KS 1, IT 1
Prof. German
März 2004

Bemerkungen zu Prüfung und Prüfer

- Ergebnis: 1,0
- lockere Prüfung, kein Ton vom Beisitzer
- teils allgemeine Fragen ("erzählen Sie mal was über XYZ"), teils Fragen direkt zu einem Thema
- allgemein: Verständnis, Zusammenhänge scheinen ihm viel wichtiger zu sein als Detailwissen
- große Themensprünge, aber ich hatte das Gefühl, Prof. German hatte einen genauen Plan, was er mich fragen wollte, könnte also schwierig sein, auf sicheres Terrain zu lenken.
- KS 1: Skript + Übungen genügen hier meiner Meinung nach.
- IT 1: Folien ("Skript") genau anschauen, v.a. auch Graphen in den Kapiteln 3 und 5, bei Unklarheiten im Kurose/Ross nachlesen

Fragen

KS 1

- F: QoS - Dienstgüten, was gibt es denn da so?

  A: Quality of Message (Bitfehlerrate, Paketfehlerrate, Reihenfolgeerhaltung, ...), Quality of Addressing, Quality of Confidentiality (Abhörbarkeit, Verfälschbarkeit), Quality of Timeliness (Delay, Jitter, Durchsatz, ...)
- F: Machen Sie doch mal zwei Beispiele und vergleichen sie bzgl. ihrer Dienstgüteanforderungen.

  A: Datenkommunikation, Fabrikkommunikation; Vergleich bzgl. Fehlerraten, Delay, Durchsatz
- F: Netzmanagement: Vergleichen Sie Internet-Management-Architektur, OSI-Management-Architektur

  A: Informationsmodell, Organisationsmodell, Kommunikationsmodell verglichen
- F: Endliche Automaten - was ist das? Erzählen Sie doch mal.

  A: Formale Definition, Unterschied zu erweiterten endlichen Automaten, direkte Kopplung/Kanalkopplung
- F: SDL ist ja eine automatenbasierte Sprache. Zeichnen Sie mal ein Diagramm in SDL.

  A: einfacheres Beispieldiagramm hingemalt, System mit Blöcken und Kanälen, "Zoom" in einen der Blöcke (hierarchische Dekomposition), Prozesse, "Zoom", SDL-Automat
- F: Okay. Wie kann man da jetzt Zeitverhalten mit reinbringen?

  A: Hier bin ich zunächst auf die Schiene MSC gerutscht, hab dann aber, während ich erzählt habe, gemerkt, daß man mit MSC ja nur Nachrichtenfolgen, nicht direkt aber Zeitverhalten beschreiben kann; konnte das ohne Unterbrechung erklären ("das geht damit ja aber gar nicht, Sie wollten bestimmt auf Folgendes hinaus...") und dann über Modellierung diskreter Zeit ("ticks") und kontinuierlicher Zeit mit Automaten erzählen.
- F: Prozessalgebren - erzählen Sie mal was dazu.

  A: Definition; Konstruktivität: Kompositionalität, Abstraktionsfähigkeit, Kalkül für Äquivalenz von Prozessen; Präfixnotation, Menüoperator, Parallelschaltung, jew. mit kleinem Beispiel (inhaltlich also im Prinzip die ersten paar Seiten über CSP)
- Okay, dann gehen wir mal zu IT 1. (puh!)

IT 1

- F: Transportschicht, TCP: Wie funktioniert da die Fehlerkontrolle? Auf Nachfrage: Dazu gehört natürlich auch Flußkontrolle.

  A: Bitfehler: Internet Checksum im Header; Flusskontrolle: Empfänger-Window, Rückmeldungen, max. so viele ungeACKte Pakete unterwegs, wie noch in den Empfangspuffer passen (bzw. mit Window Scale Factor: ein Vielfaches davon)

- F: Wovon hängt der Durchsatz ab?

  A: Rate und Delay. Dazu sollte ich Graph von Folie 3-73 zeichnen und erklären.

- F: Und was macht man bei Packet Losses?

  A: Fast Retransmit nach drittem Duplicate ACK.

- F: Was ist statistisches Multiplexing?

  A: Erst kurz was zu FDM/TDM erzählt, dann, was bei statistischem Multiplexen passiert.

- F: Vorteil, Nachteil?

  A: Bessere Auslastung; Dienstgüten wie Delay, Durchsatz, ... können nicht mehr garantiert werden.

- F: NAT-Routing. Wie funktioniert das?

  A: Umschreiben von TCP-Headern, NAT-Tabelle im Router, Zuordnung interne IP/Port-Paare ¡-¿ Router-Port.

- F: Routing - Border Gateway Protocol. Was ist das, wie funktioniert es?

  A: Path Vector Protocol, ähnlich Distance Vector, Pfade werden "advertised"; Protokoll, mit dem sich (wie der Name schon sagt) Border Gateways verschiedener AS unterhalten.

- F: Sicherheit - SSL. Wie funktioniert das?

  A: Hier hab ich erst mal einen Schreck gekriegt, das hab ich mir nämlich gar nicht so genau angeschaut. Ihm hat Folgendes gereicht: Sicherung für TCP-Verbindungen; Serverbetreiber hat Public/Private-Key-Pair, läßt Public Key von CA unterschreiben; Browser oder allgemein Client-Software hat PubKey der CA; Client holt sich Zertifikat vom Server, prüft mit CA-PubKey dessen Authentizität, extrahiert den PubKey des Servers, verschlüsselt damit generierten (symmetrischen) Sitzungsschlüssel und schickt diesen dem Server. Ab dann: Verschlüsselung der Verbindung mittels Sitzungsschlüssel.