Doing your part for security

Yeo Eng Hee

(SVU/Acad Computing, Computer Centre)

While, most of SVU’s systems have strong security measures, users also need to be aware of the part they can play in making SVU a more secure environment for everyone. Userids and passwords need to be managed properly, including regular changing of password, choosing string passwords and using secure means of logins to SVU systems. With everyone’s cooperation in observing these simple guidelines, we’ll be able to maintain a safe and secure environment for everyone to work in. Remember, if a system is compromised, everyone suffers.

There has been a rise in the number of security attacks as observed in the SVU system log files. If you have a system that is connected to the Internet, do not be surprised to see, in your system log files, entries that indicate attempts by external hackers to gain login access via commonly known account names, such as, root, admin, guest, test, etc. Thankfully, most of our systems have strong security measures, such as using ‘strong’ passwords, disabling of the guest account and other commonly used account names.

On the part of the user, it is also important to note that the user’s own account may also be at risk, if users are ignorant of some of the security measures that they can take to safeguard their own account and data. We would like to list out some of them:

Userid and password management – it is important that you do not share your userid or password with anyone. Firstly, if a hacker knows your userid, he already has one foot in the door. Now he only needs to guess your password. Therefore, do not make your userid commonly known. In addition, your choice of password is also an important safeguard, as easily guessable passwords will make it easy for programs to go through a dictionary list of words and permutations of the words to guess your password. Examples of weak password may be your birthday (8Nov1984), your home address (angmokio, or even angm0k10), or your phone number. So, how to choose a strong password, and yet make it easy to remember? Use the following guidelines:

- Do not use dictionary words, or variations of dictionary words
- Use a combination of alphabets and numbers, even other symbols like +, -, $, etc. Caveat: I’ve noticed some users use control characters, for example CTRL-C, but beware, some systems may interpret these special characters differently. So, it is better to avoid them.
- Use upper and lower case characters.
• Use long passwords – note that for SVU systems, some operating systems do not accept more than 8 characters, and this leads to problems logging into these systems. Therefore, a suitable length would be 6-8 characters, nothing less.

• Use mnemonics – for example, “I love to go fishing at Changi” may translate to IltgfaC. But make sure that the phrase is not a commonly used phrase.

**Change your password frequently** – yes, it is a chore, but changing your password regularly will ensure that your password is always known to you, and you only. Your password may have been guessed, but the hackers may continue to use it secretly, if he covers his tracks properly. Changing passwords will prevent this.

**Telnet and FTP are not secure** – many may not be aware that these older communication protocols are not encrypted. It is very easy for a hacker to examine your network communication packets to obtain your keystrokes and so, whatever you type will be seen by the whole world. Do you dare to type your userid and password in a telnet and ftp session? So, what do we use instead of these? Ssh and sftp are secured versions of telnet and ftp respectively. Communications are encrypted in the packets, and therefore, harder for hackers to see what you type. Although setting up ssh may be more involved, it is worth it to use these encrypted protocols. Some systems, for example newer versions of Linux, are already using ssh as the default and ssh comes pre-installed in these systems.

With everyone’s cooperation in observing these simple guidelines, we’ll be able to maintain a safe and secure environment for everyone to work in. Remember, if a system is compromised and had to be brought down, everyone suffers.