

Final Reflection

May 6, 2021

Before this class, what was your knowledge and/or familiarity with side-channels, using python for applied statistics, using python for repeatable experimentation, or using hardware capture devices (e.g., chipwhisperer platform)?

Before this class, I was familiar with the concept of side-channels, some high level descriptions of how to use them, and a brief understanding of when they might be used to extract information. As far as using python for stats and hardware capture devices I had no experience. I had previously used python to script the running of multiple experiments/tests, but I had no experience with platforms like Jupyter Notebooks and that style of repeatability.

Based on your answer to question 1, what did you learn during phase one of the course?

In regards to Side-Channels my knowledge went much more in depth. I learned a lot about how one could actually conduct these kinds of attacks and the work needed in the modeling and planning phase to successfully exploit them. I also got a breadth in python's uses as a data science language and for statistical analysis by getting roughly familiar with a wide array of tools that we were able to use.

What did you learn about in phase two? (Note this might go beyond the main topics of the course, e.g., self/independent-learning, team-work, e.t.c.)

I learned a lot about how electricity and power work in the physical world as I worked on our pump controller. Getting the voltage glitching attack to do anything was quite difficult, but it gave me a much deeper understanding of how the entire process works from top to bottom.

Are there lessons and/or knowledge and/or techniques, beyond side channels, that you might use in the future?

I think all of the data analysis skills and tools that we used for visualizing all of the side-channel related stuff will be useful in the future. Numpy, pandas, and scikit are all things I hear about regularly but just never got around to learning before this course.

In your own words, what is a side channel?

A side channel is a source of leakage of information through an unintended, or unavoidable, avenue.

What, if any, feedback do you have for Dr. Borowczak?

I felt that the ChipWhisperer demos were of far less value to me to learn something than the ones made by Dr. B. I think trying to use entirely ones created by him would help the understanding of those more complicated topics.