FREIE UNIVERSITÄT BOZEN
LIBERA UNIVERSITÀ DI BOLZANO
FREE UNIVERSITY OF BOZEN · BOLZANO

Fakultät für Informatik | Facoltà di Scienze e tecnologie informatiche | Faculty of Computer Science

Distributed Systems

Written Examination

24.6.2015

FIRST NAME		**LAST NAME**	
STUDENT NUMBER		**SIGNATURE**	

Instructions for students:

Write First Name, Last Name, Student Number and Signature where indicated.

Do not speak to any other student during the examination. If you speak to another student, your examination will be cancelled.

It is ok to make assumptions, but write them down.

You are allowed to bring one handwritten A4 sheet of paper to the exam.

Write neatly and clearly.

Good luck!

1. Protocol Stack

Protocols are conceptually arranged in a stack, where packages from upper layers are encapsulated in packages from lower layers, and layers provide services to each other.

(i) Which service does the IP protocol provide to protocols in the transport layer above, and which services of the underlying data link layer does it use?
(4 points)

For the following tasks, consider that all protocols headers are 30 Byte. Consider an HTTP package containing 1900 Bytes of payload, which is transmitted over an Ethernet with a maximum transmission unit (MTU) of 1000 Bytes.

(ii) Name the protocols that are involved in the transmission of the HTTP package.
(3 points)

(iii) Draw the packages that are transmitted over the physical medium, clearly marking package sizes, and the location of headers and payload.
(8 points)

(iv) What is the bandwidth overhead due to the protocols?
(3 points)

2. Data Link Layer

Consider the (7,4)-Hamming code from the lecture, where the parity bits in a word $(d_1,d_2,d_3,d_4,p_1,p_2,p_3)$ are calculated as

$p_1=d_1 \oplus d_2 \oplus d_3$,
$p_2=d_2 \oplus d_3 \oplus d_4$,
$p_3=d_3 \oplus d_4 \oplus d_1$.

(i) Decode the following words in this code, marking possible errors you find.
0010111 1111100 1010110

(8 points)

Consider a channel with an error probability of 10^{-4} per bit, and consider that frames with a size of 1000 bits shall be transmitted.

(ii) Which method of error handling is preferable, error correction on the receiver side using Hamming codes, or error detection on the receiver side with parity bits, and subsequent retransmission of frames containing errors?

(10 points)

(iii) Besides the bandwidth overhead of both methods, which other aspect may be relevant for comparing the methods?

(2 points)

3. Transport Layer

There exist two major protocols in the transport layer, TCP and UDP.

(i) What is the difference between them?

(4 points)

(ii) Give one example of a protocol implemented using TCP, and one example of a protocol implemented using UDP. What are the reasons for the respective choices?

(4 points)

TCP uses AIMD (additive increase, multiplicative decrease) as a method for congestion handling.

(iii) Simulate the first six steps of congestion handling using AIMD for two flows A and B, starting with 0% and 80% network utilization, respectively.

(8 points)

(iv) Can MIAD (multiplicative increase, additive decrease) be used as well for congestion handling? Explain your answer.

(4 points)

4. Cryptography

RSA is a classical asymmetric cryptosystem.

(i) Decode the three ciphertext symbols 5, 9 and 3 using the private RSA key (7,11). What are the corresponding plaintext symbols?

(8 points)

(ii) How can RSA key pairs be used for encrypted communication, and how can they be used for verifying a sender's identity?

(4 points)

(iii) What are certificate authorities, and which role do they play for RSA encryption?

(4 points)

(iv) Why is the security of DNS important, and how can DNS be attacked?

(4 points)

5. Coordination

Synchronizing clocks is a major issue in distributed systems.

(i) An approach to clock synchronization could be that every peer copies the time shown on http://www.timeanddate.com/. Describe what could go wrong when using this method.

(4 points)

(ii) What are concurrent events with respect to Lamport's logical clock algorithm? Give an example.

(3 points)

Leader election is another important step in the maintenance of distributed systems.

(iii) Give a detailed description of one leader election algorithm.

(8 points)

(iv) What happens in your algorithm if the old leader comes back to life after another peer, that has noticed the old leader's failure, has initiated an election? Does the algorithm still function correctly?

(5 points)