20:01 Let's start a band together!

Neighbors, please join me in reading this twentieth 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 the study of weird machines. This release is a gift to our fine neighbors in Leipzig, DC, and other good cities.

If you are missing the first twenty issues, we suggest asking 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, the thirteenth in Montréal, the fourteenth in São Paulo, San Diego, or Budapest, the fifteenth in Canberra, Heidelberg, or Miami, the sixteenth release in Montréal, New York, or Las Vegas, the seventeenth release in São Paulo or Budapest, the eighteenth release in Leipzig or Washington, D.C., the nineteenth in Montréal, or the twentieth in Heidelberg, Knoxville, Canberra, Baltimore, or Raleigh. Two collected volumes are available through No Starch Press, wherever fine books are sold.

We begin with a sermon about preserving books for the long haul on page 5, which imagines a technique by which we could put unused pages of Flash memory to good use, preserving the books of our civilization just as well as the fine folks of the Ezra synagogue in Cairo did a thousand years ago.

On page 7, Travis Goodspeed and Axelle Apvrille introduce us to the RF430FRL152H chip from Texas Instruments, an NFC tag with a built-in microcontroller that runs from FRAM instead of Flash memory. Not only is it handy for emulating other NFC Type V tags, but we'll also learn how to dump memory from a locked tag with a custom mask ROM.

In this day of hardware virtualization, we often take emulation for granted, and it is no surprise that programs for one platform run on another. But on page 14, Charles Mangin presents an Altair 8800 emulator that runs accurately on the Apple `][`, with fewer registers and less configurable memory!

You might recall that in March of 2018, there was a bit of drama around an arbitrary physical memory read vulnerability in AMD's Ryzen platform, but did you ever understand the bug well enough to exploit it? Those of us who merely made a flippant comment on Twitter about disclosure policies, and therefor must ask forgiveness for our crass ways, can find a thorough and technical explanation with code examples by David Kaplan on page 25.

Quite a few of us first learned Z80 assembly language for our calculators in high school, and on page 32, we bring you Brandon Wilson's short history of TI graphing calculator hacking. You'll learn how the TI-85's memory backups were used to corrupt function pointers in the Custom menu, how the TI-83+ RSA512 signing keys were factored in bedrooms, and how the Z80 emulation mode of the eZ80 calculators left holes through which the operating system could be patched.

Ryan O'Neill, whom you might know as Elfmaster, is back on page 45 with an accurate technical description of `ld`'s `-separate-code` feature that changes the ways in which ELF segments are parsed and might be infected.

Page 62 presents a nice little riddle in cryptographic numerology by Cornelius Diekmann, which is itself generated by a Python script.

We then continue to a second crptography rant, in mildly more explicit language, by Ben Perez on page 68.

And EVM concludes this release with tricks for detecting the boundaries between statically linked objects. He begins by noticing that functions at the beginning of a module are more likely to call forward than backward, while by the end of the module the call backward more than forward until the beginning of the next module, when they abruptly begin to call forward again. Through this and other tricks, plus a lot of necessary calibration, he presents a polished toolkit for cutting apart linked objects on page 73.

On page 80, the last page, we pass around the collection plate. Our church has no interest in bitcoins or wooden nickels, but we'd love your donation of a reverse engineering story. Please send one our way.