A, K_{s2}\}_{k_{AS}^{-1}}\}_{k_A}, A, \{K_{s1}, X, time\}_{K_{TGS}}, \{K_{s1}, TGS, time\}_{K_{s2}}$

Der Angreifer leitet die Anfrage von  $A$  an den  $AS$  als seine eigene weiter. Da die Antwort in Wirklichkeit für  $X$  bestimmt ist steht nur in Teilen, welche  $X$  ersetzen kann, oder im Ticket. Da das Ticket mit  $K_{TGS}$  verschlüsselt ist kann  $A$  dies nicht überprüfen.  $X$  kann nun alle Verbindungen entschlüsseln und an den Server weiterleiten und dabei alle Pakete entschlüsseln. (siehe Abbildung 8)

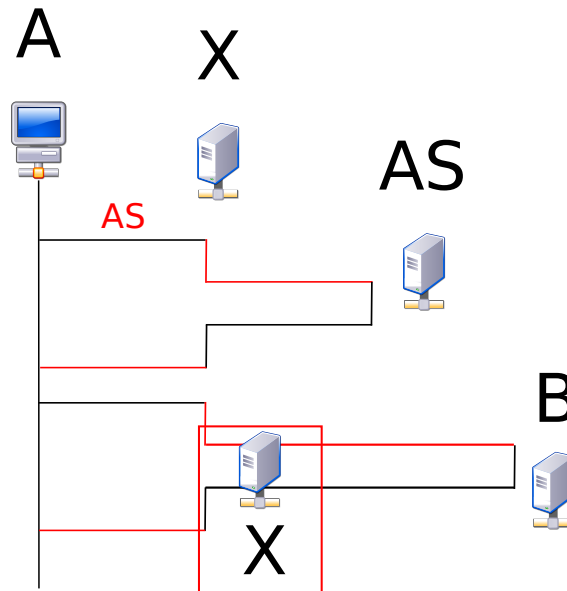


Abbildung 8: Abhören der Kerberospakete

Die Bilder des Servers und des Clients stammen von <http://ftp.gnome.org/pub/GNOME/sources/gnome-themes-extras/0.9/gnome-themes-extras-0.9.0.tar.gz> und stehen unter der LGPL 2.1 or later. Die Grafik steht als abgeleitetes Werk auch unter LGPL 2.1 or later.

Eine weitere Möglichkeit ist es gegenüber  $A$  die Identität des Servers anzunehmen und so geheime Informationen zu gewinnen. Dies ist in der Abbildung 9 dargestellt. (vgl. [CJT<sup>+</sup>06, S. 8])

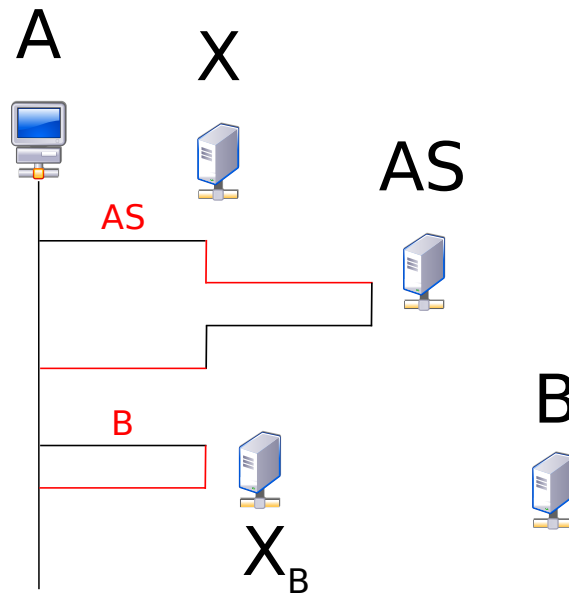


Abbildung 9: Vortäuschen einer Serveridentität

Die Bilder des Servers und des Clients stammen von <http://ftp.gnome.org/pub/GNOME/sources/gnome-themes-extras/0.9/gnome-themes-extras-0.9.0.tar.gz> und stehen unter der LGPL 2.1 or later. Die Grafik steht als abgeleitetes Werk auch unter LGPL 2.1 or later.

