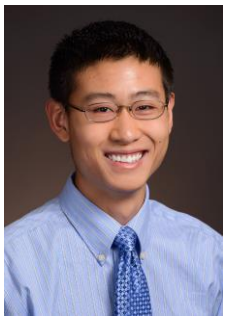
Carnegie Mellon University
Computer Science Department

THESIS ORAL



Daming Dominic Chen

Mitigating Memory-Safety Bugs with Efficient Out-of-Process Integrity Checking

Thursday, June 17, 2021 – 9:00 a.m. – REMOTE

Computer programs written in low-level languages with manual memory management, like C and C++, can contain unintentional memory safety bugs due to developer error. Examples of these bugs include spatial buffer overflows, as well as temporal use-after-frees and double frees, which can be leveraged by attackers to exploit programs by altering their runtime behavior. Indeed, statistics from both Google Chrome and Microsoft show that ~70% of all security vulnerabilities in their codebases involve memory safety bugs.

Past work has proposed various strategies to eagerly detect or lazily mitigate such bugs. Eager approaches detect memory safety bugs by checking pointer operations, whereas lazy mitigations prevent exploitation by validating program data. To improve accuracy, mitigations may need to maintain internal state (metadata) about program execution, which must also be protected from corruption. This has been achieved using different techniques, including software-based address space partitioning, and hardware-based fine-grained instruction monitoring. Nevertheless, these approaches suffer from significant complexity, brittleness, or incompatibility, which reduces their efficiency and effectiveness.

In this thesis, we observe that existing mitigations are limited by their decision to maintain internal metadata within the same process. We show that augmenting hardware with a small, secure, and efficient AppendWrite inter-process communication (IPC) primitive allows metadata storage and policy checking to be performed in a separate isolated process, which improves both security and performance. We implement this design in our HerQules framework, which we show is capable of protecting both control-flow integrity and data-flow integrity. We evaluate our approach on a variety of real-world programs, including multiple benchmark suites, the NGINX web server, and the Google Chromium web browser.

Thesis Committee:
Phillip B. Gibbons, Chair
James C. Hoe
Bryan Parno
Taesoo Kim, Georgia Institute of Technology