30 years ago, in November 1988, Robert Morris wreaked havoc on the Internet. Exploiting already known, but poorly patched software vulnerabilities, his worm infected 10% of all connected machines. Parts of the Internet were unavailable for days, and costs were estimated to reach millions of dollars. Whether or not accidentally, Morris’ actions had immense consequences: not only did he become the first person to be tried and convicted under the 1986 Computer Fraud and Abuse Act, Morris also profoundly shaped the field of computer security. Ever since the events of November 2, 1988, security researchers in both industry and academia have put endless of hours in studying and mitigating vulnerabilities, in particular those of the type that Morris exploited: memory errors.

Today, despite three decades of research, memory errors still undermine the security of our systems. Even if we consider only classic buffer overflows — a popular subset of memory error vulnerabilities — this class of memory errors has been lodged in the top-3 of the top 25 most dangerous software errors for years. Experience shows that attackers, motivated nowadays by profit rather than fun, have been effective at finding ways to circumvent protective measures. Many attacks today start with a memory error corruption that provides an initial foothold for further infection.

In this dissertation, we analyze and advance computer security defenses that aim to stop the exploitation of memory errors. We intersect this domain from two core dimensions where such errors occur: in software, and in hardware.

First, we analyze advanced code-reuse attacks — one of the most elaborate types of software-based memory error exploitation — and how we can defend legacy binaries against them. One of the most promising ways to mitigate code-reuse attacks is Control-Flow Integrity (CFI). Unfortunately, enforcing it without access to source code is hard in practice, and existing defenses often leave enough wiggle room for an attacker to launch successful exploits. In this dissertation, we propose new binary-level defenses that improve the precision of CFI — reducing...
the wiggle room just enough to stop attacks from being successful. Moreover, we explore how much leeway an attacker still has after applying different types of code-reuse defenses, including our own.

Second, we study Rowhammer — a hardware-based memory error — and its impact on mobile platforms. This disturbance error is the result of the ever increasing density of memory chips, a necessity to be able to put more and faster DRAM memory in devices. It equips attackers with a powerful primitive: a single bit flip in memory that is not under control of the attacker. Ever since its discovery, Rowhammer-based memory corruption attacks have been used to exploit a variety of ecosystems, including the desktop, browser, and even the cloud. In this work, we show that mobile devices are also susceptible to Rowhammer. We demonstrate how an attacker can leverage this to escalate privileges. Moreover, we propose a lightweight countermeasure that can eradicate the majority of the Rowhammer attack surface.