1 Call to Worship

Neighbors, please join me in reading this fourth issue 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 three 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, or the third in Hamburg. This fourth issue is an epistle to the good neighbors at the Troopers Conference in Heidelberg and the neighboring RaumZeitLabor hackerspace in Mannheim.

We begin with Section 2, in which our own Rt. Revd. Dr. Pastor Manul Laphroaig condemns the New Math and its modern equivalents. The only way one can truly learn how a computer works is by smashing these idols down to bits and bytes.

Like our last two issues, this one is a polyglot. It can be interpreted as a PDF, a ZIP, or a JPEG. In Section 3, Ange Albertini demonstrates how the PDF and JPEG portions work. Readers will be pleased to discover that renaming `pocorgtfo03.pdf` to `pocorgtfo03.jpg` is all that is required to turn the entire issue into one big cat picture!

Joshua Wise and Jacob Potter share their own System Management Mode backdoor in Section 4. As this is a journal that focuses on nifty tricks rather than full implementation, these neighbors share their tricks for using SMM to hide PCI devices from the operating system and to build a GDB stub that runs within SMM despite certain limitations of the IA32 architecture.

In Section 5, Travis Goodspeed shares with us three mitigation bypasses for a PIP defense that was published at Wireless Days. The first two aren't terribly clever, but the third is a whopper. The attacker can bypass the defense's filter by sending symbols that become the intended message when left-shifted by *one eighth of a nybble*. What the hell is an eighth of a nybble, you ask? RTFP to find out.

Conventional wisdom says that by XORing a bad RNG with a good one, the worst-case result will be as good as the better source of entropy. In Section 6, Taylor Hornby presents a nifty little PoC for Bochs that hooks the RDRAND instruction in order to backdoor /dev/urandom on Linux 3.12.8. It works by observing the stack in order to cancel out the other sources of entropy.

We all know that the Internet was invented for porn, but Assaf Nativ shows us in Section 7 how to patch a feature phone in order to create a Kosher Phone that can't be used to access porn. Along the way, he'll teach you a thing or two about how to bypass the minimal protections of Nokia 1208 feature phone's firmware.

In the last issue's CFP, we suggested that someone might like to make Dakarand as a 512-byte X86 boot sector. Juhani Haverinen, Owen Shepherd, and Shikhin Sethi from FreeNode's #osdev-offtopic channel did this, but they had too much room left over, so they added a complete implementation of Tetris. In Section 8 you can learn how they did it, but patching that boot sector to double as a PDF header is left as an exercise for the loyal reader.

Section 9 presents some nifty research by Josh Thomas and Nathan Keltner into Qualcomm SoC security. Specifically, they've figured out how to explore undocumented eFuse settings, which can serve as a basis for further understanding of Secure Boot 3.0 and other pieces of the secure boot sequence.

In Section 10, Frederik Braun presents a nifty obfuscation trick for Python. It seems that Rot-13 is a valid character encoding! Stranger encodings, such as compressed ones, might also be possible.

Neighbor Albertini wasn't content to merely do one crazy concoction for this file. If you unzip the PDF, you will find a Python script that encrypts the entire file with AES to produce a PNG file! For the full story, see the article he wrote with Jean-Philippe Aumasson in Section 11.

Finally, in Section 12, we do what churches do best and pass around the donation plate. Please contribute any nifty proofs of concept so that the rest of us can be enlightened!


$10^2+11^2+12^2+13^2+14^2$
365