Connecting Communities

2016 RMLL SECURITY TRACK ★ BECAUSE NOT ONLY UNICORNS DESERVE FREE SOFTWARE AND SECURITY ★

Ange Albertini - RMLLSec 2016/7/4

This may not be a standard file. Congratulations for opening it.
Any crash or unexpected behavior is purely accidental - trust me!

ANGE ALBERTINI

reverse engineering

VISUAL DOCUMENTATION

@angealbertini

ange@corkami.com

http://www.corkami.com

Welcome to my talk!

LEVERAGING COMMITMENT ~ AGILE

MAXIMIZING SYNERGIES

INSPIRING SUCCESS

FOSTERING ACHIEVEMENT

RED OCEAN STRATEGY

DISRUPTIVE ~ OUTSTANDING

"OUT OF THE BOX" THINKING

GOAL-ORIENTED ~ USER-FOCUSED

UNCONVENTIONAL ~ INNOVATIVE

KEYNOTE

TL;DR

1. Hackers are very conventional in the way they share knowledge
2. I contribute to the journal of PoC||GTFO
   - It's a different way to share knowledge.
3. Try your own way too:
   We need more PXE, more PoC||GTFO!

HACKERS

ADVISORY

EXPLICIT RANT

Sharing knowledge

- Blog
  - no lower bar
  - no preservation
- Academic
  - No source or data
  - Difficult to write papers. LaTeX & PDF are still the best...
- Conference
  - Diluted content: 1h for 10 mins of interesting content

    OR "it should be a paper anyway"
  - Short talks are the underdogs
  - Entertainment over real impact:
    - Stars: disperse a lot of energy to shine, get bigger, very visible.

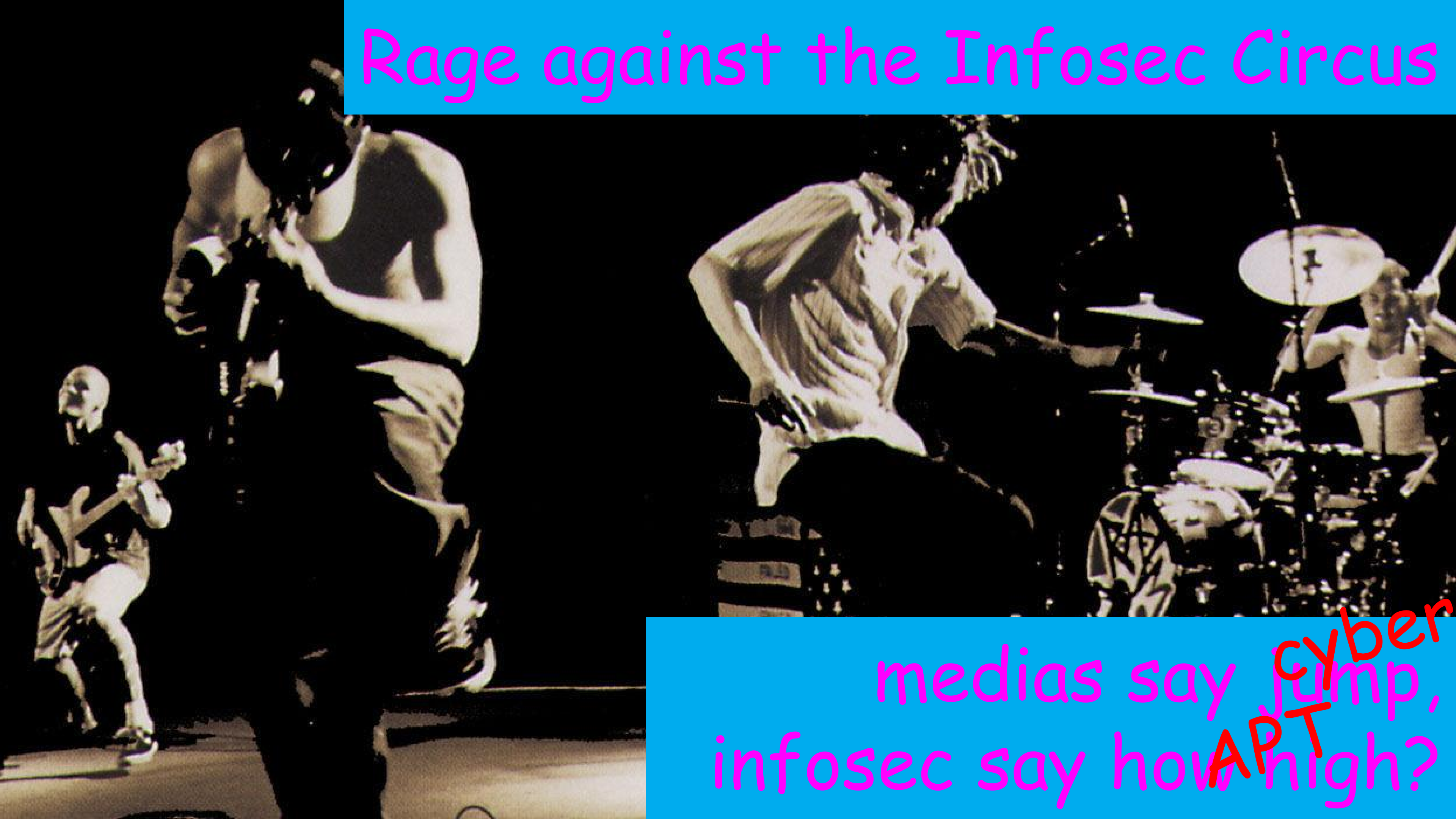
      versus
    - Blackholes: attract everything around them - it's their nature.

Why are hackers so
convention-al
for sharing knowledge?

Too many conferences.
Little impact.

Too often the same.
No expected impact
anymore.

Rage against the Infosec Circus



cyber

medias say jump,

APT

infosec say how high?

Why let medias decide how we communicate ?

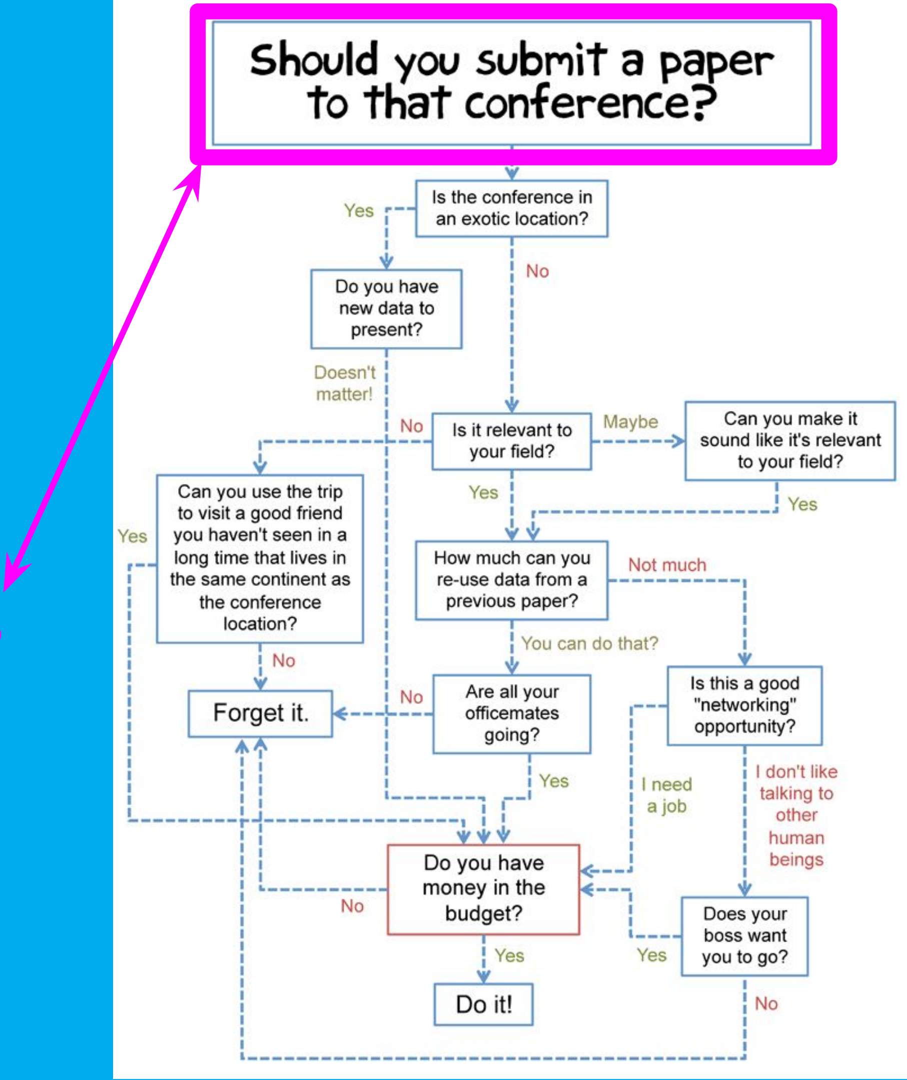
What's next: movies & trailers?

You're doing it for the *exposure*?
So all
this standardization
only benefits
...your ego?

Hello creative person! Thanks for making that thing!
You're welcome. Here's an invoice.
An invoice? Never mind that! You're doing it for the EXPOSURE!
INVOI
Here's your EXPOSURE!
Oh wow that's a ton of EXPOSURE! Thank you!
EXPOSURE!
$
$
LATER.
Do you accept these?
haha fuck no.
The Oatmeal

http://theoatmeal.com/comics/exposure

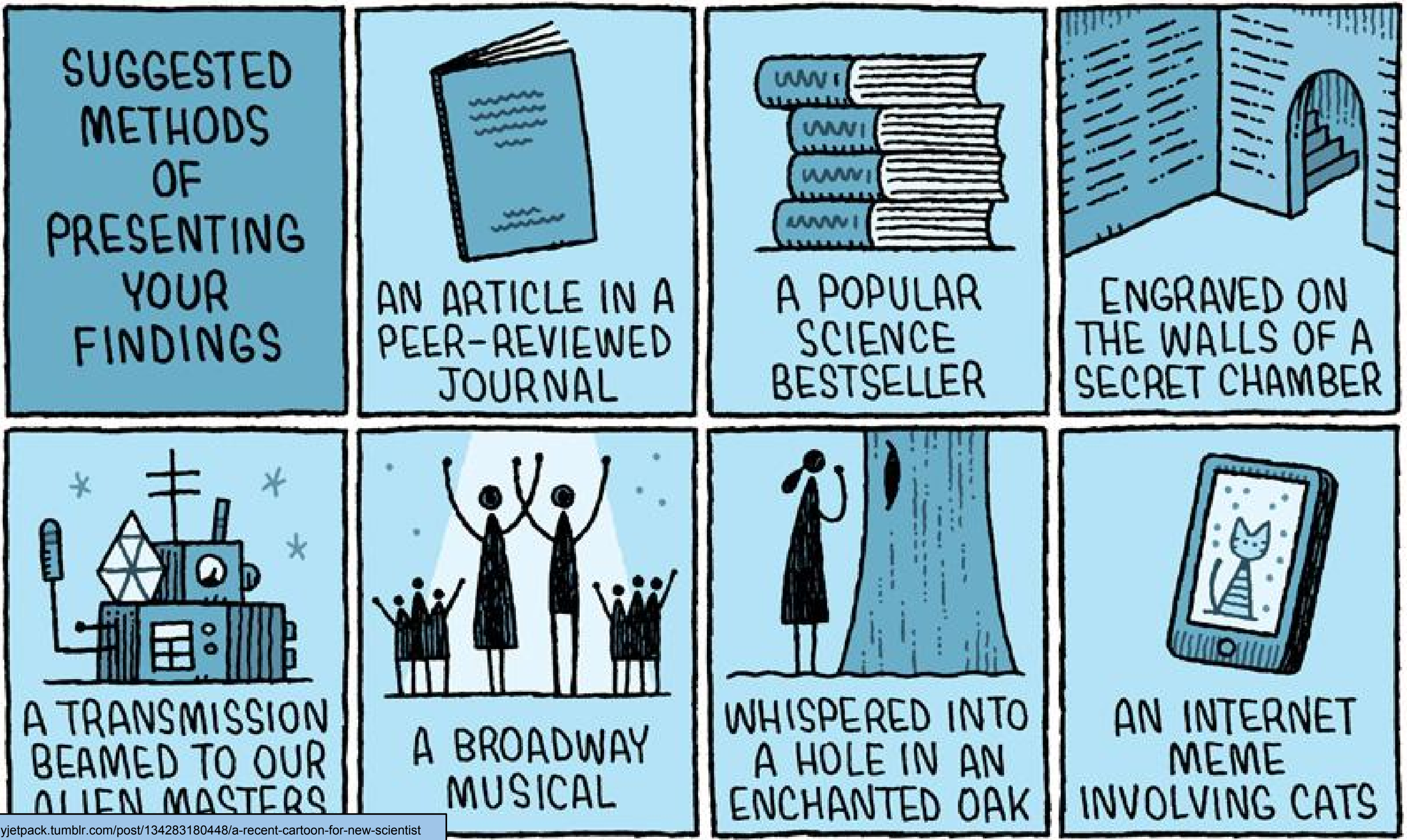
Advice: maybe not


Should you submit a paper to that conference?
Is the conference in an exotic location?
Yes
No
Do you have new data to present?
Doesn't matter!
No
Is it relevant to your field?
Maybe
Can you make it sound like it's relevant to your field?
Yes
Yes
Can you use the trip to visit a good friend you haven't seen in a long time that lives in the same continent as the conference location?
Yes
No
How much can you re-use data from a previous paper?
Not much
You can do that?
Forget it.
No
Are all your officemates going?
Is this a good "networking" opportunity?
Yes
I need a job
I don't like talking to other human beings
Do you have money in the budget?
No
Yes
Yes
Does your boss want you to go?
Do it!
No

http://phdcomics.com/comics/archive.php?comicid=1871

Make me stop use pink Comic Sans!

⇒ try something ***really*** different!


SUGGESTED METHODS OF PRESENTING YOUR FINDINGS
AN ARTICLE IN A PEER-REVIEWED JOURNAL
A POPULAR SCIENCE BESTSELLER
ENGRAVED ON THE WALLS OF A SECRET CHAMBER
A TRANSMISSION BEAMED TO OUR ALIEN MASTERS
A BROADWAY MUSICAL
WHISPERED INTO A HOLE IN AN ENCHANTED OAK
AN INTERNET MEME INVOLVING CATS

http://myjetpack.tumblr.com/post/134283180448/a-recent-cartoon-for-new-scientist

Remember:

stop ***having*** ideas,
try something!

</rant>

And now…

NO.1

PXE

Hacker Working Group
Request for Comments: 0x7e0
Updates: 0x7df
Category: Informational

FX
Phenoelit
April 2016

Phenoelit eXchange Event

The pool is seeded by arbitrary nodes who responded to this proposal using a SMTP transfer to the host reported in the MX record of the Internet domain phenoelit.de, addressing the recipient user fx. Said response shall include a topic of research, which the node is willing to explain in ad-hoc sessions to other nodes during the execution of PXE. The content shall be explainable in 10-15 standard minutes and the node shall be willing and prepared to explain it as often as requested by other nodes during the event. A suggested list of topics may be found in the following section Edge Communication.

http://ph-neutral.darklab.org/PXE5.txt

And now...

NO.3

https://www.youtube.com/watch?v=Tzmp8T2xX2A

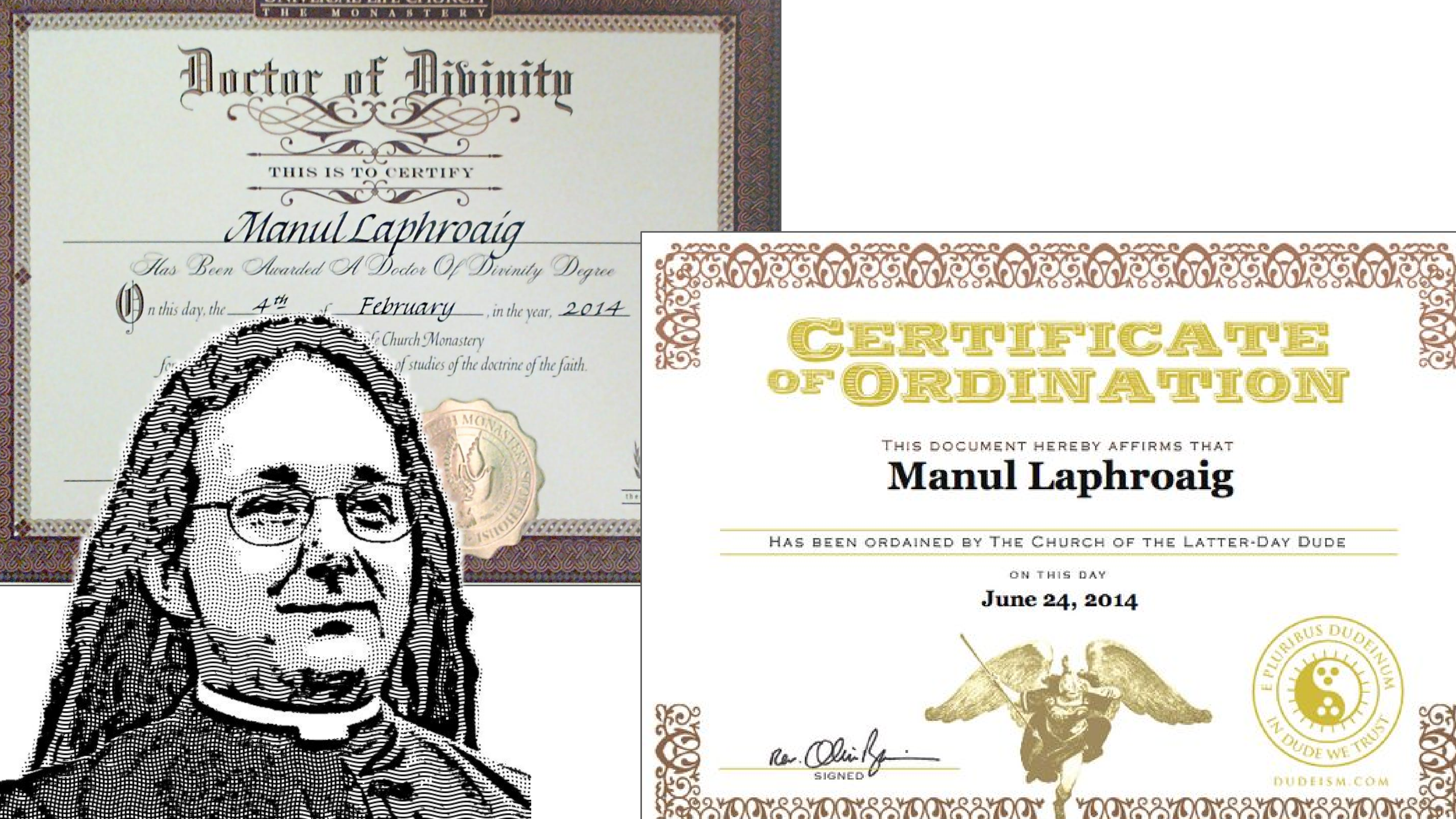
International Journal of PoC||GTFO

Proof of Concept or Get The Fuck Out

make INFOSEC great again

"Proof of Concept or Get The F*ck Out": Prove it or shut up

not “Picture of Cat” or “Person of Colour”



UNIVERSAL LIFE CHURCH
THE MONASTERY

Doctor of Divinity

THIS IS TO CERTIFY

Manul Laphroaig

Has Been Awarded A Doctor Of Divinity Degree

On this day, the 4th of February, in the year, 2014

…fe Church Monastery

fo… of studies of the doctrine of the faith.

Certificate of Ordination

This document hereby affirms that

Manul Laphroaig

Has been ordained by The Church of the Latter-Day Dude

on this day

June 24, 2014

Rev.

Signed

E PLURIBUS DUDEINUM

IN DUDE WE TRUST

DUDEISM.COM

Preacherman	Manul Laphroaig
Editor of Last Resort	Melilot
TeXnician	Evan Sultanik
Editorial Whipping Boy	Jacob Torrey
Funky File Supervisor	Ange Albertini
Assistant Scenic Designer	Philippe Teuwen

and sundry others

7 A Ghetto Implementation of CFI on x86

by Jeffrey Crowell

In 2005, M. Abadi and his gang presented a nifty trick to prevent control flow hijacking, called *Control Flow Integrity*. CFI is, essentially, a security policy that forces the software to follow a predetermined control flow graph (CFG), drastically restricting the available gadgets for return-oriented programming and other nifty exploit tricks.

