**8-1 Journal**

Aaron Ciminelli

SNHU

CS-410-R1913 Software Reverse Engineering 23EW1

JOE L. PARKER, (B.S, M.S.I.T, Ed.D (c))

October 16th , 2023

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

Reverse engineering can have a significant impact on improving cloud-based IT systems. Firstly, it can aid in identifying security vulnerabilities by enabling developers to comprehend the internal workings of connected IoT devices. By analyzing the code and architecture of IoT devices, vulnerabilities can be detected and resolved to enhance security systems. Secondly, reverse engineering can enhance the interoperability of cloud-based IT systems. This can be achieved by identifying and comprehending IoT devices' protocols and APIs to communicate with cloud-based IT systems. Thirdly, reverse engineering can improve the performance of cloud-based IT systems by analyzing and optimizing how IoT devices interact with them. In summary, it provides valuable insight that can strengthen the integration between IoT devices and the cloud.

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

Reverse engineering has a vital role in patching cloud-based IT systems. When software or firmware powering cloud infrastructure has vulnerabilities, developers can use reverse engineering to understand the root cause and effectively patch it. This approach helps create patches that are minimally disruptive to existing systems. Furthermore, reverse engineering can validate that a patch fixes the vulnerability without causing new issues. This is critical for maintaining the security and stability of cloud-based services.

Reverse engineering is often used to identify and fix security vulnerabilities in cloud-based IT systems. Once a vulnerability is identified, security researchers use reverse engineering to understand how it works and how it can be exploited. This knowledge is then used to develop a patch that fixes the vulnerability.

In some cases, reverse engineering can patch cloud-based IT systems by analyzing malware that has infected them. By reverse engineering the malware, security researchers can identify the vulnerabilities it exploits and develop patches to fix them.

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

IoT devices often lack basic security measures and are vulnerable to exploitation due to various reasons. First, many IoT devices are manufactured quickly and cheaply to reach the market fast, prioritizing time and cost over security. Second, their limited computing power makes it difficult to implement sophisticated security measures. Third, consumers often neglect to change default passwords or update firmware. Reverse engineering helps to identify these deficiencies so that manufacturers can enhance security in upcoming product generations. Additionally, it enables researchers to discover vulnerabilities and advocate for recalls or patches when flaws are uncovered.

There are several reasons why a significant number of IoT devices are already infected with malware, and many more are vulnerable to exploitation. Some of the most common reasons include insecure coding practices, which can introduce security vulnerabilities to the devices. Many IoT devices also lack regular security updates, leaving them vulnerable to attackers for extended periods. Weak default passwords are also a significant problem, making it easy for attackers to access the devices.

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

Reverse engineering is a valuable process that gives users a deeper understanding of emerging technologies like IoT and cloud computing. Users can make informed decisions about their adoption by revealing their advantages and flaws. Furthermore, it promotes accountability among developers to create secure and resilient IT systems upfront, knowing that their work can be scrutinized. However, it is important to note that it can also enable malicious actors to exploit uncovered vulnerabilities. Therefore, responsible disclosure practices are crucial to minimize this risk. In summary, reverse engineering plays a significant role in the healthy evolution of emerging technologies.

Additionally, it can aid in developing new products and services based on existing IoT devices and cloud-based IT systems. For instance, reverse engineering can help create new security products that can protect IoT devices and cloud-based IT systems from attack. Lastly, it also has the potential to improve interoperability between different IoT devices and cloud-based IT systems, which can lead to new and innovative applications.

**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?**

Reverse engineering is a vital tool for evaluating the effectiveness and strengthening the development of new technologies. There are several other emerging fields where reverse engineering could prove beneficial or is already being used. For instance, AI is already being used to automate some aspects of reverse engineering to identify patterns in data for discovering security vulnerabilities. In the future, AI could be further utilized to automate the reverse engineering process for better efficiency and effectiveness. Blockchain technology could be leveraged to create a secure and transparent way to share reverse engineering information, leading to improved collaboration between researchers and developers and faster discovery and resolution of security vulnerabilities. As quantum computing is an emerging field, reverse engineering could help researchers analyze early quantum computers and programs, uncovering their limitations and areas for improvement. Similarly, reverse engineering DNA sequencing techniques and bioinformatics algorithms could lead to advances in biotechnology. As new technologies emerge, reverse engineering will be crucial in evaluating their effectiveness and development.

**Resources:**

AWS. (2023). *Whitepapers*. AWS Whitepapers. https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/aws-best-practices-ddos-resiliency.html

Davis, S. (2022, April 15). *TechInsights takes reverse engineering into the cloud*. Semiconductor Digest. https://www.semiconductor-digest.com/techinsights-takes-reverse-engineering-into-the-cloud/

Gartner, Inc. (n.d.). *The latest cloud computing technology and Security*. Gartner. https://www.gartner.com/en/information-technology/insights/cloud-strategy

IEEE Computer Society. (n.d.). *IEEE Transactions on Dependable and secure computing*. IEEE Xplore. https://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=8858

Mello, J. P. (2021, June 19). *Reverse engineering attacks: 6 tools your team needs to know*. TechBeacon. https://techbeacon.com/security/reverse-engineering-attacks-6-tools-your-team-needs-know

Paloalto . (2020). *The State of Cloud Native Security*. Paloalto Networks . https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en\_US/resources/guides/prisma-cloud-compute-edition-licensing-guide

Wethington, D. (2023, April 25). *The History Of Cloud Computing: The Theory*. DOMA Technologies. https://www.domaonline.com/2021/08/10/history-of-cloud-computing-1/