1 Read me if you want to live!

Neighbors, please join me in reading this fourteenth 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 reverse engineering and worshippers of weird machines. This fourteenth release is given on paper to the fine neighbors of São Paulo, San Diego, and Budapest.

If you are missing the first thirteen 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, the fifth in Montréal, the sixth in Las Vegas, the seventh from his parents' inkjet printer during the Thanksgiving holiday, the eighth in Heidelberg, the ninth in Montréal, the tenth in Novi Sad or Stockholm, the eleventh in Washington D.C., the twelfth in Heidelberg, or the thirteenth in Montréal.

After our paper release, and only when quality control has been passed, we will make an electronic release named `pocorgtfo13.pdf`. It is valid as PDF, ZIP, and PostScript; please read it with Adobe Reader, `unzip`, and `gv`.

We begin on page 5 with the story of how **STAR RAIDERS** by Doug Neubauer for the Atari 400 was taken apart by Lorenz Weist, from a mere ROM cartridge dump to annotated and literate 6502 disassembly. By a stroke of luck, Lorenz was able to read Doug's original source code for the game after completing his reverse engineering project, giving him the rare opportunity to confirm his understanding of the game's design and behavior.

On page 24, James Forshaw introduces us to a nifty little trick for simplifying reliable exploitation of race condition vulnerabilities. Rather than spin up a dozen attempts to improve racetrack odds, he instead induces situations with pathological performance penalties to Windows NT system calls, stunning the threads of execution that might interfere with his exploit for twenty minutes or more!

Micah Elizabeth Scott continues to send us brilliant articles that refuse to be described by a single abstract, so let's just say that on page 30 she explains a USB magic trick in which her FaceWhisperer board—combining the Facedancer and the Chip Whisperer—is able to reliably glitch the USB stack of an embedded device to dump its firmware. Or, we could say that on page 30 she explains how to use undocumented commands from that firmware dump to program the Harvard device by ROP. Or, we could say that on page 30 she shows you to read RFID tags with a Wacom tablet. These tricks are all the same article, and you'd be a fool not to read it.

In PoC||GTFO 10:8, Travis Goodspeed jailbroke the Tytera MD380 radio to allow for firmware extraction and patching. Since then, a lively open source project has sprung up, with fancy new features and fixes to old bugs. On page 38, he describes how to rip the AMBE audio codec out of the radio firmware, transforming it into a command line audio processing tool that runs on any Linux workstation. Similar tricks can be used to quickly toss together emulators for many ARM and PowerPC embedded systems, re-using their library functions, or fuzzing their parsers in the familiar environment of an everyday laptop.

Evan Sultanik is back with a safe cracking adventure that could only be expressed as a play in three acts, narrated by our own Pastor Manul Laphroaig. Speaking parts are available for Alice Feynman, Bob Schrute, Havva al-Kindi, and the ghost of Paul Erdős. You'll find Evan's script on page 43.

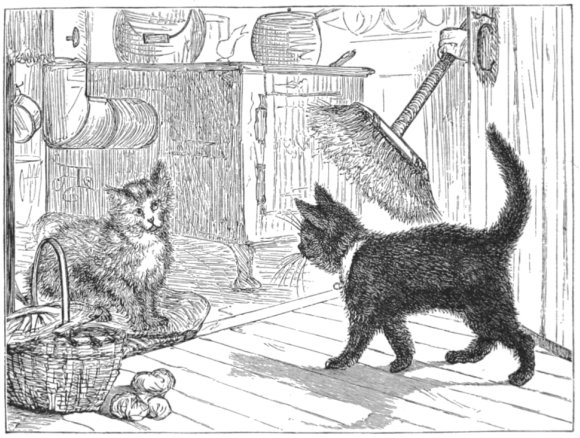
Matt Knight has been reverse engineering the PHY of LoRa, a low-power protocol for sub-GHz wireless networking over long distances. On page 48 you will find not just the protocol details that allowed him to write an open source receiver, but, far more importantly, you will also find the methods by which he reverse engineered this information from captured packets, vague application notes, and the outright lies of the patent application.

Pastor Manul Laphroaig, your friendly neighborhood evangelist of the gospel of the weird machines, has a sermon for you on page 60. He reminds us that science takes place neither on stage in front of a live studio audience nor in committees and government offices, but over a glass of fine scotch that's accompanied by finer conversation of practitioners. In the same way that we oughtn't put Tim the "Tool Man" Taylor in charge of vocational education, we ought to leave the teaching of science to those who do it, not those who talk about it on TV.

Geoff Chappell is an old-school reverse engineer, an x86 archaeologist who has spent the past twenty-four years reading Windows binaries to identify all the forgotten features and corner cases that the rest of us might take for granted.[1] On page 63, he introduces us to the mystery of Microsoft's Shim Database Compiler, an unpublished tool for compiling driver shims that doesn't seem to be available to the outside world. Geoff shows us that, in fact, the tool is available, wrapped up inside of a GUI as `QFixApp.exe` or `CompatAdmin.exe`. By patching the program to expose its intact `winmain()`, he can recover the long-lost `ShimDBC.exe` for compiling Windows driver compatibility shims from XML!

Evan Sultanik and Philippe Teuwen have teamed up on page 71, to explain the inner workings of `pocorgtfo13.pdf`, which you can rename to read as `pocorgtfo13.zip` or `pocorgtfo13.ps`.

On page 72, the last page, we pass around the collection plate. Our church has no interest in cash or cheques, but we'd love your donation of a nifty reverse engineering story. Please send one our way.



[1] Geoff was the first to discover Aaron R. Reynolds' "AARD" code from the beta release of Windows 3.1 that intentionally broke compatibility with DR-DOS. He also has a delightful article on exactly how AOL exploited a buffer overflow in their own AOL Instant Messenger client to distinguish it from Microsoft's clone, MSN Messenger.