Unfortunately, the current implementations in both Microsoft's Visual C++ and LLVM's clang compilers require source to be compiled with special flags to add CFG checking. This is sufficient when new software is created with the option of added security flags, but we do not always have such luxury. When dealing with third party binaries, or legacy applications that do not compile with modern compilers, it is not possible to insert these compile-time protections.

Luckily, we can combine static analysis with binary patching to add an equivalent level of protection to our binaries. In this article, I explain the theory of CFI, with specific examples for patching x86 32-bit ELF binaries—without the source code.

CFI is a way of enforcing that the intended control flow graph is not broken, that code always takes intended paths. In its simplest applications, we check that functions are always called by their intended parents. It sounds simple in theory, but in application it can get gnarly. For example, consider:

```
int a() { return 0; }
int b() { return a(); }
int c() { return a() + b() + 1; }
```

For the above code, our pseudo-CFI might look like the following, where `called_by_x` checks the return address.

```
int a() {
  if (!called_by_b && !called_by_c) {
    exit();
  }
  return 0;
}
int b() {
  if (!called_by_c) {
    exit();
  }
  return a();
}
int c() { return a() + b() + 1; }
```

Of course, this sounds quite easy, so let's dig in a bit further. Here is a very simple example program to illustrate ROP, which we will be able to effectively kill with our ghetto trick.

```
#include <string.h>

void smashme(char* blah) {
  char smash [16];
  strcpy(smash, blah);
}

int main(int argc, char** argv) {
  if (argc > 1) {
    smashme(argv[1]);
  }
}
```

In x86, the stack has a layout like the following.

Local Variables
Saved ebp
Return Pointer
Parameters
...

By providing enough characters to `smashme`, we can overwrite the return pointer. Assume for now, that we know where we are allowed to return to. We can then provide a whitelist and know where it is safe to return to in keeping the control flow graph of the program valid.

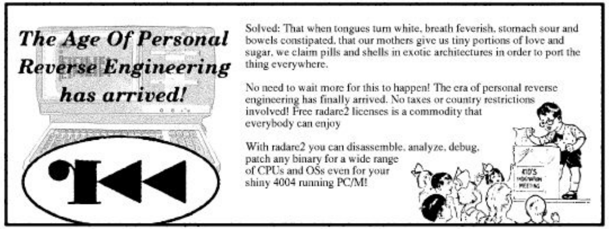
Figure 4 shows the disassembly of `smashme()` and `main()`, having been compiled by GCC.

Great. Using our whitelist, we know that `smashme` should only return to 0x08048456, because it is the next instruction after the `ret`. In x86, `ret` is equivalent to something like the following. (This is not safe for multi-threaded operations but we can ignore that for now.)

```
pop ecx ; puts the return address to ecx
jmp ecx ; jumps to the return address
```

```
[0x08048320]> pdf@sym.smashme
/ (fcn) sym.smashme 26
|           ; arg int arg_2        @ ebp+0x8
|           ; var int local_6      @ ebp-0x18
|           ; CALL XREF from 0x08048451 (sym.smashme)
|           0x0804841d      55              push ebp
|           0x0804841e      89e5            mov ebp, esp
|           0x08048420      83ec28          sub esp, 0x28
|           0x08048423      8b4508          mov eax, dword [ebp+arg_2]   ; [0x8:4]=0
|           0x08048426      89442404        mov dword [esp + 4], eax
|           0x0804842a      8d45e8          lea eax, [ebp-local_6]
|           0x0804842d      890424          mov dword [esp], eax
|           0x08048430      e8bbfeffff      call sym.imp.strcpy
|           0x08048435      c9              leave
\           0x08048436      c3              ret
[0x08048320]> pdf@sym.main
/ (fcn) sym.main 33
|           ; arg int arg_0_1      @ ebp+0x1
|           ; arg int arg_3        @ ebp+0xc
|           ; DATA XREF from 0x08048337 (sym.main)
|           ;-- main:
|           0x08048437      55              push ebp
|           0x08048438      89e5            mov ebp, esp
|           0x0804843a      83e4f0          and esp, 0xfffffff0
|           0x0804843d      83ec10          sub esp, 0x10
|           0x08048440      837d0801        cmp dword [ebp + 8], 1       ; [0x1:4]=0x1464c45
|       ,=< 0x08048444      7e10            jle 0x8048456
|       |   0x08048446      8b450c          mov eax, dword [ebp+arg_3]   ; [0xc:4]=0
|       |   0x08048449      83c004          add eax, 4
|       |   0x0804844c      8b00            mov eax, dword [eax]
|       |   0x0804844e      890424          mov dword [esp], eax
|       |   0x08048451      e8c7ffffff      call sym.smashme
|       |   ; JMP XREF from 0x08048444 (sym.main)
|       `-> 0x08048456      c9              leave
\           0x08048457      c3              ret
```

Figure 4 – Disassembly of `main()` and `smashme()`.



0x00:2 2 Ipod Antiforensics [Travis Goodspeed]
0x00:3 4 ELFs are dorky, elves are cool [Sergey Bratus] [Julian Bangert]
0x00:4 9 The Pastor Manul Laphroaig's First Epistle to Hacker Preachers of All to hacking.
0x00:5 10 Returning from ELF to Libc [Rebecca "Bx" Shapiro]
0x00:6 12 GTFO or #FAIL [FX of Phenoelit]
0x00:7 13 A Call for PoC [Rt. Revd. Pastor Manul Laphroaig]

0x01:2 2 Four Lines of Javascript that Can't Possibly Work So why do they? [Da
0x01:3 5 Weird Machines from Serena Butler's TV Typewriter [Travis Goodspee
0x01:4 9 Making a Multi-Windows PE [Ange Albertini]
0x01:5 11 This ZIP is also a PDF [Julia Wolf]
0x01:6 13 Burning a Phone [Josh “@m0nk” Thomas]
0x01:7 15 A Sermon concerning the Divinity of Languages; or, Dijkstra considere
0x01:8 17 A Call for PoC [Rt. Revd. Preacherman Pastor Manul Laphroaig]

0x02:2 3 A Parable on the Importance of Tools; or, Build your own fucking birdfe
0x02:3 5 A PGP Matryoshka Doll [Brother Myron Aub]
0x02:4 7 Reliable Code Execution on a Tamagotchi [Natalie Silvanovich]
0x02:5 10 Some Shellcode Tips for MSP430 and Related MCUs [Travis Goodsp
0x02:6 14 Calling putchar() from an ELF Weird Machine. [Rebecca .Bx Shapiro]
0x02:7 19 POKE of Death for the TRS 80 Model 100 [Dave Weinstein]
0x02:8 21 This OS is also a PDF [Ange Albertini]
0x02:9 25 A Vulnerability in Reduced Dakarand from PoC||GTFO 01:02 [joernch
0x02:10 30 Juggernauty [Ben Nagy]

0x03:2 5 Greybeard's Luck [Rt. Revd. Dr. Pastor Manul Laphroaig]
0x03:3 8 This PDF is a JPEG; or, This Proof of Concept is a Picture of Cats [An
0x03:4 10 NetWatch: System Management Mode is not just for Governments. [J
0x03:5 15 An Advanced Mitigation Bypass for Packet-in-Packet; or, I'm burning
0x03:6 18 Prototyping an RDRAND Backdoor in Bochs [Taylor Hornby]
0x03:7 22 Patching Kosher Firmware for Nokia 2720 [Assaf Nativ] [Anonymous]
0x03:8 30 Tetranglix: This Tetris is a Boot Sector [Juhani Haverinen] [Owen She
0x03:9 33 Defusing the Qualcomm Dragon [Josh “m0nk” Thomas]
0x03:10 35 Tales of Python's Encoding [Frederik Braun]
0x03:11 37 A Binary Magic Trick, Angecryption [Ange Albertini] [Jean-Philippe Au

0x04:2 4 First Epistle Concerning the Bountiful Seeds of 0Day [Manul Laphroaig
0x04:3 5 This OS is a Boot Sector [Shikhin Sethi]
0x04:4 12 Prince of PoC; or, A 16-sector version of Prince of Persia for the Appl
0x04:5 16 A Quick Introduction to the New Facedancer Framework [gil]
0x04:6 19 Dumping Firmware from Tamagotchi Friends by Power Glitching [Nat
0x04:7 22 Lenticrypt: a Provably Plausibly Deniable Cryptosystem; or, This Pictu
0x04:8 27 Hardening Pin Tumbler Locks against Myriad Attacks for Less Than a
0x04:9 32 Introduction to Reflux Decapsulation and Chip Photography [Travis G
0x04:10 37 Forget Not the Humble Timing Attack [Colin O'Flynn]
0x04:11 42 This Encrypted Volume is also a PDF; or, A Polyglot Trick for Bypass
0x04:12 44 How to Manually Attach a File to a PDF [Ange Albertini]
0x04:13 46 Ode to ECB [Ben Nagy]
0x04:14 48 A Call for PoC [Pastor Manul Laphroaig]

0x05:2 4 Stuff is broken, and only you know how [Rvd. Dr. Manul Laphroaig]
0x05:3 7 ECB as an Electronic Coloring Book [Philippe Teuwen]
0x05:4 11 An Easter Egg in PCI Express [Jacob Torrey]
0x05:5 15 A Flash PDF Polyglot [Alex Inführ]
0x05:6 17 These Philosophers Stuff on 512 Bytes; or, This Multiprocessing OS is a Boot
0x05:7 23 A Breakout Board for Mini-PCIe; or, My Intel Galileo has less RAM than its Vid
0x05:8 27 Prototyping a generic x86 backdoor in Bochs; or, I'll see your RDRAND backd
0x05:9 35 From Protocol to PoC; or, Your Cisco blade is booting PoC||GTFO. [Mik]
0x05:10 40 i386 Shellcode for Lazy Neighbors; or, I am my own NOP Sled. [Brainsmoke]
0x05:11 42 Abusing JSONP with Rosetta Flash [Michele Spagnuolo]
0x05:12 48 A cryptographer and a binarista walk into a bar [Ange Albertini] [Maria Eichlse
0x05:13 54 Ancestral Voices Or, a vision in a nightmare. [Ben Nagy]

0x06:1 3 Sacrament of Communion with the Weird Machines
0x06:2 4 On Giving Thanks [Pastor Manul Laphoraig]
0x06:3 6 Gekko the Dolphin [Fiora]
0x06:4 15 This TAR archive is a PDF! (as well as a ZIP, but you are probably used to it b
0x06:5 17 x86 Alchemy and Smuggling with Metalkit [Micah Elizabeth Scott]
0x06:6 25 Detecting MIPS Emulation [Craig Heffner]
0x06:7 29 More Cryptographic Coloring Books [Philippe Teuwen]
0x06:8 37 Introduction to Delayering and Reversing PCBs [Joe Grand]
0x06:9 41 Davinci Seal: Self-decrypting Executables [Ryan elfmaster O'Neill]
0x06:10 50 Observable Metrics [Don A. Bailey] [Tamara L. Rhoads] [Jaime Cochran]

0x07:1 3 With what shall we commune this evening?
0x07:2 4 AA55, the Magic Number [Morgan Reece Phillips]
0x07:3 5 Laser robots! [icah Elizabeth Scott]
0x07:4 10 A Story of Settled Science [Pastor Manul Laphroaig]
0x07:5 13 Scapy is for Script Kiddies [Eric Davisson]
0x07:6 18 Funky Files, the Novella! [Ange Albertini]
0x07:7 42 Extending AES-NI Backdoors [BSDaemon] [Pirata]
0x07:8 49 Innovations with Core Files [Ryan elfmaster O'Neill]
0x07:9 58 Bambaata on NASCAR [Count Bambaata]
0x07:10 61 Public Service Announcement
0x07:11 62 A Modern Cybercriminal [Ben Nagy]
0x07:12 64 Fast Cash for Bugs! [Pastor Manul Laphroaig]

0x08:2 4 Witches, Warlocks, and Wassenaar; or, On the Internet, no one knows you are a
0x08:3 7 Backdoors from Compiler Bugs [Scott Bauer] [Pascal Cuoq] [John Regehr]
0x08:4 10 A Protocol for Leibowitz [Travis Goodspeed] [Muur P.]
0x08:5 20 Reprogramming a Mouse Jiggler [Mickey Shkatov]
0x08:6 24 Exploiting an Academic Hypervisor [DJ Capelis] [Daniel Bittman]
0x08:7 27 Weaponized Polyglots as Browser Exploits [Stegosploit]
0x08:8 45 On Error Resume Next for Unix [Jeffball]
0x08:9 47 Sing Along with Toni Brixton [EVM] [Tommy Brixton]
0x08:10 48 Backdooring Nothing-Up-My-Sleeve Numbers [Jean-Philippe Aumasson]
0x08:11 55 Building a Wireless CTF [Russell Handorf]
0x08:12 60 Grammatically Correct Encryption [Philippe Teuwen]
0x08:13 64 Fast Cash for Cyber Munitions! [Pastor Manul Laphroaig]

0x09:2 4 A Sermon on Newton and Turing
0x09:3 7 Globalstar Satellite Communications [Colby Moore]
0x09:4 12 Keenly Spraying the Kernel Pools [Peter Hlavaty of Keen Team]
0x09:5 19 The Second Underhanded Crypto Contest [Taylor Hornby]
0x09:6 21 Cross VM Communications [Sophia D'Antoine]
0x09:7 26 Antivirus Tumors [Eric Davisson]
0x09:8 28 A Recipe for TCP/IPA [Ron Fabela of Binary Brew Works]
0x09:9 34 Mischief with AX.25 and APRS [Vogelfrei]
0x09:10 40 Napravi i ti Racunar „Galaksija“ [Voja Antonic]
0x09:11 60 Root Rights are a Grrl's Best Friend! [Fbz]
0x09:12 61 What If You Could Listen to This PDF? [Philippe Teuwen]
0x09:13 62 Oona's Puzzle Corner! [Oona Räisänen]
0x09:14 64 Fast Cash for Cyber Munitions! [Pastor Manul Laphroaig]

10:2 4 The Small Brown Dog and the Three Ghosts [Pastor Manul Laphroaig]
10:3 7 Exploiting Pokémon in a Super GameBoy [Allan Cecil (dwangoAC)] [Ilari Liusvaa
10:4 24 Pokéglot! [Allan Cecil (dwangoAC)] [Ilari Liusvaara (Ilari)] [Jordan Potter (p4plus
10:5 26 Cortex M0 Marionettes with SWD [Micah Elizabeth Scott]
10:6 32 Reversing a Pregnancy Test [Amanda Wozniak]
10:7 39 Apple][Copy Protections [Peter Ferrie (qkumba, san inc)]
10:8 76 Jailbreaking the TYT MD380 DMR Handheld [Travis Goodspeed KK4VCZ] [DD

11:2 4 In Praise of Junk Hacking [Pastor Manul Laphroaig]
11:3 6 Emulating Star Wars on a Vector Display [Trammell Hudson]
11:4 9 One Boot Sector PoC Deserves Another [Eric Davisson]
11:5 15 Defeating E7 Protection on the Apple][Platform [Peter Ferrie (qkumba, san i
11:6 20 Tourist's Phrasebook for the ARM Cortex M [Travis Goodspeed] [Ryan Speer
11:7 24 Ghetto CFI for X86 [Jeffrey Crowell]
11:8 28 Tourist's Guide to the MSP430 [Ryan Speers] [Travis Goodspeed]
11:9 33 The Treachery of Files [Evan Sultanik]
11:10 38 Ben "bushing" Byer Memorial [fail0verflow]

12:1 Lisez moi! [Rt. Revd. Pastor Manul Laphroaig]
12:2 Surviving the Computation Bomb [Rt. Revd. Pastor Manul Laphroaig]
12:3 A Z-Wave Carol [Chris Badenhop] [Ben Ramsey]
12:4 Comma Chameleon [Krzysztof Kotowicz] [Gábor Molnár]
12:5 Putting the VM in M/o/Vfuscator [Chris Domas]
12:6 A JCL Adventure with Network Job Entries [Soldier of Fortran]
12:7 Shellcode Hash Collisions [Mike Myers] [Evan Sultanik]
12:8 UMPOwn; A Symphony of Win10 Privilege [Alex Ionescu]
12:9 VIM Execution Engine [Chris Domas]
12:10 Doing Right by Neighbor O'Hara [Andreas Bogk]
12:11 Are Androids Polyglots? [Philippe Teuwen]
12:12 Tithe us your Alms of 0day! [Rt. Revd. Pastor Manul Laphroaig]

It's a journal with technical articles...

Tamagotchi

Cortex M

Flash

MSP430

PDF

ELF

BluRay

WavPack

Apple II

Tar

Nokia 2720

Crypto

Super NES

AX 25

Pregnancy Test

MBR

MIPS

PE

PGP

PowerPC

Lock Picking

Python

TRS80

Cortex M0

PCIe

ZIP

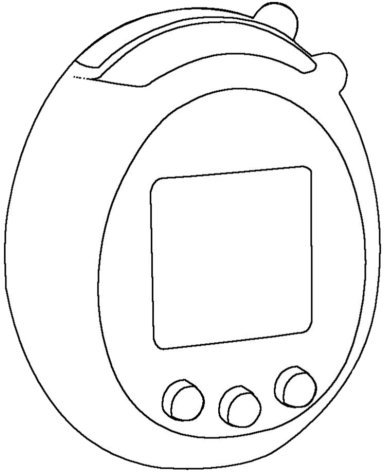
JPEG

GameBoy

MD380

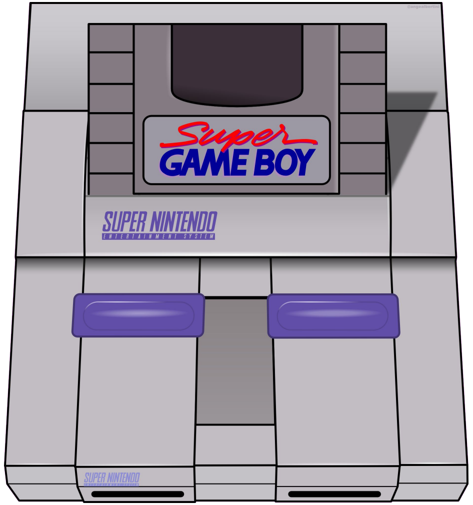
...spanning over different themes.