Als Gegenmaßnahme muss der signierte Teil der KRB\_AS\_REP-Nachricht auch den Empfänger enthalten. Wenn AS  $\{Cert_{AS}, \{time, N_A, K_{s2}, X\}_{k_{AS}^{-1}}\}_{k_X}$  senden würde, kann X das Paket nicht mehr weiterleiten. A würde merken, dass das Paket eigentlich für X bestimmt ist.

## 5 Fazit

Kerberos ist eine weit verbreitete Technologie, welche in den meisten größeren Netzwerken eingesetzt wird. Das Needham-Schroder-Protokoll als theoretische Grundlage ist mittlerweile 30 Jahre alt und es haben sich viele Kryptoanalytiker Gedanken zu dem Protokoll gemacht. Es ist daher unwahrscheinlich, dass heute noch eine Sicherheitslücke darin auftaucht. Auch die MIT Implementierung ist schon recht alt und oft begutachtet worden.

Diese Sicherheit lässt sich, aber nicht auf alle Erweiterungen übertragen. Diese können sehr viel jünger sein und weniger gut überprüft sein. Wie das Beispiel PKINIT zeigt, können hier noch Sicherheitslücken unentdeckt sein.

Kerberos 5 ist auch noch ein Proposed Standard der IETF und noch kein Internet Standard. Es sind also noch Änderungen am Protokoll möglich. Mit Blick auf die vielen Implementierungen und den verbreiteten Einsatz, ist es aber unwahrscheinlich das es noch zu grundlegenden Änderungen kommt.

Ein Angriffspunkt bleibt das KDC, da hier alle Schlüssel enthalten sind. Wenn Angreifer Zugang zu dieser Datenbank erlangen können sie im Netzwerk alles tun. Auch ein aus dem Unternehmen ausscheidender Administrator kann dieser Daten mitnehmen. Dies erfordert ein neu erstellen der wichtigsten Schlüssel. Daher sollten bei dem Einsatz von Kerberos auch einige organisatorische Rahmenprozesse definiert werden.

## A Kerberos String to Key Function in Python

StringToKey.py:

---

```
1 #!/usr/bin/env python2.5
2 #Copyright (C) 1998 by the FundsXpress, INC.
3 #
4 #All rights reserved.
5 #
6 #Export of this software from the United States of America may require
7 #a specific license from the United States Government. It is the
8 #responsibility of any person or organization contemplating export to
9 #obtain such a license before exporting.
10 #
11 #WITHIN THAT CONSTRAINT, permission to use, copy, modify, and
12 #distribute this software and its documentation for any purpose and
13 #without fee is hereby granted, provided that the above copyright
14 #notice appear in all copies and that both that copyright notice and
15 #this permission notice appear in supporting documentation, and that
16 #the name of FundsXpress. not be used in advertising or publicity
   pertaining
17 #to distribution of the software without specific, written prior
18 #permission. FundsXpress makes no representations about the
   suitability of
19 #this software for any purpose. It is provided "as is" without express
20 #or implied warranty.
21 #
22 #THIS SOFTWARE IS PROVIDED ‘‘AS IS AND WITHOUT ANY EXPRESS OR
23 #IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
24 #WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
25 #
26 #Python port from MIT Kerberos lib/crypto/dk/stringtokey.c by Stefan
   Roggensack
27
28 from nfold import krb5_nfold
29 from des3 import k5_des3_make_key
30 from derive import krb5_derive_key
31
32 from array import array
33 from exceptions import Exception
```

## A Kerberos String to Key Function in Python

---

```
34
35 def krb5int_dk_string_to_key(password, salt, params):
36     # construct input string (= string + salt), fold it, make_key it
37     if (params != ""):
38         raise Exception, "invalid params"
39     keybytes = 21
40     keylength = 24
41
42     foldkey = k5_des3_make_key(krb5_nfold(password + salt, keybytes)
43                               , keylength)
44     # now derive the key from this one
45     key = krb5_derive_key(foldkey, 'kerberos')
46     return key
```

