Dominic Drury

06/24/2024

CS-410

8-1 Journal

Reverse engineering can be used to improve cloud-based IT systems by helping to identify security vulnerabilities through dismantling the source code, even if that code is either no longer supported or not available. Reverse engineering can also be used for a patch in a cloud-based system by breaking down the recent change and separating the old code from the new code.

I think that the speed in which everyone wanted everything to be a smart device, lead to a wave of people pushing the limits in terms of innovation without stopping to think about the security. I also think that we are seeing a second wave of the same problem as everyone wants to incorporate AI into everything (even if that thing doesn’t need it). This fast-paced push to release new things faster and faster means that one of the only ways to find vulnerabilities in existing software that is out on the market is by reverse engineering it and discovering them without the source code and without proper testing.

I think the world of wearable technologies needs reverse engineering to identify vulnerabilities. For example, my watch has a bunch of downloadable third-party watch faces that all register my information like location, bpm of my heart rate, my steps, etc. This kind of data can be stolen and sold if not well protected and the entity that is doing the “protecting” could be a single person in a room typing away 100 watch faces a day to sell on the marketplace. I as the user am also left in the dark on if the entity that I am buying the watch from is reliable or malicious.