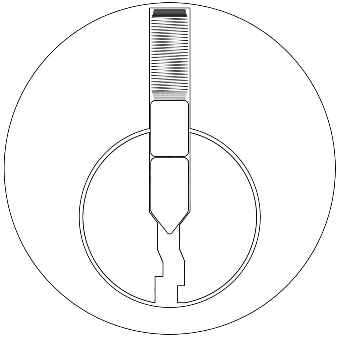
hardwares

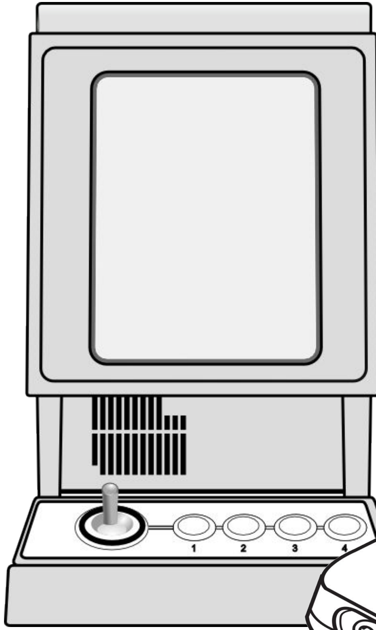


1,.?
2ABC
3DEF
*
4GHI
5JKL
6MNO
0
7PQRS
8TUV
9WXYZ
#

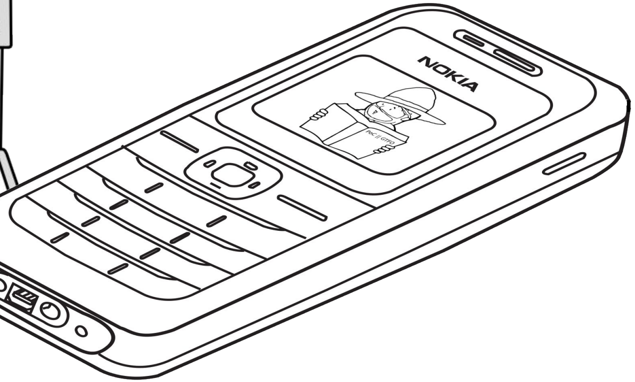
CRU


Super
GAME BOY
SUPER NINTENDO
ENTERTAINMENT SYSTEM

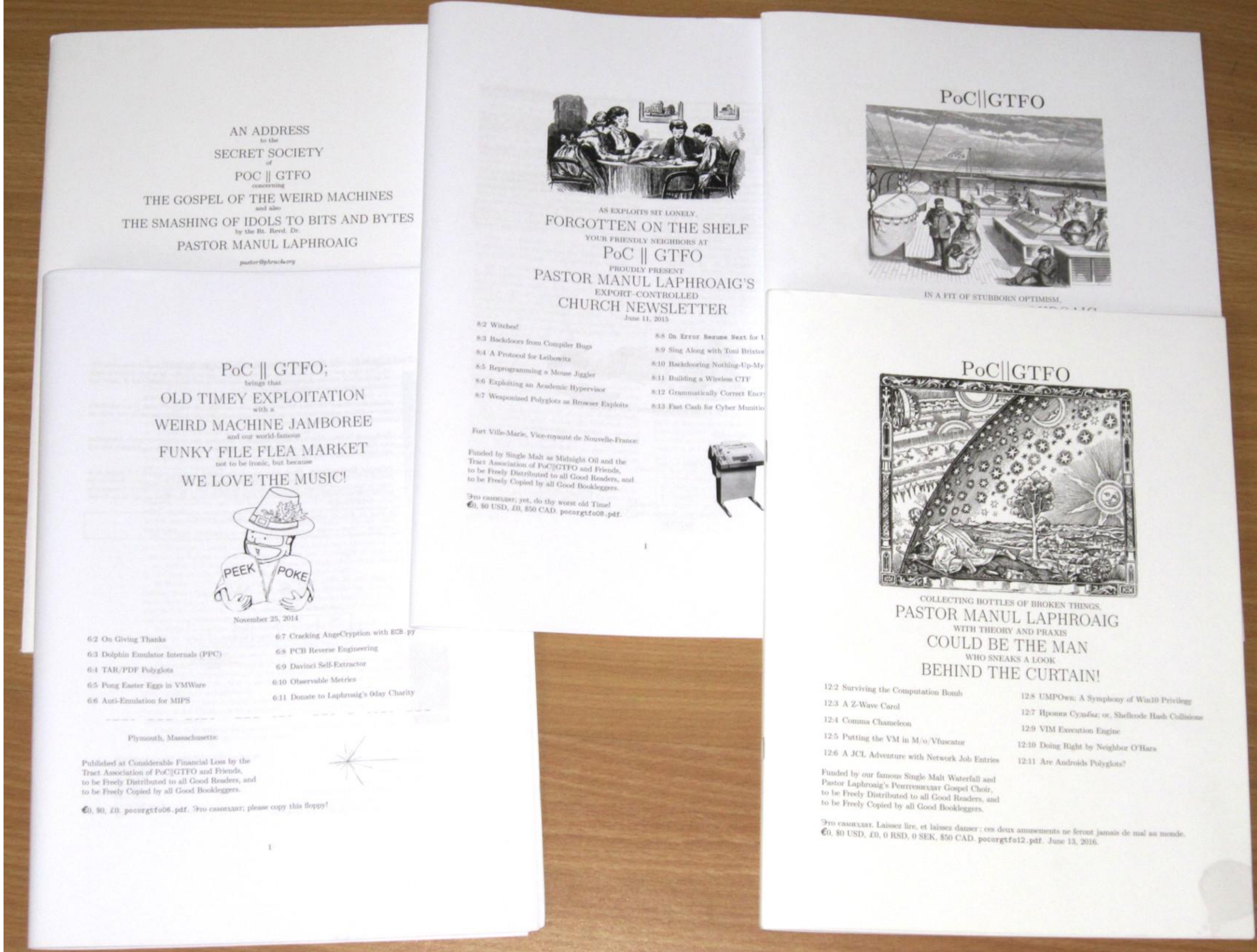



1
2
3
4

Eject


NOKIA

First available in print



AN ADDRESS
to the
SECRET SOCIETY
of
POC || GTFO
concerning
THE GOSPEL OF THE WEIRD MACHINES
and also
THE SMASHING OF IDOLS TO BITS AND BYTES
by the Rt. Revd. Dr.
PASTOR MANUL LAPHROAIG
pastor@phrack.org

AS EXPLOITS SIT LONELY,
FORGOTTEN ON THE SHELF
YOUR FRIENDLY NEIGHBORS AT
PoC || GTFO
PROUDLY PRESENT
PASTOR MANUL LAPHROAIG'S
EXPORT-CONTROLLED
CHURCH NEWSLETTER
June 11, 2015

8:2 Witches!
8:3 Backdoors from Compiler Bugs
8:4 A Protocol for Leibowitz
8:5 Reprogramming a Mouse Jiggler
8:6 Exploiting an Academic Hypervisor
8:7 Weaponized Polyglots as Browser Exploits
8:8 `On Error Resume Next` for U
8:9 Sing Along with Toni Brixton
8:10 Backdooring Nothing-Up-My-
8:11 Building a Wireless CTF
8:12 Grammatically Correct Encry
8:13 Fast Cash for Cyber Munitio

Fort Ville-Marie, Vice-royauté de Nouvelle-France:

Funded by Single Malt as Midnight Oil and the
Tract Association of PoC||GTFO and Friends,
to be Freely Distributed to all Good Readers, and
to be Freely Copied by all Good Bookleggers.

Это самиздат; yet, do thy worst old Time!
€0, $0 USD, £0, $50 CAD. `pocorgtfo08.pdf`.

1

PoC||GTFO

IN A FIT OF STUBBORN OPTIMISM,

PoC || GTFO;
brings that
OLD TIMEY EXPLOITATION
with a
WEIRD MACHINE JAMBOREE
and our world-famous
FUNKY FILE FLEA MARKET
not to be ironic, but because
WE LOVE THE MUSIC!

November 25, 2014

6:2 On Giving Thanks
6:3 Dolphin Emulator Internals (PPC)
6:4 TAR/PDF Polyglots
6:5 Pong Easter Eggs in VMWare
6:6 Anti-Emulation for MIPS
6:7 Cracking AngeCryption with `ECB.py`
6:8 PCB Reverse Engineering
6:9 Davinci Self-Extractor
6:10 Observable Metrics
6:11 Donate to Laphroaig's 0day Charity

Plymouth, Massachusetts:

Published at Considerable Financial Loss by the
Tract Association of PoC||GTFO and Friends,
to be Freely Distributed to all Good Readers, and
to be Freely Copied by all Good Bookleggers.

€0, $0, £0. `pocorgtfo06.pdf`. Это самиздат; please copy this floppy!

1

PoC||GTFO

COLLECTING BOTTLES OF BROKEN THINGS,
PASTOR MANUL LAPHROAIG
WITH THEORY AND PRAXIS
COULD BE THE MAN
WHO SNEAKS A LOOK
BEHIND THE CURTAIN!

12:2 Surviving the Computation Bomb
12:3 A Z-Wave Carol
12:4 Comma Chameleon
12:5 Putting the VM in M/o/Vfuscator
12:6 A JCL Adventure with Network Job Entries
12:8 UMPOwn: A Symphony of Win10 Privilege
12:7 Ирония Судьбы; or, Shellcode Hash Collisions
12:9 VIM Execution Engine
12:10 Doing Right by Neighbor O'Hara
12:11 Are Androids Polyglots?

Funded by our famous Single Malt Waterfall and
Pastor Laphroaig's Рентгенисдат Gospel Choir,
to be Freely Distributed to all Good Readers, and
to be Freely Copied by all Good Bookleggers.

Это самиздат. Laissez lire, et laissez danser ; ces deux amusements ne feront jamais de mal au monde.
€0, $0 USD, £0, 0 RSD, 0 SEK, $50 CAD. `pocorgtfo12.pdf`. June 13, 2016.

printed first:

⇒ hard deadline

⇒ get things done

Efficient against:
"I did X but never
took the time
to finish it"

One issue per quarter: ⇒ no rush to miss one

And no "I reserve this research for <1 time/year> event..."

Good for quality:
"Take your time" or
"Can you elaborate?"

No smaller margin:
just 1 clever trick
is enough

Good for non-mainstream content.

One's triviality/stunt could be another's solutions.

Don't be

~~evil~~ boring!

We reject, enforce quality, trim down.

Issue 10: 88 pages (cut)
Issue 11: 40 pages
Issue 12: 80 pages

An active
bi-directional
collaboration.

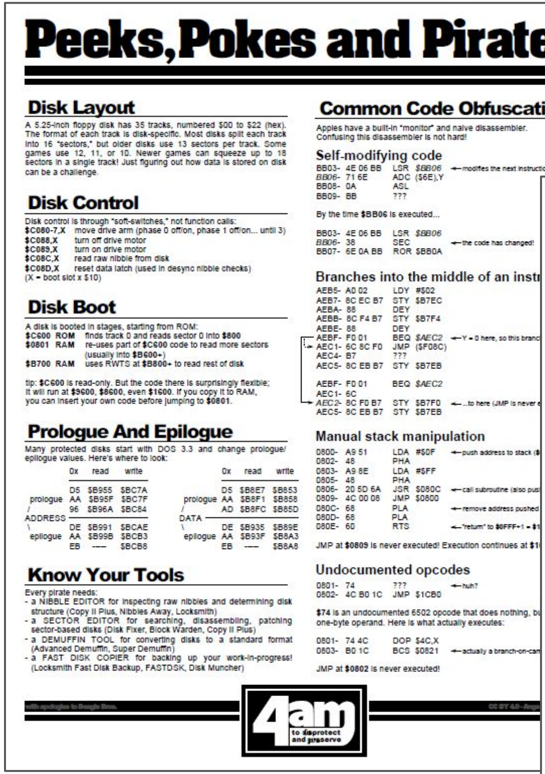
Don't submit & forget!

You have your own blog for that :)

We edit,
push,
contribute.

When both sides are interested, everybody wins.

And especially our audience.



Peeks, Pokes and Pirates

Disk Layout

A 5.25-inch floppy disk has 35 tracks, numbered $00 to $22 (hex). The format of each track is disk-specific. Most disks split each track into 16 "sectors," but older disks use 13 sectors per track. Some games use 12, 11, or 10. Newer games can squeeze up to 18 sectors in a single track! Just figuring out how data is stored on disk can be a challenge.

Disk Control

Disk control is through "soft-switches," not function calls:

$C080-7,X move drive arm (phase 0 off/on, phase 1 off/on... until 3)
$C088,X turn off drive motor
$C089,X turn on drive motor
$C08C,X read raw nibble from disk
$C08D,X reset data latch (used in desync nibble checks)
(X = boot slot x $10)

Disk Boot

A disk is booted in stages, starting from ROM:

$C600 ROM finds track 0 and reads sector 0 into **$800**
$0801 RAM re-uses part of **$C600** code to read more sectors (usually into **$B600+**)
$B700 RAM uses RWTS at **$B800+** to read rest of disk

tip: **$C600** is read-only. But the code there is surprisingly flexible; it will run at **$9600**, **$8600**, even **$1600**. If you copy it to RAM, you can insert your own code before jumping to **$0801**.

Prologue And Epilogue

Many protected disks start with DOS 3.3 and change prologue/epilogue values. Here's where to look:

	0x	read	write
	D5	$B955	$BC7A
prologue	AA	$B95F	$BC7F
/	96	$B96A	$BC84
ADDRESS			
\	DE	$B991	$BCAE
epilogue	AA	$B99B	$BCB3
	EB	----	$BCB8

	0x	read	write
	D5	$B8E7	$B853
prologue	AA	$B8F1	$B858
/	AD	$B8FC	$B85D
DATA			
\	DE	$B935	$B89E
epilogue	AA	$B93F	$B8A3
	EB	----	$B8A8

Know Your Tools

Every pirate needs:

- a NIBBLE EDITOR for inspecting raw nibbles and determining disk structure (Copy II Plus, Nibbles Away, Locksmith)
- a SECTOR EDITOR for searching, disassembling, patching sector-based disks (Disk Fixer, Block Warden, Copy II Plus)
- a DEMUFFIN TOOL for converting disks to a standard format (Advanced Demuffin, Super Demuffin)
- a FAST DISK COPIER for backing up your work-in-progress! (Locksmith Fast Disk Backup, FASTDSK, Disk Muncher)

Common Code Obfuscation

Apples have a built-in "monitor" and naive disassembler. Confusing this disassembler is not hard!

Self-modifying code

```
BB03-  4E 06 BB    LSR  $BB06     ←modifies the next instruction
BB06-  71 6E       ADC  ($6E),Y
BB08-  0A          ASL
BB09-  BB          ???
```

By the time **$BB06** is executed...

```
BB03-  4E 06 BB    LSR  $BB06
BB06-  38          SEC            ←the code has changed!
BB07-  6E 0A BB    ROR  $BB0A
```

Branches into the middle of an instr

```
AEB5-  A0 02       LDY  #$02
AEB7-  8C EC B7    STY  $B7EC
AEBA-  88          DEY
AEBB-  8C F4 B7    STY  $B7F4
AEBE-  88          DEY
AEBF-  F0 01       BEQ  $AEC2     ←Y = 0 here, so this branc
AEC1-  6C 8C F0    JMP  ($F08C)
AEC4-  B7          ???
AEC5-  8C EB B7    STY  $B7EB

AEBF-  F0 01       BEQ  $AEC2
AEC1-  6C
AEC2-  8C F0 B7    STY  $B7F0     ←...to here (JMP is never e
AEC5-  8C EB B7    STY  $B7EB
```

Manual stack manipulation

```
0800-  A9 51       LDA  #$0F      ←push address to stack ($
0802-  48          PHA
0803-  A9 8E       LDA  #$FF
0805-  48          PHA
0806-  20 5D 6A    JSR  $080C     ←call subroutine (also pus
0809-  4C 00 08    JMP  $0800
080C-  68          PLA            ←remove address pushed
080D-  68          PLA
080E-  60          RTS            ←"return" to $0FFF+1 = $1
```

JMP at **$0809** is never executed! Execution continues at $1

Undocumented opcodes

```
0801-  74          ???            ←huh?
0802-  4C B0 1C    JMP  $1CB0
```

$74 is an undocumented 6502 opcode that does nothing, bu one-byte operand. Here is what actually executes:

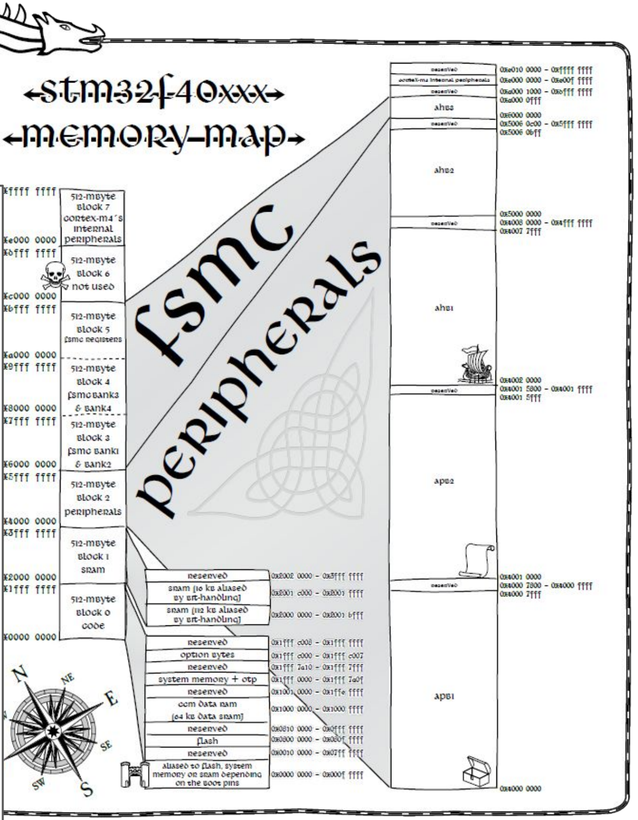
```
0801-  74 4C       DOP  $4C,X
0803-  B0 1C       BCS  $0821     ←actually a branch-on-carr
```

JMP at **$0802** is never executed!

with apologies to Beagle Bros.

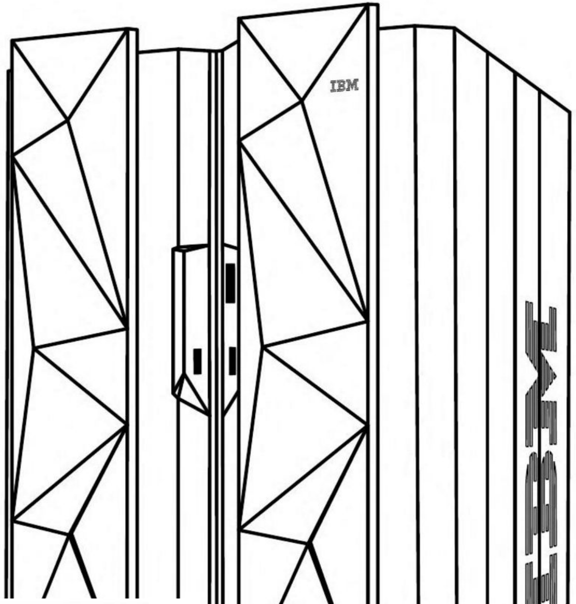
4am
to deprotect and preserve

CC BY 4.0 - Ange


stm32f40xxx
memory-map
0xffff ffff
512-mbyte block 7 cortex-m4's internal peripherals
0xe000 0000
0xdfff ffff
512-mbyte block 6 not used
0xc000 0000
0xbfff ffff
512-mbyte block 5 fsmc registers
0xa000 0000
0x9fff ffff
512-mbyte block 4 fsmc bank3 & bank4
0x8000 0000
0x7fff ffff
512-mbyte block 3 fsmc bank1 & bank2
0x6000 0000
0x5fff ffff
512-mbyte block 2 peripherals
0x4000 0000
0x3fff ffff
512-mbyte block 1 sram
0x2000 0000
0x1fff ffff
512-mbyte block 0 code
0x0000 0000
fsmc
peripherals
reserved
0x2002 0000 - 0x3fff ffff
sram (16 kb aliased by bit-handling)
0x2001 c000 - 0x2001 ffff
sram (112 kb aliased by bit-handling)
0x2000 0000 - 0x2001 bfff
reserved
0x1fff c008 - 0x1fff ffff
option bytes
0x1fff c000 - 0x1fff c007
reserved
0x1fff 7a10 - 0x1fff 7fff
system memory + otp
0x1fff 0000 - 0x1fff 7a0f
reserved
0x1001 0000 - 0x1ffe ffff
ccm data ram (64 kb data sram)
0x1000 0000 - 0x1000 ffff
reserved
0x0810 0000 - 0x0fff ffff
flash
0x0800 0000 - 0x080f ffff
reserved
0x0010 0000 - 0x07ff ffff
aliased to flash, system memory or sram depending on the boot pins
0x0000 0000 - 0x000f ffff
reserved
0xe010 0000 - 0xffff ffff
cortex-m4 internal peripherals
0xe000 0000 - 0xe00f ffff
reserved
0xa000 1000 - 0xbfff ffff
0xa000 0fff
ahb3
0x6000 0000
reserved
0x5006 0c00 - 0x5fff ffff
0x5006 0bff
ahb2
0x5000 0000
reserved
0x4008 0000 - 0x4fff ffff
0x4007 7fff
ahb1
0x4002 0000
reserved
0x4001 5800 - 0x4001 ffff
0x4001 57ff
apb2
0x4001 0000
reserved
0x4000 7800 - 0x4000 ffff
0x4000 7fff
apb1
0x4000 0000
N
NE
E
SE
S
SW

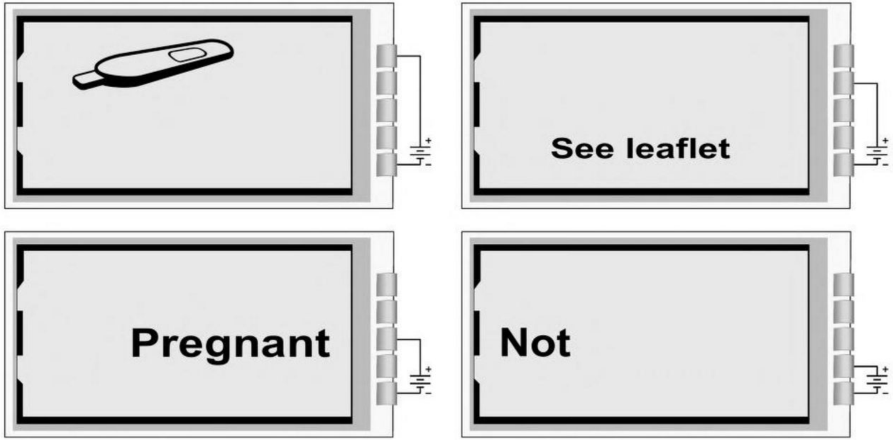
Drawings...

