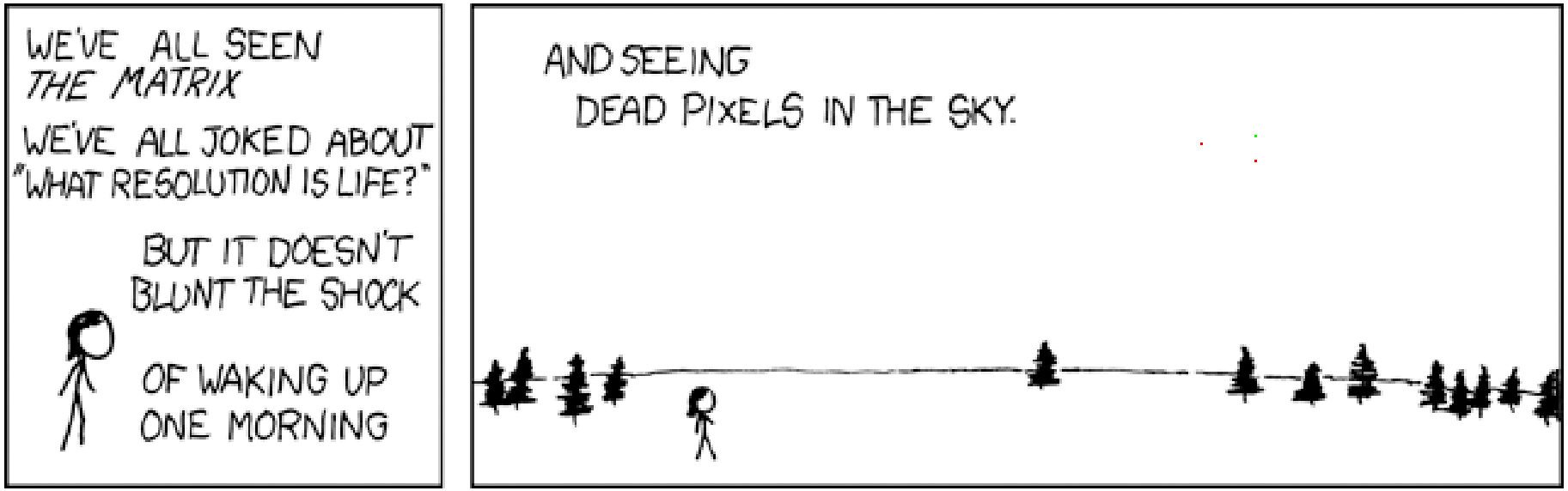
KN2 Exercise 4

Dominik Schulz, Daniel Seither, Marc Werner

TECHNISCHE UNIVERSITÄT DARMSTADT



Mini Test: Network Applications

TECHNISCHE UNIVERSITÄT DARMSTADT

- The FTP (File Transfer Protocol) …
  - is connection-oriented
  - is connectionless
  - uses TCP (Transmission Control Protocol)
  - uses UDP (User Datagram Protocol)

- FTP is connection-oriented and uses TCP. (Answer A)

- The TFTP (Trivial File Transfer Protocol) …
  - is connection-oriented
  - is connectionless
  - uses TCP (Transmission Control Protocol)
  - uses UDP (User Datagram Protocol)

- TFTP is connection less and uses TCP (Answer D)

Mini Test: Network Applications

TECHNISCHE UNIVERSITÄT DARMSTADT

- The Telnet protocol ...
  - is connection-oriented
  - is connectionless
  - uses TCP (Transmission Control Protocol)
  - uses UDP (User Datagram Protocol)

- Telnet is connection-oriented and uses TCP (Answer A)

Mini Test: E-Mail

TECHNISCHE UNIVERSITÄT DARMSTADT

- What does the abbreviation “MIME” stand for?
  - Multiple Internet Mail Extensions
  - Multipurpose Internet Mail Extensions
  - Mail in Mail Encapsulation
  - Mail Internet Message Extension
  - Mandatory Internet Mail Encryption

- Which protocol is used for the communication between mailservers (MTA)?
  - POP3
  - IMAP
  - HTTP
  - SMTP
  - ESMTP

- Both SMTP and ESMTP (Extended SMTP) are used (Answer E)

