HALucinator: Firmware Re-hosting Through Abstraction Layer Emulation

A. Clements, E. Gustafson, T. Scharnowski, P. Grosen, D. Fritz, C. Kruegel, G. Vigna, S. Bagchi, M. Payer

Our tools consist primarily of the HALucinator re-hosting environment. For performance reasons, we created two variants of this system: one for running firmware in a way that it can be easily interacted with by a user, and one for fuzzing with AFL.

HALucinator can be found at https://github.com/embedded-sec/halucinator Hal-fuzz can be found at https://github.com/ucsb-seclab/hal-fuzz Included are scripts to run the firmware used in our evaluation. hal-fuzz also includes a Dockerfile for easy setup.

These tools can, as described in the paper, be used on binaries without symbols with the help of a library matching tool such as our LibMatch. We are still working to optimize LibMatch to run without consuming excessive system resources, and packing it to be more easily distributed (it needs angr and its numerous dependencies). Thus, we include its output on our test binaries in the above repositories to make evaluating HALucinator easier. You can find its source code here: https://github.com/subwire/libmatch