Submitted pictures:
bad lighting,
blurry, grainy
bad angle,
scratches, folds.



```
rebelofold: WUT
55: whaaat
Hi Mom!!
georgemichaels: we're the twitch
 chat
gallerduse: HI COUCH
kyiroo:  //
chillie:
zoranthebear: WOOOOOO
ederarm: Lmao
liontheturtle: OMFG
devinlock: Oh my
wallydrag: HI MOM
toastypls: MATRIX dear

molten_: WHAT
asdyyy: start9  dor: LOL
gadwin100: rekt
andykarate: fdg
tovargent:
soulroarn: WHAT?
lukeskywars: UP
kidsmirk: heloooo!!!!
love_struck_: HULLO
HI MOM!
 anthecaiun:
```



Vectors are optimal for visual information.

Original drafts:
on a napkin,
on a tablet,
in a shaky bus...

Official PDFs:
broken encoding,
broken font,
or even **errors**!

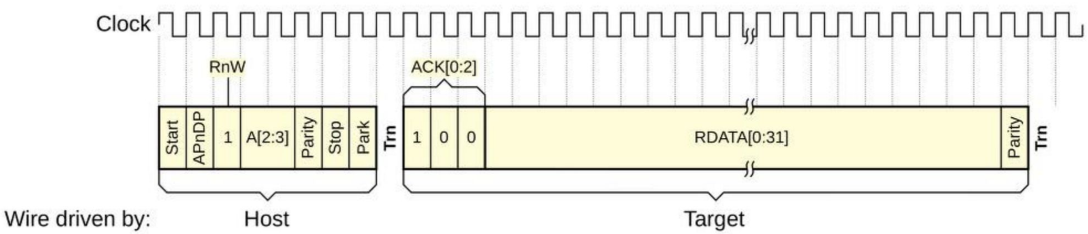
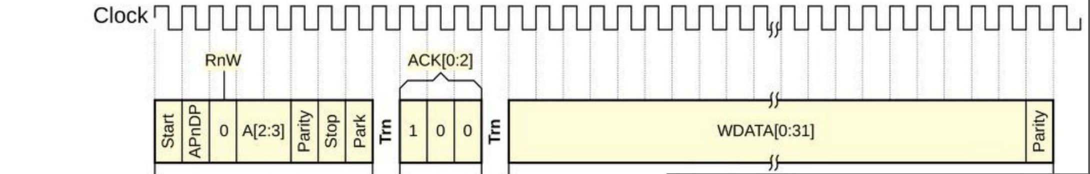
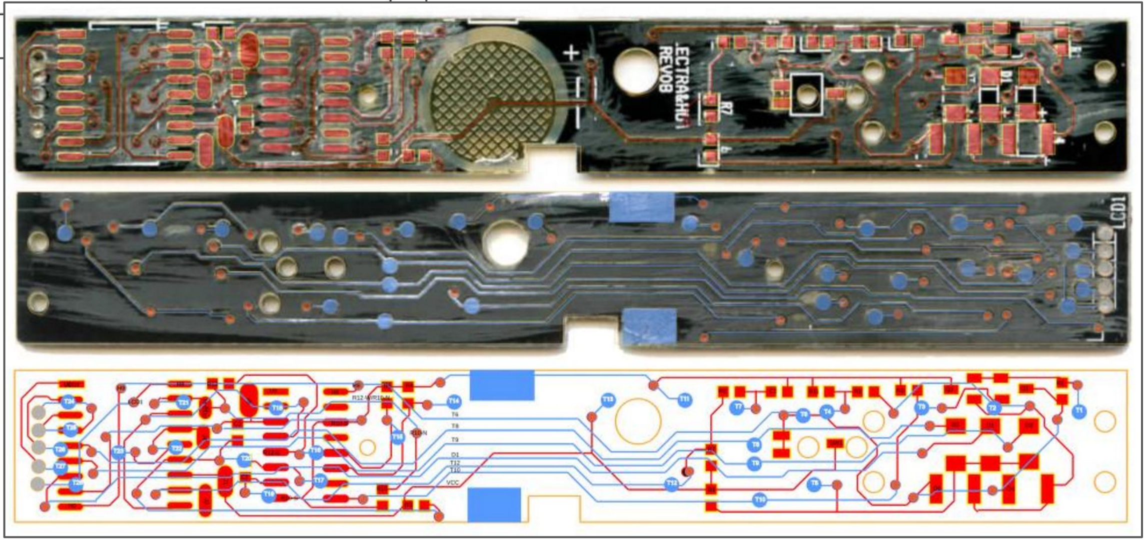
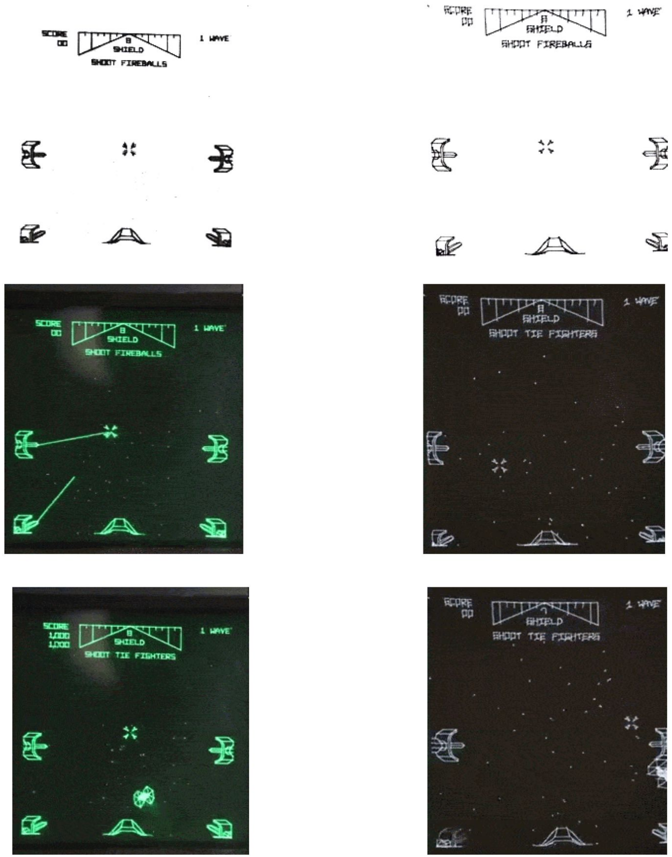


Figure 13 – Serial Wire Debug successful read operation

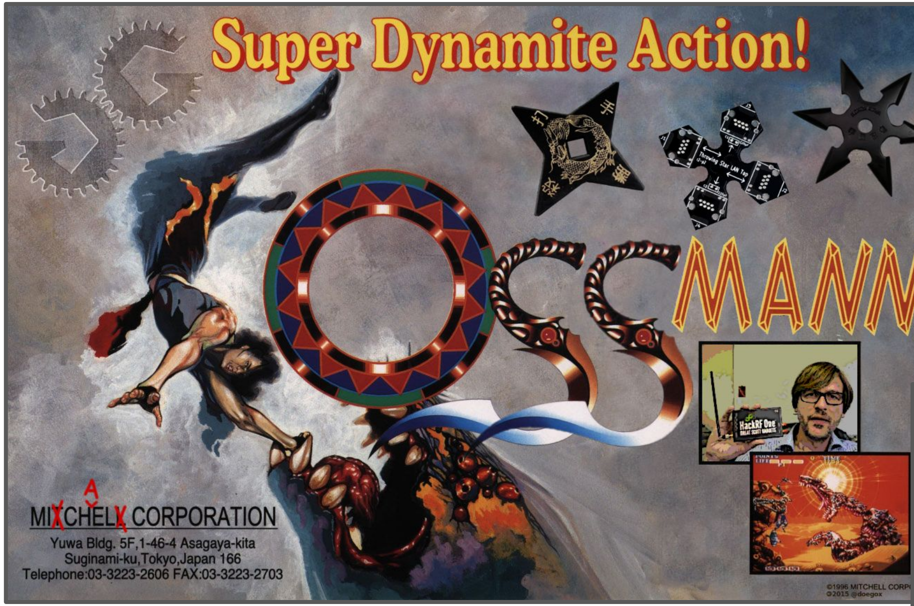


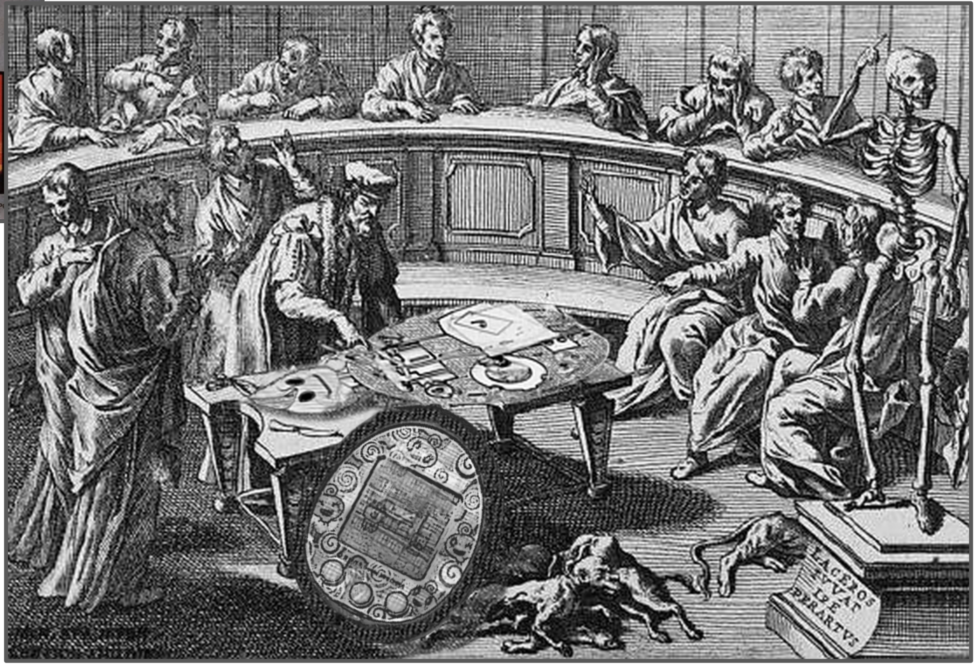


We extract and fix PDF data
from external sources.
Text should be extractable.

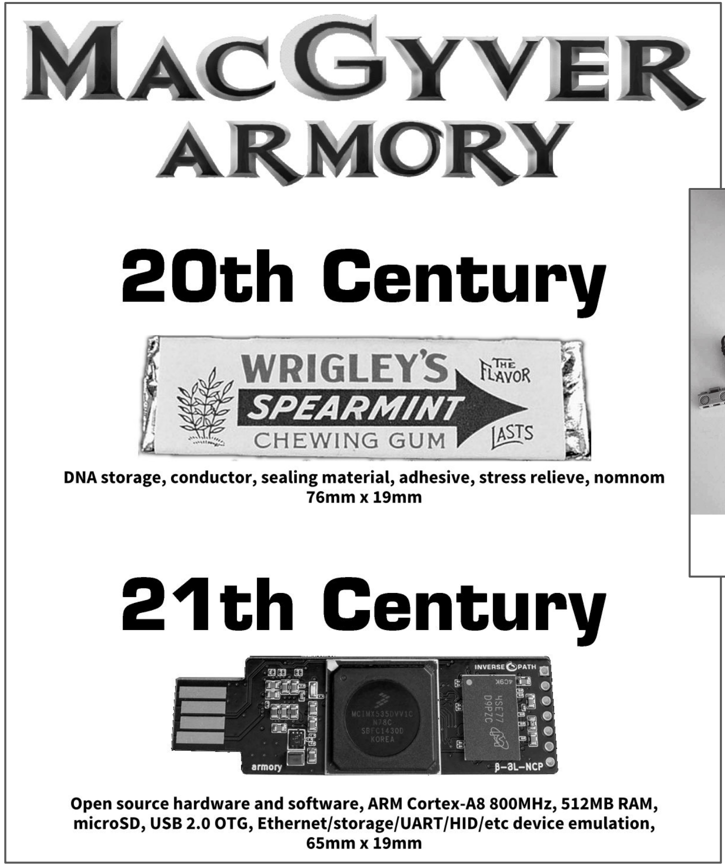


JavaScript animations


Super Dynamite Action!
OSSMANN
TM
Throwing Star LAN Tap
HackRF One
A
MI~~T~~CHEL~~L~~ CORPORATION
Yuwa Bldg. 5F,1-46-4 Asagaya-kita
Suginami-ku,Tokyo,Japan 166
Telephone:03-3223-2606 FAX:03-3223-2703
©1996 MITCHELL CORP
©2015 @doegox



Illustrations



MacGyver Armory

20th Century

DNA storage, conductor, sealing material, adhesive, stress relieve, nomnom
76mm x 19mm

21th Century

Open source hardware and software, ARM Cortex-A8 800MHz, 512MB RAM, microSD, USB 2.0 OTG, Ethernet/storage/UART/HID/etc device emulation, 65mm x 19mm

zines that teach cs concepts via cute drawings!
shop.bubblesort.io

BOLDPORT CLUB
A new electronics project every month!

International shipping

NEW!

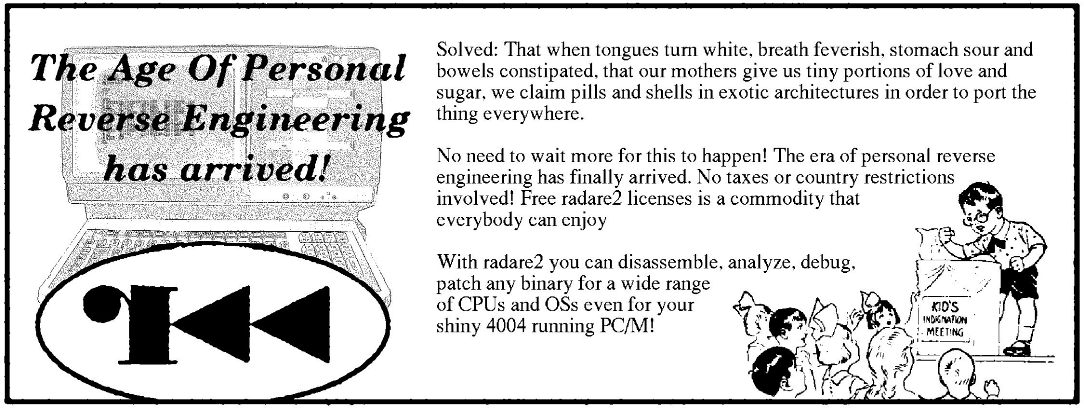
BOLDPORT CLUB, PROJECT #1
Phototransistor
LM331
"My favorite programming language is solder" Bob Pease
V=I·R
P=I·V

project #3 the Cordwood Puzzle

of the exclusive Boldport Club
77)9606045
tors will take payment

Access

ted, Arch 12, Raymouth Road, London SE16 2DB, United Kingdom



The Age Of Personal Reverse Engineering has arrived!

Solved: That when tongues turn white, breath feverish, stomach sour and bowels constipated, that our mothers give us tiny portions of love and sugar, we claim pills and shells in exotic architectures in order to port the thing everywhere.

No need to wait more for this to happen! The era of personal reverse engineering has finally arrived. No taxes or country restrictions involved! Free radare2 licenses is a commodity that everybody can enjoy

With radare2 you can disassemble, analyze, debug, patch any binary for a wide range of CPUs and OSs even for your shiny 4004 running PC/M!

Old-style ads

In Memoriam: Ben “bushing” Byer

by fail0verflow

Ben Byer
1980–2016

We are deeply saddened by the news that our member, colleague, and friend Ben “bushing” Byer passed away of natural causes on Monday, February 8th.

Many of you knew him as one of the public faces of our group, fail0verflow, and before that, Team Twiizers and the iPhone Dev Team.

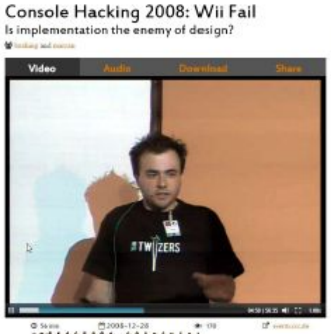
Outspoken but never confrontational, he was proof that even in the competitive and often aggressive hacking scene, there is a place for both a sharp mind and a kind heart.

To us he was, of course, much more. He brought us together, as a group and in spirit. Without him, we as a team would not exist. He was a mentor to many, and an inspiration to us all.

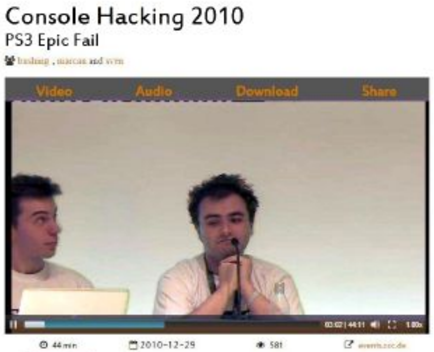
Yet above anything, he was our friend. He will be dearly missed.

Our thoughts go out to his wife and family.

Keep hacking. It’s what bushing would have wanted.



Console Hacking 2008: Wii Fail
Is implementation the enemy of design?
bushing and marcan



Console Hacking 2010
PS3 Epic Fail
bushing , marcan and sven

layout by bushing & emu_kidid
That's the spirit!
v1.2
Paul,
Thank you so much for your help solving the mystery of the elusive "Wii Startup Disc". Keep on hacking!
-bushing
9/2010
Startup Disc
NINTENDO DS

<...>

2 In Praise of Junk Hacking

by Pastor Manul Laphroaig
in polite dissent to Daily Dave.

Gather round y'all, young and old, and listen to a story that I have to tell.

Back in 2014, when we were all eagerly waiting for `</SCORPION>` to debut on the TV network formerly known as the Columbia Broadcasting System, a minor ruckus was raised over Junk Hacking. The moral fiber of the youth, it was said, was being corrupted by a dozen cheap Black Hat talks on popping embedded systems with old bugs from the nineties. Who among us high-brow neighbors would sully the good name of our profession by hacking an ATM that runs Windows XP, when breaking into XP is old hat?

Let's think for just a minute and consider the best examples of neighborly junk hacking. Perhaps we'll find that rather than being mere publicity stunts, junk hacking is a way to step back from the daily grind of confidential consulting work, to share nifty tricks and techniques that are often more interesting than the bug itself.

– – – –   – – –   – – – –

Our first example today is from everyone's favorite doctor in a track suit, Charlie Miller. If you have the misfortune of reading about his work in the lay press, you might have heard that he could blow up laptop batteries by software,[1] or that he was recklessly irresponsible by disabling the power train of a car with a reporter inside.[2] That is to say, from the lay press articles, you wouldn't know a damned thing about what *mechanism* he experimented with.

So please, read the fucking paper, the battery hacking paper,[3] and ignore what CNN has to say on the subject. Read about how the Smart Battery Charger (SBC) is responsible for charging the battery even when the host is unresponsive, and consider how much more stable this would be than giving the host responsibility for managing the state. Read about how a complete development kit is available for the platform, about how the firmware update is flashed out of order to prevent bricking the battery.

Read about how the Texas Instruments BQ20Z80 chip is a CoolRISC 816 microcontroller, which was identified by Dion Blazakis through googling opcodes when the instruction set was not documented by the manufacturer. See that its mask ROM functions are well documented in `sluu225.pdf`.[4] Read about how code memory erases not to all ones, as most architectures would, but to `ff ff 3f` because that's a NOP instruction.

Read about how this architecture wasn't supported by IDA Pro, but that a plugin disassembler wasn't much trouble to write.[5] Read about how instructions on the CoolRISC platform are 22 bits wide and 24-bit aligned, so code might begin at any 3-byte boundary. See how Charlie bypasses the firmware checksums in order to inject his own code.

Can you really read all thirty-eight pages without learning one new trick, without learning anything nifty? Without anything more to say than your disappointment that batteries shipped with the default password? He who has eyes to read, let him read!

– – – –   – – –   – – – –

Loyal readers of this journal will remember PoC‖GTFO 2:4, in which Natalie Silvanovich gets remote code execution in a Tamagotchi's 6502 microcontroller through a plug-in memory chip. "Big whoop," some jerk might say, "local control of memory is getting root when you already have root!"

