Authentication - Theoretical

Warm-up quiz

What is the purpose of authentication?

- The process of verifying the identity of an entity
- Mechanisms preventing unauthorised users access to resources
- A cryptographic primitive
- An MD5 hash

Passport control at the airport is an example of?

- Knowledge-based authentication
- Inherence-based authentication
- Possesion-based authentication
- A brute-force attack

Alice wants to encrypt a message to Bob using an assymetric encryption scheme. Who needs what keys?

- Alice needs Bob’s private key; Bob needs her public key
- Alice and Bob both needs each other’s public and private key
- Alice needs Bob’s public key; Bob needs his private key
- Alice needs her private key; Bob needs his private key.

Alice wants to send a message to Bob in such a way that he’ll know it came from her. She should:

- Encrypt the message with Bob’s private key
- Encrypt the message with her public key
- Encrypt the message with Bob’s public key
- Encrypt the message with her private key

Means of authentication

In general terms, describe what are three means of authenticating a user's identity.

Access control - Theoretical

Warm-up questions

- What is access control?
- What are the core elements of access control?
- Which of the security properties (CIA) does access control achieve?

Types of access control

- What are the characteristics of the type covered in today's lecture?
- How do these compare?
- Is there an argument to implement more than one type?

Capabilities

- What is a capability in the context of access control?
- What are typical ways of implementing these?

Access control - practical

File permissions in unix

Make a new file in kali called **test.sh** Make sure it contains the following:

```
echo "Hello World"
```

You can determine the current permissions that a file has on Linux by running the `ls -l`. Make sure the command `whoami` returns **kali** before doing the following.

- Use the given command to view the permissions of test.sh and determine what rights your user has.
- Why are you able to run the file using "bash ./test.sh" but not using "./test.sh"? Hint: determine your permissions on the bash program and compare.
- If you use the command `chmod 501 ./test.sh` on the file you are able to execute it using "./test.sh". Why is this?

- Use the command `sudo chown root ./test.sh`. You are now no longer able to execute the file. Why?
- Why does chmod 777 give read, write and execute permissions to everyone?

Permissions masks in Linux

- What is a permission mask?
- What effect would it have on new files if the command umask 0066 was run before creating them?

ACL in Linux

An alternative to using the standard unix permissions is to use ACL. You can change the ACL by using `setfacl -m` An example of a full command could be the following:

```
setfacl -m g:root:r testDir/
```

If we break down the command then the -m parameter means you want to modify it the current acl, then the "g" defines you are changing the permissions of a group, root is the the group being changed, and r is the permissions given. When you have changed the permissions using the setfcl command you are able to check them later using the getfacl command. The output of ls-l will also show a + denoting the given folder/file has ACL enabled.

- If instead of using "g" in the above command, you had replaced it with u, what would the difference be?
- By default, the ACL is only applied to the given file/folder. What is the easy way to apply it to all files inside of a folder?
- Similarly, whenever a new file/folder is created in a directory where ACL is enabled, it will not apply it to the new file. How would you make it enforce this for all new files?
- Figure out how you can remove ACL rules. There are two ways, either removing all of them or just a specific one.