5793

Group B

Word Count: 801

Meeting Time: MW 1500

March 16, 2016

Apple Security

Apple has always prided itself in the security of its products, even to the point that the majority of Apple users feel safe using using Apple computers without a virus protection software. As the technology has become more entangled, the need to keep users safe has increased. When Apple released their new operating system, OS X El Capitan, they decided to remove user access to the system's most important files; the current security system does not allow non-Apple verified products to install anything in the top level directories of the operating system. Under Utilitarian ethics, it is unethical for Apple to take away a user's access to his or her own operating system.

Apple's removal of top level permissions appears at first to be a smart choice on their part. Apple reasoned that they wanted to protect their users by not allowing malicious programs masquerading as friendly applications from installing themselves in the heart of the operating system. Under Utilitarianism, there is a lot of good produced by doing this. Apple is preventing common users from acquiring viruses due to not being computer literate. This action produces a lot of good for both Apple, who gains more support from their users, and the users themselves, who are secure. However, not all Apple users are developers; in fact the majority of programmers use Apple machines (Purdy). This is due to the accessibility of programming tools available for Apple. In addition, OS X is a UNIX based architecture. UNIX based architectures are meant to allow users to have complete control over the operating system. By removing the access to the top level directories, developers are forced to forgo installing many open source programs that are not approved by Apple. This hurts developers who produce new software and do not want to buy in to the Apple

Developer's Program. In addition, many tools that developers rely on are blocked from installation, which affects the productivity of developers. Since Apple's user base is more developers than common user, this produces a lot of harm.

Rule and Act Utilitarianism appear to favor the developer's who use OS X, but developers are not the only consumers of Apple products. To a general consumer, Apple has made a safer operating system; but has also denied users access to critical files of the operating system. Apple computers, though less likely to contract viruses, are still able to be infected. Just because a computer has locked a user out of a directory does not mean that a virus cannot find its way in. In this case, it is significantly harder for businesses that repair Apple computers to fix the problem. While employees at the Apple store may be able to handle such a situation, not everyone has access to an Apple store. Therefore, this action actually produces more harm then good.

Apple's implementation of the security features included in El Capitan was not widely known when the new operating system was announced (Haslam). Apple forces developers who want to use the Apple Store to distribute applications to sign up for a developers account. The account is not free; it costs developers $100 per year. It appears that Apple did not want to publicize the security features since it would drive developers away from using the new operating system, and therefore depriving Apple of developers who could be forced to pay to use the Apple Store. Under Act Utilitarianism, this is not necessarily a bad action. From an individual perspective, Apple does need to make a profit, and they do distribute, for free, the operating system and the majority of the tools developers need. Under an Act Utilitarianism, the goods provided by Apple to the developers contributes more good than overall harm done by the forced security measures. Rule Utilitarianism, however, focuses on the ethical actions being willed into universal rules (Quinn 75). Under Rule Utilitarianism, Apple withheld important information about its operating system from both users and developers alike. If all the important information about an operating system was omitted, then no one would use that operating system. Overall, Apple is not only hurting itself, but also its all of its consumers.

Apple's decision to block access to root files has caused many developers to completely rework

their products in order to allow users to continue to use them. Under both Act and Rule Utilitarianism, this can be seen as unethical, largely due to the fact that Apple did not publicize the new security measures included in the operating system. Apple, however, has promised a way to remove these features as the operating system becomes more popular. While this may help Apple make amends with the developers, the damage has already been done, and many developers have already designed their programs to work with the new security updates.

Works Cited

Haslam, Karen. “New security features in El Capitan and iOS 9”. 2015. <http://www.macworld.co.uk/feature/mac-software/el-capitan-ios-9-security-enhancements-3620858/>.

Purdy, Cameron. “Why do Most Professional Programmers Prefer Macs?” 2014. <https://www.quora.com/Why-do-most-professional-programmers-prefer-Macs>.

Quinn, Michael J. *Ethics for the Information Age. 6th Edition*. Boston: Pearson/Addison-Wesley, 2013.