香港公開大學　科技學院
THE OPEN UNIVERSITY OF HONG KONG
SCHOOL OF SCIENCE AND TECHNOLOGY

ELEC S212

Network Programming and Design

2018 Autumn Presentation

Assignment 4

Please e-submit this assignment via the OLE
by **27 April 2019, 23:59**

Preamble

Dear ELEC S212 Students,

You must submit your answers to this assignment by the cut-off date: **27 April 2019**.

Please note that no assignment extension is allowed for the last assignment. So plan your time and start doing the assignment as soon as you can.

There are FOUR questions in this assignment. You should submit it and the associated files in zipped format and upload it to the OLE e-submission system.

Steven Choy
ELEC S212 Course Coordinator

Question 1 (25 marks)

Complete **Lab 1.5** (attached) – Network traffic analysis and wireless network security.

Attach the following 2 files when you submit your assignment.

(a) A screen capture in named s1234567-tma4q1.jpg (substitute s1234567 with your own student ID) showing your work (similar to Figure 1.5.14). **[3 marks]**

(b) A Wireshark capture file named s1234567-tma4q1.pcap (substitute s1234567 with your own student ID) recording your work done in this Lab. **[4 marks]**

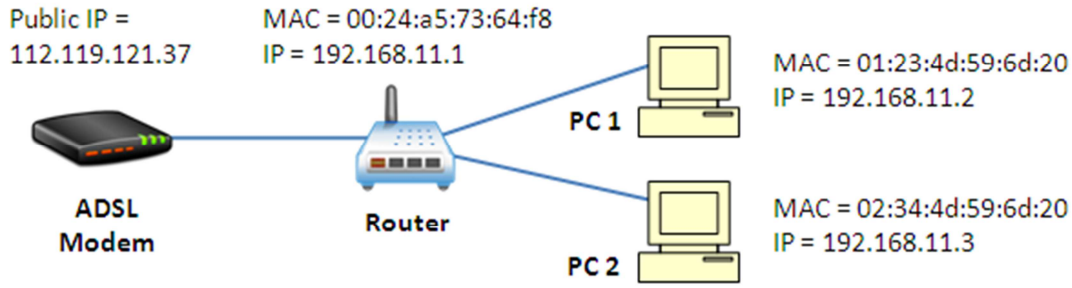
Then answer the following questions:

(c) Name **4** popular TCP/IP application protocols that are vulnerable to packet sniffing. **[4 marks]**

(d) Give a display filter that will show only HTTP POST packets. **[2 mark]**

(e) Explain why packet sniffing is easier on a network that is connected by a hub than a switch. **[4 marks]**

Consider the following diagram of a home network. Now, suppose that PC2 is now using a web browser to access a Web site (with IP address: 202.40.219.246 and local port: 2436).



(f) Complete the following information about a packet that is being **sent out from** PC2. **[4 mark]**

Ethernet II, Source: _____

Ethernet II, Destination: _____

Internet Protocol, Source: _____

Internet Protocol, Destination: _____

TCP, Source Port: _____

TCP, Destination Port: _____

(g) Complete the following information about a packet that is being **received by** PC2. **[4 mark]**

Ethernet II, Source: _____

Ethernet II, Destination: _____

Internet Protocol, Source: _____

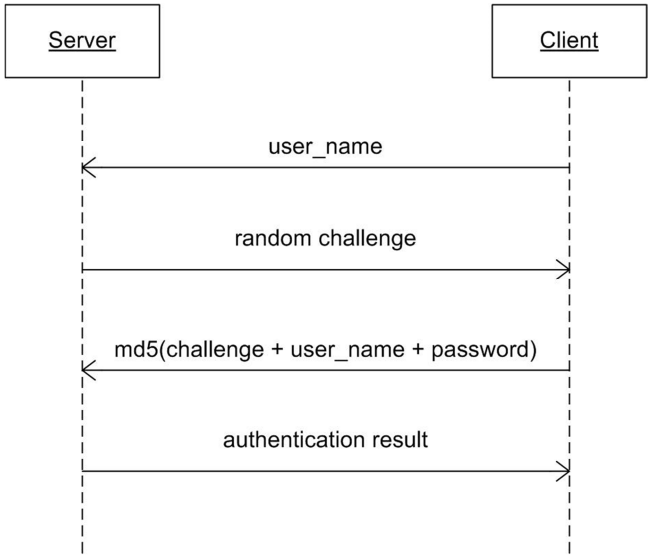
Internet Protocol, Destination: _____

TCP, Source Port: _____

TCP, Destination Port: _____

Question 2 (30 marks)

