**8-1: Journal**

Dylan Jeffery

SNHU

CS-410

Brian West

2/27/2022

Reverse engineering IoT: Why can reverse engineering be used to improve cloud-based information technology (IT) systems?

Reverse engineering can provide our cloud-based IT systems by providing us with threat prevention. Service development and product evaluation teams can fortify cloud data protection through reverse engineering because it allows them to find problems before hackers do.

Patching: How is reverse engineering used to patch cloud-based IT systems?

Reverse engineering a patch allows us to have unique insights on how easy a product is to hack. The more accustomed you are with reverse engineering toolsets, the more effective you become at hardening a system.

Vulnerability: Why is it that so many IoT devices are already infected with malware and many more are vulnerable to exploitation?

Many IoT devices were created with little to no security at all. Devices require built-in security to counter threats, and many were produced without countermeasures or protection. Aside from these reasons, users themselves contribute to devices vulnerabilities. The more devices, the more points of access. In addition, users are often responsible for setting up their own logins, and many will continue to use a default password or identical strings for both Username and Password.

Impact: How does reverse engineering impact new IT technologies, such as IoT and cloud computing?

As mentioned above, reverse engineering allows us to better understand the security vulnerabilities in whatever we may be developing. The disassembled language of a program gives us a very different perspective/representation of our control flow, variable manipulation, and memory handling among others. This can show us vulnerabilities that were perhaps overlooked in development/testing.

Future: Are there other new technologies that you can think of that either already use reverse engineering or should consider using reverse engineering in the future?

I think that with the rising applications of embedded systems many of these technologies could benefit from reverse engineering their software/firmware if they aren’t already. Some embedded chips are vulnerable via their UART ports. Some chips also may be vulnerable to fault injection. While this is risky and could permanently damage the board, in some cases this causes the chip to default into a highly privileged shell. When we specialize in what we develop for, we must be willing to think differently to produce effective security.