Distributed Systems

RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Klausur
“Sichere Verteilte Systeme”
SS 2008

Name, Vorname: _____

Matrikelnummer: _____

Studiengang: _____

Zur Beachtung:

- Die Klausur besteht aus 7 Aufgaben, 2 Bonusaufgaben und 19 Seiten.
- Schreiben Sie **auf jedes Blatt** Ihrer Lösungen Ihre Matrikelnummer.
- Bitte legen Sie Ihren Personal- und Studentenausweis auf den Tisch, damit wir die Überprüfung ohne Störung während der Klausur durchführen können.
- Es dürfen keine weiteren Hilfsmittel verwendet werden.
- Schreiben Sie Ihre Lösungen – soweit möglich – nur in die entsprechenden Stellen der Aufgabenblätter.
- Unterpunkte der Aufgaben können unabhängig voneinander gelöst werden.
- Die Klausur dauert 90 Minuten und es gibt insgesamt 100 (90 + 10 Bonus) Punkte.

Ich bestätige, dass ich die Klausur selbstständig bearbeitet habe.

_____

(Unterschrift)

Punkte:

Aufgabe	1 (10 P)	2 (18 P)	3 (18 P)	4 (11 P)	5 (11 P)	6 (13 P)	7 (9 P)	**Σ (90 P)**	Bonus (10 P)	**Σ + Bonus (100 P)**	**Note**
Punkte											
Kürzel											

Matrikelnummer:_____

Aufgabe 1: Allgemeine Grundlagen (6 + 4 = 10 Punkte)

a) Für das Design von Kommunikationsprotokollen gibt es zum einen das ISO/OSI-Referenzmodell, zum anderen das Internet-Referenzmodell. Worin liegen die *Gemeinsamkeiten* und *Unterschiede* der beiden Modelle? Welche *Gründe* sprechen für die Änderungen des Internet-Referenzmodells gegenüber dem ISO/OSI-Referenzmodell?

Matrikelnummer:_____

b) Beschreiben Sie knapp die *Aufgaben der Sicherungsschicht*. Was ist der wesentliche *Unterschied* zur physikalischen Schicht?

Matrikelnummer:_____

Aufgabe 2: Lokale Netze
(1 + 2 + 3 + 4 + 6 + 2 = 18 Punkte)

a) Worin unterscheiden sich *Brücken („Bridge“)* und *Router* bei der Kopplung von Netzen?

b) Nennen Sie *zwei Vorteile* der Token Ring Technologie im Vergleich zu Ethernet und erläutern Sie kurz, wie diese erzielt werden.

c) Sei eine (nicht sehr leistungsfähige) digitale Datenleitung gegeben, bei der maximal 500mal pro Sekunde ein Pegelwechsel durchgeführt werden kann. *Wie hoch ist die maximal erreichbare Datenrate (in bit/s) für die folgenden Kodierungsmethoden*:

1. Differentieller Manchester-Code
2. 4B/5B-Code
3. NRZ-Code

Matrikelnummer:_____

d) Berechnen Sie für die Bitfolge „101101“ die *CRC-Prüfsumme* mit dem Generatorpolynom $G(x) = x^3 + x^2 + 1$. Wie sieht die zu übertragende Bitfolge aus?

e) Ethernet beruht auf dem Zugriffsverfahren *CSMA/CD*. Wofür steht diese Abkürzung und wie funktioniert das Verfahren? Warum gibt es eine Mindestlänge für übertragene Rahmen?

Matrikelnummer:_____

f) Angenommen Sie setzen in ihrem LAN eine *Brücke* ein. Alle Rechner auf beiden Seiten der *Brücke* befinden sich im gleichen IP-(Sub)Netz. Sollte die *Brücke* Broadcast-Nachrichten zwischen den Segmenten durchlassen? Begründen Sie kurz Ihre Antwort.

Matrikelnummer:_____

Aufgabe 3: Das Internet-Protokoll (3 + 8 + 1 + 6 = 18 Punkte)

a) Benennen Sie mindestens drei elementare Unterschiede zwischen *IPv4* und *IPv6*.

b) Sie haben den IP-Adressbereich 134.2.8.0/22 zugewiesen bekommen und sollen das Netzwerk Ihres Unternehmens mit diesen IP-Adressen konfigurieren. Dieses Netzwerk soll in *5 Subnetze* unterteilt werden. Welche *Subnetz-Maske* wählen Sie zur effizienten Aufteilung des Adressraums (mit Begründung)? Geben Sie für diese Subnetze den daraus *resultierenden Adressraum* an.

Matrikelnummer:_____

c) Was versteht man unter sogenannten „*privaten Adressen*“ bei IP?

d) Ein Router empfange ein IP-Paket mit einer Gesamtlänge von 1500 Byte. Er ist allerdings nur in der Lage, Pakete mit einer Gesamtlänge von 480 Byte zu versenden. Skizzieren Sie den daraufhin eintretenden *Fragmentierungsprozess* und geben Sie die enstandenden Fragmente mit ihrer Länge an. Woran erkennt der Empfänger, dass eine Fragmentierung stattgefunden ist?

