Problem Report
CS 519

Amin Sarihi

Hunter Stuckey

Machine Learning to Break AES

Abstract:

The AES encryption algorithm has been the standard for a long time for security everywhere. Recently, groups have been finding ways to break through this encryption via side channel attacks with various means [1]. Deep learning using power traces is a way to retrieve a key from a hardware implementation of AES.   The tool that we plan to use for implementation of the deep learning algorithm is the DLSCA, which is an open source tool for side channel analysis [2]. Using machine learning to discover possible the vulnerabilities through the side channel of hardware in AES, then formulating possible countermeasures to the readings of power traces could be a great help for the security community.

Background:

Security is an important topic around the world currently, with many security vulnerabilities being found in commercial software and hardware constantly. Deep learning side-channel attacks have been proven to be effective in retrieving the keys of an AES implementation in hardware via reading the spikes in power traces during the s-box (substitution box) processing [1].

Hardware security has been an important field in the past few decades with theft of hardware IP being a serious problem in the industry recently [3]. With competition from many companies, there is increasing incentive to steal/spy on hardware IP from competitors. There is an increasing demand for better security standards and experts in the field, this project is an opportunity for us to develop skills in a field with high demand. With the possibility of attackers breaking encryption through side-channel attacks through analyzing power traces, research has to be done for possible countermeasures to help keep hardware and software secure in the future.

Project Plan:

We will use the DLSCA toolkit that is built on TensorFlow for the deep learning experiment, The DLSCA tools can be retrieved from a repository on GitHub, there is an instruction manual for getting started on using them. Setting up the software with the DLSCA toolkit will be the beginning of the project start. Learning the tools and becoming familiar with the various deep learning methods will be necessary for gathering useful data.

There is an oscilloscope/target board kit, the chipwhisperer lite, that will be used for AES implementation on the target board side and the readings will come from the oscilloscope side. The board will be retrieved from funding in the electrical engineering department for projects.

After setting up the DLSCA toolkit and retrieving the chipwhisperer kit, experimentation and testing will begin. After running many trials of running the AES algorithm on the target board and recording the data, we will run the data from the first round of s-box processing power traces into a deep learning algorithm. Using the power trace data from the first round, and knowledge of knowing the s-box itself, the deep learning algorithm should be able to find correlation of what bits the key to the AES algorithm contains [1].

With this experiment, finding the minimum amount of trials necessary for the deep learning algorithm to become accurate enough for key finding will be important for determining effectiveness. If the amount of time to find the key in an AES implementation is very great for little return, then attackers would be very dissuaded from using deep learning to find a key, but if the cost is low, then attackers would have a very easy time justifying the usage of these tools in the future for breaking into many different devices.

In the future, using different target boards with unknown characteristics could help improve our deep learning model and shed some more light on the vulnerabilities of hardware encryption. Possibly, after the first demonstration, funding could be procured for more test boards in the future.

Metrics for Success:

1. Successfully use the DLSCA tools to retrieve the keys from an AES implementation in the target board.
2. Measure the effectiveness of the side channel attacks on the AES algorithm.
3. Propose possible countermeasures to this deep learning side channel attack.

References:

[1] M. Brisfors and S. Forsmark, ‘Deep-Learning Side-Channel Attacks on AES’, Dissertation, 2019.

[2]Brisfors, Martin, and Sebastian Forsmark. "DLSCA: A Tool for Deep Learning Side Channel Analysis."

[3] https://cybersecurity.berkeley.edu/blog/damaging-effects-ip-theft/