

Übungen “Telematik” — Wintersemester 2002/2003

Lösungen zum 5. Übungsblatt

Lehrstuhl für Telematik · Universität Göttingen
Lotzestr. 16-18 · D-37083 Göttingen

<http://www.ifi.informatik.uni-goettingen.de/tmg>

Michael Ebner

Mobile Kommunikation

1 Unterscheiden Sie drahtlose (wireless) und mobile Kommunikation anhand von Beispielen.

<i>Gerät</i>	<i>Wireless</i>	<i>Mobil</i>
Stationärer Computer	×	×
Notebook in Hotel	×	√
Wireless LANs	√	×
Personal Digital Assi- stant (PDA)	√	√

(siehe Folie Teil6#56)

2 Was ist unter *indirektem* und *direktem* Routing im Falle von Mobilität zu verstehen?

Routing wird von Endsystemen durchgeführt:

indirektem Routing Die Kommunikation vom Gegenüber zum Mobilien erfolgt über den Heimganten, welcher die Kommunikation an den Mobilien weiterleitet.

direktem Routing Der Gegenüber bekommt die *foreign address* des Mobilien und korrespondiert mit dem Mobilien direkt.

(siehe Folien Teil6#70,72,76)

3 Nennen Sie zwei Arten von Adressen die ein mobiler Knoten haben kann.

- permanent address (home address)
- care-of address

(siehe Folien Teil#66,67,80)

Netzwerkmanagement

4 Beschreiben Sie das allgemeine Netzwerkmanagementmodell und die SNMP Schlüsselkomponenten.

allgemeines Netzwerkmanagementmodell

- Managing entity
- Managed device
- Agent
- Management Information Base (MIB)
- Managed object
- network management protocol

SNMP Schlüsselkomponenten

Management Information Base (MIB) distributed information store of network management data

Structure of Management Information (SMI) data definition language for MIB objects

SNMP protocol convey manager \iff managed object info, commands
security, administration capabilities major addition in SNMPv3

(siehe Folien Teil7#6,9)

Multimedia und QoS in Netzwerken

5 Was ist ein *out-of-band* und *in-band* Protokoll? Geben Sie jeweils ein Beispiel an.

- Out-of-band Daten werden über einen logisch unabhängigen Übertragungskanal übermittelt und werden unabhängig vom normalen Datenstrom an den Benutzer gesendet. Wird meistens zur Signalisierung verwendet, z.B. RTSP versendet seine Kontrollnachrichten auf diese Weise. Auch das *Common Channel Signaling System* No. 7 (SS7) für ISDN verwendet dieses Verfahren. Oder auch FTP.

- In-band Daten werden innerhalb des normalen Datenstroms mitversendet. Die Daten müssen daher vom normalen Datenstrom extrahiert werden.
Beispiel: HTTP, SMTP, POTS

(siehe Folien Teil7#63,102)

6 Nennen Sie drei Klassen von Multimedia-Anwendungen und geben Sie dazu jeweils ein Beispiel an!

- Streaming stored audio and video (Aufzeichnung von Lehrveranstaltungen)
- Streaming live audio and video (Internet-Radio)
- Real-time interactive audio and video (Video Konferenzen)

(siehe Folie Teil7#82)

7 Kann RTP Garantien für die QoS von Multimedia-Anwendungen abgeben? Begründen Sie Ihre Antwort.

Nein, RTP kann keine Garantien abgeben!

- RTP does not provide any mechanism to ensure timely delivery of data or provide other quality of service guarantees.
- RTP encapsulation is only seen at the end systems: it is not seen by intermediate routers.
- Routers providing best-effort service do not make any special effort to ensure that RTP packets arrive at the destination in a timely matter.

(siehe Folie Teil7#120)

Netzwerksicherheit

8 Was sind *symmetrische, öffentliche und private* Schlüssel?

symmetric key crypto

symmetric key crypto requires sender and receiver know shared secret key \Rightarrow Bob and Alice share know same (symmetric) key

public key cryptography

In public key cryptography sender and receiver do not share a secret key. Instead, there exists the two keys

- public encryption key known to all and
- private decryption key known only to receiver.

(siehe Folien Teil8#12,14,17)

9 Welche Funktion hat die *secure socket layer*?

Geben Sie ein Beispiel für Ihre Verwendung an.

- transport layer security to any TCP-based app using SSL services.
- Standardized as TLS (Transport-layer Security)
- security services: server authentication, data encryption, client authentication (optional)

Beispiele:

- used between Web browsers, servers for e-commerce (shttp).
- server authentication: SSL-enabled browser includes public keys for trusted CAs. Browser requests server certificate, issued by trusted CA. Browser uses CA's public key to extract server's public key from certificate. check your browser's security menu to see its trusted CAs.

(siehe Folie Teil8#66)

10 Beschreiben Sie die IPsec Architektur.

Two principle protocols:

Authentication Header (AH) protocol and

Encapsulation Security Payload (ESP) protocol

Eigenschaften:

For both AH and ESP, source, destination handshake: create network-layer logical channel called a security association (SA)

Each SA unidirectional.

Uniquely determined by: security protocol (AH or ESP), source IP address and 32-bit connection ID

(siehe Folien Teil8#69-71)

Bitte Personalausweis und Immatrikulationsbescheinigung zur Prüfung mitbringen!!!