10.5 Question 5

10.5.A Which of the following would you pick? Why?

Telnet vs SSH

As stated on slide 30 from the lecture SSH was intoduced in order to replace Telnet. Therefore SSH would be preferrable for a secure remote logon facility.

Public key vs password authentication in SSH

The password authentication in SSH is better as SSH keys are much more difficult to hack than passwords/public keys and therefore are more secure as they can have a length of up to 4096bits making them more complex and harder to brute-force. Furthrmore, the actual private SSH key is never sent to the server, hence making it impossible for malicious attackers to access the account only by hacking into the server. In the end the SSH key can also be multi-factor authenticated by adding a password.

Local database vs certified host name-to-key association SSH trust model in a small company with 5 employees for allowing them to SSH to a company server when they work remotely

As the local database needs the client to know the host's public key it would be better to use the certified host name-to-key association. Furthermore, as the company is rather small this approach is much more suitable. If the company would be larger a CA is needed in order to improve the operability and security (https://smallstep.com/blog/use-ssh-certificates/).

10.5.B Which SSH channel types would you use in the following scenarios?

You want to be able to connect to your company's internal network protected by a firewall when working from home

On slide 43 from the lecture this scenario is solved by using **remote port forwarding**.

You want to run AutoCAD installed on a remote server

As AutoCad is a graphical display the channel type would be **X11**.

You want to list running processes on a remote Linux host using *ps* command

A good option for this scenario would be to use a **session channel type** in order to execute the system command *ps* on the host.

You have a database running on a server and you want to access it remotely over a secure channel

The best option would be **local port forwarding** as this maximizes the security due to the use of a tunnel.