**8-1 Journal**

Mohamed Saleh

Southern New Hampshire University

CS 410: Software Reverse Engineering

Prof. Mark Babock

February 25,2025

As software reverse engineering allows one to learn about a program’s structure and its logic thereby leading to some critical insights regarding how a program functions which are extremely useful, however software reverse engineering is a double-edged sword, as any skill can be malpractice allowing unauthorized access to copyrighted material, security breaches exposing allegedly secured information. While cloud computing became the new norm in IT allowing governments, companies and regular users to use the internet effectively and beyond any limitations —many vulnerabilities can be exploited causing mayhem. The concern for data privacy and security became a huge concern in the computing community, as cloud providers have different models as follows IaaS, PaaS and SaaS shaping the responsibility of the data protection; moreover, providing wide range of services to secure the data. Software reverse engineering comes in handy to investigate and evaluate different providers security measures which are beneficial for both the providers and the customers.

The most significant benefit of reverse engineering is its ability to alter a program's structure, thereby directly influencing its logical flow. This process is technically referred to as patching, as it involves seamlessly integrating new code segments into the original code. Patching allows engineers to inject commands or change the behavior of the program. This capability allows us to correct security vulnerabilities without accessing the source code.

The growth of IoT is enviable, it’s estimated that the number of connected IoT devices grew 13% to 18.8 billion globally based on IoT summer 2024 report. That growth comes with great threat due to the vulnerability of IoT devices for several reasons. The majority of IoT manufacturers overlook security measures because of the limited objective from the device. IoT devices usually depend on Mico-controllers or a limited layer of operating system which limits other mature technologies to communicate or authorize access like client-server communication using SSL, also most of Mico-controllers contain extra pins for debugging purposes; that creates a loophole to patch the device with malicious code.

The great advantage of reverse engineering shines vividly in cybersecurity to analyzing software, hardware, or systems to understand their functionality, design, and behavior, often with the goal of identifying vulnerabilities, exploits, or malicious behavior. Reserve engineering assist in malware analysis, firmware and hardware analysis and digital forensics.

References

Oladipo, F.O. (2013) *(PDF) The Privacy Implications of cloud computing in the context of software reverse engineering*, *https://www.researchgate.net/*. Available at: https://www.researchgate.net/publication/279533418\_The\_Privacy\_Implications\_of\_Cloud\_Computing\_in\_the\_Context\_of\_Software\_Reverse\_Engineering (Accessed: 25 February 2025).

Sinha, S. (2025b, February 10). *State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/#:~:text=Number%20of%20connected%20IoT%20devices%20growing%2013%25%20to%2018.8%20billion.