## WEEK 3 ASSIGNMENT

**1. Research your current device and identify the following:**

1. The operating system of the device

*Currently my main desktop is dual booting into windows 10, and then into Pop OS.*

1. The kernel that operating system uses

*Windows uses its own hybrid kernel called "Microsoft Windows NT kernel" which is often referred to as a hybrid kernel. It combines the monolithic kernel and microkernal architecture. The main reason for this is usability. The hybrid nature of the kernel allows for either direct procedure calls or interprocess communication which talks to different modules.*

*Pop OS being a Linux operating system uses the monolithic kernel. The most common reason for this is resource management. monolithic kernels are very light weight in the sense that they will run more efficiently because of their architecture where all everything can run in a single address space.*

1. The release cycle of patches for that operating system

*Windows typically releases patches semi-annually but also push out more immediate patches if they are needed.*

*Pop Os is actually very fluid in their releases and tend to only release patches either when they are needed or when their parent OS ubuntu releases their own patch which tends to be about once a year. Out of all the Linux OS's pop os is one of the few that has constant patches from my experience since they are always trying to increase performance.*

1. How those patches are applied

*With both of the OS's a updating procedure is required in order to install the most recent patch. Windows patches are often pushed to a device and then auto downloaded and it’s up to you to choose if you want to update or not (if you have your setup right :) ) With Pop OS they have notifications as well when there is a system patch but you then have to run the "upgrade" utility in order to download and install it.*

Discuss the responsibility of the system owner (end user) in applying the patches. Can the end user prevent patch application? What are the positives and negatives of this approach?

*One of the constant problems that people always seem to mention with windows is that it auto updates. This is very true especially if you don't deselect the auto update setting which they purposely make it hard to find for a normal user. And even with that auto update deselected it sometimes will still update by itself. With Pop OS its entirely up to the user which is good and bad depending on your knowledge of command line. For my it’s great because I can absolutely control when patches are installed. On the negative side not having forced packages can ruin your OS experience because you forgot to install them and therefore run into problems.*

**2. Explain the difference between physical separation for security and temporal separation for security in a computing environment. Provide an example of each.**

*Temporal separation is the idea that you must operate at the right time for security to be present. It can be implemented in many ways, such as using locks, time-of-day password rules, and authentication mechanisms. time-of-day password rules could be one of the most effective ways to implement this type of security since it limits the possible times and ways someone can attempt unauthorized access.*

*Physical separation separates the equipment itself. It is the most basic type of separation and may involve physical obstacles like walls, doors, guards, etc. One of the problems with physical separation is that there is a cost to implementation. However, this type of separation is very important because equipment that is stolen or damaged cannot be used to steal or damage data from other computers.*

**3. What are the four basic permissions applied to code or data in a computer system? What other modes of access might you want to apply to code or data?**

*Read, Write, Execute, and Delete are the four basic perms that a computer system has, and they do exactly what you might think they do. In windows system for file system structure there are also permissions like full control, and list folder contents which is basically granting view perms to folder/file structure.*

*There are also access control perms which can authorize or not authorize users to access certain files and therefore programs or parts of the system.*

**4. Why should the directory of one user not be generally accessible to other users (not even for read-only access)?**

*Because that’s a breakdown in security. For instance, that one user could have permission to access a folder of files that isn't even known about or supposed to be known about by other users. So, by enabling them to see that users directory that they can therefore see that the folder or files exist.*

**5. What does it mean to have “Execute” access to a file?**

*This means that the file is available for you to run as a program file. This is something that you become very familiar with in Linux OS's since many custom files need to be granted permission to run as a executable file in order to run the program that is written in them. In a windows circumstance you are not always aware of this file permission but it’s there in order to tell the system that it’s a program file that is designed to run as a program.*