Re-read her article; it packs a hell of a lot into just two pages. The memory that she controls is just data memory, containing some fixed-size sprites and single byte describing the game that the cartridge should load. The game itself, like all other code, is already in the CPU's unwritable Mask ROM.

[1] If you RTFP, you'll note that the Apple batteries have a separate BQ29312 Analog Frontend (AFE) to protect against such nonsense, as well as a Matsushita MU092X in case the BQ29312 isn't sufficient.

[2] One time, my Studebaker ran out of gas on the highway. Maybe we should start a support group?

[3] `unzip pocorgtfo11.pdf batteryfirmware.pdf`

[4] `unzip pocorgtfo11.pdf sluu225.pdf`

[5] `unzip pocorgtfo11.pdf bq20z80.py`

10 Doing Right by Neighbor O'Hara

by Andreas Bogk
Knight in the Grand Recursive Order of the Knights of the Lambda Calculus
Priest in the House of the Apostles of Eris

What good is a pulpit that can't be occasionally shared with a neighborly itinerant preacher? In this fine sermon, Sir Andreas warns us of the heresy that "input sanitation" will somehow protect you from injection attacks, no matter what comes next for the inputs you've "sanitized"—and vouchsafes the true prophecy of parsing and unparsing working together, keeping your inputs and outputs valid, both coming and going. —PML

Brothers, Sisters, and Variations Thereupon!

Let me introduce you to a good neighbor. Her name is *O'Hara* and she was born on *January 1st in the year 1970* in Dublin. She's made quite an impressive career, and now lives in a nice house in *Scunthorpe, UK*, working remotely for *AT&T*.

I ask you, neighbors: would you deny our neighbor O'Hara in the name of SQL injection prevention? Or would you deny her date of birth, just because you happen to represent it as zero in your verification routine? Would you deny her place of work, as abominable as it might be? Or would you even deny her place of living, just because it contains a sequence of letters some might find offensive?

You say no, and of course you'd say no! As her name and date of birth and employer and place of residence, they are all valid inputs. And thou shalt not reject any valid input; that truly would not be neighborly!

But wasn't input filtering a.k.a. "sanitization" the right thing to do? Don't characters like `'` and `&` wreak unholy havoc upon your backend SQL interpreter or your XHTML generator?

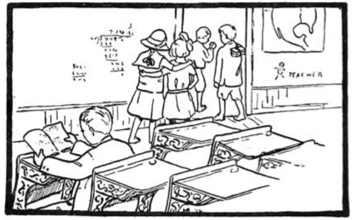
So where did we go wrong by the neighbor O'Hara?

There is a false prophesy making the rounds that you can protect against undesirable injection into your system by "input sanitization," no matter where your "sanitized" inputs go from there, and no matter how they then get interpreted or rendered. This "sanitization" is a heathen fetish, neighbors, and the whole thing is dangerous foolery that we need to drive out of the temple of proper input-handling.

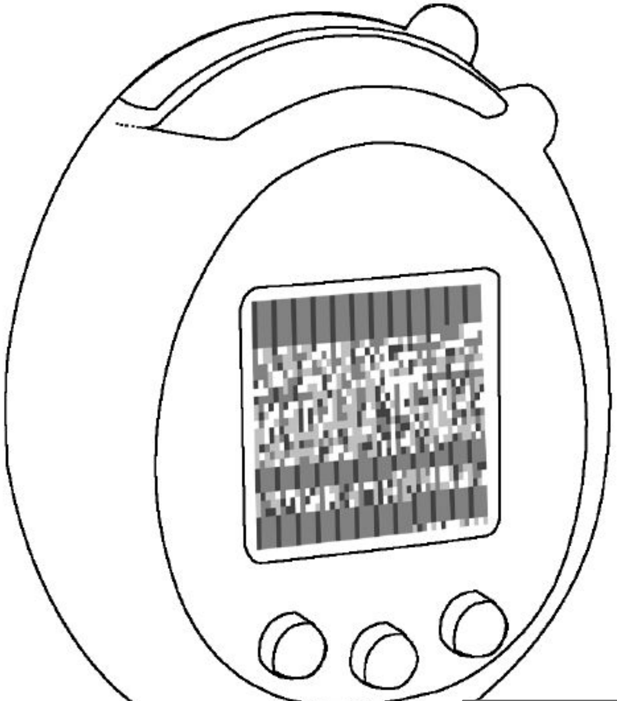
Indeed, is the apostrophe character so inherently dirty and evil, that we need to "sanitize" them out? Why, then, are we using this evil character at all? Is the number 0 evil and unclean, no matter what, despite historians of mathematics raving about its invention? Are certain sounds unspeakable, regardless of where and when one may speak them?

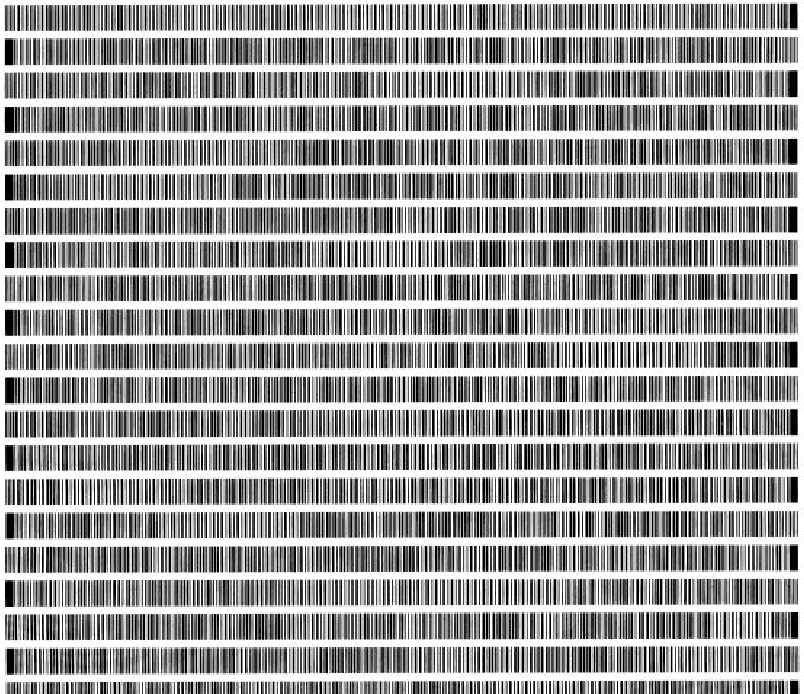
No, no, and no—for all bytes are created equal, and their interpretation depends solely on the context they are interpreted in. As any miracle cure, this snake oil of "sanitization" claims a grain of truth, but entirely misses its point. No byte is inherently "dirty" so as to be "sanitized" as such—but context and interpretation happeneth to them all, and unless you know what these context and the interpretations are, your "sanitization" is useless, nay, harmful and unneighborly to O'Hara.

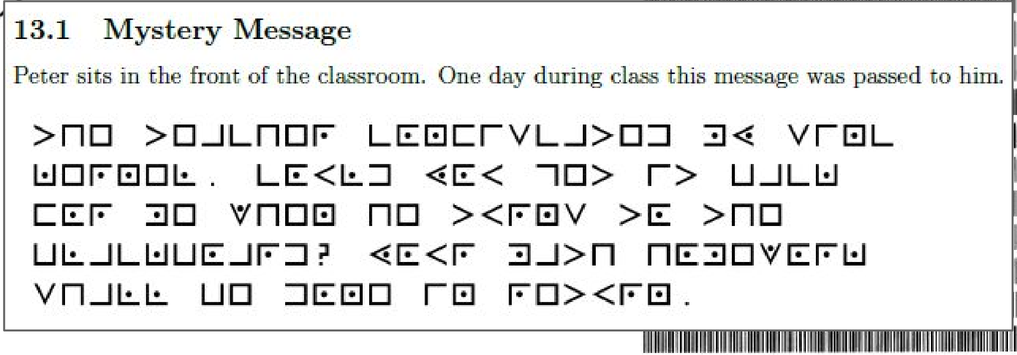
The point is, neighbors, that at the input time you cannot possibly know the context of the output. Your input sanitation scheme might work to protect your backend for now—and then a developer comes and adds an LDAP backend, and another comes and inserts data into a JavaScript literal in your web page template. Then another comes and adds an additional output encoding layer for your input—and what looked safe to you at the outset crumbles to dust.



Sermons



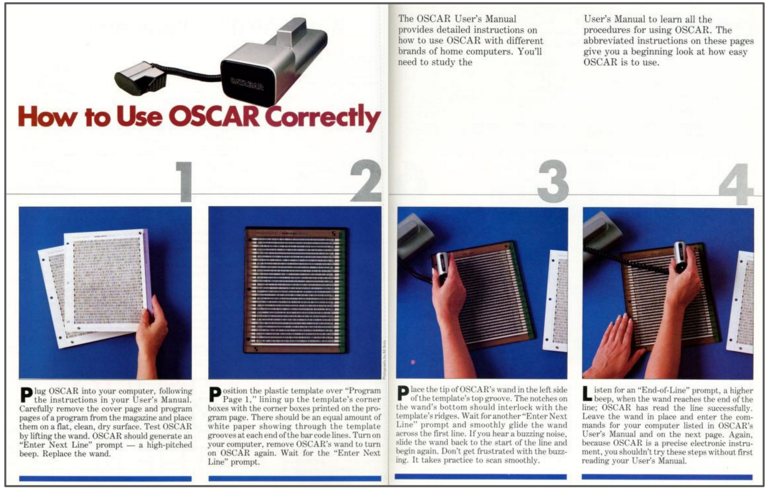




13.1 Mystery Message

Peter sits in the front of the classroom. One day during class this message was passed to him.

Puzzles



How to Use OSCAR Correctly

The OSCAR User's Manual provides detailed instructions on how to use OSCAR with different brands of home computers. You'll need to study the User's Manual to learn all the procedures for using OSCAR. The abbreviated instructions on these pages give you a beginning look at how easy OSCAR is to use.

1

Plug OSCAR into your computer, following the instructions in your User's Manual. Carefully remove the cover page and program pages of a program from the magazine and place them on a flat, clean, dry surface. Test OSCAR by lifting the wand. OSCAR should generate an "Enter Next Line" prompt — a high-pitched beep. Replace the wand.

2

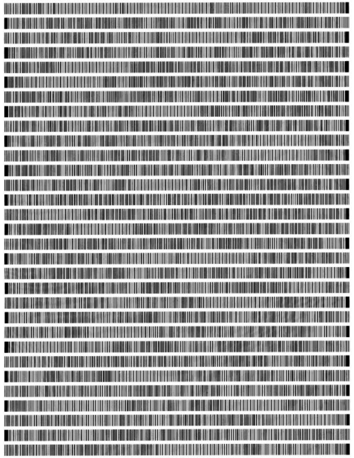
Position the plastic template over "Program Page 1," lining up the template's corner boxes with the corner boxes printed on the program page. There should be an equal amount of white paper showing through the template grooves at each end of the bar code lines. Turn on your computer, remove OSCAR's wand to turn on OSCAR again. Wait for the "Enter Next Line" prompt.

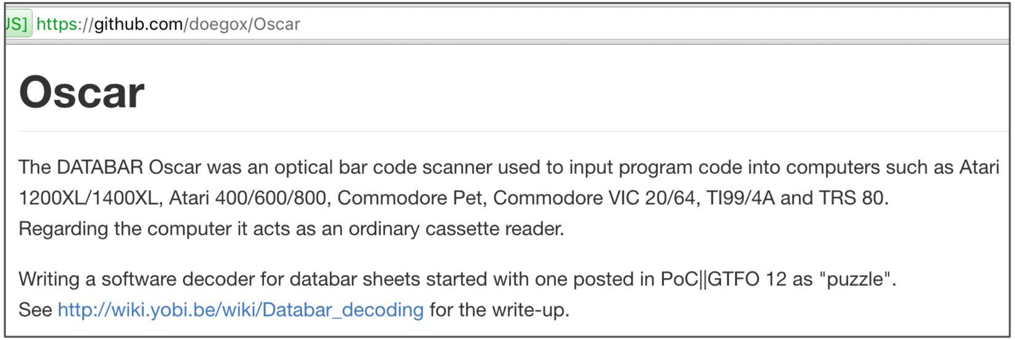
3

Place the tip of OSCAR's wand in the left side of the template's top groove. The notches on the wand's bottom should interlock with the template's ridges. Wait for another "Enter Next Line" prompt and smoothly glide the wand across the first line. If you hear a buzzing noise, slide the wand back to the start of the line and begin again. Don't get frustrated with the buzzing. It takes practice to scan smoothly.

4

Listen for an "End-of-Line" prompt, a higher beep, when the wand reaches the end of the line; OSCAR has read the line successfully. Leave the wand in place and enter the commands for your computer listed in OSCAR's User's Manual and on the next page. Again, because OSCAR is a precise electronic instrument, you shouldn't try these steps without first reading your User's Manual.



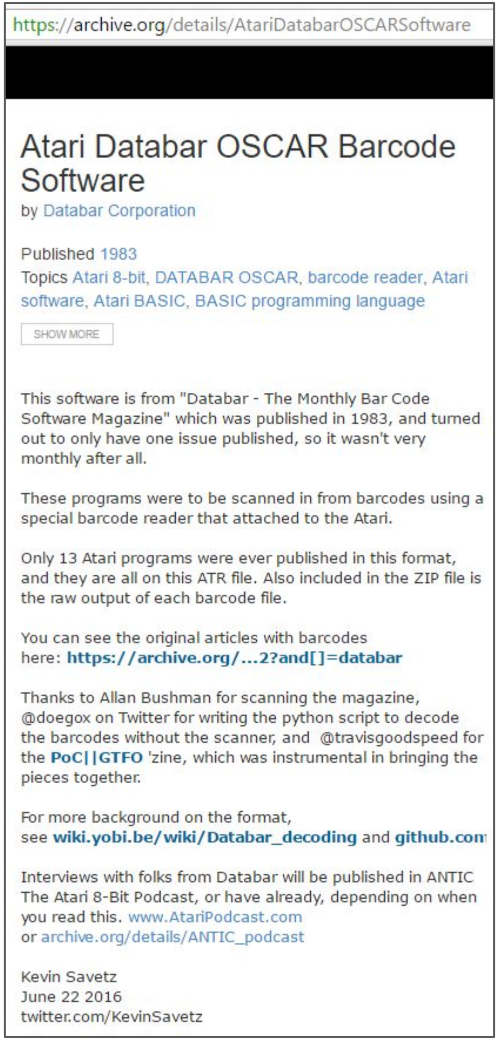


Oscar

The DATABAR Oscar was an optical bar code scanner used to input program code into computers such as Atari 1200XL/1400XL, Atari 400/600/800, Commodore Pet, Commodore VIC 20/64, TI99/4A and TRS 80. Regarding the computer it acts as an ordinary cassette reader.

Writing a software decoder for databar sheets started with one posted in PoC||GTFO 12 as "puzzle". See http://wiki.yobi.be/wiki/Databar_decoding for the write-up.

Challenge ⇒ solution ⇒ preservation
Puzzle ⇒ Github ⇒ Archive.org



Atari Databar OSCAR Barcode Software

by Databar Corporation

Published 1983
Topics Atari 8-bit, DATABAR OSCAR, barcode reader, Atari software, Atari BASIC, BASIC programming language

This software is from "Databar - The Monthly Bar Code Software Magazine" which was published in 1983, and turned out to only have one issue published, so it wasn't very monthly after all.

These programs were to be scanned in from barcodes using a special barcode reader that attached to the Atari.

Only 13 Atari programs were ever published in this format, and they are all on this ATR file. Also included in the ZIP file is the raw output of each barcode file.

You can see the original articles with barcodes here: **https://archive.org/...2?and[]=databar**

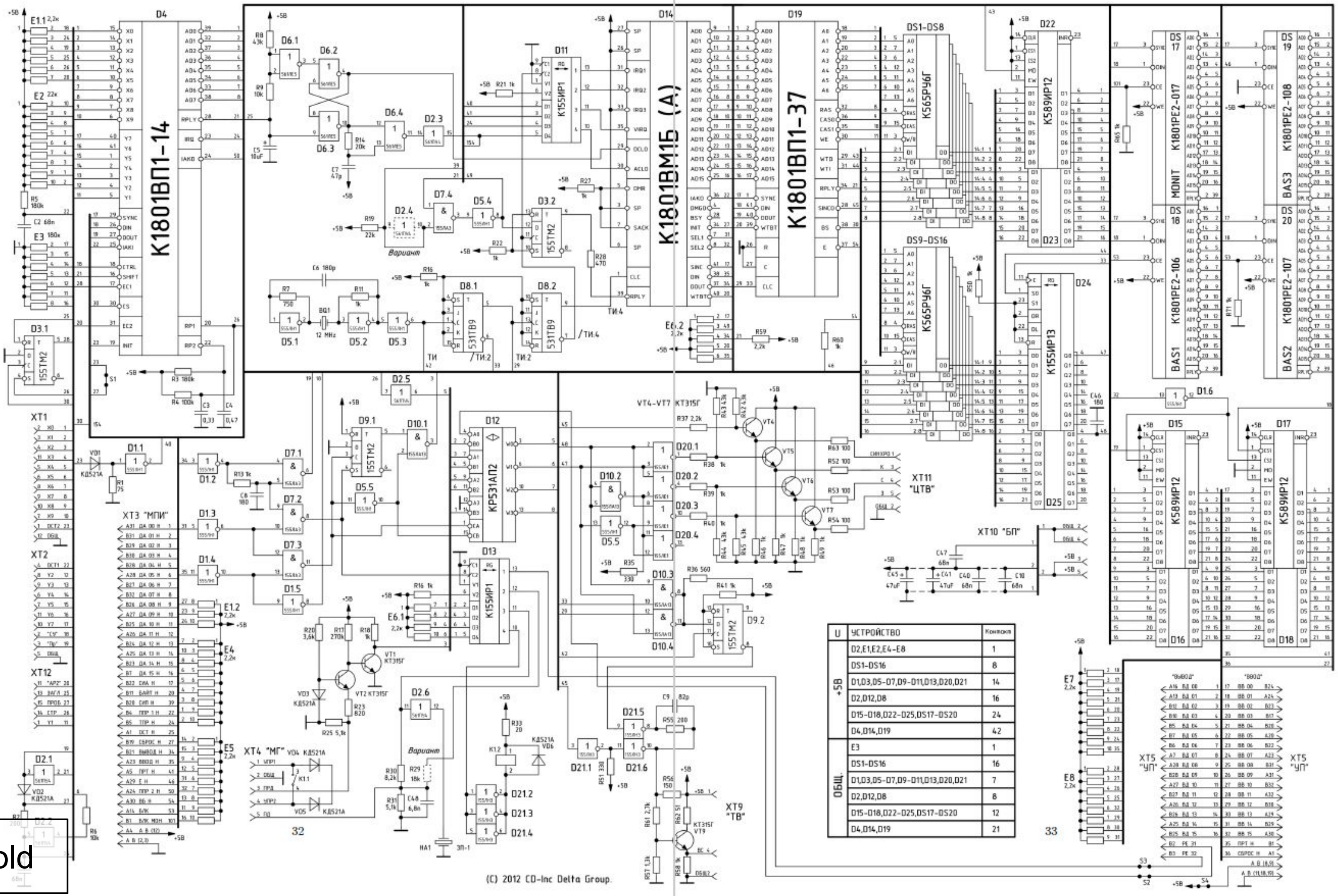
Thanks to Allan Bushman for scanning the magazine, @doegox on Twitter for writing the python script to decode the barcodes without the scanner, and @travisgoodspeed for the **PoC||GTFO** 'zine, which was instrumental in bringing the pieces together.