---

### **nfold.py:**

---

```
1 #!/usr/bin/env python2.5
2 #Copyright (C) 1998 by the FundsXpress, INC.
3 #
4 #All rights reserved.
5 #
6 #Export of this software from the United States of America may require
7 #a specific license from the United States Government. It is the
8 #responsibility of any person or organization contemplating export to
9 #obtain such a license before exporting.
10 #
11 #WITHIN THAT CONSTRAINT, permission to use, copy, modify, and
12 #distribute this software and its documentation for any purpose and
13 #without fee is hereby granted, provided that the above copyright
14 #notice appear in all copies and that both that copyright notice and
15 #this permission notice appear in supporting documentation, and that
16 #the name of FundsXpress. not be used in advertising or publicity
    pertaining
17 #to distribution of the software without specific, written prior
18 #permission. FundsXpress makes no representations about the
    suitability of
19 #this software for any purpose. It is provided "as is" without express
20 #or implied warranty.
21 #
22 #THIS SOFTWARE IS PROVIDED ‘‘AS IS AND WITHOUT ANY EXPRESS OR
```

## A Kerberos String to Key Function in Python

---

```
23 #IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
24 #WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
25 #
26 #Python port from MIT Kerberos lib/crypto/nfold.c by Stefan Roggensack
27
28 from array import array
29
30 def leastCommonMultiple(a,b):
31     """
32     Compute the Least Common Multiple (lcm) of two numbers.
33     Using the euclidean algorithm
34     """
35     temp = a*b
36     while(b != 0):
37         c = b
38         b = a%b
39         a = c
40     return temp/a
41
42 def krb5_nfold(password, outlength):
43     """
44     n-fold(k-bits):
45     l = lcm(n,k)
46     r = l/k
47     s = k-bits | k-bits rot 13 | k-bits rot 13*2 | ... | k-bits rot
48         13*(r-1)
49     compute the 1's complement sum:
50     n-fold = s[0..n-1]+s[n..2n-1]+s[2n..3n-1]+...+s[(k-1)*n..k*n-1]
51     """
52     if isinstance(password, str):
53         # Use a Array of ordinal Numbers (this should only be lower
54         # then 256)
55         password = array('B', map(ord, password))
56     inlength = len(password)
57
58     # first compute lcm(n,k)
59     lcm = leastCommonMultiple(inlength, outlength)
60     # now do the real work
```

```
61     byte = 0
62     out = array('B', chr(0)*outlength)
63
64     # this will end up cycling through k lcm(k,n)/k times, which
65     # is correct
66     for i in xrange(lcm-1,-1,-1):
67         #compute the msbit in k which gets added into this byte
68         msbit = (#first, start with the msbit in the first, unrotated
69                 byte
70                 ((inlength<<3)-1)
71                 # then, for each byte, shift to the right for each
72                 repetition
73                 + (((inlength<<3)+13)*(i/inlength))
74                 # last, pick out the correct byte within that shifted
75                 repetition
76                 +((inlength-(i%inlength))<<3)
77                 )%(inlength<<3)
78         # pull out the byte value itself
79         byte += (((password[((inlength-1)-(msbit>>3))%inlength]<<8)|
80                 (password[((inlength)-(msbit>>3))%inlength]))
81                 >>((msbit&7)+1))&0xff
82
83         # do the addition
84         byte += out[i%outlength]
85         out[i%outlength] = byte&0xff
86
87         # keep around the carry bit, if any
88         byte >>= 8
89
90     # if there's a carry bit left over, add it back in
91     if byte != 0:
92         for i in xrange(outlength-1,0,-1):
93             # do the addition
94             byte += out[i]
95             out[i] = byte&0xff
96
97             # keep around the carry bit, if any
98             byte >>= 8
99     return out.tostring()
```

---

des3.py:

---

```
1 #!/usr/bin/env python2.5
2 #Copyright (C) 1998 by the FundsXpress, INC.
3 #
4 #All rights reserved.
5 #
6 #Export of this software from the United States of America may require
7 #a specific license from the United States Government. It is the
8 #responsibility of any person or organization contemplating export to
9 #obtain such a license before exporting.
10 #
11 #WITHIN THAT CONSTRAINT, permission to use, copy, modify, and
12 #distribute this software and its documentation for any purpose and
13 #without fee is hereby granted, provided that the above copyright
14 #notice appear in all copies and that both that copyright notice and
15 #this permission notice appear in supporting documentation, and that
16 #the name of FundsXpress. not be used in advertising or publicity
       pertaining
17 #to distribution of the software without specific, written prior
18 #permission. FundsXpress makes no representations about the
       suitability of
19 #this software for any purpose. It is provided "as is" without express
20 #or implied warranty.
21 #
22 #THIS SOFTWARE IS PROVIDED "AS IS AND WITHOUT ANY EXPRESS OR
23 #IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
24 #WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
25 #
26 #Python port from MIT Kerberos lib/crypto/enc_provider/des3.c by Stefan
       Roggensack
27
28 from array import array
29 from exceptions import Exception
30 from ncrypt.cipher import EncryptCipher, DecryptCipher, CipherType
31
32 from f_parity import mit_des_fixup_key_parity
33
34 def k5_des3_make_key(random, keylength):
35     if (keylength != 24):
```

