Universität Mannheim
Fakultät für Mathematik und Informatik
Lehrstuhl für Praktische Informatik IV
Professor Dr. W. Effelsberg

Hauptdiplomklausur Informatik

September 1995 Teil: Verteilte Betriebssysteme (Gastvorlesung Dr. J. Schneider)

Name: ..... Vorname: .....

Matrikel-Nr.: ..... Semester: ..... Fach: .....

Hinweise:

a) Bitte füllen Sie sofort den Kopf des Deckblatts aus.

b) Überprüfen Sie Ihr Klausurexamplar auf Vollständigkeit (6 Seiten).

c) Tragen Sie Ihre Lösungen soweit möglich direkt in die Klausur ein.

d) Als Hilfsmittel sind nur nicht-programmierbare Taschenrechner zugelassen.

e) Zeit: 33 Minuten

Aufgabe	max. Punktezahl	Punkte
1	13	
2	10	
3	10	
Summe	33	

Aufgabe 1 [13 Punkte] *Dateiverwaltung*

a) [4 Punkte] Erklären Sie den Begriff "Globales Verzeichnis" für verteilte Dateisysteme und was die Begriffe "Namenstransparenz", "Ortstransparenz" und "Leistungstransparenz" für verteilte Dateisysteme bedeuten.

b) [6 Punkte] Erklären Sie die Zugriffssemantik bei parallelen Dateizugriffen in verteilten UNIX-Systemen ("UNIX-Semantik"). Was ist der Unterschied zur "Session-Semantik" und zur "Transaction-Semantik"?

c) [3 Punkte] Erklären Sie die Begriffe “stateful server“ und “stateless server“ im Zusammenhang mit verteilten Dateisystemen. Nennen Sie je einen Vorteil für diese beiden Verfahren.

Aufgabe 2 [10 Punkte] *Prozeßverwaltung*

a) [6 Punkte] Erklären Sie den Unterschied zwischen "Tasks" und "Threads".

b) [4 Punkte] Beschreiben Sie die Funktionsweise der UNIX Systembefehle "fork" und "join" (ggf. Skizze).

Aufgabe 3 [10 Punkte] *Sicherheit (kryptographische Verfahren)*

a) [1 Punkte] Was bedeutet der Begriff "Authentifizierung"?

b) [4 Punkte] Erklären Sie kurz die Funktionsweisen "symmetrischer" ("private key") und "asymmetrischer" ("public key") Verfahren.

c) [5 Punkte] Ein asymmetrisches Verfahren kann zum Zwecke der Authentifizierung eingesetzt werden. Im folgenden Kommunikationsablauf ist hierbei jedoch eine Zeile fehlerhaft. Markieren Sie die fehlerhafte Zeile und geben Sie an, wie sie richtig lauten müßte.

P $\rightarrow$ Q	:	"Ich bin P."
Q $\rightarrow$ P	:	n
P	:	berechne $n' = \{n\}_{kp-1}$
P $\rightarrow$ Q	:	n'
Q $\rightarrow$ A	:	"Gib P's public key"
A	:	berechne $c = \{P, kp\}_{ka-1}$
A $\rightarrow$ Q	:	P, c
Q	:	ermittle $\{P, kp\}$ aus c mittels ka überprüfe $n = \{n'\}_{kp-1}$

P, Q	Prozesse
A	Authentifizierungs-Server
n	"nonce"
kp	öffentlicher Schlüssel von P
$kp-1$	geheimer Schlüssel von P
ka	öffentlicher Schlüssel von A
$ka-1$	geheimer Schlüssel von A
$\{m\}_k$	Schlüssel k angewandt auf Nachricht m