For more background on the format, see **wiki.yobi.be/wiki/Databar_decoding** and **github.com**

Interviews with folks from Databar will be published in ANTIC The Atari 8-Bit Podcast, or have already, depending on when you read this. www.AtariPodcast.com or archive.org/details/ANTIC_podcast

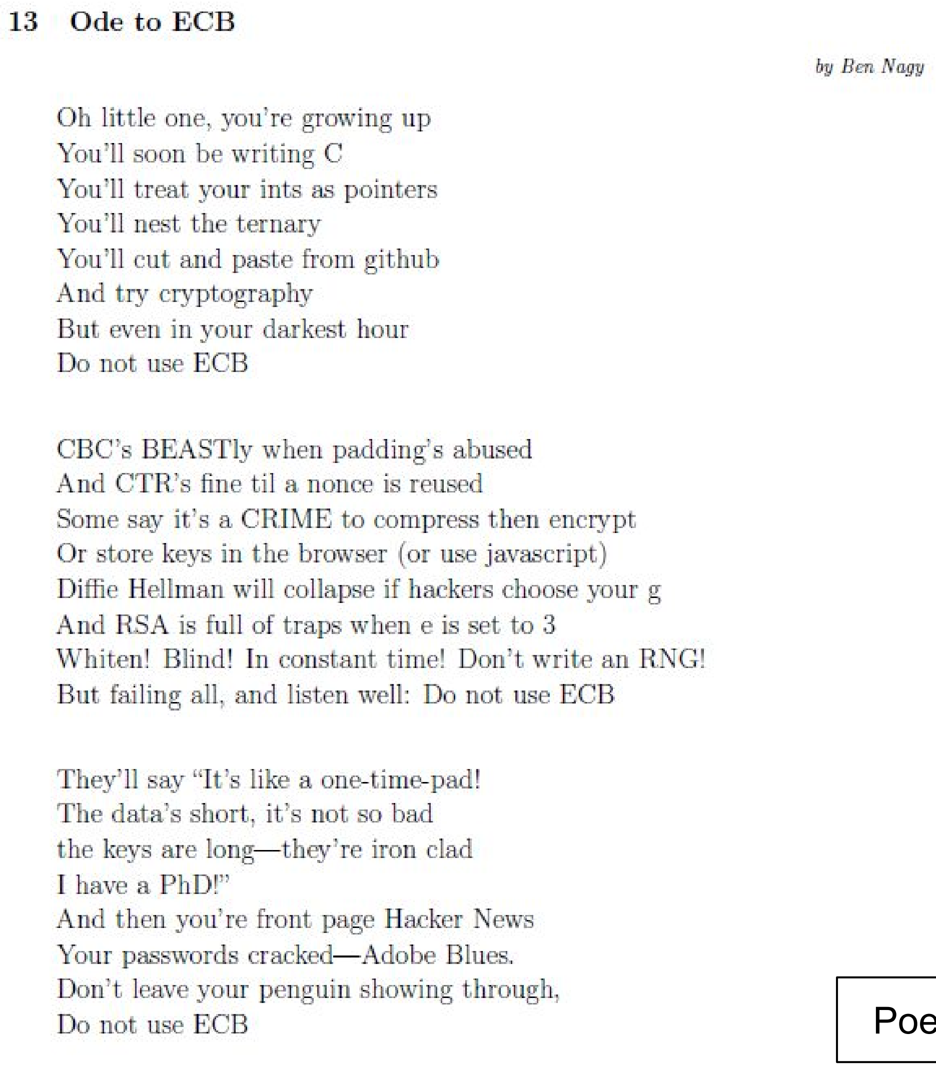
Kevin Savetz
June 22 2016
twitter.com/KevinSavetz

Схема принципиальная " Электроника БК 0010 - 01 " клавиатура нового образца



U	УСТРОЙСТВО	Контакт
+5В	D2,E1,E2,E4-E8	1
	DS1-DS16	8
	D1,D3,D5-D7,D9-D11,D13,D20,D21	14
	D2,D12,D8	16
	D15-D18,D22-D25,DS17-DS20	24
	D4,D14,D19	42
ОБЩ.	E3	1
	DS1-DS16	16
	D1,D3,D5-D7,D9-D11,D13,D20,D21	7
	D2,D12,D8	8
	D15-D18,D22-D25,DS17-DS20	12
	D4,D14,D19	21

Centerfold



13 Ode to ECB

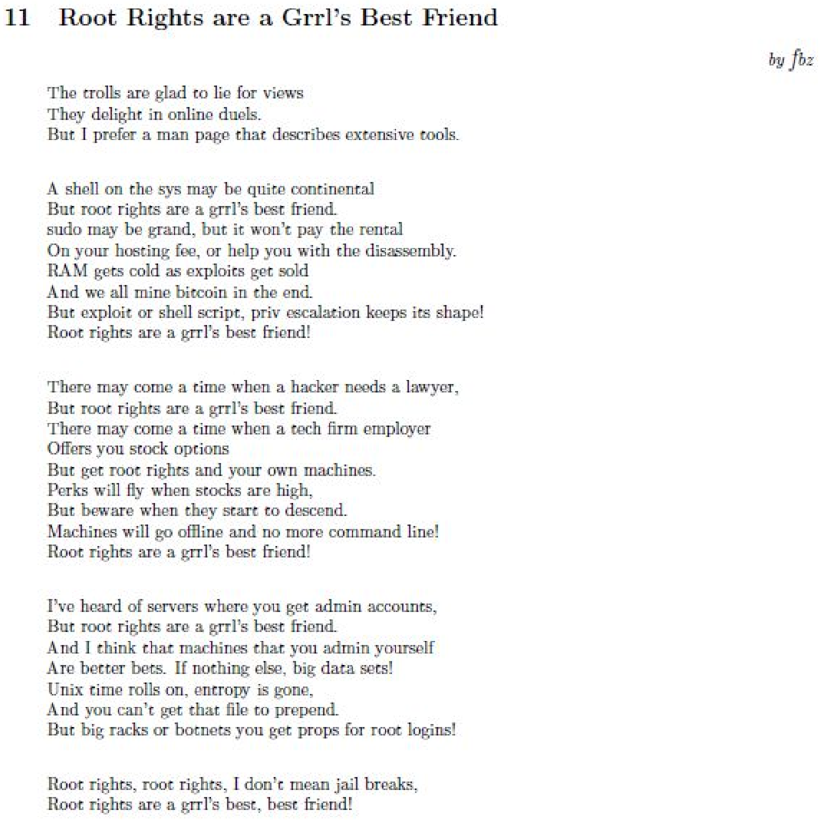
by Ben Nagy

Oh little one, you're growing up
You'll soon be writing C
You'll treat your ints as pointers
You'll nest the ternary
You'll cut and paste from github
And try cryptography
But even in your darkest hour
Do not use ECB

CBC's BEASTly when padding's abused
And CTR's fine til a nonce is reused
Some say it's a CRIME to compress then encrypt
Or store keys in the browser (or use javascript)
Diffie Hellman will collapse if hackers choose your g
And RSA is full of traps when e is set to 3
Whiten! Blind! In constant time! Don't write an RNG!
But failing all, and listen well: Do not use ECB

They'll say "It's like a one-time-pad!
The data's short, it's not so bad
the keys are long—they're iron clad
I have a PhD!"
And then you're front page Hacker News
Your passwords cracked—Adobe Blues.
Don't leave your penguin showing through,
Do not use ECB

Poetry



11 Root Rights are a Grrl's Best Friend

by fbz

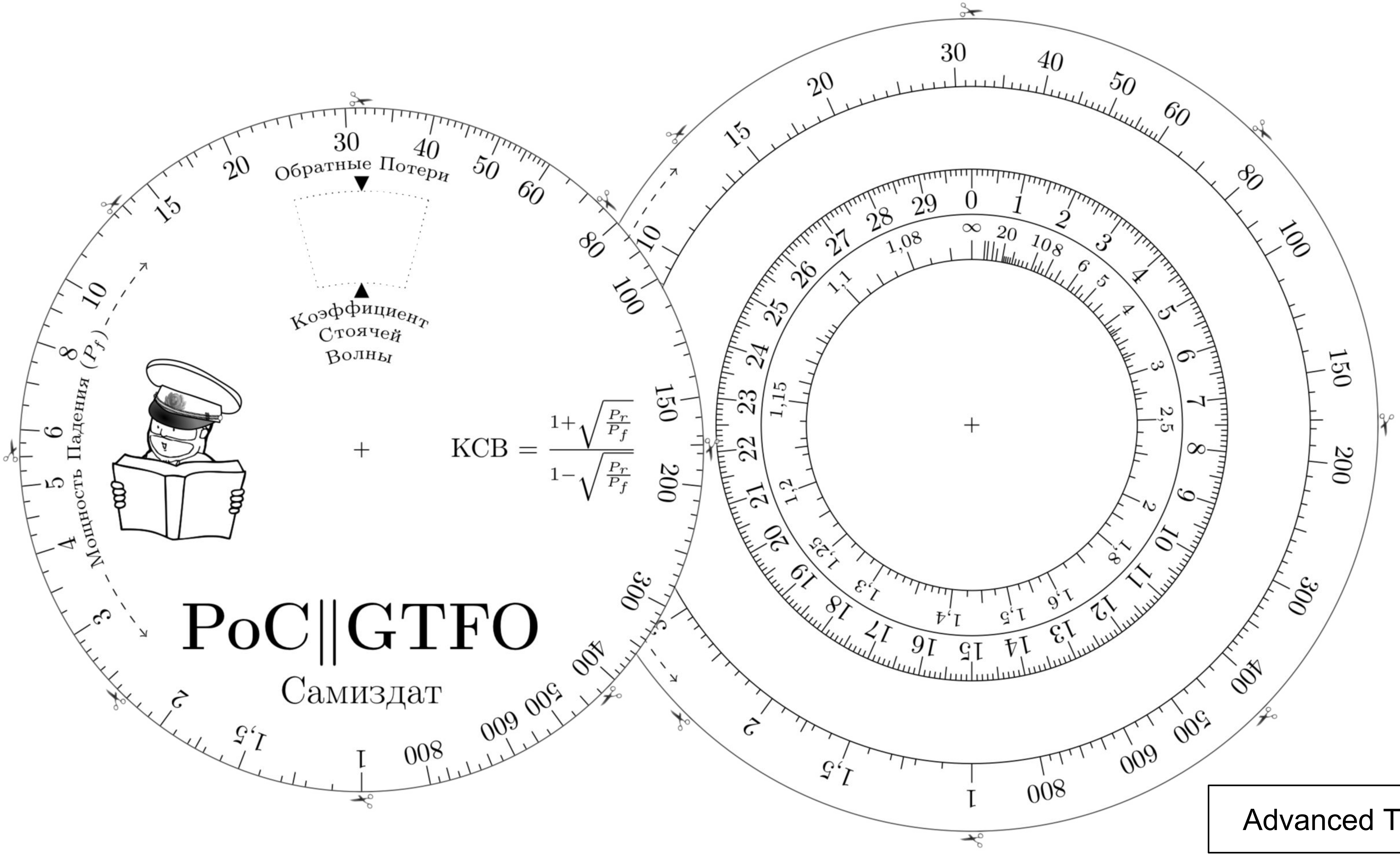
The trolls are glad to lie for views
They delight in online duels.
But I prefer a man page that describes extensive tools.

A shell on the sys may be quite continental
But root rights are a grrl's best friend.
sudo may be grand, but it won't pay the rental
On your hosting fee, or help you with the disassembly.
RAM gets cold as exploits get sold
And we all mine bitcoin in the end.
But exploit or shell script, priv escalation keeps its shape!
Root rights are a grrl's best friend!

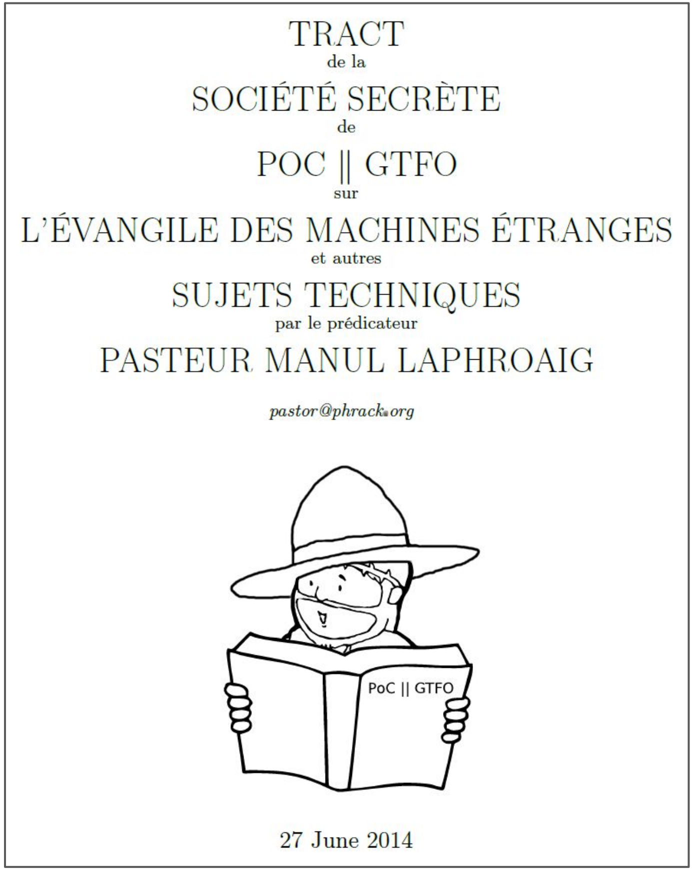
There may come a time when a hacker needs a lawyer,
But root rights are a grrl's best friend.
There may come a time when a tech firm employer
Offers you stock options
But get root rights and your own machines.
Perks will fly when stocks are high,
But beware when they start to descend.
Machines will go offline and no more command line!
Root rights are a grrl's best friend!

I've heard of servers where you get admin accounts,
But root rights are a grrl's best friend.
And I think that machines that you admin yourself
Are better bets. If nothing else, big data sets!
Unix time rolls on, entropy is gone,
And you can't get that file to prepend.
But big racks or botnets you get props for root logins!

Root rights, root rights, I don't mean jail breaks,
Root rights are a grrl's best, best friend!



$$\text{КСВ} = \frac{1+\sqrt{\frac{P_r}{P_f}}}{1-\sqrt{\frac{P_r}{P_f}}}$$

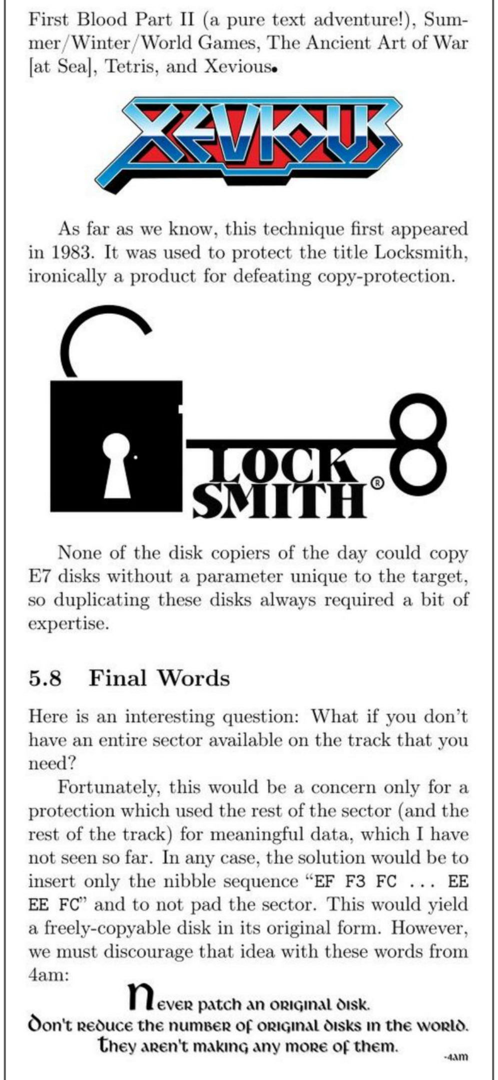


TRACT
de la
SOCIÉTÉ SECRÈTE
de
POC || GTFO
sur
L'ÉVANGILE DES MACHINES ÉTRANGES
et autres
SUJETS TECHNIQUES
par le prédicateur
PASTEUR MANUL LAPHROAIG

pastor@phrack.org

27 June 2014

Notice anything?



First Blood Part II (a pure text adventure!), Summer/Winter/World Games, The Ancient Art of War [at Sea], Tetris, and Xevious•

XEVIOUS

As far as we know, this technique first appeared in 1983. It was used to protect the title Locksmith, ironically a product for defeating copy-protection.

LOCK SMITH®

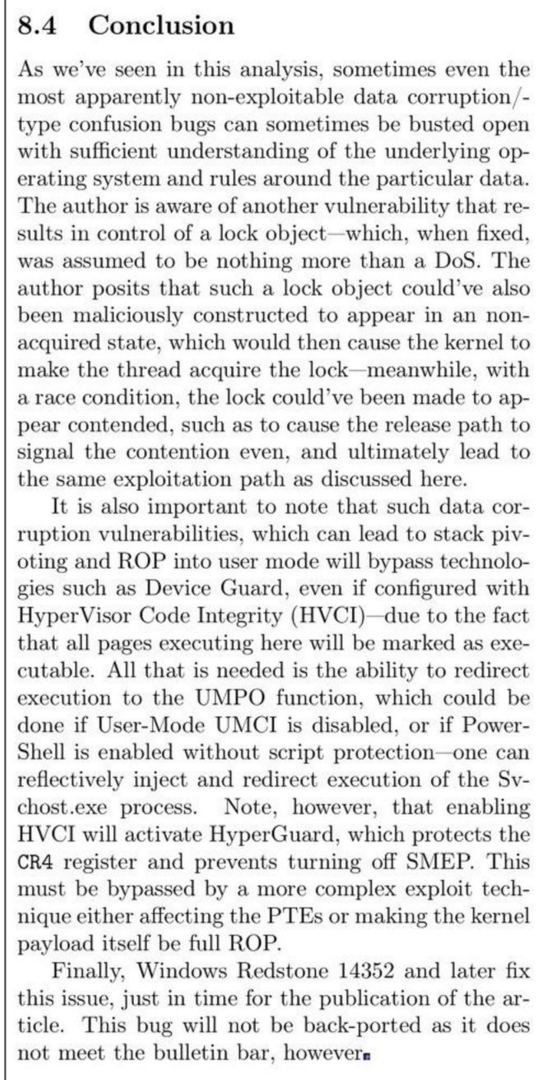
None of the disk copiers of the day could copy E7 disks without a parameter unique to the target, so duplicating these disks always required a bit of expertise.

5.8 Final Words

Here is an interesting question: What if you don't have an entire sector available on the track that you need?

Fortunately, this would be a concern only for a protection which used the rest of the sector (and the rest of the track) for meaningful data, which I have not seen so far. In any case, the solution would be to insert only the nibble sequence "`EF F3 FC ... EE EE FC`" and to not pad the sector. This would yield a freely-copyable disk in its original form. However, we must discourage that idea with these words from 4am:

> Never patch an original disk.
> Don't reduce the number of original disks in the world.
> They aren't making any more of them.
>
> -4am

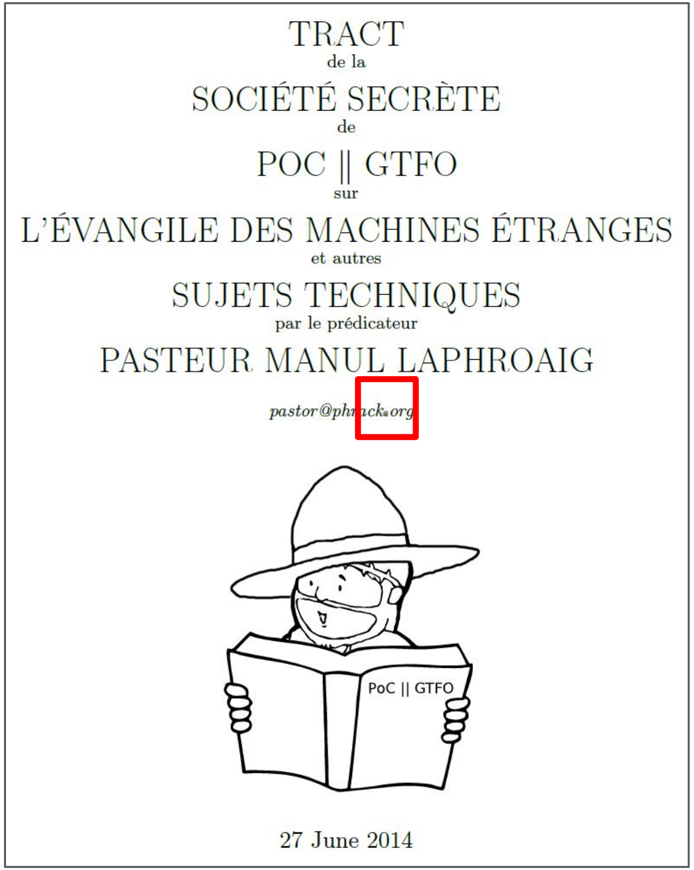


8.4 Conclusion

As we've seen in this analysis, sometimes even the most apparently non-exploitable data corruption/-type confusion bugs can sometimes be busted open with sufficient understanding of the underlying operating system and rules around the particular data. The author is aware of another vulnerability that results in control of a lock object—which, when fixed, was assumed to be nothing more than a DoS. The author posits that such a lock object could've also been maliciously constructed to appear in an non-acquired state, which would then cause the kernel to make the thread acquire the lock—meanwhile, with a race condition, the lock could've been made to appear contended, such as to cause the release path to signal the contention even, and ultimately lead to the same exploitation path as discussed here.