## A Kerberos String to Key Function in Python

---

```
36     raise Exception, 'KRB5_BAD_KEYSIZE'
37     if (len(random) != 21):
38         raise Exception, 'KRB5_CRYPTO_INTERNAL'
39     key = array('B', [0]*keylength)
40     if isinstance(random, str):
41         # Use a Array of ordinal Numbers (this should only be lower
42         then 256)
43         random = array('B', map(ord, random))
44     # take the seven bytes, move them around into the top 7 bits of the
45     # 8 key bytes, then compute the parity bits. Do this three times.
46     for i in xrange(0,3):
47         key[i*8:i*8+7] = random[i*7:i*7+7]
48         key[i*8+7] = (((key[i*8]&1)<<1) |
49                       ((key[i*8+1]&1)<<2) |
50                       ((key[i*8+2]&1)<<3) |
51                       ((key[i*8+3]&1)<<4) |
52                       ((key[i*8+4]&1)<<5) |
53                       ((key[i*8+5]&1)<<6) |
54                       ((key[i*8+6]&1)<<7))
55         mit_des_fixup_key_parity(key)
56     return key.tostring()
57
58 def encrypt(key, iv, plain_text):
59     cipherType = CipherType('DES-EDE3', 'CBC')
60     enc = EncryptCipher(cipherType, key, iv)
61     cipher_text = enc.finish(plain_text)
62     return cipher_text
```

---

derive.py:

---

```
1 #!/usr/bin/env python2.5
2 #Copyright (C) 1998 by the FundsXpress, INC.
3 #
4 #All rights reserved.
5 #
6 #Export of this software from the United States of America may require
7 #a specific license from the United States Government. It is the
8 #responsibility of any person or organization contemplating export to
9 #obtain such a license before exporting.
10 #
```

## A Kerberos String to Key Function in Python

---

```
11 #WITHIN THAT CONSTRAINT, permission to use, copy, modify, and
12 #distribute this software and its documentation for any purpose and
13 #without fee is hereby granted, provided that the above copyright
14 #notice appear in all copies and that both that copyright notice and
15 #this permission notice appear in supporting documentation, and that
16 #the name of FundsXpress. not be used in advertising or publicity
    pertaining
17 #to distribution of the software without specific, written prior
18 #permission. FundsXpress makes no representations about the
    suitability of
19 #this software for any purpose. It is provided "as is" without express
20 #or implied warranty.
21 #
22 #THIS SOFTWARE IS PROVIDED ‘‘AS IS AND WITHOUT ANY EXPRESS OR
23 #IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
24 #WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
25 #
26 #Python port from MIT Kerberos lib/crypto/enc_provider/des3.c by Stefan
    Roggensack
27
28 from array import array
29 from exceptions import Exception
30
31 from nfold import krb5_nfold
32 from des3 import encrypt, k5_des3_make_key
33
34 def krb5_derive_key(inkey, in_constant):
35     blocksize = 8
36     keybytes = 21
37     keylength = 24
38     rawkey = array('B')
39
40     if len(inkey) != keylength:
41         raise Exception, 'KRB5_CRYPT0_INTERNAL'
42
43     # initialize the input block
44     out = in_constant if (len(in_constant) == blocksize) else
        krb5_nfold(in_constant, blocksize)
45
46     # loop encrypting the blocks until enough key bytes are generated
```

## A Kerberos String to Key Function in Python

---

```
47     for n in xrange(0, keybytes, blocksize):
48         out = encrypt(inkey, chr(0)*8, out)[:blocksize]
49
50         if ((keybytes - n) <= 8):
51             rawkey.fromstring(out[:keybytes - n])
52         else:
53             rawkey.fromstring(out)
54
55     # postprocess the key
56     return k5_des3_make_key(rawkey, keylength)
```

