Chris DeVisser
ENGL 109
Prof. Jay Dolmage
2017-09-26

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 pointless 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, but also restrictions we found more annoying. We started self-learning how to make workarounds for things like missing Windows 7 features (we had XP). Before long, we had set our sights higher. By this point, we used school computers in a highly customized way. But setting them up for this essentially every time we logged in was tedious. We wanted to be able to run a script when we log in, but these logon scripts were not available for us to use by the school.

However, we discovered one day 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 make 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 time 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. Other abilities we were curious about included bypassing the credits used for printing, and rendering useless the monitoring software teachers could use 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 could be possible. While not perfect, I did actually concoct a proof of concept using my old friend, the logon script. I made a simple program that would log keystrokes and did my setup. I would keep this program in a location accessible by everyone in the network. Specifically, a folder in my own account's space with appropriate permissions and the means to find it from elsewhere. There were two types of logon script available. The first was the one we discovered. When running the school's

logon scripts, we could hijack them. This would happen per network account. The second was the normal Windows registry key that many programs use to start when the user logs in. This happens per computer. The idea was that my account's hijacking logon script would set up the computer's logon script to create an account logon script for whoever else logs in. Thus, the program would spread to their account. Any computer they use after that would also be "infected". The computers restarting and reverting changes overnight would not affect accounts. It is reasonable to think that this could spread to an administrator account, which we could detect and use as wanted.

Now I made a proof of concept and demonstrated that the idea worked in a very isolated environment, but of course we never actually used the idea. 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 when the computer reboots. We also devised a way 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 important to me. I used it constantly, at school and at home. Yet for something so important, I was very good at losing it and needing to buy a new one. What if there were a way for me to find them? Well, it just so happened that I had everything I needed to make this happen. 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. With FDR running on every computer when it started, it would look for any USB devices being plugged in. When this happened, it could compare the unique ID and see if it matched any of the lost flash drives it was looking for. Should they match, it would record the time, user, computer, and room. This information would be accessible only to the owner and me, and 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 there, if any.

After testing it out myself, the time came. I "lost" a cheap flash drive and waited. Later that day, I noticed it being used. Going to the computer it was plugged into, I was able to find it. 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 was able 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, but in order to work, had to shadily run across the network. Did anything come out of it? Not really. But it wasn't pointless; all the learning I did in order for this to become a reality has truly given me an edge in continuing my life as a professional

software developer. I truly learned how to learn by myself and approach problems from different angles until something worked.

Our other efforts were not in vain. We handed the school board a large report documenting the vulnerabilities we found and what we did. They were not amused to say the least, especially considering what was mentioned here was the tip of the iceberg, but everything worked out. The CEO of that monitoring software was more impressed with how we broke that, throwing us a pizza party that we combined with a showing of V for Vendetta. But most of all, I can feel truly proud of my recovered flash drive.