

Fragebogen 7

Teil 1: Betriebsprotokolle

- 1) Wie arbeitet SNMP in etwa? Nenne einige Beispiele für Informationen in einer *Management Information Base (MIB)*. Warum ist es naheliegend, als unterliegende Repräsentationstechnik eine Typdefinitionssprache wie ASN.1 einzusetzen?
- 2) Welches Problem löst das *Boot Protocol (bootp)* bzw. das *Dynamic Host Configuration Protocol (dhcp)* in etwa? Kurze Beschreibung. Mit welcher ungewöhnlichen Situation müssen diese Protokolle umgehen?
- 3) Wie arbeitet die IPv6-Autokonfiguration in etwa?

Teil 2: Sicherheit in verteilten Systemen

- 4) Skizziere einige typische Angriffe auf vernetzte Systeme.
- 5) Erläutere kurz die Bedeutung der Begriffe *Geheimhaltung*, *Integrität*, *Nichtabstreitbarkeit* und *Authentisierung*. Wie kann man diese Sicherheitsdienste in etwa realisieren?
- 6) Wodurch unterscheiden sich *symmetrische* und *asymmetrische* Chiffren? Warum gibt es bei symmetrischen Verfahren ein Schlüsselverteilungsproblem?
- 7) Wie funktioniert eine *digitale Unterschrift* in etwa? Wofür können *Hash*-Funktionen eingesetzt werden?
- 8) Wo kann man öffentliche und geheime Schlüssel sinnvollerweise ablegen? Wozu benötigt man *Zertifikate*?
- 9) Welche Aufgabe erfüllt ein *Key Management Protocol*? Wozu kann man das *Diffie-Hellman*-Verfahren verwenden? Wie kann dies mit einer Authentisierung kombiniert werden?
- 10) Wie arbeitet eine *Firewall* in etwa? Welche Aufgabe hat ein Paketfilter?
- 11) Welche Probleme können durch einen *NAT (Network Address Translator)* gelöst werden? Welche potentiellen Probleme entstehen dadurch?
- 12) Was ist ein *Virtual Private Network (VPN)*?