---

### fparity.py:

---

```
1  #!/usr/bin/env python2.5
2  #These routines check and fix parity of encryption keys for the DES
3  #algorithm.
4  #
5  #They are a replacement for routines in key_parity.c, that don't
   require
6  #the table building that they do.
7  #Mark Eichin -- Cygnus Support
8  #
9  #Python port from MIT Kerberos lib/crypto/des/f_parity.c by Stefan
   Roggensack
10
11 def mit_des_fixup_key_parity(key):
12     """
13     des_fixup_key_parity: Forces odd parity per byte; parity is bits
14     8,16,...64 in des order, implies 0, 8, 16, ... vax order.
15     """
16     for i in xrange(0, len(key)):
17         key[i] &= 0xfe
18         key[i] |= 1^pstep(pstep(pstep((key[i]), 4), 2), 1)
19
20     return key
21 def parity_char(x):
22     return pstep(pstep(pstep((x), 4), 2), 1)
23 def pstep(x, step):
24     return (((x)&smask(step))^(((x)>>step)&smask(step)))
25 def smask(step):
```

```
26     return ((1<<step)-1)
```

---

**nfoldtests.py:**

---

```
1  #!/usr/bin/env python2.5
2  from nfold import krb5_nfold
3  import binascii
4  import unittest
5
6  class rfc3961_nfold(unittest.TestCase):
7      def test1(self):
8          #         64-fold("012345") =
9          #         64-fold(303132333435) = be072631276b1955
10         self.assertEqual(krb5_nfold(unicode.encode(u'012345')), 64/8),
11                          binascii.unhexlify('be072631276b1955'))
12
13     def test2(self):
14         #         56-fold("password") =
15         #         56-fold(70617373776f7264) = 78a07b6caf85fa
16         self.assertEqual(krb5_nfold(unicode.encode(u'password')), 56/8),
17                          binascii.unhexlify('78a07b6caf85fa'))
18
19     def test3(self):
20         #         64-fold("Rough Consensus, and Running Code") =
21         #         64-fold(526f75676820436f6e73656e7375732c20616e642052756e
22         #         6e696e6720436f6465) = bb6ed30870b7f0e0
23         self.assertEqual(krb5_nfold(unicode.encode(u'Rough Consensus,
24         and Running Code')), 64/8),
25                          binascii.unhexlify('bb6ed30870b7f0e0'))
26
27     def test4(self):
28         #         168-fold("password") =
29         #         168-fold(70617373776f7264) =
30         #         59e4a8ca7c0385c3c37b3f6d2000247cb6e6bd5b3e
31         self.assertEqual(krb5_nfold(unicode.encode(u'password')),
32                          168/8),
33                          binascii.unhexlify('59e4a8ca7c0385c3c37b3f6d2000247cb6e6bd5b3e'))
34
35     def test5(self):
36         #         192-fold("MASSACHVSETTS INSTITVTE OF TECHNOLOGY")
```

## A Kerberos String to Key Function in Python

---

```
31 # 192-fold(4d41535341434856534554545320494e5354495456544520
32 # 4f4620544543484e4f4c4f4759) =
33 # db3b0d8f0b061e603282b308a50841229ad798fab9540c1b
34 self.assertEqual(krb5_nfold(unicode.encode(u'MASSACHVSETTS
    INSTITVTE OF TECHNOLOGY'), 192/8),
    binascii.unhexlify('db3b0d8f0b061e603282b308a50841229ad798fab9540c1b'))
35
36 def test6(self):
37 # 168-fold("Q") =
38 # 168-fold(51) =
39 # 518a54a2 15a8452a 518a54a2 15a8452a
40 # 518a54a2 15
41 self.assertEqual(krb5_nfold(unicode.encode(u'Q'), 168/8),
    binascii.unhexlify('518a54a215a8452a518a54a215a8452a518a54a215'))
42
43 def test7(self):
44 # 168-fold("ba") =
45 # 168-fold(6261) =
46 # fb25d531 ae897449 9f52fd92 ea9857c4
47 # ba24cf29 7e
48 self.assertEqual(krb5_nfold(unicode.encode(u'ba'), 168/8),
    binascii.unhexlify('fb25d531ae8974499f52fd92ea9857c4ba24cf297e'))
49
50 def test8(self):
51 # 64-fold("kerberos") =
52 # 6b657262 65726f73
53 self.assertEqual(krb5_nfold(unicode.encode(u'kerberos'), 64/8),
    binascii.unhexlify('6b65726265726f73'))
54
55 def test9(self):
56 # 128-fold("kerberos") =
57 # 6b657262 65726f73 7b9b5b2b 93132b93
58 self.assertEqual(krb5_nfold(unicode.encode(u'kerberos'),
    128/8),
    binascii.unhexlify('6b65726265726f737b9b5b2b93132b93'))
59
60 def test10(self):
61 # 168-fold("kerberos") =
62 # 8372c236 344e5f15 50cd0747 e15d62ca
63 # 7a5a3bce a4
```

