Should I Trust What's in My Computer? Using Current Draw Analysis to Identify Malicious Firmware in Solid State Drives

McDowell, Ryan (School: Rockbridge Academy)

Solid State Drives (SSDs) are increasingly replacing traditional computer hard drives. However, SSDs are controlled by potentially vulnerable firmware, and users cannot directly confirm if the firmware is behaving properly. Other researchers previously used power consumption of SSDs (measured via current draw) to gain some insight into how SSDs operate, but only studied unmodified, commercial SSD firmwares. The objectives of this project were to determine whether current draw analysis could identify potentially malicious firmware and whether changes to former methods could yield higher classification accuracy. Specifically, I examined encryption, a frequent submodule of malware. I created five different firmware variants for an open-source SSD, three of which performed encryption. An oscilloscope recorded the current draw as the firmware variants performed write operations with files of varying size. 1600 recordings were used to train three types of classifiers, which would attempt to distinguish between these firmwares. Using the classification methods of previous researchers yielded 51% and 58% accuracy when detecting simple (XOR) and industrial-level (AES) encryption, respectively. In contrast, I discovered a different data representation that provided little gain with XOR but increased accuracy with the more realistic AES to better than 95%. In particular, training classifiers with 10 second samples, rather than shorter segments as in previous research, maximized accuracy. Furthermore, KNN, the predominant classifier in previous research, did not produce the best accuracy. These results demonstrate the usefulness of current draw analysis for detecting some malicious firmware and provide a basis for future development of more complex detection methods.

Awards Won:

National Security Agency Research Directorate : Honorable Mention "Cyber Pioneer"