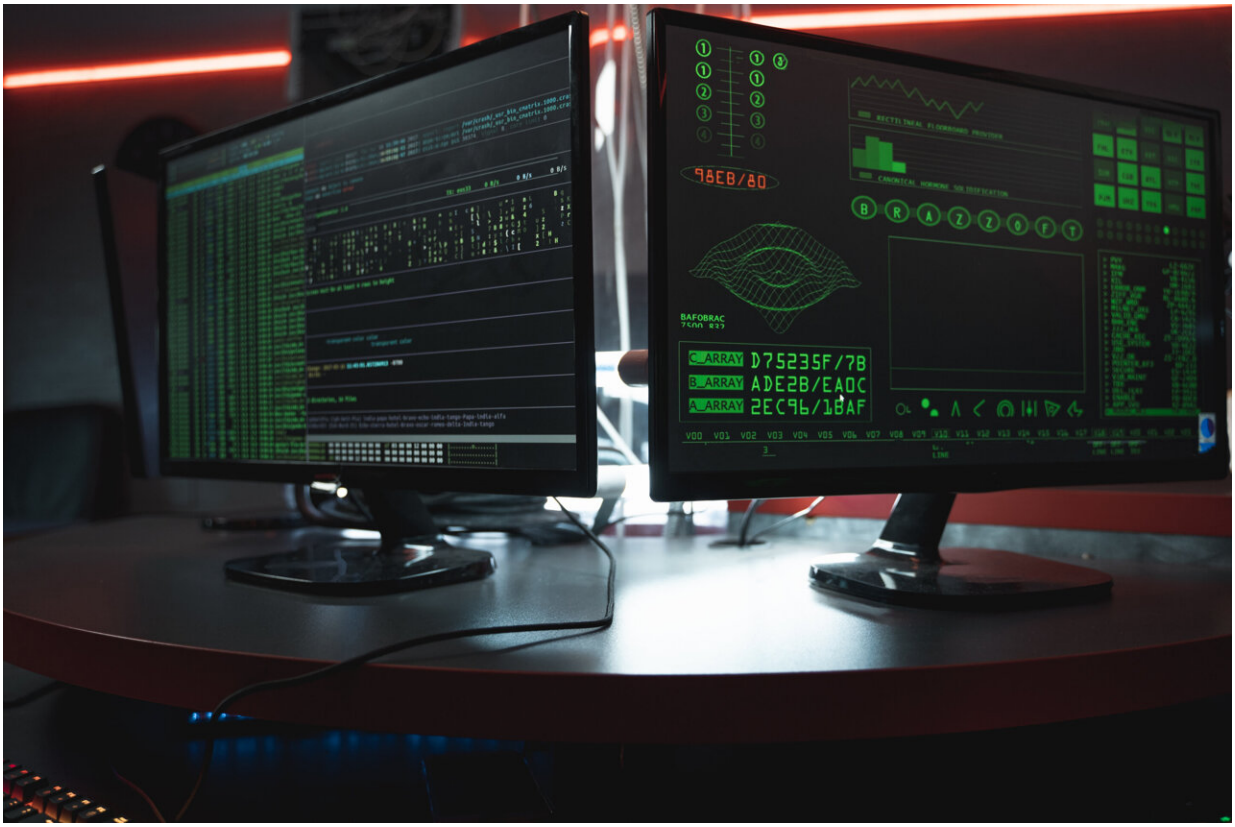
Researchers design new techniques to bolster memory safety

June 23 2021



Credit: Tima Miroshnichenko from Pexels

Because corporations and governments rely on computers and the internet to run everything from the electric grid, healthcare, and water systems, computer security is extremely important to all of us. It is

increasingly being breached: Numerous security hacks just this past month include the Colonial Pipeline security breach and the JBS Foods ransomware attacks where hackers took over the organization's computer systems and demanded payment to unlock and release it back to the owners. The White House is strongly urging companies to take ransomware threats seriously and update their systems to protect themselves. Yet these attacks continue to threaten all of us on an almost daily basis.

