Chris Gollnick

CS410-T3717

Module 8 Journal

26 February 2022

**Reverse engineering IoT:**

The benefits of reverse engineering in IoT are in relation to manipulation and customization of the product. Since many IoT devices are running variations of open-source software and generic hardware, it becomes easier to find general information about the sof6tware and hardware. As such, reversing can allow the user to create they’re own firmware to customize their needs for the product or prevent vulnerabilities they find.

**Patching:**

Reverse engineering can improve cloud infrastructure as a means of maintenance and security. BY utilizing reverse engineering a developer or engineer can simulate various types of attacks on the cloud system. As such they will then be able to identify the vulnerabilities, exploits, and weaknesses that exist in the system. This in turn will allow the team to be able to create patches to the program to help improve the security of the program and its data.

**Vulnerability:**

Many IoT devices are infected or susceptible to infection due to the nature of the technology used within them. Where many IoT devices utilize general boards and microcontrollers its easy for them to have their instructions be found and easy to engineer or reverse engineer them for nefarious needs. As such, when you buy a new IoT device, if it doesn’t check for updates immediately, the device can then be infected through a bot probing for it.

**Impact:**

Reverse engineering offers new insights and challenges for emerging technologies. On one hand it gives the user, developer, or I.T. endpoint the ability to see what exactly is being executed, how, and when. This can then allow for conscious choices of whether to use the device or if possible deploy their own patches to improve it. Likewise, those same methods allow you find new ways to inject attacks to harvest data, hijack the device, or use it for illegal observance. This means that the companies developing these technologies have to be more careful and constantly testing for exploits and fixing them to prevent such activities from happening.

**Future:**

I am unsure whether currently used, but anything in the digital health market should consider using it. With the evolution of smartwatches and fitness trackers that are constantly connected to the internet, there are certainly security considerations that reverse engineering could help with. One example that comes to mind is the Apple Watch. It started this idea of automatic reporting when you’re in an accident that has taken off and been furthered by other companies. This idea is a security issue that I think reverse engineering could shed some light on how it determines when those incidents occur to begin the emergency call method. Reverse engineering could allow them to examine how accessible that protocol is and how vulnerable. A vulnerability for that feature could allow a killer for hire to hijack the targets device and deactivate that method thus ensuring EMS is never contacted when the target gets into a fatal accident. While the scenario is low on likelihood of happening, it is possible and should be a consideration for these companies. The reality is this type of technology is building a reliance on it with the users that the ability to think to take out a phone and call 911 will soon be a thing of the past.