It is also important to note that such data corruption vulnerabilities, which can lead to stack pivoting and ROP into user mode will bypass technologies such as Device Guard, even if configured with HyperVisor Code Integrity (HVCI)—due to the fact that all pages executing here will be marked as executable. All that is needed is the ability to redirect execution to the UMPO function, which could be done if User-Mode UMCI is disabled, or if PowerShell is enabled without script protection—one can reflectively inject and redirect execution of the Svchost.exe process. Note, however, that enabling HVCI will activate HyperGuard, which protects the `CR4` register and prevents turning off SMEP. This must be bypassed by a more complex exploit technique either affecting the PTEs or making the kernel payload itself be full ROP.

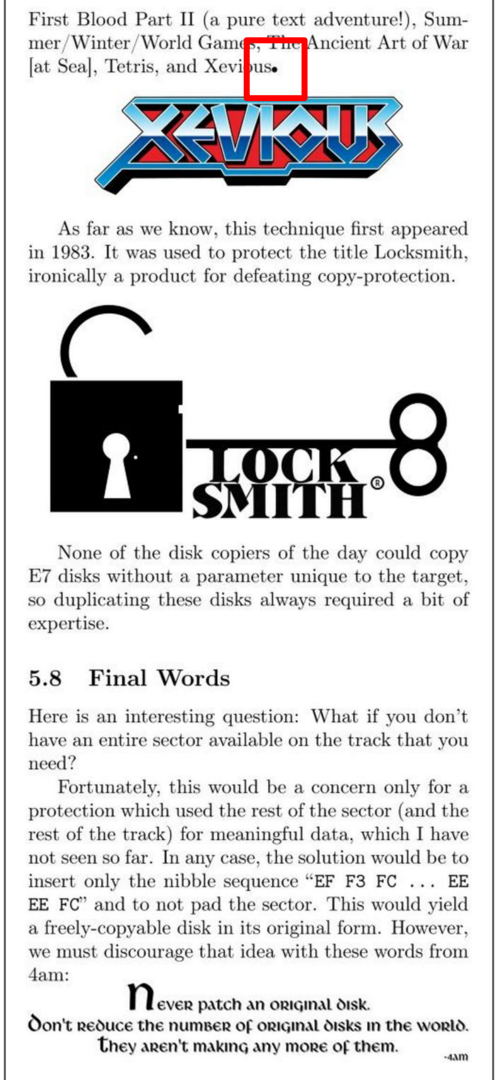
Finally, Windows Redstone 14352 and later fix this issue, just in time for the publication of the article. This bug will not be back-ported as it does not meet the bulletin bar, however■



TRACT
de la
SOCIÉTÉ SECRÈTE
de
POC || GTFO
sur
L'ÉVANGILE DES MACHINES ÉTRANGES
et autres
SUJETS TECHNIQUES
par le prédicateur
PASTEUR MANUL LAPHROAIG

pastor@phrack.org

27 June 2014



First Blood Part II (a pure text adventure!), Summer/Winter/World Games, The Ancient Art of War [at Sea], Tetris, and Xevious.

As far as we know, this technique first appeared in 1983. It was used to protect the title Locksmith, ironically a product for defeating copy-protection.

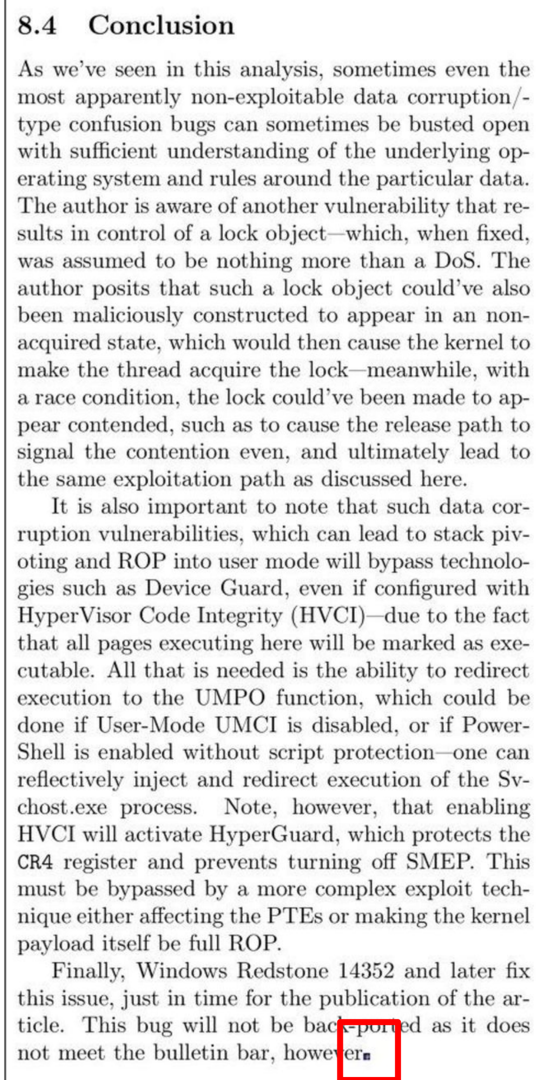
None of the disk copiers of the day could copy E7 disks without a parameter unique to the target, so duplicating these disks always required a bit of expertise.

5.8 Final Words

Here is an interesting question: What if you don't have an entire sector available on the track that you need?

Fortunately, this would be a concern only for a protection which used the rest of the sector (and the rest of the track) for meaningful data, which I have not seen so far. In any case, the solution would be to insert only the nibble sequence "`EF F3 FC ... EE EE FC`" and to not pad the sector. This would yield a freely-copyable disk in its original form. However, we must discourage that idea with these words from 4am:

> Never patch an original disk.
> Don't reduce the number of original disks in the world.
> They aren't making any more of them.
> -4am



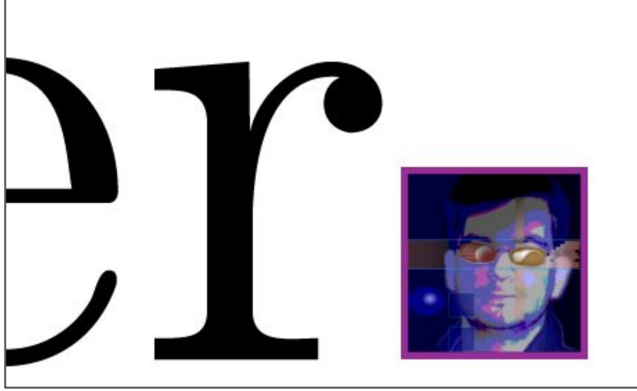
8.4 Conclusion

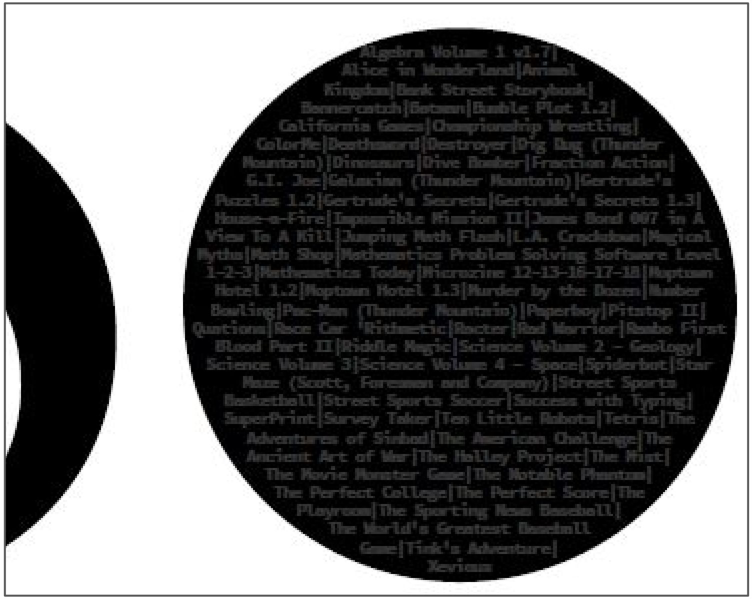
As we've seen in this analysis, sometimes even the most apparently non-exploitable data corruption/-type confusion bugs can sometimes be busted open with sufficient understanding of the underlying operating system and rules around the particular data. The author is aware of another vulnerability that results in control of a lock object—which, when fixed, was assumed to be nothing more than a DoS. The author posits that such a lock object could've also been maliciously constructed to appear in an non-acquired state, which would then cause the kernel to make the thread acquire the lock—meanwhile, with a race condition, the lock could've been made to appear contended, such as to cause the release path to signal the contention even, and ultimately lead to the same exploitation path as discussed here.

It is also important to note that such data corruption vulnerabilities, which can lead to stack pivoting and ROP into user mode will bypass technologies such as Device Guard, even if configured with HyperVisor Code Integrity (HVCI)—due to the fact that all pages executing here will be marked as executable. All that is needed is the ability to redirect execution to the UMPO function, which could be done if User-Mode UMCI is disabled, or if PowerShell is enabled without script protection—one can reflectively inject and redirect execution of the Svchost.exe process. Note, however, that enabling HVCI will activate HyperGuard, which protects the `CR4` register and prevents turning off SMEP. This must be bypassed by a more complex exploit technique either affecting the PTEs or making the kernel payload itself be full ROP.

Finally, Windows Redstone 14352 and later fix this issue, just in time for the publication of the article. This bug will not be back-ported as it does not meet the bulletin bar, however.

Let me help you...



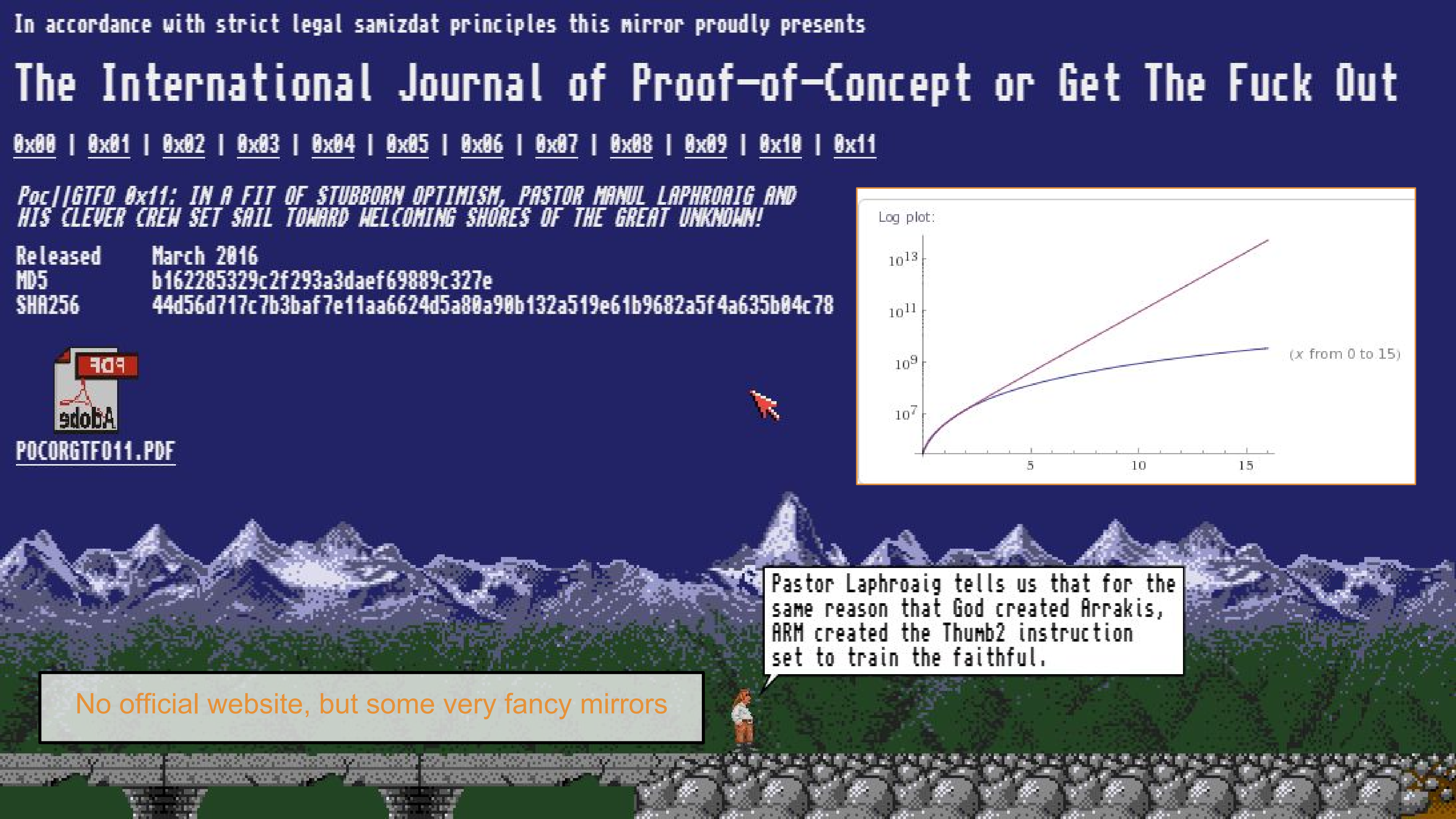


Algebra Volume 1 v1.7|
Alice in Wonderland|Animal
Kingdom|Bank Street Storybook|
Bannercatch|Batman|Bumble Plot 1.2|
California Games|Championship Wrestling|
ColorMe|Deathsword|Destroyer|Dig Dug (Thunder
Mountain)|Dinosaurs|Dive Bomber|Fraction Action|
G.I. Joe|Galaxian (Thunder Mountain)|Gertrude's
Puzzles 1.2|Gertrude's Secrets|Gertrude's Secrets 1.3|
House-a-Fire|Impossible Mission II|James Bond 007 in A
View To A Kill|Jumping Math Flash|L.A. Crackdown|Magical
Myths|Math Shop|Mathematics Problem Solving Software Level
1-2-3|Mathematics Today|Microzine 12-13-16-17-18|Moptown
Hotel 1.2|Moptown Hotel 1.3|Murder by the Dozen|Number
Bowling|Pac-Man (Thunder Mountain)|Paperboy|Pitstop II|
Questions|Race Car 'Rithmetic|Racter|Road Warrior|Rambo First
Blood Part II|Riddle Magic|Science Volume 2 - Geology|
Science Volume 3|Science Volume 4 - Space|Spiderbot|Star
Maze (Scott, Foresman and Company)|Street Sports
Basketball|Street Sports Soccer|Success with Typing|
SuperPrint|Survey Taker|Ten Little Robots|Tetris|The
Adventures of Sinbad|The American Challenge|The
Ancient Art of War|The Halley Project|The Mist|
The Movie Monster Game|The Notable Phantom|
The Perfect College|The Perfect Score|The
Playroom|The Sporting News Baseball|
The World's Greatest Baseball
Game|Tink's Adventure|
Xevious

Space saving, the
PoC||GTFO way :)

Of course, it's not just a fancy document :)

The electronic release comes a few days ***after*** the print.



In accordance with strict legal samizdat principles this mirror proudly presents

The International Journal of Proof-of-Concept or Get The Fuck Out

0x00 | 0x01 | 0x02 | 0x03 | 0x04 | 0x05 | 0x06 | 0x07 | 0x08 | 0x09 | 0x10 | 0x11

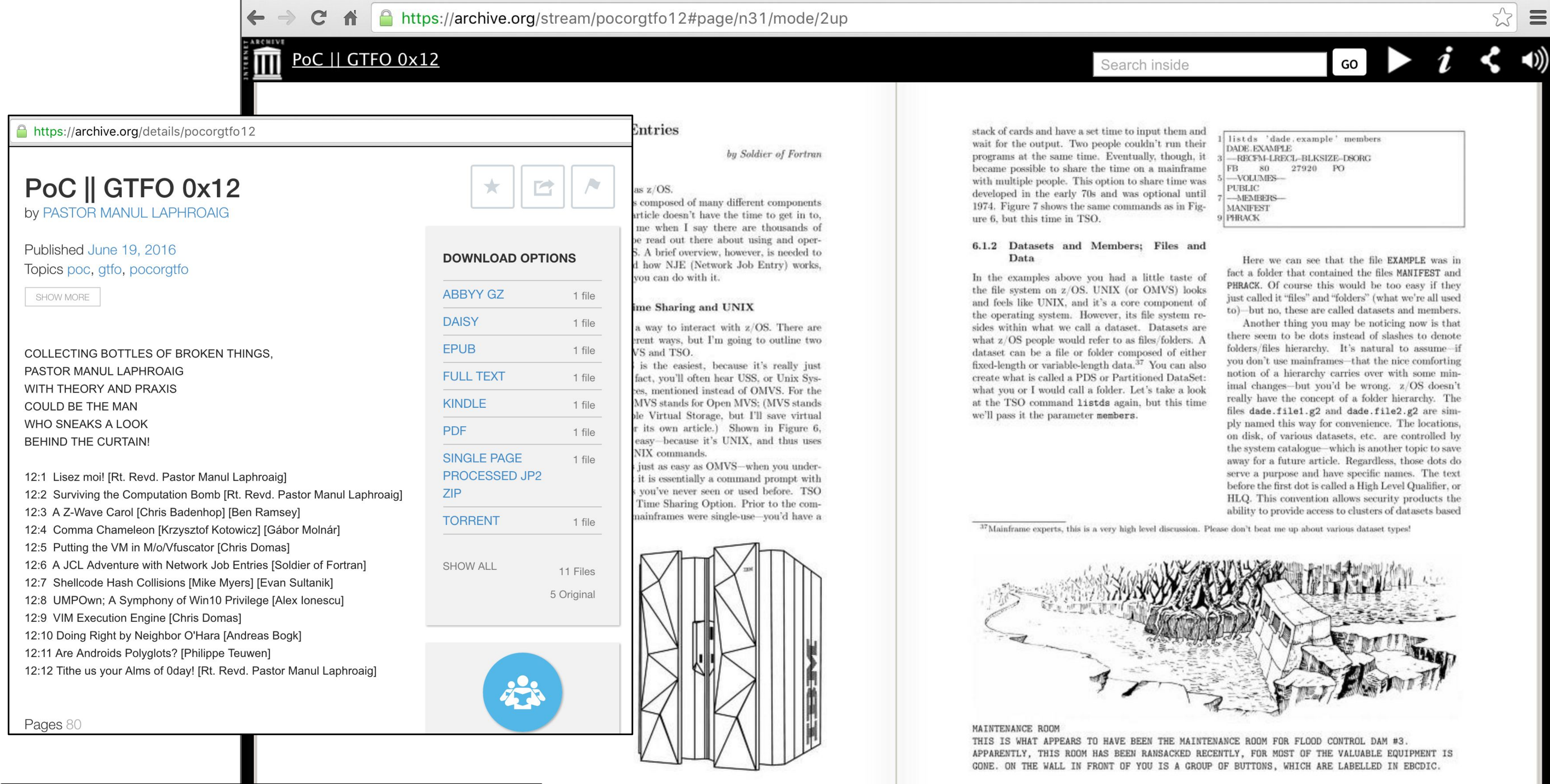
POC||GTFO 0x11: IN A FIT OF STUBBORN OPTIMISM, PASTOR MANUL LAPHROAIG AND HIS CLEVER CREW SET SAIL TOWARD WELCOMING SHORES OF THE GREAT UNKNOWN!

Released	March 2016
MD5	b162285329c2f293a3daef69889c327e
SHA256	44d56d717c7b3baf7e11aa6624d5a80a90b132a519e61b9682a5f4a635b04c78

POCORGTFO11.PDF

PDF
Adobe
Log plot:
10^{13}
10^{11}
10^{9}
10^{7}
5
10
15
(x from 0 to 15)
Pastor Laphroaig tells us that for the same reason that God created Arrakis, ARM created the Thumb2 instruction set to train the faithful.

No official website, but some very fancy mirrors



https://archive.org/details/pocorgtfo12

PoC || GTFO 0x12

by PASTOR MANUL LAPHROAIG

Published June 19, 2016
Topics poc, gtfo, pocorgtfo

COLLECTING BOTTLES OF BROKEN THINGS,
PASTOR MANUL LAPHROAIG
WITH THEORY AND PRAXIS
COULD BE THE MAN
WHO SNEAKS A LOOK
BEHIND THE CURTAIN!