## A Kerberos String to Key Function in Python

---

```
64     self.assertEqual(krb5_nfold(unicode.encode(u'kerberos'),
65                          168/8),
66                          binascii.unhexlify('8372c236344e5f1550cd0747e15d62ca7a5a3bcea4'))
67
68     def test11(self):
69         #     256-fold("kerberos") =
70         #         6b657262 65726f73 7b9b5b2b 93132b93
71         #         5c9bdcda d95c9899 c4cae4de e6d6cae4
72
73     self.assertEqual(krb5_nfold(unicode.encode(u'kerberos'),
74                          256/8),
75                          binascii.unhexlify('6b65726265726f737b9b5b2b93132b935c9bdcdad95c9899c4ca
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
2645
2646
2647
2648
2649
2650
2651
2652
2653
2654
2655
2656
2657
2658
2659
2660
2661
2662
2663
2664
2665
2666
2667
2668
2669
2670
2671
2
```

```
23     key=      "6d2fcdf2d6fbbc3ddcadb5da5710a23489b0d3b69d5d9d4a"
24     self.assertEqual(krb5int_dk_string_to_key(passwd, salt, ''),
25                      binascii.unhexlify(key))
26     def test4(self):
27         salt=  u"ATHENA.MIT.EDUJuri\u0161i\u0107".encode('utf8')
28         passwd= u"\u00DF".encode('utf8')
29         key=      "16d5a40e1ce3bacb61b9dce00470324c831973a7b952feb0"
30         self.assertEqual(krb5int_dk_string_to_key(passwd, salt, ''),
31                          binascii.unhexlify(key))
32     def test5(self):
33         salt=  "EXAMPLE.COMpianist".encode('utf8')
34         passwd= u"\u0834\u0DD1E".encode('utf8')
35         key=      "85763726585dbc1cce6ec43e1f751f07f1c4cbb098f40b19"
36         self.assertEqual(krb5int_dk_string_to_key(passwd, salt, ''),
37                          binascii.unhexlify(key))
38
39     # A.3.  DES3 DR and DK
40     def test6(self):
41         key=
42             "dce06b1f64c857a11c3db57c51899b2cc1791008ce973b92"
43         usage=      "0000000155"
44         DR=
45             "935079d14490a75c3093c4a6e8c3b049c71e6ee705"
46         DK=
47             "925179d04591a79b5d3192c4a7e9c289b049c71f6ee604cd"
48
49         self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
50                                     binascii.unhexlify(usage)),
51                          binascii.unhexlify(DK))
52
53     def test7(self):
54         key=
55             "5e13d31c70ef765746578531cb51c15bf11ca82c97cee9f2"
56         usage=      "00000001aa"
57         DR=
58             "9f58e5a047d894101c469845d67ae3c5249ed812f2"
59         DK=
60             "9e58e5a146d9942a101c469845d67a20e3c4259ed913f207"
```

```
55     self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
56                             binascii.unhexlify(usage)),
57                             binascii.unhexlify(DK))
58
59 def test8(self):
60     key=
61         "98e6fd8a04a4b6859b75a176540b9752bad3ecd610a252bc"
62     usage=
63         "0000000155"
64     DR=
65         "12fff90c773f956d13fc2ca0d0840349dbd39908eb"
66     DK=
67         "13fef80d763e94ec6d13fd2ca1d085070249dad39808eabf"
68     self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
69                             binascii.unhexlify(usage)),
70                             binascii.unhexlify(DK))
71
72 def test9(self):
73     key=
74         "622aec25a2fe2cad7094680b7c64940280084c1a7cec92b5"
75     usage=
76         "00000001aa"
77     DR=
78         "f8debf05b097e7dc0603686aca35d91fd9a5516a70"
79     DK=
80         "f8dfbf04b097e6d9dc0702686bcb3489d91fd9a4516b703e"
81
82     self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
83                             binascii.unhexlify(usage)),
84                             binascii.unhexlify(DK))
85
86 def test10(self):
87     key=
88         "d3f8298ccb166438dcb9b93ee5a7629286a491f838f802fb"
89     usage=
90         "6b65726265726f73"
91     DR=
92         "2270db565d2a3d64cfbfdc5305d4f778a6de42d9da"
93     DK=
94         "2370da575d2a3da864cebfdc5204d56df779a7df43d9da43"
95
96     self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
97                             binascii.unhexlify(usage)),
```

```
82         binascii.unhexlify(DK))
83
84     def test11(self):
85         key=
86             "c1081649ada74362e6a1459d01dfd30d67c2234c940704da"
87         usage=
88             "0000000155"
89         DR=
90             "348056ec98fcc517171d2b4d7a9493af482d999175"
91         DK=
92             "348057ec98fdc48016161c2a4c7a943e92ae492c989175f7"
93
94     self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
95         binascii.unhexlify(usage)),
96         binascii.unhexlify(DK))
97
98     def test12(self):
99         key=
100             "5d154af238f46713155719d55e2f1f790dd661f279a7917c"
101         usage=
102             "00000001aa"
103         DR=
104             "a8818bc367dadacbe9a6c84627fb60c294b01215e5"
105         DK=
106             "a8808ac267dada3dcbe9a7c84626fbc761c294b01315e5c1"
107
108     self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
109         binascii.unhexlify(usage)),
110         binascii.unhexlify(DK))
111
112     def test13(self):
113         key=
114             "798562e049852f57dc8c343ba17f2ca1d97394efc8adc443"
115         usage=
116             "0000000155"
117         DR=
118             "c813f88b3be2b2f75424ce9175fbc8483b88c8713a"
119         DK=
120             "c813f88a3be3b334f75425ce9175fbe3c8493b89c8703b49"
121
122     self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
123         binascii.unhexlify(usage)),
124         binascii.unhexlify(DK))
```

```
110
111     def test14(self):
112         key=
113             "26dce334b545292f2feab9a8701a89a4b99eb9942cecd016"
114         usage=
115             "00000001aa"
116         DR=
117             "f58efc6f83f93e55e695fd252cf8fe59f7d5ba37ec"
118         DK=
119             "f48ffd6e83f83e7354e694fd252cf83bfe58f7d5ba37ec5d"
120
121         self.assertEqual(krb5_derive_key(binascii.unhexlify(key),
122                                     binascii.unhexlify(usage)),
123                         binascii.unhexlify(DK))
124
125 if __name__=="__main__":
126     unittest.main()
```

