**Permissions**

In a Unix-like operating system, permissions control who can do what to which files and directories. The permissions of an individual file or directory are visually represented as a 10-character string:

drwxrwxrwx

Your browser does not support playing HTML5 video. You can instead. Here is a description of the content: Linux-filepath-permissions

Let's break down each character. The first one just tells you whether you're looking at a file or a directory:

* -: Regular file (e.g. -rwxrwxrwx)
* d: Directory (e.g. drwxrwxrwx)

The next 9 characters are broken up into 3 sets of rwx and represent the permissions themselves for the "owner", "group", and "others", in order. Each group of 3 represents the permissions for reading, writing, and executing, in order. So, for example:

* rwx: All permissions
* rw-: Read and write, but not execute
* r-x: Read and execute, but not write
* The first 3 characters are "owner" permissions. The "owner" is usually just the user who created the file or directory, but it can be manually changed.
* The next 3 characters are "group" permissions. Unix-like systems support groups of users and a file or directory can be assigned to a single group. To be honest, unless you're a system administrator, you won't often worry about groups.
* The last 3 characters are "others" permissions. This is everyone else.

In my experience, when you're doing programming work on your own local machine, you mostly just care about the "owner" permissions because that's usually you. Here are some full examples:

* -rwxrwxrwx: A file where everyone can do everything
* -rwxr-xr-x: A file where everyone can read and execute, but only the owner can write
* drwxr-xr-x: A directory where everyone can read (ls the contents) and execute (cd into it), but only the owner can write (modify the contents)
* drwx------: A directory where only the owner can read, write and execute