Trent Giever

Case Project 1-4

What are Your Layers?

6/27/18

What are your layers?

The complexity of computer hackers has come along ways from the dancing animated “you been hacked.” The need to have protection in a dangerous cyber world with more and more data stolen reported, and the ease for criminals to get away with it because of crypto currency’s. One solution is to have multiple layers of protection to help protect from the dangers lurking in the fiber optic lines.

For the main computer I do most of my work on is a HP laptop that I got 7 months ago that consumer reports liked and seems almost as thin as a tablet but has fast 16 GB ram and 1TB hard drive and a dedicated 4 GB graphics card. The second computer I have at home that I use is another HP laptop mostly as a backup and is from 2011 and the graphics card in it would not handle Windows 10, so it is Windows 7 and is extremely slow from having only 6 GB ram after graphics takes its chunk. The third computer I use is the CBC computers in the library that are open for anyone to use. The computers are decent for how many users junk builds up on them and are much easier to print with the web print program on them. The fourth computer that I use the most is my iPad Pro 10.5 that I do many writing assignments and read canvas documents on.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | New HP Laptop | Old HP laptop | CBC computers | iPad Pro 10.5 |
| Layering | The network has a password, and then the computer is not discoverable on a network for sharing to decrease the hack potential. The computer has both the Microsoft defender and the defender program from charter to protect the computer from viruses. | The same as the new HP but does not have the Microsoft Defender since it is part of newer versions. The computer is also more at risk by not having updates to fix flaws. | To gain access to any of the important items that a student hacker would want like changing grades would have to go through multiple layers of protection both locally and on the server system | Apple allows someone who has tried more than 10 times to break into the device can cause a complete wipe. Any changes to the account require 2 factor authentication and works with a different device on the account or by text/email. |
| Limiting | The home computer is pin protected and once login has happened can change any settings. | The old computer is password protected and once login and wait about 15 minutes to get the computer fully started can then change any settings. | The computers can only be logged in by the school log in account. After login the student/ professor (not computer science) has a limited ability and can make no changes to the computer that is not needed for the basic user. | The iPad is pin protected, and only a few apps have pin protection, and the Apple password book is finger print protected. |
| Diversity | The diversity of having both the security of having both the Microsoft defender and the charter defender program can have two different programs that protect the system. | Not much diversity in the system. | I don’t know the exact layers but has to be a diverse mix of tactics to prevent the cyber Security students from changing all of the grades to 4’s with unknown tactics. | The iPad is secured by Apple, and Apple does a good job at protecting the devices from viruses and protecting the patients to reduce the risk of a problem. |
| Obscurity | The computer scan happens on a constant weekly time, and could allow a system hack happen for 6 days 11….. hours without being noticed. Not very secure in obscurity. | Since the computer is not used much it is very secure obscurity. | The exact Obscurity is not known but has to some extent exist. | The iPad Obscurity is the random backups during charging to safe guard the data. |
| Simplicity | The security and ease of the computer allows my non-techie mother to be able to open the programs and click the button to run security scans. | The computer is like the new one but is only slower. It is also the Microsoft version my mother prefers from years of using. | CBC has make it easy to login and be able to do what the average computer user’s needs. | Apple has made simplicity that anyone can use, but still safe. Compared to some androids that come pre-installed with viruses from kind makers. |

What I found during the research into the varies computers is that most devices are perfect in one category, but terrible in a different category. The trick is to find the balance for the need of the system. The balance that I find while researching is like a key under the door mat that will slow down, but not stop the thieves wanting in (Karl, 2008). The system needs the be simple for a new hire to learn, but at the same time can’t be giving away data from it being easy to read. One solution is to make the variables and flow of code the most difficult to read for non-trained person at the computer/server place. The next important idea is to limit how many people have access to the knowledge of the system since 58% of unauthorized access comes from insiders that know the system (Ciampha, 2018). The next idea is that random changes to the system like updates and security scans can make would be attackers not as likely interested in this system. The diversity part I found online is that the U.S. network infrastructure is not vulnerable to an all-in-one attack by being a mixture of different types and levels of security that are protecting the servers’ data from attackers. Small scale attacks are possible like the east coast attack a few years ago that crimpled the networks but must be very techie to be able to launch all the needed viruses at the same time before anyone noticed it to be able cripple the U.S. or the world (cdixon, 2010). The last category is to me the one that is a combination of all the others and that is layering. Layering is to have different safeguards hidden so that one trap does not open the credit card data but must go through several very different tasks to reach the more challenging and less instant rewarding data. To have good layering is a combination of all four of the others that makes the data less desirable. The computers above have different methods for securing the data, but the biggest thing is that they all have different layers that are slightly unique that makes them harder to stop working after the first virus received.

In the ever-changing world of data misusage and data hacks it is easier to put data online with the mixture of layering at each data storage company that helps make each server system harder to steal data from. The current system is not perfect since viruses are more advanced than ever, and the ease of Facebook sharing someone’s data. A study came out a few years ago that if I am remembering correctly about half of bitcoin is used to move around illegal money like payments for viruses and drug money. The internet has changed to bring cat videos and have cat videos with viruses to trick the user. The need for the 5-basic computer/server security needs is getting more important than ever.

# References

cdixon. (2010, January 12). *Security through diversity.* Retrieved from cdixon.org: http://cdixon.org/2010/01/12/security-through-diversity/

Ciampha, M. (2018). *security+ guide to network security funamentals* (6 ed.). Boston, MA: Cengage.

Karl. (2008, December 7). *Whar real liefe examples of security by obscurity have you seen/ worked with?* Retrieved from Stackoverflow: https://stackoverflow.com/questions/347948/what-real-life-examples-of-security-by-obscurity-have-you-seen-worked-with