

1 Please stand; now, please be seated.

Neighbors, please join me in reading this ninth 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 software exploitation and the worship of weird machines. If you are missing the first eight 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, or the eighth in Heidelberg. This is our second epistle to Montréal, because we love that city and its fine neighbors.

Page 4 contains our own Pastor Manul Laphroaig's rant on the recent Wassenaar amendments, which will have us all burned as witches.

On page 7, Scott Bauer, Pascal Cuoq, and John Regehr present a backdoored version of `sudo`, but why should we give a damn whether anyone can backdoor such an application? Well, these fine neighbors abuse a pre-existing bug in CLANG that snuck past seventeen thousand assertions. Thus, the backdoor in their version of `sudo` *provably doesn't exist* until after compilation with a particular compiler. Ain't that clever?

On page 10, Travis Goodspeed and his neighbor Muur present fancy variants of digital shortwave radio protocols. They hide text in the null bits between PSK31 letters and in the space between RTTY bytes. Just for fun, they also transmit Morse code from 100 Mbit Ethernet to a nearby shortwave receiver!

It's common practice in some IT departments to use a Mouse Jiggler, such as the Weibetech MJ-3, to keep a screensaver from password protecting a seized computer while waiting for a forensic analyst. Mickey Shkatov took one of these doodads apart, and on page 20 he shows how to reprogram one.

On page 24, DJ Capelis and Daniel Bittman present a hypervisor exploit that was unwanted by the academic publishers. As our Right Reverend has better taste than the Unseen Academics, we happily scooped up their neighborly submission for you, our dear reader.

Saumil Shah says that a good exploit is one that is delivered in style, and Bukowski says that style is the answer to everything, a fresh way to approach a dull or dangerous thing. On page 27, Saumil presents us with tricks for encoding browser exploits as image files. Saumil has style.

Back in the days of Visual Basic 6, there was a directive, `on error resume next`, that instructed the interpreter to ignore any errors. Syntax error? Divide by zero? Wrong number of parameters? No problem, the program would keep running, the interpreter doing its very best to do *something* with the hideous mess of spaghetti code that VB programmers are famous for. On page 45, Jeffball from DC949 commits the criminal act of porting this behavior to C on Linux.

On page 47, Tommy Brixton sings a heartbreaking classic, Unbrick My Part!

On page 48, JP Aumasson talks about those fancy little NUMS—Nothing Up My Sleeve—numbers. He keeps a lot of them up his sleeves.


On page 55, Russell Handorf teaches us how to build a Wireless CTF on the cheap, broadcasting a number of different protocols through Direct Digital Synthesis on a Raspberry Pi.

On page 60, Philippe Teuwen explains how he made this PDF into a polyglot able to secure your communications by encrypting plain English into—wait for it—plain English! Still better, all cipher text is grammatical English!

On page 64, the last and most important page, we pass around the collection plate. Pastor Laphroaig doesn't need a touring jumbo jet like those television and radio preachers; rather, this humble worshiper of the weird machines just needs an arms-export license in order to keep his church newsletter legal under the the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. From those of you who are not Lords of War, we also gladly accept alms of PoC.

SWTP 6800 OWNERS—WE HAVE A CASSETTE I/O FOR YOU!

The CIS-30+ allows you to record and playback data using an ordinary cassette recorder at 30, 60 or 120 Bytes/Sec. No Hassle! Your terminal connects to the CIS-30+ which plugs into either the Control (MP-C) or Serial (MP-S) Interface of your SWTP 6800 Computer. The CIS-30+ uses the self clocking 'Kansas City'/Biphase Standard. The CIS-30+ is the FASTEST, MOST RELIABLE CASSETTE I/O you can buy for your SWTP 6800 Computer.



PerCom has a Cassette I/O for your computer!
Call or Write for complete specifications

Kit — \$69.95*
Assembled — \$89.95*
(manual included)
* plus 5% f/shipping

PERCOM PerCom Data Co.
P.O. Box 40598 • Garland, Texas 75042 • (214) 276-1968

PerCom — 'peripherals for personal computing'

TEXAS RESIDENTS ADD 8% SALES TAX