**EMCS2430: Human Factors: People and Software**

2. The Danger and Reach of Malicious Software

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

Part I

*People sometimes say things like “I have a Mac, I should be fine!” What might they mean by this? And do you think they’re justified?*

This is simply a remnant of day past when OS’s like XP and DOS were simply “too easy” to hack, and most attackers decided to attack Windows machines. Consequently, Windows machines got a ( well earned ) bad reputation of being virus prone. Today the saying is not justified, is outdated and not based on anything that is real. When it comes down to it this mindset is just complacency. The only shred of truth in this claim is the fact that Apple users update their software more frequently and faster than windows or android users. Updated software is not impervious but it is hard to hack than software with known open issues.

<https://www.huffingtonpost.com/jason-glassberg/are-apple-products-really_b_10241742.html>

Part II

*What is the limit of the damage malicious software can do? It’s bounded by all the authority that you, the person running it, has. If you can read a file, so can it. If you can delete a file, so can it. If you can connect to the Internet, so can it. And so on. The program you are running is running as you. (If it surfs for child pornography, it’s doing so as you, too.) Not understanding that the program is essentially running on your behalf, and hence has all of your authorities, is a central problem in security.*

*The world of your smartphone or tablet—anything that runs Android or iOS (or other mobile operating systems)—is different. Can you see why?*

I am not sure there is a limit. RBAC systems have a bad habit of saving the names of users, their roles and the limit of authority in config files. It’s quite common that a hacker with use the current access to find other users, then assume their identity. In general, attackers will just keep moving laterally until they can find a way to escalate privileges.