Boran YILDIRIM
21401947

Homework 1

CS 442
February 25, 2019

Question 1

What is the difference between authentication and authorization?

First define the meanings of two terms:

Authentication: The process or action of verifying the identity of a user or process [1].

Authorization: A document giving official permission [2].

Authentication is done to identify users of the system by using credentials such as email, username and/or password. For example, when a person opens *facebook.com*, system asks his/her email address and password to identify the user. Once user enters his/her credentials correct, *facebook.com* confirms his/her identity and shows the profile or homepage belongs to him/her. The main purpose of authentication is identifying who you are.

Authorization is done to determine users access level after the authentication process is successfully operated. For example, after a user successfully enters *facebook.com*, s/he may choose to upload new photos or delete existing ones of his/her photos. S/he also sees other people's photos, which stands for *read* access. However, s/he cannot delete someone else's photo since s/he is not authorized to *write* to other people's database information.

To conclude, authentication is about who you are and authorization is about what you can *read/write*.

Question 2

What is public-key cryptography?

Public-key cryptography, aka asymmetric cryptography, is a cryptographic system that uses pairs of keys [3]. One of these keys is public and other is private. Public-key can be distributed publicly without considering any security issue since encrypted message with public key can just be decrypted by private-key. On the other hand, private-key must be kept privately to secure the system. This encryption work as one way so if someone knows your public-key, s/he cannot derive private-key.

Question 3

Describe the steps needed to login using public key cryptography.

1. New key pairs for ssh authentication are created by *ssh-keygen* which is a tool for creating new authentication key pairs for ssh [4]. *Public* and *private* keys are created with *ssh-keygen*.

   ```
   ssh-keygen -t rsa -b 4096
   ```

   Private key file *id_rsa* and public key file *id_rsa.pub* are generated by RSA algorithm [5] using 4096 bits.

2. After login with password to the ssh server, *authorized_keys list* is added to server by using commands below.

   ```
   mkdir -p ~/.ssh
   touch ~/.ssh/authorized_keys
   ```

   By using *ssh-copy-id* generated ssh key is installed to server as an authorized key.

   ```
   ssh-copy-id -i ~/.ssh/id_rsa.pub user@host
   ```

   This logs into the server host, and copies the public key to the server, and configures them to grant access by adding them to the *authorized_keys list* [6]. Just public key is copied to the server, private key *id_rsa* is kept secretly on local machine.

3. After logout and login back to system as before, system authenticates *user@host* without asking password. It uses the generated *private key* on local machine.

To identify the user, ssh server encrypts a file with *public key* to challenge the client. If the client has the corresponding *private key*, it will decrypt the message and show it owns the associated *private key*. Then, server can setup the connection for the client.

References

[1] Authentication dictionary meaning
https://en.oxforddictionaries.com/definition/authentication

[2] Authorization dictionary meaning
https://en.oxforddictionaries.com/definition/authorization

[3] Public-key cryptography
http://en.0wikipedia.org/wiki/Public-key_cryptography

[4] ssh-keygen
https://www.ssh.com/ssh/keygen/

[5] RSA algorithm
https://en.0wikipedia.org/wiki/RSA_(cryptosystem)

[6] ssh-copy-id
https://www.ssh.com/ssh/copy-id