Tekeli-li

The Great Deep Project

Team Members

Michael Weatherby
Michael Fitch
Blake Janes
Eric Del Valle

Coverage Guided Fuzzer

- CGF is mostly finished, we now have example plugins written in both C and Python. This will allow people to see a more in depth use of both available plugin architectures.
- A guide has been written on how to use both plugins, as they both attack the same surface.

File Fuzzer

- Reversed and (more or less) understood
- Uses the AFL approach to fuzzing a file

- To do:
  - Code simple file fuzzer in Python for the guide
  - Write the guide to file fuzzing

find_mm_offset() Function

- The find_mm_offset() function in Shoggoth returns incorrect values for recent versions of the linux kernel
- Verified it is not a problem with Untangle
- A potential solution was found in the addition of a memory randomizer between versions of the linux kernel, however testing revealed this was not the problem.
- Further testing is needed

Reverse Engineering Untangle's Firewall

- Firewall implementation is in a mix of bash, python, java, c, and more.
- Languages outside of c are out of scope, so we're reversing functionality to find how the c libraries are used to define an attack surface.