---

### Tests.py:

---

```
1 import unittest
2
3 from StringToKeyTests import rfc3961_StringToKey
4 from nfoldtests import rfc3961_nfold
5
6 suite1 = unittest.makeSuite(rfc3961_StringToKey, 'test')
7 suite2 = unittest.makeSuite(rfc3961_nfold, 'test')
8 alltests = unittest.TestSuite((suite1, suite2))
9 unittest.main()
```

---

## **B Abkürzungen**

|              |                                       |
|--------------|---------------------------------------|
| <i>A</i>     | Alice                                 |
| <b>AES</b>   | Advanced Encryption Standard          |
| <i>AS</i>    | Authentication Server                 |
| <b>ASN.1</b> | Abstract Syntax Notation One          |
| <i>B</i>     | Bob                                   |
| <b>DES</b>   | Data Encryption Standard              |
| <b>IETF</b>  | Internet Engineering Task Force       |
| <b>KDC</b>   | Key Distribution Center               |
| <b>KRB5</b>  | Kerberos 5                            |
| <b>LDAP</b>  | Lightweight Directory Access Protocol |
| <b>MIT</b>   | Massachusetts Institute of Technology |
| <b>NFS</b>   | Network File System                   |
| <b>SSH</b>   | Secure Shell                          |
| <b>TGS</b>   | Ticket Granting Server                |
| <b>TGT</b>   | Ticket Granting Ticket                |
| <i>X</i>     | Eve                                   |

