Telematics

Winter Semester 2010/11

Number:	13. Assignment
Issued:	27.01.11
Tutorial:	03.02.11
Lecturer:	Prof. Dr. Güneş, Dipl.-Inf. Blywis
Contact:	{guenes, blywis}@inf.fu-berlin.de

Exercise 1, TCP Checksum:

The TCP header contains a checksum field.

1. What algorithm is applied?
2. Which "parts" of the TCP segment are protected by the checksum?
3. Why does the approach violate the principles of a layered network architecture and why is the violation necessary?

Exercise 2, DNS, SMTP, POP3, IMAP:

	Bob	Alice
IP address:	192.45.56.127	208.115.92.45
Name server:	192.47.56.2	208.115.92.2
SMTP server:	`mail.server.org`	`mail.server.org`
Email Address:	`bob@realword.org`	`alice@wonderland.org`

1. Explain the differences between SMTP, POP3, and IMAP.
2. Let's consider user Bob wants to send an email to user Alice. In order to establish a connection with the SMTP server, the server's name has to be resolved into an IP address by DNS. Explain which messages are exchanged and between which hosts when recursive name resolution is used. Assume that only the name server responsible for the domain `server.org` can answer the request.
3. Now it is Alice's turn to reply to Bob. Explain which messages are exchanged when using iterative name resolution. Assume that only the name server responsible for the domain `server.org` can answer the request.
4. Explain how Bob's SMTP server finds the MTA responsible for accepting email messages on behalf of Alice.

Exercise 3, E-Mail:

1. Inspect the full email header of a message, which you have received and discuss the contents.
2. Can you approximate when the message was actually sent?
3. How are attachments transfered?

Exercise 4, DNS Infrastructure:

1. Discuss the vulnerability of DNS.
   - Read the fact sheet issued by the ICANN regarding an attack on the DNS root servers in 2007: Download
   - Additionally, read the (nicely illustrated) article "An Illustrated Guide to the Kaminsky DNS Vulnerability".
2. What is a DNS amplification attack?
3. Why are we so dependent on DNS?

Exercise 5, Asymmetric Key Cryptography:

Discuss public-private key encryption.

1. Explain the difference between symmetric and asymmetric encryption.
2. Discuss the role of the public and private key to implement *encryption* and *authentication*.
3. What is the basic idea of a digital signature?

Exercise 6, Cryptographically Generated Addresses (CGA):

Read and discuss RFC 3972.

1. Why is a network layer address authentication important?
2. How can you implement an autonomous, self–consistent address authentication?

Exercise 7, Simple Network Management Protocol (SNMP):

1. Which device specific information are mutually available to both the SNMP agent and SNMP management system? How is this information encoded?
2. Explain the difference between *public* and *private* MIB.
3. What is the most important improvement of SNMPv3 in contrast to previous versions?
4. Explain how you can identify the port that a host is connected with on an SNMP capable switch.

Exercise 8, Cookies:

Read and discuss Michal Zalewski's article HTTP cookies, or how not to design protocols.

1. Why are cookies required?
2. What is so critical about cookies and why is there no good specification?