Mini Test: Web + Web Services

TECHNISCHE UNIVERSITÄT DARMSTADT

- Which organization is responsible to standardize the „web“?
  - ICANN
  - Microsoft and Netscape
  - IETF
  - W3C (World Wide Web Consortium)
  - ISO

- What are the benefits using persistent connections with HTTP?
  - reduction of network congestion
  - reduction of administrative overhead for TCP
  - every request or response gets own connection
  - multiple requests and responses can be sent on one connection

- Answer C

Mini Test: Web + Web Services

TECHNISCHE UNIVERSITÄT DARMSTADT

- Which of the following statements are true with regard to UDDI?
  - UDDI describes the technical interface of a Web Service
  - UDDI contains a data model to describe aspects of Web Services
  - Information about companies offering Web Services are described in so called „green pages“
  - Using UDDI it is possible to search for and to access Web Services dynamically
  - UDDI is obligatory when using Web Services

- Answer B

Problem 1: Web Services

TECHNISCHE UNIVERSITÄT DARMSTADT

a. Describe / depict an interaction between a service requestor, a service provider and a service broker using the Web Service related standards shown during the lecture.

- provider registers it's service via UDDI with the broker
- requestor contacts broker via UDDI API to find an appropriate service provider
- broker responds with service descriptions in WSDL
- requestor sends actual request via SOAP to provider
- provider answers with SOAP response

Problem 1: Web Services

TECHNISCHE UNIVERSITÄT DARMSTADT

b. Compare the Web Service technology with traditional RPC. What are the similarities? What are advantages and disadvantages of the Web Service technology in comparison to RPC?

- web services can be used as an RPC mechanism
- WS are less platform and language dependent (formats based on XML)
- WS communication uses more bandwidth and needs additional processing (plaintext vs. binary, XML vs. XDR etc.)
- use of HTTP adds optional encryption and authentication "for free"

Problem 1: Web Services

TECHNISCHE UNIVERSITÄT DARMSTADT

c. Describe the concept of the „colored“ pages in UDDI. Is the information documented in the UDDI repository sufficient to use the corresponding Web Services efficiently?

- different types of information:
  - white pages: information about the identity of providers
  - yellow pages: classification of providers by type of service
  - green pages: technical description of services (in WSDL)

Problem 2: Network File Systems

TECHNISCHE UNIVERSITÄT DARMSTADT

There are different flavors of network file systems in use in real world scenarios. In this exercise you should compare the AFS (Andrew File System) to NFS (Network File System) and CIFS (Common Internet File System, e.g. Samba).

- Architecture
  - CIFS, NFS: simple client-server architecture
  - AFS: distributed filesystem

- Transport protocol
  - AFS, NFSv3: UDP
  - CIFS, NFSv4: TCP

Problem 2: Network File Systems

TECHNISCHE UNIVERSITÄT DARMSTADT

- Authentification
  - NFSv3: ip address of client
  - NFSv4: ip address of client, user-based auth. (Kerberos)
  - AFS: user-based auth. (Kerberos)
  - CIFS: user-based auth. (Plaintext, LM, NTLM, Kerberos)

- Best used in...
  - NFSv3: centrally administered local networks (no caching, weak security mechanisms)
  - NFSv4: local networks (no caching)
  - AFS, CIFS: local and wide area networks
  - AFS: big installations (complex server structure)
  - CIFS: Windows-centric networks

Problem 3: Electronic Mail

TECHNISCHE UNIVERSITÄT DARMSTADT

- Which port numbers are assigned to SMTP, POP3, and IMAP?
  - SMTP: 25
  - POP3: 110
  - IMAP: 143

  - Additional there is the submission port 587 which is used to send mails from a mail user agent (MUA) to the first mailserver (MTA). On the submission port the STARTTLS command normally is enforced.

