SaTC: NSF-BSF: CORE: Small: Attacking and Defending the Lifespan of Mobile and Embedded Flash Storage

Submitted by Donald Porter on Wed, 03/13/2019 - 2:19pm

Project Details

Lead PI

Donald Porter

Performance Period

Oct 01, 2018 - Sep 30, 2021

Institution(s)

University of North Carolina at Chapel Hill

Award Number

1816263

Ranked 412 out of 2290 Group Projects.
308 related hits.

This project explores approaches to attack and defend the lifespan of flash storage in small mobile devices. While the project focuses on smartphones, the research is applicable to any small flash-based device that allows users to install applications, including smart watches, Internet-of-Things (IoT) devices, computerized medical equipment, and computer-managed critical infrastructure. It is well understood that, over time, writing to flash storage will physically wear out the device. This problem is considered a nonissue with respect to enterprise Solid State Drives (SSDs). However, preliminary findings of this research indicate that wear is unresolved in the context of smartphones. A malicious, unprivileged application can secretly render a phone permanently inoperable in a few short days or weeks, and current mobile systems have no protection against this attack. The risk is exacerbated by the fact that mobile device users typically trust their app store ecosystem and are in the habit of trying out third-party apps with a sense of safety. The goal of this project is to develop ways to alleviate the problem.

Our society is rapidly moving into the era of ubiquitous computing. Users depend on smartphones for wide-ranging aspects (such as commerce, education, and healthcare), and wearables and internet-connected gadgets likewise proliferate. Moreover, an increasing amount of critical infrastructure is internet-connected via small embedded devices, which may thus control physical systems. This research identifies and addresses a critical vulnerability that seriously undermines the ability of users to trust that downloading a new application will not ruin their mobile devices. If unmitigated, this vulnerability might severely hamper the usability of such devices. To address the problem, this project is studying the input/output behavior of mobile devices and applications. Based on this behavioral analysis, the project explores new attacks on and defenses for flash wear. The end goal is to create defenses that are minimally disruptive to end users, yet provide a lower bound on the lifetime expectancy of the device. This work advances the state of the art of operating systems by creating techniques to manage permanently consumable resources.

Donald Porter

Related Artifacts

Other

- Attacking and Defending the Lifespan of Mobile and Embedded Flash Storage | Download

CORE Small Division of Computer and Network Systems (CNS) Cyber-Physical Systems (CPS) Software Systems