This question requires you to write a client program in C that implements a simple form of challenge-response authentication. When the client program connects to the server, the server will send a random challenge phrase to the client. The client program appends the user name and the shared secret password to the challenge phrase, and creates an MD5 hash out of the resulting string. The MD5 hash is then sent back to the server for authentication. The authentication process is illustrated in the following diagram:



The following shows the output of the correctly implemented client program:

```
[tma4]$ ./wisdom
Usage: wisdom server_ip_address user_name password
[tma4]$ ./wisdom 127.0.0.1
Usage: wisdom server_ip_address user_name password
[tma4]$ ./wisdom 127.0.0.1 jacky
Usage: wisdom server_ip_address user_name password
[tma4]$ ./wisdom 127.0.0.1 jacky ELECS212
[SENT] jacky
[RECV] 10489371
[SENT] 4194a2c24bbb653525a9040f3354d76e
[RECV] I don't know you. I have no advice for you.
[tma4]$ ./wisdom 127.0.0.1 jacky ELECS212-2010
[SENT] jacky
[RECV] 470760907
[SENT] f4ebf1ad626ba0653872301ba0b5d445
[RECV] Nothing is certain but death and taxes.
[tma4]$ ./wisdom 127.0.0.1 jacky ELECS212-2010
[SENT] jacky
[RECV] 2024027421
[SENT] 0390ca7f7d0720a3b5a099c26c0982e8
[RECV] Only fools and horses work.
[tma4]$
```

The authentication server has been written for you. Your task is to write the client program only.

Copy all files from the ~jacky/public/tma4 directory into a tma4 directory under your home on the server. You only need to modify the file wisdom.c (and optionally, wisdom.h, if you find it necessary).

Some hints have been provided in the provided template source file wisdom.c. Please read them carefully.

To compile the server and the client programs, use the commands "make server" and "make client" respectively. For details, you may inspect the provided Makefile yourself.

To test your program, you will need to modify SERVER_PORT defined in wisdom.h. We suggest you to use the port 8xxx where xxx are the last 3 digits of your student ID.

Make sure you place all files under a tma4 directory under your home on the server. Otherwise, you may not earn any mark for this question.

Question 3 (21 marks)

Online banking (or e-banking) is a common place in our daily life. However, it would not be successful without trust models of PKI (Public-key infrastructure, an authentication infrastructure based on public key cryptography). Use your own words to describe the following terms. For each of them, give **an example** that is specific to your online transaction with an e-banking service.

(a) Asymmetric key encryption algorithm

(b) Public key

(c) Certification authority (CA)

(d) Digital certificates

(e) X.509

(f) Digital signature

(g) Transport Layer Security

Question 4 (24 marks)

A new European style Café s will be open in Wan Chai, Hong Kong. The business owner would like to deploy a wireless LAN ordering system so that waiter or waitress can take order right from the spot of the customer's table using whatever appropriate handheld device you recommend. The Café will also provide both wireless Internet access and a few wired PCs with Internet access for customers' use.

Write a technical proposal (including, but not limited to, the network design, recommended Internet access method and cost estimation) on how such a cost-effective system can be deployed. In your proposal, you DO NOT need to discuss on the project management perspective. You can address the key objectives in network design and discuss the conflicting factors that can cause network design to succeed if they are balanced well.

Note: This is an open question and draws on many aspects of the knowledge you learned from the course. You can make any reasonable and logical assumptions.

END OF Assignment 4