FIT9137 Workshop Week 10

Topics

- Application Layer
  - HTTP Protocol: web service
  - SMTP Protocol: email service

Covered Learning Outcomes:

- Analyse and formulate the functions of communication architectures of local area networks, wide area networks and the Internet.
- Examine networks using the underlying fundamental theories, models, and protocols for data transmission.

Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (peers) to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

• ACTIVITY A: Application Layer Protocols

Activity A.1 - HTTP Protocol: web service

In this exercise we will communicate directly with a web server using command line and we will send HTTP protocol requests directly to the server and receive the server responses.

Download the file `FIT9137_w10.imn` from Moodle and save it in the shared folder on the host machine (your laptop or PC). Open core and from the file menu open the downloaded core configuration from the shared folder in the VM (under `/media` folder starting with `sf_`). Perform the following tasks.

STEP 1. Start the emulation.

STEP 2. Open a terminal on the node `selene` and issue the following command:

```
telnet www.argos.edu 80
```

The `telnet` command is a program that uses the `Telnet` protocol for remote access. As the protocol is a text-based protocol we can use it for other text-based protocols provided that we know how these protocols work. That is, we know the inner working

of the protocols, the request format, message structure, etc. The number `80` tells the `telnet` program to connect to port `80` of the server at URL `www.argos.edu`. If everything goes well, you should see a prompt as follows:

```
Trying 10.1.1.71...
Connected to www.argos.edu.
Escape character is '^]'.
```

Anything that we type here will be sent to the server.

STEP 3. Type the following request:

```
GET /index.html
```

What do you receive from the server? Does the response differ from what you would see in a browser (e.g., `lynx`)?

STEP 4. Connect to the server again (step 2) and try the following request:

```
GET /index.html HTTP/1.1
Host: www.argos.edu
```

You need an additional new line (enter) after the `Host` field line to indicate that you are done with the fields. What differences do you observe?

Additional fields

```
HTTP/1.1 200 OK
Date:
Server:
Last-Modified:
ETag:
Accept-Ranges:
Content-Length:
```

Connection is kept open for few seconds after the page is delivered (persistent)

STEP 5. How can we visit the page provided via link in the default page (what happens when you click on a link in a browser)?

identify the link enclosed in `<a href></a>` and find the path to the resource the link is pointing to then

```
GET /alink.html
```

or

```
GET /alink.html HTTP/1.1
Host: www.argos.edu
```

- # ACTIVITY B: Application Layer Protocols

Activity B.1 - SMTP Protocol: email service

In this exercise we will communicate directly with a mail server using command line and we will send SMTP protocol messages directly to the server to send an email.

STEP 1. In the terminal on the node `selene` enter the following command to connect to the mail server:

```
telnet mail.argos.edu 25
```

Since SMTP protocol is also a text-based protocol we can use the `telnet` program to communicate with the server. This time we specify port 25 which is reserved for SMTP protocol. If everything goes well you should see a prompt as follows:

```
Trying 10.1.1.72...
Connected to mail.argos.edu.
Escape character is '^]'.
220 mail ESMTP Postfix (Ubuntu)
```

The line `220 mail ESMTP Postfix (Ubuntu)` is the greeting sent by the mail server.

Note: In Week-2 we have created users David, Julie, Susan & Jack in VM. The CORE uses these VM system groups & users for sending and receiving emails.

STEP 2. Send an email from `muni@argos.edu` to `david@argos.edu` following the example from https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol in section *SMTP transport example* of the page or from the lecture slide.

Change the sender, receiver, and message header fields accordingly.

```
helo selene
mail from: muni@argos.edu
rcpt to: david@argos.edu
data

From: "Monash Uni" <muni@argos.edu>
To: "David Copperfield" <david@argos.edu>
Date: Tue, 03 May 2022 12:00:00 +1000
Subject: Week 9 Lab

Hello David

Have you completed your week 9 Workshop Activities?

Regards
Monash Uni

.

quit
```

STEP 3. Open a terminal session on the node `mail-argos` and check if the email has arrived under the folder `/var/mail`. The emails will be placed in a file for each user under the aforementioned directory. If the email is delivered, you should find a file named `david` in that directory.

STEP 4. Send another email but this time change the source email address to another address (any email address that you would like). Can you send the email? Does the email arrive in David's mailbox? Does this behavior pose any problem? Discuss your answers with your tutor.

yes, and yes, anyone can pretend to be anyone. Solution authenticates users, use PGP/GPG or SMIME to authenticate messages, use DKIM to authenticate users from participating domains.

STEP 5. Open Wireshark on `eth1` interface of the node `phoenix` and then send another email from the node `selene` with some fictitious confidential message. What can you observe in Wireshark from the communication between the node `selene` and the mail server? Can you identify any possible issue with what you observe? Discuss your answers with your tutor.

you can see the content of the communication in clear text. Yes, disclosure of confidential messages. Solution use Secure SMTP although this does not guarantee end-to-end encryption only one leg of client-server connection. Use use PGP/GPG or SMIME for end-to-end encryption. Both ends must use the same mechanism and participate.