21:01 Don't give up on your library card!

Neighbors, please join me in reading this twenty-second 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 friends in D.C., Berlin, and Fort Washington, Pennsylvania.

If you are missing the first twenty one releases, 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, the twentieth in Heidelberg, Knoxville, Canberra, Baltimore, or Raleigh, or the twenty-first in Leipzig or Washington, D.C. Three collected volumes are available from No Starch Press, wherever fine books are sold.

The old joke goes that Stalin's 1936 Constitution of the USSR guaranteed freedom of speech, but that rat bastard never made any promises about freedom *after* speech. On page 6, our own Pastor Manul Laphroaig takes a step back from the tragedy of so many brilliant works being unpublished or unwritten, to consider another question: If you had the power to censor just the bad stuff, would you use it?

A long time ago in a fancy bar in Tel Aviv, Yannay Livneh told us of a bug in the IPIP tunneling protocol that might allow for convenient injection of an IP frame into a remote network, that this might be nested to create a very complicated route, and that a large number of machines on the Internet were possibly vulnerable. His proof of concept took just a week or two, but the coordinated disclosure dragged on for many months, and the only way you can repay this blood debt is by reading his fine article on page 7.

Suppose that you have some firmware, but you don't want us meddlesome reverse engineers to run that same firmware under a debugger, even after they've defeated the readout protection. On page 8, Balda describes a grab bag of these anti-debugging tricks.

Travis Goodspeed and EVM have spent the past year collecting three hundred gigabytes of microcontroller SDKs, which they've parsed and blinded into a SQL database. Accessible through a JSON API, this database allows such nifty queries as function name recovery and I/O port naming. See page 11.

EVM has also been playing with a baseball scoreboard, the FairPlay 710. On page 17, he describes his method for attaching this ancient artifact to a modern network, allowing parents in his town to display the scores from the comfort of the bleachers.

Our fine journal frequently runs tourist guides to strange CPU architectures. On page 24, Christopher Hewitt introduces us to Altera's original Nios architecture, a soft CPU from the year 2000 that was largely forgotten after Intel's acquisition of the FPGA company in 2015. This particular Nios machine was used in a GPS-disciplined oscillator that Chris wanted to repurpose for other uses.

С С С Р

ГЛАВНОЕ УПРАВЛЕНИЕ
ПО ОХРАНЕ ВОЕННЫХ
И ГОСУДАРСТВЕННЫХ
ТАЙН В ПЕЧАТИ
при Совете Министров СССР

„_____" _____ 1960 г.

№_____

Москва, Ж-74, Китайский пр., 7
Телефон К 4-46-63

Those of our readers old enough to have used a rotary telephone might have explored the network with a blue box or at least made free payphone calls with a red box. Younger readers might've made their own small telephone networks with VoIP and other newfangled technologies. An anonymous article on page 31 goes beyond those tricks, to show you how a rotary telephone network might be built from scratch with vintage technology.

Netspooky is a damned clever code golpher who is new to these pages. On page 42, you'll find a technique for producing palindrome ELF files. Harvey Phillips also describes his own techniques for machine code palindromes, applied to an X86 bootloader on page 50. These were both written for 2020's Binary Golf Grand Prix, and we eagerly await what clever things they'll do this year.

Suppose that you have a bit of raw firmware that you're pretty sure is executable code, but you don't yet know the architecture. You might try looking for common sequences, or you might check that relative function calls match entry points. EVM has a simpler method, which is to draw a windrose diagram of byte frequencies, skipping universally common ones like `0x00`. Page 55.

In the early eighties, a gizmo called the Text Lite PX-1000 allowed folks to encrypt short messages with DES, then transmit them by audio coupler modem. At some point the NSA got nervous about this, purchased all outstanding units, and convinced the manufacturer to update the ROM to support a unique and proprietary encryption protocol, rather than the standard for which it was made. On page 59, Stefan Marsiske explains how he reverse engineered the backdoored algorithm and cracked it with modern tooling.

It's not so uncommon to find a firmware image, but not a load address. On page 67, EVM describes a generalized solution to this problem, first defining function entry points as a function of the load address and then solving for the load address that matches a strong majority of any absolute calls.

Robert Graham has often lectured our editors on the virtues of state machine implementations of software, as a leaner and meaner alternative to the object oriented monstrosities that might be more organized, but are undeniably more computationally expensive. On page 71, he applies his highfalutin performance optimizations to the `wc` command.

On page 80, we pass the collection plate, not for bitcoins or wooden nickles, but for nifty stories.