# Spectre

Readme for the Spectre CPU exploit.

## Attribution

The source code originates from the example code provided in the “Spectre Attacks: Exploiting Speculative Execution” paper found here: https://spectreattack.com/spectre.pdf

The original source code was provided by Erik August’s gist, found here: https://gist.github.com/ErikAugust/724d4a969fb2c6ae1bbd7b2a9e3d4bb6

## Building

On the terminal run:

make

The output binary is ./spectre.out.

## Executing

To run spectre with default cache hit threshold of 80, and the secret example string “The Magic Words are Squeamish Ossifrage.” as the target, run ./spectre.out with no command line arguments.

**Example:** ./spectre.out

The cache hit threshold can be specified as the first command line argument. It must be a whole positive integer.

**Example:** ./spectre.out 80

## Tweaking

If you’re getting improper results, you may need to tweak the cache hit threshold. This can be done by providing a threshold as the first command line argument.

While a value of 80 appears to work for most desktop CPUs, a larger value may be required for slower CPUs, and the newest desktop CPUs can go as low as 15.