

16:13 Laphroaig's Home for Unwanted Polyglots and Oday

from the desk of Pastor Manul Laphroaig,
Tract Association of PoC||GTFO.

Dearest neighbor,

Our scruffy little gang started this самиздат journal a few years back because we didn't much like the academic ones, but also because we wanted to learn new tricks for reverse engineering. We wanted to publish the clever tricks that make reverse engineering and polyglots possible, so that folks could learn from others' experience. Over the years, we've been blessed with the privilege of editing these tricks, of seeing them early, and of seeing them through to print.

Now it's your turn to share a trick or two, that nifty little truth that other folks might not yet know. It could be simple,³⁹ or a bit advanced.⁴⁰ Whatever your nifty tricks, if they a clever, we would like to publish them.



Do this: write an email telling our editors how to reproduce *ONE* clever, technical trick from your research. If you are uncertain of your English, we'll happily translate from French, Russian, Southern Appalachian, and German. If you don't speak those languages, we'll draft a translator from those poor sods who owe us favors.

Like an email, keep it short. Like an email, you should assume that we already know more than a bit about hacking, and that we'll be insulted or—WORSE!—that we'll be bored if you include a long tutorial where a quick reminder would do.

Use 7-bit ASCII if your language doesn't require funny letters, as whenever we receive something typeset in OpenOffice, we briefly mistake it for a ransom note.

Teach me how to falsify a freshman physics experiment by abusing floating-point edge cases. Show me how to enumerate the behavior of all illegal instructions in a particular 6502.

Don't tell us that it's possible; rather, teach us how to do it ourselves with the absolute minimum of formality and bullshit.

Like an email, we expect informal language and hand-drawn diagrams. Write it in a single sitting, and leave any editing for your poor preacherman to do over a bottle of fine scotch. Send this to pastor@phrack.org and hope that the neighborly Phrack folks—praise be to them!—aren't man-in-the-middleing our submission process.

Yours in PoC and Pwnage,
Pastor Manul Laphroaig, T.G. S.B.

HARDWARE
APPLE 201-839-3478
MICRO-WARE DIST. INC.

THE PERFORMER PRINTER FORMATTER BOARD for Epson, OKI, NEC 8023, CITOH 8510 provides resident screen dump and print formatting in firmware. Plugs into Apple slot and easily accessed through PR# command — Use with standard printer cards. \$49.00 specify printer.

THE MIRROR FIRMWARE FOR NOVATION APPLE CAT II® The Data Communication Handler ROM Emulates syntax of another popular Apple Modem product with improvements. Plugs directly on Apple CAT II Board. Supports Videx and Smarterm 80 column cards, touch tone and rotary dial, remote terminal, voice toggle, easy printer access and much more. List \$39.00 — Introductory Price \$29.00.

PARALLEL PRINTER CARD
A Universal Centronics type parallel printer board complete with cable and connector. This unique board allows you to turn on and off the high bit so that you can access additional features in many printers. Use with EPSON, CITOH, ANADEx, STARWRITER, NEC, OKI and other with standard Centronics configuration. \$139.00

DOUBLE DOS Plus
A piggy-back board that plugs into the disk-controller card so that you can switch select between DOS 3.2 and DOS 3.3. DOUBLE DOS Plus requires APPLE DOS ROMS. P.O. BOX 113 POMPTON PLAINS, NJ 07444 \$39

³⁹To reveal a bad RNG, make a scatter plot of pairs of values. If you see snowflakes, the RNG is easily broken.

⁴⁰To compare Thumb instructions *a* and *b* while ignoring linker relocations, test for $a = b || a \& b \& 0xF000 = 0xF000$.