

## Übung 6

Dieses Übungsblatt hat wegen des bevorstehenden Semesterendes eine deutlich verkürzte Laufzeit und gibt nur „Gummi-Punkte“ (d. h. der Notenschlüssel für die Vornote bezieht sich auf eine Gesamtpunktzahl von 50 Punkten).

- 1) Wie gehen die folgenden Protokolle/Kommunikationsszenarien mit Datentransparenz um?
  - a) FTP
  - b) SMTP
  - c) Anwendungsprotokolle auf ASN.1-Basis
  - d) Austausch von HTML-strukturierten Dokumenten

(2 Gummi-Punkte)
  
- 2) Entwerft eine REST-basierte Web-Schnittstelle für das Verwalten der gruppenweisen Abgabe von Übungszetteln in „Rechnernetze“ auf Basis des URI <http://www.ute.de/rn-ueb>. Darüber sollen die folgenden Dienste erbracht werden:
  - Erzeugen/Löschen einer Übungsgruppe.
  - Hochladen einer Abgabe.
  - Löschen einer Abgabe.
  - Lesen einer Abgabe.

Zu einem Zeitpunkt  $t$  gibt es die Gruppen 1 und 2. Für beide wurde bereits die Abgabe der 1. Übung hochgeladen. Wie könnten die folgenden Anfragen REST-basiert kodiert werden?

  - a) Hochladen von Übung 2 von Gruppe 1.
  - b) Erzeugen einer neuen Gruppe.
  - c) Lesen von Übung 1 von Gruppe 2.

Visualisiert den Zustand der Übungsverwaltung nach Ausführung dieser Anfragen?

(2 Gummi-Punkte)
  
- 3) Warum kann SSH auf Zertifikate verzichten?

(1 Gummi-Punkt)

*Abgabe:* Schriftlich am Mi 04.07.2018 (ACHTUNG: Irregulärer Abgabetermin!!).

## Fragebogen 6

### Teil 1: Web: Komponenten und Services

- 1) Was ist ein Web-Service?
- 2) Worin unterscheidet sich der XML-RPC/SOAP-Ansatz von *REST (Representational State Transfer)*?
- 3) Was ist ein *Web-Feed*?
- 4) Der URL/URI in einer typischen Web-Anfrage identifiziert den zuständigen Web-Server. Wie kann eine solche Anfrage stattdessen an einen Cache geleitet werden?
- 5) Was versteht man im Zusammenhang mit Web-Anwendungen unter *mobilem Code*? Warum wird er häufig in einer *Sandbox* ausgeführt?
- 6) Welche Aufgabe erfüllt *AJAX*?
- 7) Was sind *Web Sockets*?
- 8) Warum spielt die Entwicklung von standardisierten Anwendungsprotokollen in Zukunft vermutlich eine geringere Rolle als früher?

### Teil 2: Klassische Internet-Anwendungen: Telnet, FTP; NFS

- 9) Für welchen Zweck ist TELNET entwickelt worden?
- 10) Welches zusätzliche Problem muß dazu von TELNET gelöst werden?
- 11) Welche Funktionalitäten stellt FTP in etwa zur Verfügung?
- 12) Warum werden für FTP mehrere TCP-Verbindungen verwendet?
- 13) Welche Dienstleistung erbringt NFS?
- 14) Was bedeutet der Begriff *Idempotenz* im NFS-Zusammenhang (d.h. wie wirkt sich dies auf den Zugriff auf einen NFS-Server aus)?

### Teil 3: E-Mail

- 15) Welche beiden Teilschichten werden bei MHS und RFC 822/SMTP unterschieden? Grenze die Aufgaben dieser beiden Teilschichten gegeneinander ab.
- 16) Was leistet *SMTP*?
- 17) Welche Probleme von RFC 822/SMTP werden von *MIME (Multipurpose Internet Mail Extension)* gelöst? Wie in etwa?
- 18) Worin unterscheidet sich das Zugriffsverfahren von IMAP4 von dem POP3-Modell?

#### Teil 4: Informationssicherheit

- 19) Skizziere einige typische Angriffe auf vernetzte Systeme.
- 20) Erläutere kurz die Bedeutung der Begriffe *Geheimhaltung*, *Integrität*, und *Authentisierung*. Wie kann man diese Sicherheitsdienste in etwa realisieren?
- 21) Wofür können *Hash*-Funktionen in diesem Zusammenhang eingesetzt werden?
- 22) Wodurch unterscheiden sich *symmetrische* und *asymmetrische* Chiffren?
- 23) Warum gibt es bei symmetrischen Verfahren ein Schlüsselverteilungsproblem?
- 24) Gibt es auch bei asymmetrischen Verfahren ein Schlüsselverteilungsproblem? Begründung.
- 25) Wozu benötigt man *Zertifikate*? Welche Rolle spielen *Root Certificates*?
- 26) Wozu kann man das *Diffie-Hellman*-Verfahren verwenden? Was hat dies mit Authentisierung zu tun?
- 27) Wie arbeitet TLS in etwa?
- 28) Was ist das Besondere an QUIC?
- 29) Welche Aufgaben erfüllt SSH?
- 30) Wie arbeitet eine *Firewall* in etwa?
- 31) Welche Probleme können durch einen *NAT (Network Address Translator)* gelöst werden? Welche potentiellen Probleme entstehen dadurch?
- 32) Was ist ein *Virtual Private Network (VPN)*?

#### Teil 5: Internet of Things (IoT)

- 33) Was meinen wir, wenn wir sagen, dass für das Internet of Things in zwei Richtungen skaliert werden muß?
- 34) Durch welche wesentlichen Parameter zeichnet sich ein Sensornetz nach IEEE 802.15.4 aus?
- 35) Wie erfolgt der Medienzugriff in IEEE 802.15.4-Netzen?
- 36) Was ist *6LoWPAN*?
- 37) Auf welcher Netztopologie arbeitet *RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks)*? Wie erfolgt die Wegewahl auf der Basis von RPL? Worin unterscheiden sich dabei *Storing Mode* und *Non-Storing Mode*?
- 38) Für welchen Anwendungszweck wurde *CoAP (Constrained Application Protocol)* entwickelt? Worin unterscheidet es sich von HTTP?
- 39) Welche wesentlichen Eigenschaften hat CBOR?