7 Security (mgk25)

(a) (i) What effect does the Unix/Linux/macOS system call chroot have (or the GNU/Linux command-line tool of the same name)? [2 marks]

(ii) What kinds of resource can chroot restrict access to? How can the developer of a program P use chroot? How can the user of a program P use chroot? [4 marks]

(iii) Why would a developer or user of a program want to do this? Give a concrete example. [4 marks]

(iv) Name two other kinds of resource on a Unix system for which access is not affected by chroot. [2 marks]

(b) User jane types the following three commands into her Linux shell:

```
$ id
uid=1002(jane) gid=1002(jane) groups=20(dialout),513(staff)
$ ls -l ptool
-rwsr-xr-x 1 ptusr ptgrp 59640 Mar 22 2020 ptool
$ ./ptool
```

(i) State the various user and group identities associated with the started ptool process, by copying and completing the following table:

<table>
<thead>
<tr>
<th></th>
<th>real</th>
<th>effective</th>
<th>saved</th>
</tr>
</thead>
<tbody>
<tr>
<td>user ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>group ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>supplementary groups</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[4 marks]

(ii) Which values is the ptool process permitted to provide in the seteuid() system call? [2 marks]

(c) Microsoft’s Active Directory Domain Service stores information about users and computers in an LDAP object tree. It controls access to such objects using an extension of the access-control list mechanism also used for Windows NTFS files. What additional field does Active Directory ACEs use compared to NTFS ACEs and what is its purpose? [2 marks]