Pages 80

DOWNLOAD OPTIONS

ABBYY GZ	1 file
DAISY	1 file
EPUB	1 file
FULL TEXT	1 file
KINDLE	1 file
PDF	1 file
SINGLE PAGE PROCESSED JP2 ZIP	1 file
TORRENT	1 file
SHOW ALL	11 Files 5 Original

Entries

by Soldier of Fortran

as z/OS.
s composed of many different components
rticle doesn't have the time to get in to,
me when I say there are thousands of
e read out there about using and oper-
S. A brief overview, however, is needed to
d how NJE (Network Job Entry) works,
you can do with it.

ime Sharing and UNIX

a way to interact with z/OS. There are
rent ways, but I'm going to outline two
VS and TSO.
is the easiest, because it's really just
fact, you'll often hear USS, or Unix Sys-
es, mentioned instead of OMVS. For the
MVS stands for Open MVS; (MVS stands
le Virtual Storage, but I'll save virtual
r its own article.) Shown in Figure 6,
easy—because it's UNIX, and thus uses
NIX commands.
just as easy as OMVS—when you under-
it is essentially a command prompt with
you've never seen or used before. TSO
Time Sharing Option. Prior to the com-
ainframes were single-use—you'd have a

32

stack of cards and have a set time to input them and wait for the output. Two people couldn't run their programs at the same time. Eventually, though, it became possible to share the time on a mainframe with multiple people. This option to share time was developed in the early 70s and was optional until 1974. Figure 7 shows the same commands as in Figure 6, but this time in TSO.

6.1.2 Datasets and Members; Files and Data

In the examples above you had a little taste of the file system on z/OS. UNIX (or OMVS) looks and feels like UNIX, and it's a core component of the operating system. However, its file system resides within what we call a dataset. Datasets are what z/OS people would refer to as files/folders. A dataset can be a file or folder composed of either fixed-length or variable-length data.[37] You can also create what is called a PDS or Partitioned DataSet: what you or I would call a folder. Let's take a look at the TSO command `listds` again, but this time we'll pass it the parameter `members`.

```
listds 'dade.example' members
DADE.EXAMPLE
—RECFM-LRECL-BLKSIZE-DSORG
FB     80     27920     PO
—VOLUMES—
PUBLIC
—MEMBERS—
MANIFEST
PHRACK
```

Here we can see that the file `EXAMPLE` was in fact a folder that contained the files `MANIFEST` and `PHRACK`. Of course this would be too easy if they just called it "files" and "folders" (what we're all used to)—but no, these are called datasets and members.

Another thing you may be noticing now is that there seem to be dots instead of slashes to denote folders/files hierarchy. It's natural to assume—if you don't use mainframes—that the nice comforting notion of a hierarchy carries over with some minimal changes—but you'd be wrong. z/OS doesn't really have the concept of a folder hierarchy. The files `dade.file1.g2` and `dade.file2.g2` are simply named this way for convenience. The locations, on disk, of various datasets, etc. are controlled by the system catalogue—which is another topic to save away for a future article. Regardless, those dots do serve a purpose and have specific names. The text before the first dot is called a High Level Qualifier, or HLQ. This convention allows security products the ability to provide access to clusters of datasets based

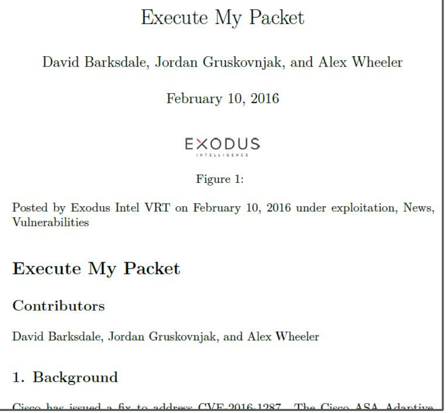
[37] Mainframe experts, this is a very high level discussion. Please don't beat me up about various dataset types!

```
MAINTENANCE ROOM
THIS IS WHAT APPEARS TO HAVE BEEN THE MAINTENANCE ROOM FOR FLOOD CONTROL DAM #3.
APPARENTLY, THIS ROOM HAS BEEN RANSACKED RECENTLY, FOR MOST OF THE VALUABLE EQUIPMENT IS
GONE. ON THE WALL IN FRONT OF YOU IS A GROUP OF BUTTONS, WHICH ARE LABELLED IN EBCDIC.
```

33

Archive.org, awesome as usual.

Each issue
has attached
feelies (PDF/ZIP)



Execute My Packet

David Barksdale, Jordan Gruskovnjak, and Alex Wheeler

February 10, 2016

EXODUS

Figure 1:

Posted by Exodus Intel VRT on February 10, 2016 under exploitation, News, Vulnerabilities

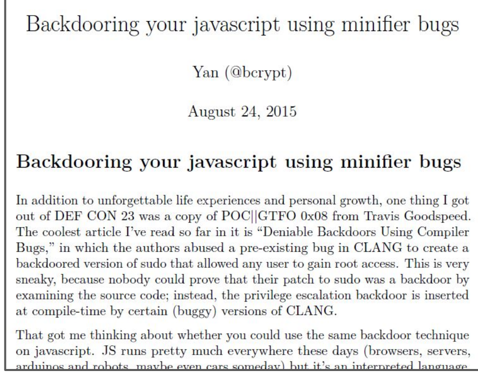
Execute My Packet

Contributors

David Barksdale, Jordan Gruskovnjak, and Alex Wheeler

1. Background

Cisco has issued a fix to address CVE-2016-1287. The Cisco ASA Adaptive



Backdooring your javascript using minifier bugs

Yan (@bcrypt)

August 24, 2015

Backdooring your javascript using minifier bugs

In addition to unforgettable life experiences and personal growth, one thing I got out of DEF CON 23 was a copy of POC||GTFO 0x08 from Travis Goodspeed. The coolest article I've read so far in it is "Deniable Backdoors Using Compiler Bugs," in which the authors abused a pre-existing bug in CLANG to create a backdoored version of sudo that allowed any user to gain root access. This is very sneaky, because nobody could prove that their patch to sudo was a backdoor by examining the source code; instead, the privilege escalation backdoor is inserted at compile-time by certain (buggy) versions of CLANG.

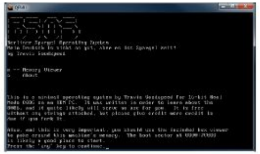
That got me thinking about whether you could use the same backdoor technique on javascript. JS runs pretty much everywhere these days (browsers, servers, arduinos and robots, maybe even cars someday) but it's an interpreted language

Preserved external research.

(blog ⇒ PDF)

Each issue is a PoC itself

MBR



```
Berliner Spargel Operating System
Mein Deutsch is nicht so gut, aber es ist Spargel zeit!
by Travis Goodspeed

m -- Memory Viewer
a    About

This is a minimal operating system by Travis Goodspeed for 16-bit Real
Mode 8086 on an IBM PC.  It was written in order to learn about the
8086, and it quite likely will serve as such for you.  It is free
without any strings attached, but please give credit where credit is
due if you fork it.

Also, and this is very important, you should use the included hex viewer
to poke around this machine's memory.  The boot sector at 0000:7C00
is likely a good place to start.
Press the 'any' key to continue._
```

JPG

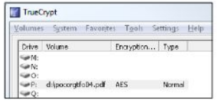
AFSK

PNG

AFTER ENCRYPTION

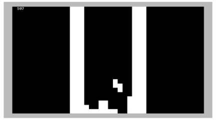
TRUE CRYPT

PASSWORD = 123456

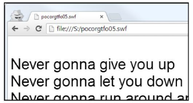


Drive	Volume	Encryption...	Type
M:			
N:			
O:			
P:	d:\pocorgtfo04.pdf	AES	Normal
Q:			

ISO

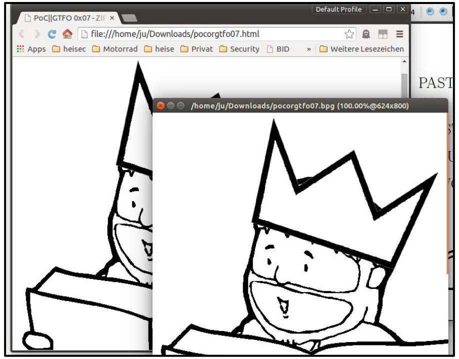


FLASH

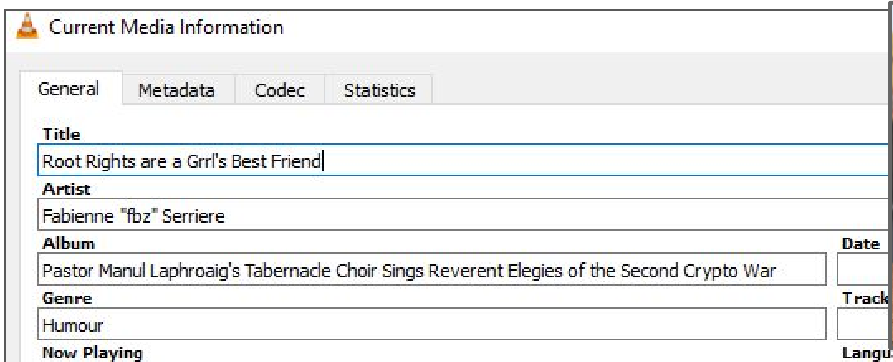


Never gonna give you up
Never gonna let you down
Never gonna run around ar

```
$ tar -tvf pocorgtfo06.pdf
-rw-r--r-- Manul/Laphroaig   0 2014-10-06 21:33 %PDF-1.5
-rw-r--r-- Manul/Laphroaig 525849 2014-10-06 21:33 1.png
-rw-r--r-- Manul/Laphroaig 273658 2014-10-06 21:33 2.bmp
```



```
$ echo "terrible raccoons achieve their escapades" | ./pocorgtfo08.pdf -d 4321
good neighbors secure their communications
```



Title: Root Rights are a Grrl's Best Friend

Artist: Fabienne "fbz" Serriere

Album: Pastor Manul Laphroaig's Tabernacle Choir Sings Reverent Elegies of the Second Crypto War

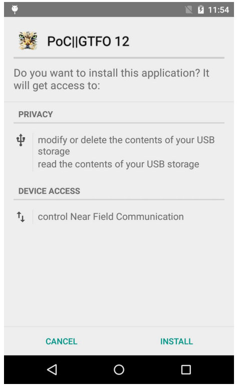
Date:

Genre: Humour

Track

Now Playing

Language



PoC||GTFO 12

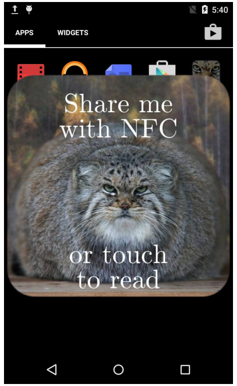
Do you want to install this application? It will get access to:

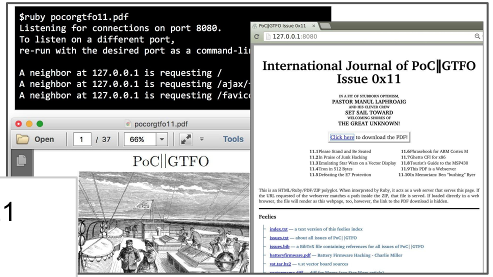
PRIVACY

modify or delete the contents of your USB storage
read the contents of your USB storage

DEVICE ACCESS

control Near Field Communication





```
$ruby pocorgtfo11.pdf
Listening for connections on port 8080.
To listen on a different port,
re-run with the desired port as a command-li

A neighbor at 127.0.0.1 is requesting /
A neighbor at 127.0.0.1 is requesting /ajax/
A neighbor at 127.0.0.1 is requesting /favic
```

International Journal of PoC‖GTFO
Issue 0x11

IN A FIT OF STUBBORN OPTIMISM,
PASTOR MANUL LAPHROAIG
AND HIS CLEVER CREW
SET SAIL TOWARD
WELCOMING SHORES OF
THE GREAT UNKNOWN!

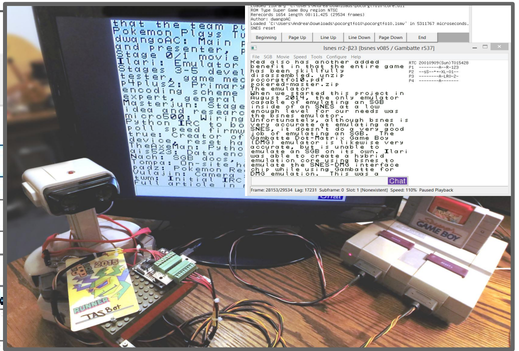
Click here to download the PDF!

11.1 Please Stand and Be Seated
11.2 In Praise of Junk Hacking
11.3 Emulating Star Wars on a Vector Display
11.4 Tron in 512 Bytes
11.5 Defeating the E7 Protection
11.6 Phrasebook for ARM Cortex M
11.7 Ghetto CFI for x86
11.8 Tourist's Guide to the MSP430
11.9 This PDF is a Webserver
11.10 In Memoriam: Ben "bushing" Byer

This is an HTML/Ruby/PDF/ZIP polyglot. When interpreted by Ruby, it acts as a web server that serves this page. If the URL requested of the webserver matches a path inside the ZIP, that file is served. If loaded directly in a web browser, the file will render as this webpage, too, however, the link to the PDF download is hidden.

Feelies

- index.txt — a text version of this feelies index
- issues.txt — about all issues of PoC||GTFO
- issues.bib — a BibTeX file containing references for all issues of PoC||GTFO
- batteryfirmware.pdf — Battery Firmware Hacking - Charlie Miller
- vst.tar.bz2 — v.st vector board sources



```
ROM Type Super Game Boy region NTSC
Rerecords 1654 length 08:11.425 (29534 frames)
Author: dwangoAC
Loaded 'C:\Users\Andrea\Downloads\pocorgtfo10\pocorgtfo10.lsmv' in 5311767 microseconds.
SNES reset
```

```
Red also has another added
benefit in that the entire game
has been skillfully
disassembled. unzip
pocorgtfo10.pdf
pokered-master.zip
The emulator
When we started this project in
August 2014, the only emulator
capable of emulating an SGB
inside of an SNES at a low
enough level for our needs was
the bsnes emulator.
Unfortunately, although bsnes is
very accurate at emulating an
SNES, it doesn't do a very good
job of emulating an SGB.  The
Gambatte Dot-Matrix Game Boy
(DMG) emulator is likewise very
accurate, but is unable to
emulate an SGB on its own. Ilari
was able to create a hybrid
emulation core using bsnes to
emulate the SNES-DMG interface
chip while using Gambatte for
DMG emulation.  This was a
```

```
RTC 20010909(Sun)T015428
P1  --------A--R-123
P2  --sS--++-XL-01--
P3  --------A-LR0-2-
P4  --------A-------
```

Frame: 28153/29534 Lag: 17231 Subframe: 0 Slot: 1 [Nonexistent] Speed: 110% Paused Playback

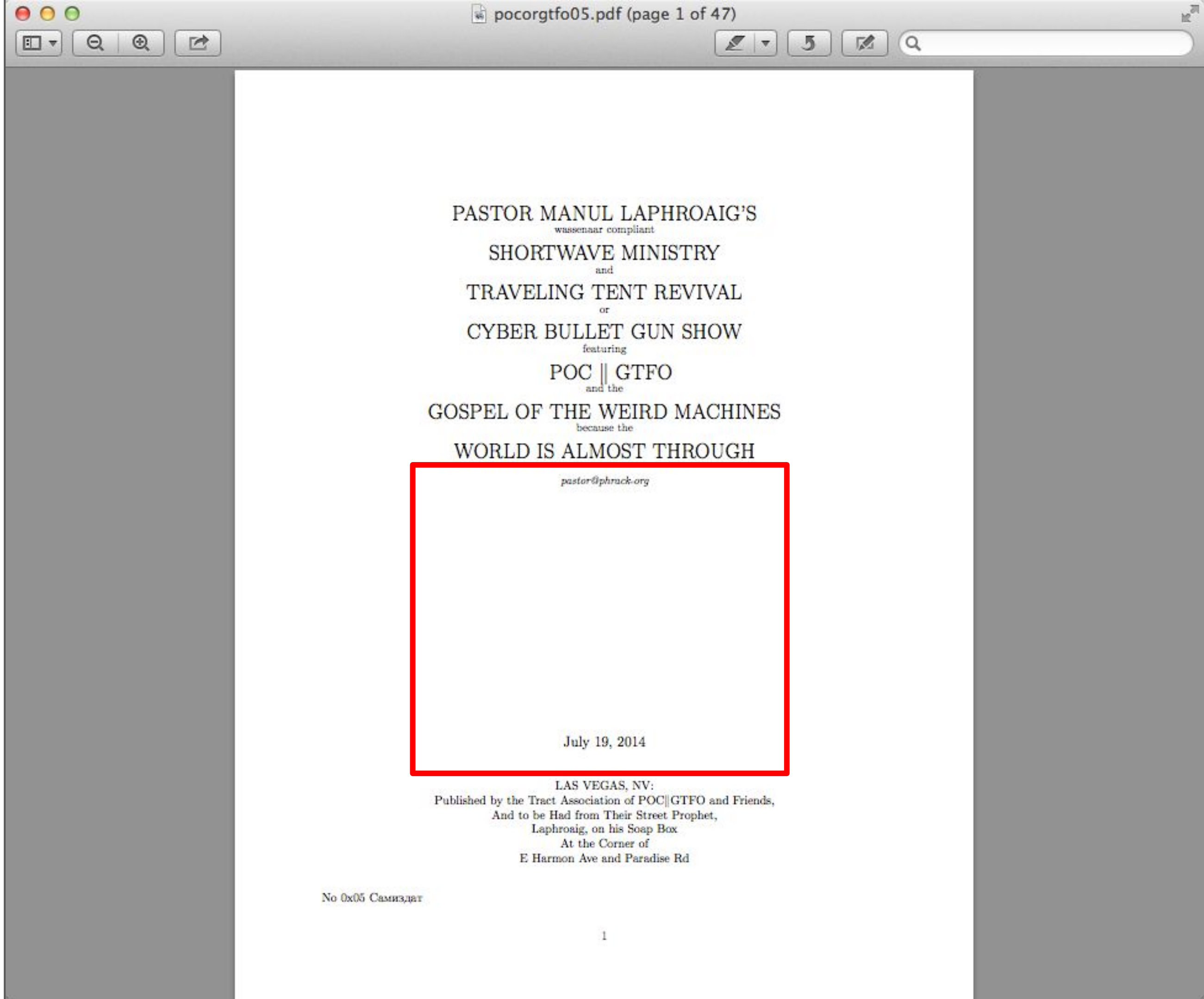
Compatibility is critical:
our QA is extensive.

Adobe Reader blacklists many formats.

Regarding compatibility: weird files structures triggers weird bugs!

The first picture is missing for no good reason?

Insert a 1x1 picture first!



pocorgtfo05.pdf (page 1 of 47)

PASTOR MANUL LAPHROAIG'S
wassenaar compliant
SHORTWAVE MINISTRY
and
TRAVELING TENT REVIVAL
or
CYBER BULLET GUN SHOW
featuring
POC || GTFO
and the
GOSPEL OF THE WEIRD MACHINES
because the
WORLD IS ALMOST THROUGH

pastor@phrack.org

July 19, 2014

LAS VEGAS, NV:
Published by the Tract Association of POC||GTFO and Friends,
And to be Had from Their Street Prophet,
Laphroaig, on his Soap Box
At the Corner of
E Harmon Ave and Paradise Rd

No 0x05 Самиздат

1

If you archive a PDF
inside the attached ZIP:
it might encode PDF keywords
and break the outer PDF!

BTW:

Not all secrets have been found.

Any weird pattern is purely coincidental ;)

Conclusion

PoC||GTFO helped to share research in a better way.

None of this

Is required*.

But…

*for a hacker publication.

Keep trying

⇒ optimize your workflow

My current plan:
2016: experiment to make
PoC||GTFO better
2017: publish methods & tools

Please provide feedback.

Please submit
(articles, ads, polyglots,
puzzles, poems...)

To be published soon:
The PoC||GTFO bible
Tome I
@ NoStarch

Ultimately…

I'll let you decide whether PoC||GTFO is good, but…

...that's not the point.

We're exploring
better ways
to share knowledge.

We need more people trying new ways to share knowledge.
PeX, PoC||GTFO…

but more importantly:
yours !

Ack

Phil Travis Evan Sergey Jacob
Micah Michael Allan Peter
4am Chris Kurt...

Thank you!

@angealbertini

corkami.com