**Journal**

Justin Starr

Department of STEM

CS 410 – Software Reverse Engineering

Dr. Philomena Ogoh

October 27, 2024

**Journal**

The following is a short analysis of why reverse engineering can be used to improve cloud-based information technology (IT) systems, how reverse engineering is used to patch cloud-based IT systems, why so many IoT devices are already infected with malware and many more are vulnerable to exploitation, how reverse engineering impacts new IT technologies, such as IoT and cloud computing, and what other new technologies either already use reverse engineering or should consider using reverse engineering in the future.

**Reverse Engineering IoT**

Reverse engineering can be used to improve cloud-based information technology (IT) systems similarly to ways reverse engineering is used to improve legacy systems. It can help by identifying vulnerabilities that could potentially be exploited by attackers, leading to more secure systems and future awareness when developing new systems. Reverse engineering can also help us gain insights into the inner workings of a system, especially when source code is unavailable, and overall, to improve systems and their performance including finding and fixing bugs that could also lead to other vulnerabilities.

**Patching**

When patching cloud-based IT systems, reverse engineering can be employed to identify where within these systems vulnerabilities exist and how they either have been or how they could potentially be exploited. It can also be used to understand how existing exploits work to stop attackers from causing any more damage than they might have already caused, leading to the patching of one or more systems to stop an existing attack or prevent its spread. Also, reverse engineering can be used to patch cloud-based IT systems because once a fix is found for a vulnerability, patches or updates can be released to clients to update their systems, making them safe from the current threat that the patch aimed to fix.

**Vulnerability**

Two significant reasons why so many IoT devices are already infected with malware and many more are vulnerable to exploitation are because of password re-use/defaults, and re-branding of IoT devices (Shwartz et al., 2018). IoT devices typically store user credentials and passwords within their file systems, which more often than not contain default passwords, such as an “admin” username and “password” string for the password, or something similar or easy to guess. Using sophisticated decryption methodologies, these passwords can easily be decrypted, sometimes within minutes depending on the number of possible combinations, causing IoT devices to be highly susceptible to intrusion by any motivated attacker.

Today, IoT devices are becoming increasingly popular and the demand to produce them is also increasing. One way this is accomplished is through re-branding, which is the creation of new devices where the internal design is the same as other IoT devices with slight modifications made to the outside for cosmetic purposes (Shwartz et al., 2018). The reason why this is bad is because the inner workings of devices are simply copied over and over and produced for a wide range of products and companies. This leads to a mass production of devices that may have already been infected with malware or devices that contain known vulnerabilities that could be easily exploited by an attacker, which is why so many IoT devices are already infected with malware or become available out of the box with potential vulnerabilities.

**Impact**

Reverse engineering impacts new technologies, such as IoT and cloud computing by helping to improve security across devices and computing environments, which leads to the production of better and safer products, whether it be a device or an application running in a serverless cloud environment. Reverse engineering allows us to have a deeper understanding of device firmware, providing developers with the insights required to produce these safer and more secure products. It also promotes research, innovation, and insights by providing a method for developers to understand the inner workings of existing technology which can lead to better designs in the future, better resource optimization, and regulatory compliance.

**Future**

One technology that is still relatively new and not widely understood is the development of artificial intelligence technology. This technology could benefit substantially from reverse engineering because it could give us further insights into the complex inner workings of artificially intelligent systems. Their models are oftentimes more complex than we can understand and by further analyzing these models we can better understand their structures and why they behave the way they do. This could lead to further AI optimization by improving their algorithms, which will enhance their performance and further improve their reliability.

**References**

Shwartz, O., Mathov, Y., Bohadana, M., Elovici, Y., & Oren, Y. (2018). Reverse Engineering

IoT Devices: Effective Techniques and Methods. *IEEE internet of Things Journal, 5*(6), 4965-4976. <https://doi.org/10.1109/JIOT.2018.2875240>