Matrikelnummer:_____

Aufgabe 4: Routing (4 + 3 + 4 = 11 Punkte)

a) Beschreiben Sie die Funktion sowie die Vor- und Nachteile der *Leitungs- bzw. Paketvermittlung*.

b) Erläutern Sie kurz den Zweck und die Funktionsweise des *ARP-Protokolls*. Auf welcher Schicht arbeitet es?

Matrikelnummer:_____

c) Was ist der Hauptunterschied zwischen *Distance Vector* und *Link State* Routing? Nennen Sie die Vor- und Nachteile beider Verfahren.

Matrikelnummer:_____

Aufgabe 5: TCP (2 + 4 + 2 + 3 = 11 Punkte)

a) Beschreiben Sie kurz das Verfahren beim *Aufbau* einer TCP-Verbindung.

b) Skizzieren Sie mögliche *Fehlersituationen* der Datenübertragung durch IP und beschreiben Sie kurz, wie TCP diese behebt.

Matrikelnummer:_____

c) Angenommen, die Round-Trip-Time (d.h. die Laufzeit eines Signals vom Sender zum Empfänger und zurück) betrage 200ms und die TCP-Fenstergröße der kommunizierenden Prozesse sei durch 25000 Byte limitiert. Welche *maximale Übertragungsrate (Byte/s)* könnte in dieser Situation erreicht werden?

d) Skizzieren Sie kurz den *Slow-Start-Algorithmus* in TCP. Wozu wir er verwendet?

Matrikelnummer:_____

Aufgabe 6: Kryptographie (3 + 8 + 2 = 13 Punkte)

In der Kryptographie unterscheidet man generell zwischen symmetrischen und asymmetrischen Verfahren.

a) Da bei dem symmetrischen Verfahren DES die Schlüssellänge zu gering ist, wurde 3DES eingeführt. DES wird drei Mal angewendet, wobei bei der ersten und dritten Anwendung mit einem Schlüssel k_1 verschlüsselt wird, in der zweiten Anwendung allerdings wird mit einem Schlüssel k_2 entschlüsselt. *Warum wählt man bei der zweiten Anwendung eine Entschlüsselung und keine Verschlüsselung?*

b) Ein bekanntes asymmetrisches Verfahren ist *RSA*. Sie belauschen eine per RSA gesicherte Kommunikation und erhalten den verschlüsselten Text c = 3. Der öffentliche Schlüssel, der zur Verschlüsselung verwendet wurde, ist <e = 29, n = 91>. *Ermitteln Sie den zugehörigen privaten Schlüssel und dekodieren Sie die Nachricht.*

Matrikelnummer:_____

c) Sie verwenden *Diffie-Hellman*, um einen Schlüsselaustausch über das Internet vorzunehmen. Können Sie auf diese Weise zuverlässig einen Schlüssel für z.B. AES vereinbaren (mit Begründung)?

Matrikelnummer:_____

Aufgabe 7: Sichere Internet-Protokolle (6 + 3 = 9 Punkte)

Um eine sichere Kommunikation mit Internet-Protokollen zu erreichen, gibt es einerseits IPsec, andererseits SSL/TLS.

a) Welche *Sicherheitsfunktionen* sind bei *IPSec* definiert? Wie werden sie in das normale IP-Protokoll integriert?

b) Was ist der *wesentliche Unterschied* zwischen IPsec und SSL/TLS?

Matrikelnummer:_____

Bonusaufgaben
(5 + 5 = 10 Punkte)

Um die Klausur zu bestehen, müssen Sie genügend Punkte in den Aufgaben 1-7 erreichen. Mit diesen zusätzlichen Bonusaufgaben können Sie Ihre Note verbessern.

Bonusaufgabe 1: TCP Kanaleffizienz

Gegeben sei ein Übetragungskanal mit 1 Gbit/s Bandbreite und mit 1ms Round-Trip-Time. Welche *Kanaleffizienz* kann bei TCP maximal erreicht werden? (Hinweis: Das TCP *Window* Header-Feld ist 16 Bit groß.)

Matrikelnummer:_____

Bonusaufgabe 2: Netzwerkkonfiguration

Sie möchten in Ihrem Unternehmen 20 Kundenterminals einrichten. Um den Administrationsaufwand jedes einzelnen Rechners zu minimieren, entscheiden Sie sich für eine Diskless-Lösung, d.h. die Rechner würden ohne Festplatte laufen und müssten nur das Betriebssystem beim Start von einem zentralen Server herunterladen. Dazu verbinden Sie zunächst alle Rechner über einen Ethernet-Switch. Welche IP-basierten *Dienste* müssen Sie auf dem zentralen Server bereitstellen, damit Ihr Netzwerk funktioniert? Begründen Sie Ihre Antwort und erläutern Sie kurz die zugrundeliegenden *Protokolle*.

Matrikelnummer:_____