- Which port numbers are assigned to SMTP, POP3, and IMAP over SSL?
  - SMTPS: 465 (not on the IANA list of well known ports anymore. Removed in favour of STARTTLS in SMTP)
  - POP3S: 995
  - IMAPS: 993

Problem 3: Electronic Mail

TECHNISCHE UNIVERSITÄT DARMSTADT

- Which encryption algorithm is used to transmit the password if the mail client uses the POP3 protocol to retrieve the messages?
  - POP3 itself does not specify an encryption algorithm for passwords. Most server however support various encryption algorithms for the password.
  - Those are mainly implemented trough the SASL extensions. The most common are:
    - PLAIN (no encryption)
    - CRAM-MD5 (based on the MD5 algorithm)
    - DIGEST-MD5 (like CRAM-MD5 but with additional integrity checks)
  - or APOP as specified in RFC 1460

Problem 3: Electronic Mail

TECHNISCHE UNIVERSITÄT DARMSTADT

- The SMTP specification does not include passwords to secure the authentification process while sending an email. How to hinder a student which is connected via dialup to send impersonated emails (e.g. with the name BillGates@Microsoft.com?
  - block all connections from dialup ip ranges
  - on the outbound smtp server only allow registered addresses
  - use SPF (Sender Policy Framework) or another schema to identify allowed SMTP hosts for a domain such as SenderID or DomainKeys

- Paul uses a vacation daemon to automatically reply to incoming messages. After initializing the daemon he sends a mail to Peter. However, Peter has activated his vacation daemon, too. What will happen?
  - the two mailservers will send each other vacation messages back and forward as they will answer on each incoming message with another vacation reply which then will trigger a vacation reply again.

Problem 4: Electronic Mail, Base64 and QP

TECHNISCHE UNIVERSITÄT DARMSTADT

Consider a binary file of the size 3072 bytes.

a) *How long will the base64 encoded file be? Assume that after each 74 characters and at the end of the message a CR+LF are inserted.*

Solution: (3072 bytes / 3 bytes) * 4 Characters = 4096 Chars

4096 Chars / 74 Chars per Line = 56 Lines -> 112 additonal Chars (CR LF)

4096 + 112 = 4208 Chars

Problem 4: Electronic Mail, Base64 and QP

TECHNISCHE UNIVERSITÄT DARMSTADT

b) *Does the ANSI character encoding cause problems to base64?*

Solution: Yes, since the mapping of values resulting from the base64 transformation to ANSI characters would include control characters needed by SMTP, e.g. „-.“, „.“, „<“, „>“

c) The MIME protocol (RFC 1521) uses base64 to encode attachments for transmission. Which of the following character(-groups) can be / cannot be used within base64? 1) Characters 2) Numbers 3) „/“ 4) „+“ 5) „@“

Solution: The „@“-Sign is not used by base64. Only characters, number and „/“ as well as „+“ are used by base64. 26 lower-case characters + 26 upper-case characters + 10 numbers + 1 „/“ + 1 „+“ = 64.

Problem 4: Electronic Mail, Base64 and QP

TECHNISCHE UNIVERSITÄT DARMSTADT

- **d)** *Encode the following 8-bit ASCII text from Goethe in quoted-printable format. Assume that a line break is encoded using the ASCII squence of the two chars CR and LF.*

  Bäume leuchtend, Bäume blendend,

  Überall das Süße spendend,

  In dem Glanze sich bewegend,

  1) *How long is the quoted printable encoded file?*

  B=E4ume leuchtend, B=E4ume blendend,\r\n

  =DCberall das S=FC=DFe spendend,\r\n

  In dem Glanze sich bewegend,\r\n

  Lenght: 102 Characters

Problem 4: Electronic Mail, Base64 and QP

TECHNISCHE UNIVERSITÄT DARMSTADT

2) *How long is the base64 encoded file?*

QuR1bWUgbGV1Y2h0ZW5kLCBC5HVtZSBibGVuZGVuZCwNCtxiZXJhbGwgZGFzIFP832Ugc3BlbmRlbmQsDQpJbiBkZW0gR2xhbnplIHNpY2ggYmV3ZWdlbmQs

Length: 128 Characters (but depends on input encoding ISO8859, UTF-8, ...)

3) *What is the most efficient encoding: base64 or quoted-printable?*

Since the **Quoted-Printable** encoding is shorter, it is more efficient in this case. In general it depends on the part of non-7bit-ASCI characters. For an german text Quoted-Printable would be more efficient in most cases, but for a binary file Base64 is usually more efficient.

