F.T. Breuer, O. Kramer, M. Stolpe Dortmund, 26. Dezember 2008

Übungen zur Vorlesung

Betriebssysteme, Rechnernetze und verteilte Systeme II

Wintersemester 2008

Blatt 13

Aufgabe 13.1 (1 Pkt.) Definieren Sie den Begriff „Verteilter Algorithmus“ kurz und präzise.

Aufgabe 13.2 (3 Pkte.) Das Atommodell verwendet zeitlich punktuelle Ereignisse.

(a) Durch welche Annahmen ist es möglich von Ereignissen zu sprechen? Wodurch wird ein Ereignis definiert?

(b) Wann sind zwei Ereignisse voneinander kausal abhängig?

(c) Nennen Sie jeweils ein Ereignis, das von den Ereignissen e_4 und e_5 in Abbildung 1 (i) abhängig, (ii) unabhängig ist.

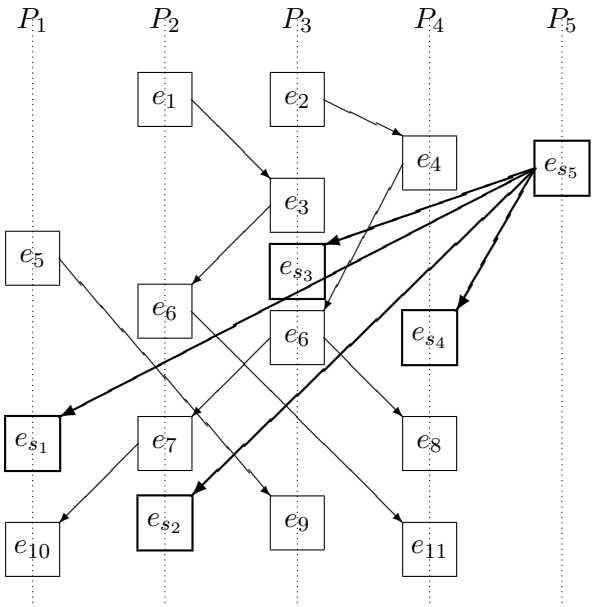

Abbildung 1: Ereignisse eines verteilten Algorithmus

Aufgabe 13.3 (3 Pkte.) Ein Schnappschuß betrifft den Wunsch, den Gesamtzustand eines verteilten Systems festzustellen, um ihn lokal auswerten zu können.

(a) Begründen oder widerlegen Sie, dass die beiden folgenden Aussagen für einen verteilten Algorithmus mit den Knotenprozessen $P_1 \dots P_n$ äquivalent sind. Der Schnappschuss wird durch die Ereignisse e_{s_i} jeweils für den Knoten P_i geschrieben.

1. Schnappschuss ist konsistent.
2. Alle Ereignisse e_{s_i} sind paarweise kausal unabhängig.

(b) Für den verteilten Algorithmus der Abbildung 1 wird durch die Ereignisse e_{P_1}, e_{P_2} und e_{P_3} ein Schnappschuss erzeugt. Da kein korrekter Schnappschuss-Algorithmus verwendet wird, kann dieser konsistent oder nicht konsistent sein. Begründen Sie, warum dieser Schnappschuss nicht konsistent ist. Inwiefern spiegelt der Schnappschuss etwas Unmögliches wider? Nehmen Sie bei Ihrer Begründung auf konkrete Ereignisse bezug.

(c) Warum ist es meistens nicht sinnvoll, gleichzeitige Schnappschüsse zu erstellen? Begründen Sie zwei Aspekte kurz.

Aufgabe 13.4 (3 Pkte.) Alice, Bob und Trudy haben keine Lust mehr auf Nachrichtenverschlüsselung und Datenspionage und wollen stattdessen den größten gemeinsamen Teiler (ggT) ihres Alters berechnen. Um Zeit zu sparen, wollen sie einen verteilten Algorithmus verwenden und zwar auf Basis des Satzes von Euklid und zwar dessen modifizierter Variante.

Sei $x > y$, dann gilt

$$\text{ggT}(x, y) = \text{ggT}(y, mod(x - 1, y) + 1) \tag{1}$$

(a) Hilf Ihnen, indem Du einen kurzen verteilten Algorithmus in Pseudocode schreibst, mit dessen Hilfe verteilt der ggT ihres Alters berechnet werden kann.

(b) Spiele verschiedene Kommunikationsszenarien durch. Erhalten die drei immer dieselbe Lösung?

(c) Alice und Bob rechnen gemeinsam. Bob addiert seine Zahl x und die von Alice empfangene Zahl y. Das Ergebnis x' überträgt er an Alice und berechnet − während er auf die Antwort von Alice wartet − seine neue Zahl als $x = x' + 3$. Alice geht genauso wie Bob vor, addiert jedoch statt einer 5 eine 3 in jedem Schritt. Was müssten beide addieren, um die Fibonacci-Folge zu berechnen? Bob hat sich verrechnet, merkt das aber erst nach Versenden des Ergebnisses. Wie kann er im nächsten Schritt den Fehler korrigieren? Unter welchen Bedingungen geht das nicht?

Aufgabe 13.5 (zusätzlich 3 Pkte.) Im Verlauf der Vorlesung haben Sie im Zusammenhang mit QoS die Begriffe Edge- und Core-Router kennengelernt.

(a) Auf welchen grundlegenden Ansatz für QoS beziehen sich diese beiden Begriffe? Erläutern Sie den Grundgedanken des Ansatzes.

(b) Welche Funktionen werden auf (i) Edge-Routern und welche auf (ii) Core-Routern implementiert?

(c) Was verstehen Sie unter dem Begriff Pro-Hop-Behaviour?

(d) Bei einem anderen Ansatz zu QoS kann es leicht zu Problemen bezüglich der Skalierbarkeit kommen. Warum? Wie heißt der angesprochene Ansatz?

Aufgabe 13.6 (zusätzlich 3 Pkte.) Gegeben sei folgende Notation:

d_A: privater Schlüssel von Alice, e_A: öffentlicher Schlüssel von Alice,
d_B: privater Schlüssel von Bob, e_B: öffentlicher Schlüssel von Bob,
s_r: zufälliger symmetrischer Schlüssel, $H(\cdot)$: Hash-Funktion,
m: Nachricht, $+$: Operation „Konkatenation“.

Beachten Sie, dass es im Folgenden um praxisnahe digitale Signaturen und Verschlüsselung geht, d. h. Sie müssen am Ende der Bearbeitung alle Elemente der Notation an mindestens einer Stelle verwendet haben.

(a) Alice möchte Bob gegenüber nachweisen, dass sie Nachricht m (z. B. eine E-Mail) verfasst hat (Authentizität) und dass die Nachricht bei der Übertragung nicht verändert wurde (Integrität). Beschreiben Sie in formaler Notation, welche Daten Alice an Bob senden muss. Es sollte deutlich werden, welche Operationen Alice ausführt.

(b) Die Nachricht an Bob soll zusätzlich nur von Bob gelesen werden können. Beschreiben Sie erneut formal, was Alice an Bob senden muss.

(c) Erstellen Sie — ähnlich wie auf den Folien zu sicheren E-Mails — ein Diagramm, das zeigt, welche Schritte Bob ausführt, um die empfangene Nachricht aus Aufgabe b) zu entschlüsseln und auf ihre Authentizität hin zu überprüfen.