Marcantonio Soda

CSE-343

Professor Chuah

16 April 2022

The main issue defined in the paper was that by exploiting idle power management mechanisms, VM isolation can be breached, causing an attacker VM to be able to receive data from a victim VM if the two share a common processor. This is able to be done if malicious code implanted on the victim machine encodes data and stimulates a core in such a way that the attacker can probe the uncore to receive the encoded data.

The strengths of this paper far outweigh the weaknesses. The researchers provided a great breadth of background information needed for the reader to understand the implications of the paper. While they cover a great breadth of information on low-level power management, they go into sufficient depth on each topic for the reader to grasp the needed information without becoming overwhelmed. The purpose of the paper is to identify a problem that can be simply stated. The researchers provide copious amounts of tests to prove that the problem exists. They provide a few very useful graphics to illustrate complex topics in a meaningful way. The authors even go so far as to provide attack cases to show the practical implications of the proven vulnerability, which is helpful but leaves a bit to be desired.

Despite how well-done the research and the paper was, there are a few small shortcomings. The researchers could have done a better job at explaining just how big of an issue the proven security vulnerabilities are. After reading the paper, I did not feel that the risks of this sort of covert channel are severe enough to warrant any change to the idle power management systems of the computers of the world. For example, the SSH keystroke detection attack seemed pretty useless. The paper did not effectively explain why an SSH keystroke detection attack could be detrimental to a cloud service. On the other hand, being able to probe network traffic intensity seems like it could be a huge security risk, but the paper did not effectively illustrate how detrimental the attack could be.

Overall, I do not feel that the issues proposed by the paper are very relevant today. There are a lot of hoops that an attacker would have to jump through to even be able to get information from a victim VM. Mainly, infecting it with a script that stimulates a core in a way that sends encoded data. If they are able to infect a VM with malicious code, why not infect it with something more useful? This is the biggest critique I have. Why would an attacker choose to setup and use this particular covert channel when there are so many more reliable attacks that he/she could choose from? Furthermore, the paper explicitly states that the idle power management dependency is a feature, not a design shortcoming. It needs to be tuned to optimize risk/reward. The researchers do not go into sufficient depth as to how idle power management mechanisms should be adjusted to combat this vulnerability. They state four countermeasures that would work, but would be absolutely terrible in terms of either power efficiency or speed. After reading the paper and understanding the vulnerability that the researchers proved, I believe that the current state of idle power management mechanisms should remain unchanged, which is a conclusion that I do not think the authors wanted a reader to make.