Problem 5: Electronic Mail Header, Security

TECHNISCHE UNIVERSITÄT DARMSTADT

- Which E-Mail Client was used to compose and send the message?
  - It seems like the message was composed with the web.de Freemail Webinterface running on host freemailng0801.web.de
- Which email address was used to send the email?
  - KN2.KOM@web.de
- Will replies be sent to the same address?
  - Yes as there is no additional Reply-To Header
- Which mailserver (MTA) was first one to process the email?
  - fmmailgate04.web.de

Problem 5: Electronic Mail Header, Security

TECHNISCHE UNIVERSITÄT DARMSTADT

- Which other mailservers have been involved in forwarding the mail?
  - fmmailgate04.web.de
  - mailserver3.hrz.tu-darmstadt.de
  - (KOM.tu-darmstadt.de)
  - mailserver.KOM.e-technik.tu-darmstadt.de
  - mx02.web.de

- What is the meaning of “X-“tags (e.g. X-TUD) in the E-Mail header?
  - The X- Header specify additional headers not mentioned in the RFC or specified later

Problem 6: MIME

TECHNISCHE UNIVERSITÄT DARMSTADT

Consider the listing below which shows an email message.

```
From: s.michael@isp.de
To: f.jan@kom.tu-darmstadt.de
MIME-Version: 1.0
Message-Id: <199707011607.SAA20302@kom.tu-darmstadt.de>
Content-Type: multipart/mixed; boundary= "boundary42"
content-transfer-encoding: 7-bit
--boundary42
Content-Type: text/plain; charset=us-ascii
<i>I hope this video will be helpful for the demo</i>
--boundary42
Content-Type: message/external-body;
access-type="anon-ftp";
site="ftp.isp.de";
directory="/pub/media";
name="demo01.mpeg"
Content-Type: video/mpg
content-transfer-encoding: base64
--boundary42
```

Problem 6: MIME

TECHNISCHE UNIVERSITÄT DARMSTADT

a) How can an email client recognize that the message may contain non-text content?

The „mixed“ part of the Content-Type provides this information (RFC2046, 5.1.3)

b) How can the email client recognize that the message has more than one part? How can the different parts be identified? In which order are the parts presented?

Again, the *Content-Type: multipart/mixed* header and several instances of boundaries (--boundary42 in this case).

The parts are separated by instances on the boundary marker.

The parts are presented in the order given in the text, since no special ordering information is available.

Problem 6: MIME

TECHNISCHE UNIVERSITÄT DARMSTADT

c) How does the text part look like when displayed by the email client? Why?

The text part will look like this:

I hope this video will be helpful for the demo

I would only be interpreted as HTML if a proper Content-Type, like text/html, would be given.

d) This message uses a form of Reference Based Mailing to send video data. What are the advantages and disadvantes for using this scheme?

- Advantages
  - Smaller Message size thus faster download and no wasted bandwith or storage space
- Disadvantages
  - The referenced information is not immedately available and has to be downloaded separately
  - The referenced information is not archived with the mail, so it may be gone sometime and the information originally contained in the message may not be accessible anymore

Problem 7: (Web-)Caching

TECHNISCHE UNIVERSITÄT DARMSTADT

a. Please list the different types of caching you are aware of. Please do not only consider caching servers.

- web browser's cache
- proxy server
- web server: caching dynamically generated content

b. List a situation in which a caching proxy may slow down the response time seen by the client.

- content is not yet available at the proxy
  - new content
  - dynamic content generated for a particular user
  - Slower connection to the proxy then to the actual server
  - High proxy load

Problem 7: (Web-)Caching

TECHNISCHE UNIVERSITÄT DARMSTADT

c. List a situation in which a caching proxy may save network bandwidth. (Note: be very careful to state the precise condition.) Specify what part of the network experiences savings in network bandwidth.

- multiple users of the proxy server navigate to the same web site
  - traffic between web server and target network / proxy server is reduced

d. List and describe a situation in which a proxy server may be a bottleneck in an organization's Internet-access.

- throughput of proxy server is lower than the uplink

Problem 7: (Web-)Caching

TECHNISCHE UNIVERSITÄT DARMSTADT

e. Why do application providers often do not want their HTML pages to be cached?

- the most recent version of their website should be shown to the user
- the more page views a web site generates, the more revenue it's owner can generate by showing ads

f. Can you imagine a way that existence of a caching proxy may make a client computer more susceptible to attack.

- A proxy adds an additional target for attackers:
  - successful attackers may inject malicious code into any web page a user of the proxy requests
  - proxy is a single point of failure (denial of service attack)

Questions?

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Any Questions?**