Thermal Covert Channels on SmartSSDs

Theodoros Trochatos, Anthony Etim, Jakub Szefer

Yale University

CASLAB.io

Project Overview

Continued expansion of cloud computing offerings now includes SmartSSDs [1]. Because of the FPGA component of the SmartSSD, cloud users who access the SmartSSD can instantiate custom circuits within the FPGA. This includes possibly malicious circuits for measurement of power and temperature. Normally, cloud users have no remote access to power and temperature data, but with SmartSSDs they could abuse the FPGA component to learn this information. This work shows for the first time that heat generated by a cloud user accessing the SSD component of the SmartSSD and the resulting temperature increase, can be measured by a different cloud user accessing the FPGA component of the same SmartSSD by using the ring oscillator (RO) circuits to measure temperature. The thermal state remains elevated for a few minutes after the SSD is heated up and can be measured from the FPGA side by a subsequent user for up to a few minutes after the SSD heating is done. Based on this temporal thermal state of the SmartSSD, a novel thermal communication channel is demonstrated for the first time.

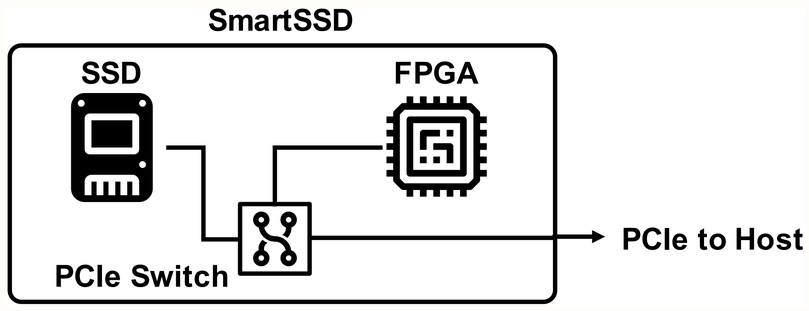

Figure 1: Block diagram of a SmartSSD.

Threat Model

This work assumes a typical cloud-computing setting where users are allocated to hardware, they pay for and when a user is done using the hardware, it is allocated to another user. We assume a sender is a user who aims to covertly communicate sensitive data to a receiver and that they both use the SmartSSD to perform the covert communication. We assume that in this cloud-computing setting, the sender and receiver are able to be allocated to the same SmartSSD and that sender and receiver can reliably be scheduled one after the other on the same SmartSSD.

We assume the cloud provider may block access to thermal sensors of the SmartSSD. However, because of the access to the FPGA component of the SmartSSD, we assume the users can instantiate any circuit they wish in the FPGA, including an RO sensor to spy on thermal and voltage changes.

Measuring SSD Heating with ROs

We demonstrate that an attacker could measure the SmartSSD temperature using ROs, instead of doing temperature measurements using the SSD disk and FPGA utilities, which could be easily blocked by the cloud provider. To demonstrate this, we run the RO measurements on the FPGA part of the SmartSSD, while the disk cools down, after the SSD has been heated using the FIO stress test. We stressed the disk to reach target maximum T_{max} temperature and then we perform the measurements at 30 seconds intervals, while the disk temperature cools down.

Figures 3 and 4 show the RO measurements for 10 minutes after the SSD was heated up using stress test on our university remote server and public server, respectively.

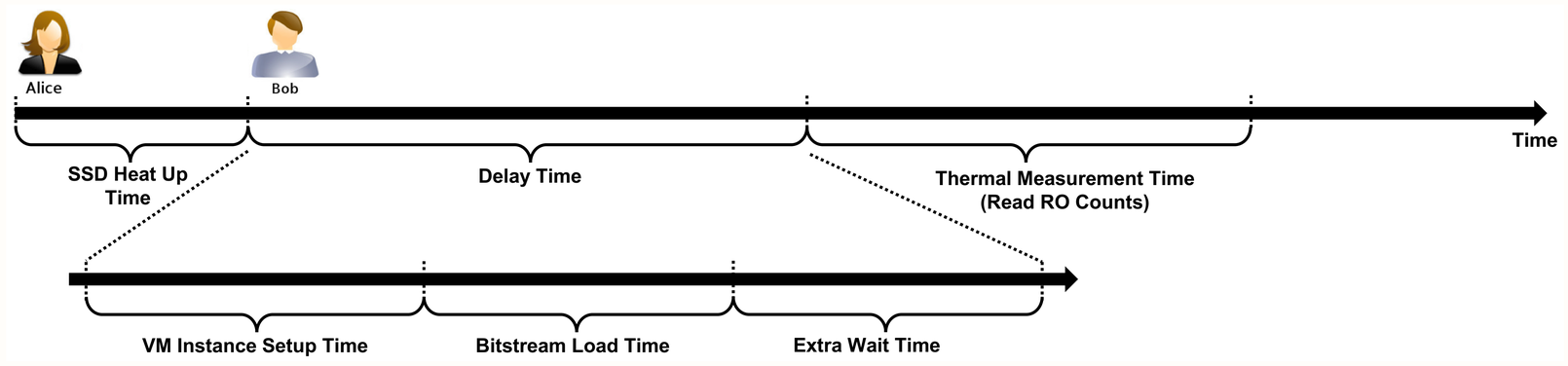

Figure 2: Timeline demonstrating the new covert channel between Alice and Bob, who share access to the same cloud-based SmartSSD. For simplicity, we include the time required for the users to switch in the VM Instance Setup Time. The time in the timeline is not shown to scale.