## C Literaturverzeichnis

- [BMB<sup>+</sup>05] BLESS, Roland ; MINK, Stefan ; BLASS, Erik-Oliver ; CONRAD, Michael ; HOF, Hans-Joachim ; KUTZNER, Kendy ; SCHÖLLER, Marcus: *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen*. Berlin Heidelberg New-York : Springer, 2005. – ISBN 978-3-54021-845-6
- [CJT<sup>+</sup>06] CERVESATO, Iliano ; JAGGARD, Aaron D. ; TSAY, Joe-Kai ; SCEDROV, Andre ; WALSTAD, Christopher: Breaking and Fixing Public-Key Kerberos. In: OKADA, Mitsu (Hrsg.) ; SATOH, Ichiro (Hrsg.): *Eleventh Annual Asian Computing Science Conference — ASIAN'06*. Tokyo, Japan, 6–8 December 2006 <http://theory.stanford.edu/~iliano/papers/asian06.pdf>, 164–178
- [DS81] DENNING, Dorothy E. ; SACCO, Giovanni M.: Timestamps in key distribution protocols. In: *Commun. ACM* 24 (1981), Nr. 8, S. 533–536. – ISSN 0001-0782
- [Eck01] ECKERT, Claudia: *IT-Sicherheit*. München : Oldenbourg, 2001. – ISBN 978-3-48657-851-5
- [Gar03] GARMAN, Jason: *Kerberos: The Definitive Guide*. Sebastopol : O'Reilly Media, 2003. – ISBN 978-0-59600-403-3
- [KNT91] KOHL, John ; NEUMAN, Clifford ; TS'O, Theodore: The Evolution of the Kerberos Authentication Service. In: *Proceedings of the Spring 1991 EurOpen Conference*, 1991 [ftp://athena-dist.mit.edu/pub/kerberos/doc/krb\\_evol.PS](ftp://athena-dist.mit.edu/pub/kerberos/doc/krb_evol.PS)
- [NS78] NEEDHAM, Roger M. ; SCHROEDER, Michael D.: Using encryption for authentication in large networks of computers. In: *Commun. ACM* 21 (1978), Nr. 12, S. 993–999. – ISSN 0001-0782
- [NT94] NEUMAN, Clifford ; TS'O, Theodore: Kerberos: An Authentication Service for Computer Networks. In: *IEEE Communications Magazine* 32 (1994), Nr. 9, 33–38. <http://gost.isi.edu/publications/kerberos-neuman-tso.html>

- [RFC3961] RAEBURN, K.: *Encryption and Checksum Specifications for Kerberos 5*. RFC 3961 (Proposed Standard). <http://www.ietf.org/rfc/rfc3961.txt>. Version: Februar 2005 (Request for Comments)
- [RFC4120] NEUMAN, C. ; YU, T. ; HARTMAN, S. ; RAEBURN, K.: *The Kerberos Network Authentication Service (V5)*. RFC 4120 (Proposed Standard). <http://www.ietf.org/rfc/rfc4120.txt>. Version: Juli 2005 (Request for Comments). – Updated by RFCs 4537, 5021
- [RFC4537] ZHU, L. ; LEACH, P. ; JAGANATHAN, K.: *Kerberos Cryptosystem Negotiation Extension*. RFC 4537 (Proposed Standard). <http://www.ietf.org/rfc/rfc4537.txt>. Version: Juni 2006 (Request for Comments)
- [RFC4556] ZHU, L. ; TUNG, B.: *Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)*. RFC 4556 (Proposed Standard). <http://www.ietf.org/rfc/rfc4556.txt>. Version: Juni 2006 (Request for Comments)
- [RFC5021] JOSEFSSON, S.: *Extended Kerberos Version 5 Key Distribution Center (KDC) Exchanges over TCP*. RFC 5021 (Proposed Standard). <http://www.ietf.org/rfc/rfc5021.txt>. Version: August 2007 (Request for Comments)
- [RM03] REIMER, Stan ; MULCARE, Mike: *Active Directory for Microsoft Windows Server 2003*. Redmond : Microsoft Press, 2003. – ISBN 978-0-73561-577-9