Computer Networks Fall 2016
Problem Sheet #5

Tom Wiesing

November 15, 2016

1 Problem 5a

1.1 Problem

What is an SSH subsystem?

1.2 Solution

As described in the *ssh man page* a subsystem (usually given in the form of a remote command with the `-s` flag) is is a software that provides faciltitates for ssh to be used as a secure transport layer for other applications.

2 Problem 5b

2.1 Problem

What does the following configuration of user joe do? Explain each line in your own words.

```
Host            *
ControlMaster   auto
ControlPath     /users/joe/.ssh/%r@%h:%p
ControlPersist  10m
```

2.2 Solution

This configuration allows multiple ssh clients to share a single connection. The first line makes sure that all following lines apply to connections to a host matching the pattern *, i.e. to all hosts. The second line tells SSH to automatically make use of existing connections or if they do not exist, to create a process running in the background without asking. The third line tells SSH where to store which process in the background is connected to which host. In this case it should be stored in a file /users/joe/.ssh/%r@%h:%p where %r will be replaced by the remote username, %h will be replaced by the remote hostname and %p will be replaced by the remote port. The final line tells ssh to terminate background processes 10 minutes after the initial connection using it has been terminated.

3 Problem 5c

3.1 Problem

What is the effect and purpose of the following command?

```
ssh -nNt -L 8888:ieeexplore.ieee.org:80 joe@server.com
```

How many TCP connections are involved and what are their endpoints? Which TCP connection carries encrypted traffic, which TCP connection carry plaintext? In which situations is this useful?

3.2 Solution

The purpose of the command is to allow local TCP connections to port 8888 to be securely forwarded to the server at `server.com` and from there (unsecurely) forward them to port 80 on `ieeexplore.ieee.org`.

We will now discuss the command one flag at a time. In general the command establishes a connection to `server.com` as a user `joe`. The `-n` command prevents any further input to the server from being read from `stdin`. The `-N` prevents any remote command (that would usually be started automatically) from being executed. The `-t` prevent a terminal from being allocated on the remote server. The `-L 8888:ieeexplore.ieee.org:80` enables the forwarding of TCP connections. This consists of three parts, the local port `8888`, the destination `ieeexplore.ieee.org` and the destination port `80`.

Overall, the command sets up 1 TCP connection and 1 additional per local connection to `localhost:8888`. The first TCP connection is the one that establishes the ssh connection to `server.com`. This TCP connection carries encrypted traffic. Per (plaintext-carrying) connection to `localhost:8888`, the traffic is sent through the existing SSH TCP connection and then from `server.com` a new TCP connection to `ieeexplore.ieee.org` on port 80 is established. This connection is also carrying plaintext.

4 Problem 5d

4.1 Problem

What is an SSH agent? What is the effect of the `-A` option in the following shell command? In which situations is this useful?

```
ssh -A joe@server.com
```

4.2 Solution

An ssh agent is the part of SSH that takes care of authenticating the user on the remote server. With the `-A` flag, the agent is forwarded to the remote server. This allows any ssh connections started from the remote server to use any authentication method stored locally. This can be useful when using a server as an entry point to a system that is otherwise protected from the outside.