ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. F. Mattern
Übung Verteilte Systeme
D-INFK
HS 2010

Theoretische Übungsserie B

Überarbeitete Version vom 24.11.2010

Bemerkungen

Diese Übungen dienen zur Vorbereitung auf die schriftliche Prüfung. Sie sind freiwillig und werden nicht korrigiert. Insgesamt gibt es zwei theoretische Übungsserien, die den Vorlesungsteil von Prof. Mattern abdecken. Eine Besprechung und Diskussion möglicher Lösungen der Übungsserie B findet im Rahmen der Vorlesung am 19. November statt.

Wenn Sie Fragen oder Anmerkungen zu den theoretischen Übungen haben, wenden Sie sich bitte an Benedikt Ostermaier (`ostermaier@inf.ethz.ch`).

B1. Lamport-Zeit

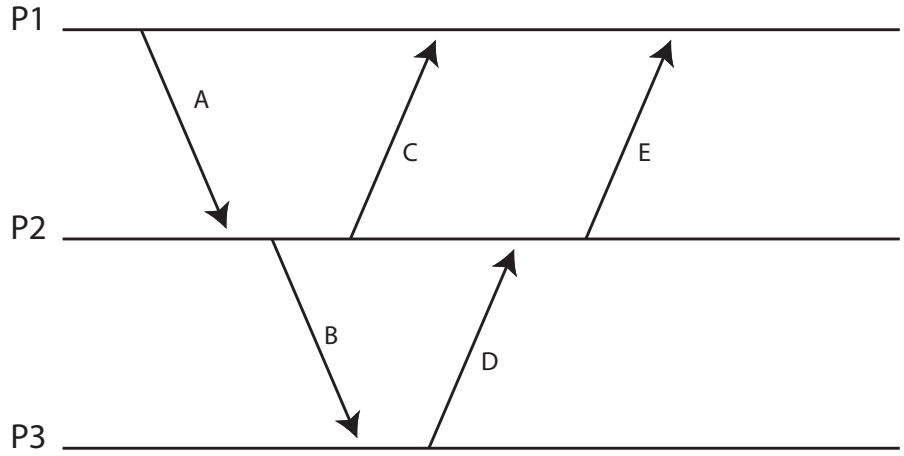

Abbildung 1: Zeitdiagramm

Im folgenden bezeichnet $\prec$ die Kausalrelation auf Ereignissen ("happened before"), C ist die Abbildung von Ereignissen auf Zeitstempel (die durch natürliche Zahlen repräsentiert werden).

1. Geben Sie ein Paar von Ereignissen aus Abb. 1 an, welche nicht kausal abhängig sind.

2. Fügen Sie in Abb. 1 eine Nachricht N ein, für die gilt

$$\text{A.receive} \prec \text{N.send} \ \wedge C(\text{N.receive}) < C(\text{E.send})$$

   wobei Sie Absender und Empfänger der Nachricht (die unterschiedlich sein sollen) frei wählen können, sofern die Bedingung erfüllt ist.

3. Fügen Sie auf ähnliche Art eine Nachricht M ein, für die gilt

$$\text{M.send} \prec \text{C.send} \ \wedge C(\text{B.receive}) < C(\text{M.receive})$$

   und die von P2 gesendet und von P3 empfangen wird.

Bemerkung: Die Notation X.send bzw. X.receive bezeichnet das *send*- bzw. *receive*-Ereignis der Nachricht X.

B2. Wechselseitiger Ausschluss mit Lamport-Zeit

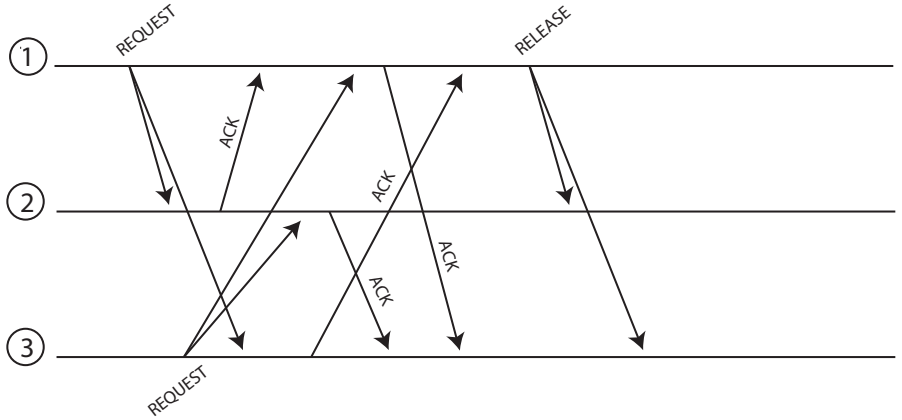

Abbildung 2: Wechselseitiger Ausschluss mit Lamport-Zeit

In Abb. 2 ist ein Zeitdiagramm dargestellt mit Nachrichten von drei Prozessen. Prozesse 1 und 3 bewerben sich um den exklusiven Zugriff auf eine gemeinsame Ressource. Die Prozesse wenden das aus der Vorlesung bekannte Verfahren zum wechselseitigen Ausschluss an, das Lamport-Zeit und verteilte Warteschlangen benutzt.

1. Geben Sie die Sende- und Empfangszeitstempel für jedes Ereignis an.
2. Geben Sie für die Prozesse 1 und 3 an, wie die Warteschlange des jeweiligen Prozesses nach jedem Sende- bzw. Empfangsereignis aussieht.
3. Sind beim Einreihen in die Warteschlange die Sende- oder die Empfangszeitstempel zu verwenden? Warum?
4. Welche Bedingung muss erfüllt sein, damit Prozess 1 auf die Ressource zugreifen kann?
5. Markieren Sie den Zeitpunkt im Zeitdiagramm, zu dem Prozess 1 bzw. Prozess 3 auf die Ressource zugreifen kann.

