Chris DeVisser
ENGL 109
Prof. Jay Dolmage
2017-10-01

My High School Solution to Lost Flash Drives

Back in 2011, I went to high school, as would any normal kid my age. As time progressed, my friends and I were slowly discovering our love of programming. All of us took a number of computer classes, also spending our lunches and other free time on the school computers, discovering a breadth of techniques we could use to make our various arbitrary programs.

Naturally, our high school had put restrictions on the computers that we used day in, day out. This included usual restrictions like not being able to use the official registry editor (the registry can be thought of as computer-wide settings), but also restrictions that we found more annoying. Little did the school know, overcoming these restrictions was the perfect motivation. We began rigorously self-learning what we needed to make workarounds. As the school used Windows XP, we also emulated Windows 7 features such as Aero Peek (clicking the bottom-right corner to minimize all windows), and Aero Snap (dragging a window to the edge of the screen to make it fill that half of the screen). Before long, we had set our sights higher. By this point, we used school computers in a highly customized way. But performing all the setup for this every time we logged in was tedious. We wanted to be able to automate this setup when logging in. This is precisely what a logon script accomplishes, but these logon scripts were not made available by the school for us to use.

However, one day, we found out how to make it work. To tell the truth, it was an accident. One of my friends had put a third-party program into his documents folder. Next time he logged on, he noticed that this program was run several times. We used this to our advantage to write the logon scripts we so desired. Mine included replacing my entire school workspace with my trusty flash drive. Day by day, everything I cared about was on my flash drive. The last step was moving my actual school desktop and documents to the flash drive. With the help of my logon script, the desktop that loaded would actually be stored on my flash drive, negating the possibility of forgetting to take home an important file. Because of constantly moving between school and home, having my flash drive as a common workspace was life-saving for effort.

As our high school life continued, we enjoyed our newfound ability, but we still didn't know why it worked. We desperately wanted an answer. And one day, we found one. In a semi-hidden network location, we discovered the school's own logon scripts, along with all other schools in the board. However, within these scripts, we also found credentials for a curious network account. It was a special-purpose account that didn't have access to much, but it fueled our desire to find more. Two other goals we set, for curiosity's sake, were printing without expending credits, and bypassing the monitoring software used by teachers to watch and control students' computers. With so much free time and determination, we eventually discovered multiple ways to do both.

We continued to have fun discovering vulnerabilities and to set our sights ever higher. Eventually, our goal got as ridiculous as the potential for full control. While we would never interfere with the network, we were excited by the prospect of finding out that full control was possible. While not perfect, I did actually formulate a proof of

concept using my old friend, the logon script. I made a simple program that would log keystrokes. I would keep this program in a location accessible by everyone in the school, which was something we had previously figured out. There were two ways we could do something when a person logs in. The first was the one we discovered: The school's logon scripts would unintentionally run our own. This would be tied to the network account. The second was the normal Windows registry key that many programs use to start when the user logs in. This is tied to the computer, running when anyone logs into it. The idea was that the per-account logon script would set up the registry key to create a copy of the logon script for whoever else logs into that computer. By doing this, the program would spread to their account. Any computer they used after that would also be "infected". The computers were set up to discard registry changes every night, but this would not affect the "infected" accounts themselves. It is reasonable to think that once unleashed, the program would eventually spread to an administrator account, which we could detect and make use of.

Now I demonstrated that the idea worked in a very controlled environment, but of course we never actually went further than that. Regardless, we showed it had the potential, and that was good enough for us. After this, we discovered a more direct method of attaining our goal of full control. We found out how to install a program that would start when the computer starts and would not disappear overnight like changes to the computer's settings normally would. We also devised a strategy to perform this method across the network during the night. This was truly the height of what we did. We could make any program run on every computer. This is when I had a bright idea.

My flash drive was incredibly important to me. I used it constantly, at school and at home. Yet for something so crucial, I was very good at losing it; I bought a fair number of new flash drives over the years. What if there were a way for me to find my flash drive after losing it? Well, it just so happened that I had everything I needed to bring this concept to life. Thus was FDR born. Flash Drive Recovery. The saving grace for all the people like me who kept losing flash drives.

It starts with registering the flash drive. With the simple press of a button, the program would figure out a unique ID for the drive and record it in a file. Later, if the owner was anything like I was, the flash drive would get lost. At this point, another simple button press and the system would spring into action. Running on every computer from start-up, FDR would look for any USB devices being plugged in. When this happened, FDR could compare the unique ID and see if it matched any of the lost flash drives. Should the IDs match, FDR would record the time, user, flash drive name, computer, and room. This information would be accessible only to the owner and me. Then, the fun part could begin. From the username, we could use the student's real name to meet with them. The computer, room, and time would easily determine which class was present, if any.

After testing FDR myself, the time came to see it work from start to finish. I "lost" a cheap flash drive and waited. Later that day, I noticed activity. Venturing to the reported computer, I was able to find my flash drive. Success! But FDR's true moment would come later that year. It happened again. My flash drive was gone. Where had I lost it? I reported it missing to the program, and through a hunt that lasted a few days, I eventually found and recovered it. No more buying new flash drives all the time!

All in all, through information gathered by FDR and some cross-referencing, I had the ability to help any interested person in the school. But could I? For all intents and purposes, the program magically located the flash drive. But a large number of students using it would draw suspicion. In the end, the program had the potential to help many students – I even had a teacher inquiring about it – but in order to work, it had to shadily run in the background across the network. Did anything come out of it? Not really. But it wasn't pointless; all the learning I did so this could become a reality has certainly given me an edge in continuing my life as a professional software developer. I truly learned how to educate myself as needed and how to approach problems from different angles until something works.

Our other efforts were not in vain either. We handed the school board a large report documenting the vulnerabilities we found. They were not amused to say the least, especially considering that the ones conveyed here were the tip of the iceberg. In the end, though, everything worked out. The CEO of the school's monitoring software was impressed that we broke that, throwing us a pizza party, which we combined with a showing of *V for Vendetta*. But most of all, I can feel truly proud of my recovered flash drive.