University of Glasgow | School of Computing Science

ptr-tidy: Automatic Rejuvenation of Raw Pointers in C++

Artem Usov (2296905U)

March 2, 2021

ABSTRACT

1. INTRODUCTION

Most ordinary computer users demand that the machine they are using provides them with a responsive, secure and productive environment to complete their tasks. The programs that are most responsible for this are complex systems programs such as the underlying operating system, device drivers and web browsers. Systems programming often involves memory management, that is requesting memory from operating system to be used and managed by the program. This is done when the amount of memory that we need cannot be known at the time of compilation of the program. However doing so creates the opportunity for memory safety errors [1] which are notoriously challenging to avoid.

How challenging one might ask?

In a presentation by Matt Miller, a security engineer at Microsoft, it is shown that around 70% of their vulnerabilities that are addressed through a security updates are due to memory safety issues [3]. In another presentation at the Linux Security Summit it is shown that in several other top projects such as Firefox, macOS, Ubuntu and Android all had over half of their CVEs attributed to issues with memory safety [2]. This is at industry-leading companies who are renowned for hiring top talent. Such memory safety vulnerabilities can be exploited, and due to new regulations such as the GDPR, these issues are more commonly exposed to the general public and punished by regulators. An example is a fine of č20m for a British Airways data breach by the British Information Commissioner's Office [4].

2. BACKGROUND

3. EVALUATION

4. CONCLUSIONS

Acknowledgments.

References

[1] D. Dhurjati, S. Kowshik, V. Adve, and C. Lattner. Memory safety without runtime checks or garbage collection. In *Proceedings of the 2003 ACM SIGPLAN conference on Language, compiler, and tool for embedded systems*, pages 69–80, 2003.

[2] A. Gaynor and G. Thomas. Linux kernel modules in rust. In *Proceedings of the Linux Security Summit North America 2019*, 2019.

[3] M. Miller. Trends, challenge, and shifts in software vulnerability mitigation, 2019. URL `https://github.com/microsoft/MSRC-Security-Research/raw/master/presentations/2019_02_BlueHatIL/2019_01%20-%20BlueHatIL%20-%20Trends%2C%20challenge%2C%20and%20shifts%20in%20software%20vulnerability%20mitigation.pdf`.

[4] I. C. Office. Ico fines british airways č20m for data breach affecting more than 400,000 customers, 2020. URL `https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-`