CS4615 - P2 - NETWORK AUTHENTICATION PRACTICAL

Overview

The task in this practical is to extend the provided Client/Server such that CHAP authentication is included. Client and Server execute a simple data exchange as shown in Listing 1 and Listing 2. The protocol uses messages in JSON format; the client sends a HELLO message to which the server responds with a HELLO_ACK message. Thereafter the Client sends a DATA message and the Server finally responds with a CLOSE message. The aim is to expand the messages (include additional fields) such that the Client can be authenticated by the server when receiving the DATA message.

```
connecting to server
connected to server
--> sending HELLO
--> sent data:  {"sqnr": 1, "type": "HELLO"}
waiting for message from server
<-- received data: {"sqnr": 1, "type": "HELLO_ACK"}
<-- HELLO_ACK received, connected!
--> sending DATA
--> sent data:  {"sqnr": 2, "type": "DATA", "data": "DATADATADATA"}
waiting for message from server
<-- received data: {"sqnr": 2, "type": "CLOSE"}
<-- CLOSE received
connection closed
```

Listing 1. Client Side

```
starting server
client connected to server:  (’127.0.0.1’, 59978)
waiting for message from client
<-- received data: {"sqnr": 1, "type": "HELLO"}
<-- HELLO received, connected!
--> sending HELLO_ACK
--> sent data:  {"sqnr": 1, "type": "HELLO_ACK"}
waiting for message from client
<-- received data: {"sqnr": 2, "type": "DATA", "data": "DATADATADATA"}
<-- DATA received: DATADATADATA
--> sending CLOSE
--> sent data:  {"sqnr": 2, "type": "CLOSE"}
connection closed
```

Listing 2. Server Side

Comments

As challenge a random integer number can be provided. A random integer number can be created with the function *random.randint()*. An MD5 hash can be created using *hashlib.md5()*. The user password can be stored at client and server in cleartext.

CS4615 Continuous Assessment - PART 2

Please submit an answer to the following question with your CS4615 Continuous Assessment. Your answer should not be longer than half a page (You can use figures or code pieces to illustrate your answer).

Question P2 [2 MARKS]: Challange Collision Probability

Assume in a CHAP authentication a 32bit integer is used as challenge. Assume that k authentication procedures are carried out. What is the probability that all k challenges are unique? Plot the result as a graph (probability in dependence of k).