Operating Systems with C/C++
Semester 1, 2013
Eike Ritter

The University of Birmingham
5 November, 2013

Assessed Exercise 3

Deadline: Friday 22 November, 4pm

The Task

The purpose of this exercise is to write part of firewall in user space. The firewall should implement checks on outgoing DNS-queries. More precisely, the firewall maintains a blacklist of sites for which DNS-queries are rejected. It also maintains a list of sites which have been queried (including the ones which have been rejected).

Your program should work as follows:

- You should use the `netfilter-queue`-library on the virtual machine provided. This library is not installed by default–install it with the command

  ```
  sudo aptitude install libnetfilter-queue-dev
  ```

  You need internet access to do this. You need to do this only once.

- The netfilter-queue-library lets you handle each packet which has been re-directed by the kernel firewall code in user space. To set this up, you need to initialise the kernel firewall with

  ```
  sudo iptables-restore ⟨directory⟩/iptables.conf
  ```

  where the file `iptables.conf` is available from the webpages. The number after `--dport` is the port number for which the kernel-level firewall passes all packets arriving on this port to user space.

- An example user space program which demonstrates the use of the netfilter-queue library can be found on the webpage.

- You should provide two programs. One is the server program which processes the packets supplied by the kernel and maintains the blacklist and the list of sites have been queries. The other program is the client program has commands for displaying both lists, and setting the blacklist. A new blacklist overrides the old one. The communication between these two programs should use sockets.

- To make marking easier, the server program should accept exactly one argument, namely the port number it listens on. There should be two ways of calling the client program. The first one is

  ```
  <program> <hostname> <port> L
  ```

where `<program>` is the program name, `<hostname>` is the hostname where the server program runs and `<port>` is the port on which the server listens. This way of calling the client program outputs the list of requests and indicates whether they have been accepted or not. The second way of calling the program is

```
<program> <hostname> <port> W <filename>
```

where `<program`, `<hostname}` and `<port>` are as above, and `<filename>` is the name of the file containing the blacklist. This file contains one line for each site which is to be blocked. This way of calling resets the list of blocked sites.

- Use of the netfilter-queue library requires root privileges. Hence only root will be able to execute these programs successfully. You should abort immediately with an error if a non-root user tries to execute these programs. Use the system call `geteuid` for this check. The root user has always a user ID of 0.

- You need to ensure that your program handle concurrency correctly. In particular, as packets may arrive at any time, several instances of the procedures handling the packets may be executed at the same time.

You may assume that each packet for the outgoing port 53 is a DNS-packet. The site which is queried is stored from byte 54 as follows: for each component of a site (the string between dots), first the length of the component is stored, and then the component itself. If the length of the next component is 0, the end of the site has been reached. For a visualisation of the packet structure, use wireshark with the filter `udp.port == 53`.

Marking Scheme

Please use the School submission system for submitting your code. Please submit only the source files you have written yourself. We will compile and run your code on the virtual machine and mark it accordingly. Please in particular note that we will use the compiler option introduced in the lecture and will deduct 6 marks immediately if there is any compiler error or warning.

We will award marks as follows:

- 5 marks for correct usage of the netfilter_queue library.

- 5 marks for correct handling of the blacklist.

- 5 marks for correct handling of the list of outgoing queries.

- 5 marks for the correct functioning of the program displaying the list and setting the blacklist.