Related Research

# Research 1

In the article written by P. Deb1, the author discusses different metrics that previous research has done in the area of Spectre and Meltdown mitigation effects on high performance computing (HPC) clusters and servers. The author mentions that consumer grade workstations have not been studied as close and attempts to generate metrics to help show those effects. The article lays out several different metrics for consumer-grade computers and several tests to help measure their performance before and after operating system patches are applied to the test device. My research adopts similar tests and methodology but applies to a narrower set of systems that is specifically geared toward the internet of things (IOT) devices.

[1] P. Deb, "An Analysis on Effects after Mitigating Meltdown and Spectre Vulnerabilities", DAFFODIL INTERNATIONAL UNIVERSITY, 2018 [Online]. Available: http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/2568/P11684%20%283%25%29.pdf?sequence=1&isAllowed=y. [Accessed: 27- Jun- 2021]

# Research 2

In the article written by A. Prout, et al2, the authors discuss the various variants of the Spectre and Meltdown vulnerabilities as they relate to HPC clusters. The article focuses on the MIT Lincoln Laboratory Supercomputing Center HPC platform and its performance before and after operating system kernel patches for network connection establishment, disk access, and computationally intensive MATLAB programs. My research focuses on more consumer-oriented statistics like graphics processing, CPU speed, disk I/O, and RAM speed. The focus on my research is also on consumer and enterprise grade IOT devices and their performance hit.

[2] A. Prout et al., "Measuring the Impact of Spectre and Meltdown", *2018 IEEE High Performance extreme Computing Conference (HPEC)*, 2018. Available: 10.1109/hpec.2018.8547554 [Accessed 11 July 2021].

# Research 3

In the article written by M. Löw3, the author discusses the different systems, processors, and operating systems that are affected by the Spectre and Meltdown vulnerabilities. The research collates available information on patches and performance metrics for the various effected products. The article also mentions the variants of the vulnerabilities and how they break confidentiality of the system. While ARM processors are discussed and a list of the effected processors, my research takes a closer look at IOT devices that use ARM processors and collects more specific metrics on what performance hits a device would take after receiving a kernel patch for the system to mitigate the threat posed by the vulnerabilities. My research uses the information to help decide what architecture to test and what to look for.

[3]M. Löw, "Overview of Meltdown and Spectre patches and their impacts", in *Workshop on Advanced Microkernel Operating Systems*, Hessen, Germany, 2018, pp. 53-61.