B3. Namen

1. Was versteht man unter dem Binden und dem Auflösen von Namen? Nennen Sie ein Beispiel für einen Dienst, der diese Operationen zur Verfügung stellt.

2. Was ist der Unterschied zwischen iterativer und rekursiver Namensauflösung?

3. Unter welchen Voraussetzungen kann Caching bei der Auflösung von Namen effizienzsteigernd eingesetzt werden?

4. Nehmen Sie an, die Abbildung von Namen auf Objektadressen wird in einem lokalen Cache eines Clients gespeichert. Ein bereits gebundener und im Cache aufgrund einer früheren Anfrage enthaltener Name wird nun an eine andere Adresse gebunden, das alte Objekt bleibt aber weiterhin aktiv.
   a) Welches Problem tritt nun beim Client auf? Kann der Client dieses Problem erkennen?
   b) Tritt das Problem auch bei solchen Clients auf, die statt der Adresse den zuständigen Nameserver im Cache halten?

5. Zur Erhöhung von Effizienz und Fehlertoleranz werden Nameserver repliziert. Für welche Nameserver ist dies besonders relevant? Begründen Sie Ihre Antwort.

B4. Client-/Server

1. Bei Web-basierten Diensten wird oft ein Bezeichner in Links codiert ("URL rewriting"), um die aktuelle Transaktion zu identifizieren. Wie könnte ein Unbefugter eine laufende Transaktion "übernehmen" und was kann man gegen diese Gefahr tun?

2. Welches Problem entsteht bei einem zustandsbehafteten Server, wenn viele Clients abstürzen, bevor sie ihre Transaktionen beendet haben?

3. Erläutern Sie kurz ein paar Vorteile von zustandslosen gegenüber zustandsbehafteten Client/Server-Protokollen und umgekehrt.

B5. Middleware

1. Wie werden in CORBA verschiedene Programmiersprachen zur Implementierung der Anwendung unterstützt? Welchen Vorteil hat die Unterstützung mehrerer Sprachen?
2. Welche Funktionen übernimmt ein Stub in CORBA?
3. Was ist der ORB? Wo wird er ausgeführt?
4. Warum wird CORBA heutzutage nicht mehr weiterentwickelt?
5. Was versteht man unter Objekt-Serialisierung? Für was wird sie benötigt? Nennen Sie ebenfalls Beispiele, wie die Serialisierung in Middlewaresystemen realisiert wird.

B6. Jini

1. Erläutern Sie kurz die Funktion von Leases.
2. Eine Besonderheit von Jini ist das Ausnutzen der Mobilität von Java-Code. Welche Code-Teile werden übertragen und welche Möglichkeiten ergeben sich dadurch?

B7. Sicherheit

1. Auf welche Herausforderungen trifft man bei der Schlüsselverteilung in verteilten Systemen?

2. Beschreiben Sie zwei mögliche Lösungsansätze zur Schlüsselverteilung.

3. In der Vorlesung wurde der Diffie-Hellman-Algorithmus besprochen.
   a) Für was wird er verwendet?
   b) Beschreiben Sie kurz das Verfahren.
   c) Was ist ein möglicher Angriff und wie könnte man sich dagegen verteidigen?

4. Wie funktioniert zertifikatsbasierte Authentifizierung? Von welchem weitverbreiteten System wird sie verwendet?

5. Wenn One-Time-Pads ein perfektes Verschlüsselungssystem darstellen, warum werden diese dann heutzutage nicht global eingesetzt?

6. Mit Einwegfunktionen lassen sich Einmalpasswörter erzeugen und leicht überprüfen. f sei eine Einwegfunktion und x_1 ein initiales Passwort, aus dem eine Passwortkette erzeugt wird:
$$x_1 \rightarrow^f x_2 \rightarrow^f \ldots \rightarrow^f x_{n-1} \rightarrow^f x_n$$
   a) Um die Passwörter zur Authentisierung nutzen zu können, muss x_n zunächst zum Server S übertragen werden. Welche der folgenden Anforderungen müssen erfüllt sein:
      i. Ein Angreifer darf nichts über x_n erfahren, die Übertragung muss also geheimnisbewahrend erfolgen.
      ii. Es muss sichergestellt sein, dass x_n bei der Übertragung nicht verändert wird.
   b) Wir nehmen an, es sei $n = 100$. Dem Server S wird x_{100} bekanntgemacht. Ein Client C schreibt die Werte $x_1, x_2, \ldots, x_{99}$ in eine Liste. Bei der ersten Anmeldung an S verwendet er x_{99} und streicht diesen Wert von der Liste. Beim zweiten Mal verwendet C aus Versehen x_{89} (statt x_{98}). Welche Gefahr besteht, wenn dieser Wert von einem Angreifer abgehört wird und S den Anmeldeversuch einfach ignoriert, weil $f(x_{89}) \neq x_{99}$?

7. Im Kerberos-Protokoll erhält ein Client vom KDC (Key Distribution Center) ein verschlüsseltes TGT (Ticket Granting Ticket). Kann dieses TGT von einem anderen Client verwendet werden, um vom TGS (Ticket Granting Service) ein ST (Service Ticket) anzufordern? Begründung!

8. Nennen Sie zwei Gründe, warum in Kerberos KDC und TGS getrennt sind.