SUID, SGID and the Sticky Bit

There are also some more special permissions. You can add this by prepending another number in the **numeric mode** of the **chmod** command. These special permissions are **SUID** (4), **SGID** (2) and the **Sticky bit** (1).
SUID and **SGID** are usually set on the executable files. If the **SUID** is set on an executable file, that means that the file will be executed from the file owner. In other words, the effective user that runs that file will be the file owner, no matter who you are logged in as.
Same goes for the **SGID**. The file will be executed with the member of the file group, it doesn't matter if you belong to that group.
If the **SGID** is set ona a directory, all of the files created in it will have the same file group as that directory.
Sticky bit is usually just set on directories. It will prevent anyone from modifiying files in that directory, with the exception of the files they own. Only the owner will be able to remove his own files and noone else.
These permissions will be shown instead of the **x** execute permissions. **s** in the place of the file owners execute permissions means that the **SUID** is set on that file. **SGID** will be represented with **s** also, but in the place of the file groups **x** bit. **t** represents **sticky bit** in the place of the others permissions execute bit. If these letters are lower-case, that means that the underlying execute bit is also set on the file. If they are upper-cased that means that the execute bit is not set in that place.