Covert Channel Design

Figure 2 shows the design of the covert channel for two users targeting to covertly communicate information via the SmartSSD. First, Alice starts her virtual machine, obtains and heats up the SmartSSD by running the Flexible IO (FIO) SSD stress test. Next, Alice terminates her instance. Following that, Bob starts up a new instance with access to the same SmartSSD. After the VM instance is started, the FPGA bitstream with the RO sensors is loaded. Finally, thermal measurements are taken to learn the thermal state of the SSD and thus the information is transmitted by Alice. In the evaluation, there may also be extra waiting time, as it is shown in the figure, to account for different delays between Alice and Bob.

In this covert channel, Alice transmits one bit of data by either heating up the SSD (transmits 1) or staying idle (transmits 0). Multiple SmartSSDs can be used in parallel to increase the bandwidth proportionally to the number of SmartSSDs used.

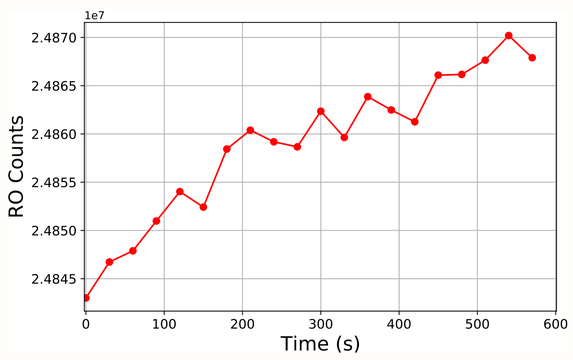

Figure 3: University remote server RO counts after stress tests, showing RO count increase as the SSD temperature cools off back to baseline.

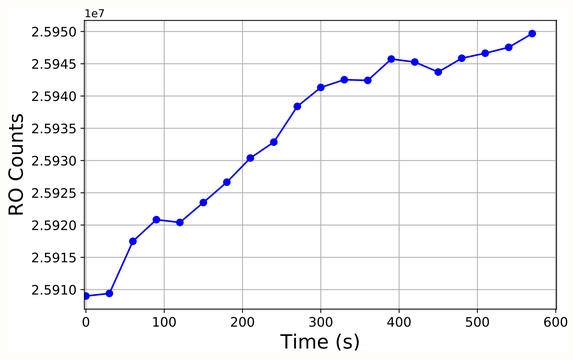

Figure 4: Public cloud server RO counts after stress tests, showing RO count increase as the SSD temperature cools off back to baseline.

Covert Channel Results

Our results for the university server and the public cloud server are shown in Figure 5 and Figure 6, respectively. It can be clearly seen that we achieve the highest accuracy within the first 4 to 5 minutes when using both the SmartSSD temperature and RO counts data. Therefore, within these 4 to 5 minutes the heat generated by one user can be observed by another user who later uses the same SmartSSD and as a result a transfer of data through a covert channel takes place. As the delay time increases, it should be noted that the accuracy drops.

This is consistent as it becomes difficult to differentiate between a 1 or 0 for longer periods of time as the SmartSSD returns to the baseline temperature.

For comparison, the accuracy of the covert channel using the SSD thermal sensor is also shown. It can be seen that RO count based covert channel has only about 10% lower accuracy. Thus, even if there is no access to the SSD thermal sensors, the attackers can always use the RO sensor based covert communication with high accuracy. Further, Manchester encoding could be used for even better accuracy and thus our evaluation gives conservative results for the accuracy of the novel thermal temporal channel.

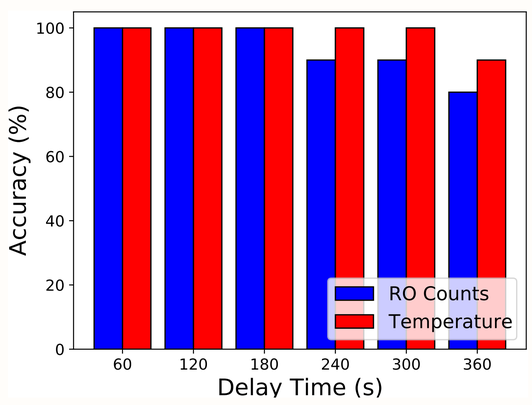

Figure 5: University remote server covert channel transmission test accuracy with different delay times.

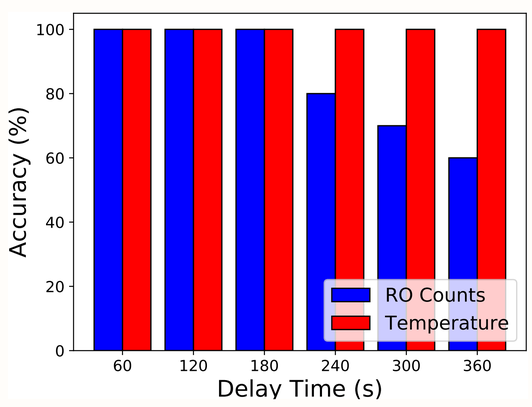

Figure 6: Public cloud server covert channel transmission test accuracy with different delay times.

Conclusion

This work explored security threats to FPGA-enabled SmartSSDs. This paper in particular showed that heat generated by one user can be observed by another user who later uses the same SmartSSD. Based on the thermal state of the SmartSSD, a covert data transfer can be achieved through simple On-Off Keying (OOK). Use of multiple SmartSSDs in parallel can further, significantly improve the data throughput of the covert channel. The new temporal thermal covert channel in SmartSSDs was demonstrated on a public cloud provider as well as on an in-lab server.

References

[1] "Samsung smartssd," https://www.xilinx.com/applications/data-center/computational-storage/smartssd.html.