1 Sacrament of Communion with the Weird Machines

Neighbors, please join me in reading this seventh release of the International Journal of Proof of Concept or Get the Fuck Out, a friendly little collection of articles for ladies and gentlemen of distinguished ability and taste in the field of software exploitation and the worship of weird machines. If you are missing the first six issues, we the editors suggest pirating them from the usual locations, or on paper from a neighbor who picked up a copy of the first in Vegas, the second in São Paulo, the third in Hamburg, the fourth in Heidelberg, or the fifth in Montréal, or the sixth in Las Vegas.

This release is dedicated to Jean Serrière, F8CW, who used his technical knowledge and an illegal shortwave transceiver to fight against the Nazi occupation of France. His wife Alice Serrière once, when asked "Where are the tubes?" showed occupying soldiers the leaky pipes in their basement.

In Section 2, the Pastor reminds us that there are things that we must be thankful for, with a parable freshly drawn from the Intertubes.

In Section 3, Fiora shares with us a collection of nifty tricks necessary to emulate modern Nintendo Gamecube and Wii hardware both quickly and correctly. Tricks involve fancy MMU emulation, ways to emulate PowerPC's `bl`/`blr` calling convention without confusing an X86 branch predictor, and subtle bugs that must be accounted for accurate floating point emulation.

Continuing the tradition of getting Adobe to blacklist our fine journal, `pocorgtfo06.pdf` is a TAR polyglot, which contains two valid PoC, as in both Pictures of Cats and Proofs of Concept. In Section 4, Ange Albertini explains how this sleight of hand is performed.

In Section 5, Micah Elizabeth Scott shares the story of the Pong Easter Egg that hides in VMWare and the Pride Easter Egg that hides inside that!

In Section 6, Craig Heffner shares two effective tricks for detecting that MIPS code is running inside of an emulator. From kernel mode, he identifies special function registers that have values distinct to Qemu. From user mode, he flushes cache just before overwriting and then executing shellcode. Only on a real machine—with unsynchronized I and D caches—does the older copy of the code execute.

In Section 7, Philippe Teuwen extends his coloring book scripts from PoC‖GTFO 5:3 to exploit the AngeCryption trick that first appeared in PoC‖GTFO 3:11.

In Section 8, Joe Grand presents some tricks for reverse engineering printed circuit boards with sand paper and a flatbed scanner.

Continuing this issue's theme of tricks that allow or frustrate debugging and emulation, Ryan O'Neill in Section 9 describes the internals of his Davinci self-extracting executables in Linux. Here you'll learn how to prevent your process from being easily debugged, sidestepping `LD_PRELOAD` and `ptrace()`.

In Section 10, Don A. Bailey treats us to a fine bit of Vuln Fiction, describing a frightening Internet of All Things run by a company not so different from one that shipped a malicious driver last month.

Finally, in Section 11 we pass around the old collection plate, because—in the immortal words of St. Herbert—*the PoC must flow!*