Columbia Engineering researchers who are leading experts in computer security recently presented two major papers that make computer systems more secure at the International Symposium on Computer Architecture (ISCA), the premier forum for new ideas and research results in computer architecture. This new research, which has zero to little effect on system performance, is already being used to create a processor for the Air Force Research Lab.

"Memory safety has been a problem for nearly 40 years and numerous solutions have been proposed. We believe that memory safety continues to be a problem because it does not distribute the burden in a fair manner among software engineers and end-users," said Simha Sethumadhavan, associate professor of computer science, whose research focuses on how computer architecture can be used to improve computer security. "With these two papers, we believe we have found the right balance of burdens."

Computer security has been a long-standing issue, with many proposed systems workable in research settings but not in real-world situations. Sethumadhavan believes that the way to secure a system is to first start with the hardware and then, in turn, the software. The urgency of his research is underscored by the fact that he has significant grants from both the Office of Naval Research and the U.S. Airforce, and his Ph.D. students have received a Qualcomm Innovation Fellowship to create

practical security solutions.

Sethumadhavan's group noticed that most security issues occur within a computer's memory, specifically pointers. Pointers are used for managing memory and can lead to memory corruption that can open up the system to hackers who hijack the program. Current techniques to mitigate memory attacks use up a lot of energy and can break software. These methods also greatly affect a system's performance—cellphone batteries drain quickly, apps run slowly, and computers crash.

The team set out to address these issues and created a security solution that protects memory without affecting a system's performance. They call their novel memory security solution, ZeRØ: Zero-Overhead Resilient Operation Under Pointer Integrity Attacks.

ZeRO features a set of memory instructions and a metadata encoding scheme that protects the code and data pointers of a system. This combination eliminates performance overhead—it will not affect the speed of a system. ZeRO requires minor changes to a system's architecture and it can easily be added to modern processors. Especially critical is that, even when under attack, ZeRO can perform all these functions and avoid crashing a system.

"Zero offers memory security at no cost and it is a perfect complement to systems that mitigate memory attacks," said Mohamed Tarek, a fourth-year Ph.D. student and co-lead author of the studies. "The keys to widespread adoption of security techniques are low-performance overhead and convenience."

The second paper that Sethumadhavan's team will present, No-FAT: Architectural Support for Low Overhead Memory Safety Checks, is a system that makes security checks faster with only a small—8%—effect on the computer's performance which is 10x faster than current software

technique for detecting memory errors. The name is an allusion to no-fat milk, which, as the ads say, "has all the goodness of milk with fewer calories."

No-FAT speeds up fuzz testing, a type of automated software testing method, and it is very easy for developers to add it when building a system. The technique builds on a recent trend in software towards binning memory allocators, which uses buckets of different sizes to store memory until it is needed by the software. The researchers found that when binning memory allocation is used by the software, it is possible to achieve memory security with little impact on performance and is compatible with existing software.

Both ZeRO and No-Fat are targeted at beefing up memory systems to be more resilient against attacks while having little to no effect on a computer system's speed or power consumption. The bonus is that with both systems, programmers need to do little to nothing to harden their programs. These ideas could transform how memory safety features are currently supported in processors.

"No-FAT & ZeRO are two major steps toward putting an end to a long-standing problem," said Miguel Arroyo Ph.D. '21, who was a co-lead author of the papers. "Memory safety attacks cost the cyber community millions of dollars. Now we can avoid that and keep everyone's data safe—it's a win-win!"

Both papers were presented at the International Symposium on Computer Architecture (ISCA), June 16, 2021.

More information: "No-FAT: Architectural Support for Low Overhead Memory Safety Checks" www.cs.columbia.edu/~simha/pre … rint_isca20_zero.pdf , DOI: 10.1109/ISCA52012.2021.00082

"ZeRØ: Zero-Overhead Resilient Operation Under Pointer Integrity Attacks" www.cs.columbia.edu/~simha/pre … int_isca20_nofat.pdf , DOI: 10.1109/ISCA52012.2021.00076

Provided by Columbia University School of Engineering and Applied Science