Conference d’ouverture
[titre à venir]
Travis Goodspeed

4 June 2014
SSTIC
Rennes, Bretagne, France
Prezegenn digeriñ
[titl da zont]

Travis Goodspeed

4 June 2014
SSTIC
Roazhon, Breizh
GOOD MORNING!
GOOD MORNING!

• I hate keynotes.
  • (Except those by Fx and Dan Geer.)

• I love proofs of concept.
  • Short, nifty tricks.
  • No grand theories, no unnecessary tables.
Proofs of Concept are Proofs by Construction
Proofs of Concept are Proofs by Construction

by Travis Goodspeed
to them Ghosts who write History Books
and the Ghosts in my Drink
concerning the Good Works
and the Good Neighbors
of PoC||GTFO.

4 June 2014
SSTIC
Rennes, Brittany, France
Did you know that you can just start a journal?
Did you know that you can just start a journal?

• A neighbor and I started a journal.

• No peer review, just a benevolent dictatorship.

• Pastor Manul Laphroaig, Amateur Tyrant
International Journal of PoC || GTFO
Issue 0x00, a CFP with PoC

An epistle from the desk of Rt. Revd. Pastor Manul Laphroaig

copyright

August 5, 2013
Proceedings of the Society of PoC || GTFO
Issue 0x01, an Epistle to the 10th H2HC in São Paulo

From the writing desk, not the raven, of Rt. Revd. Preacherman Pastor Manul Laphroaig

pastaor@phrack.org
Children’s Bible Coloring Book of PoC || GTFO
Issue 0x02, an Epistle to the 30th CCC Congress in Hamburg

Composed by the Rt. Revd. Pastor Manul Laphroaig to put pwnage before politics.

pastor@phrack.org

December 28, 2013
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
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
Let’s hear some stories!
Nifty Tricks for Today

• Active Disk Antiforensics
• PGP Matryoshka Doll
• PDF+Zip Polyglot
• Angecryption
• Strange Python Encodings
Active Disk Antiforensics
PoC||GTFO 0:2
Active Disk Antiforensics

• You think of a disk as a block device.
  • Blocks are written, then read back intact.
  • Sometimes they are damaged.

• A disk is really a server.
  • Host makes requests by SCSI or ATA.
  • Software in the disk responds.
iPod is a Computer

• Low-end ARM with hardware MP3 decoding.

• Custom operating systems
  • iPod Linux, Rockbox

• Disk Mode is implemented in software.
  • C code translates USB Mass Storage to ATA.
iPod Disk Layout

- First sector is MBR.
- Then comes the iPod Firmware.
- Finally, there is a FAT32 or HFS+ partition for music.
iPod Disk Layout

• First sector is MBR.
• Then comes the iPod Firmware.
• Finally, there is a FAT32 or HFS+ partition for music.

This is *NEVER* legitimately read by the host!
Fingerprinting a Host OS

- Windows
  Reads the Master Boot Record (MBR) 9 times.

- FreeBSD
  Speaks some antique SCSI requests.

- OpenBSD
  Doesn’t delay on SCSI errors.

- Linux
  Varies by automounter.
Fingerprinting Disk Imaging

- **tar -cf mnt.tar /mnt**
  Follows the filesystem structures, never reading empty space, or deleted files, or orphaned inodes.

- **dd if=/dev/sdc of=forensics.img**
  This reads from the beginning to the end, in order, as large blocks, without reading ahead, and without following filesystem or partition structs.
So let’s make a trap!

- Pick an unused sector early in the disk.
- The sector must be one that is *NEVER* read.
- If this sector is read anyways,
  - Erase all future sectors.
  - Reply with legitimate-looking garbage.
Disk Imaging my iPod

//These sectors are for 2048-byte sectors.
//Multiply by 4 for devices with 512-byte sectors.
if(cur_cmd.sector>=10000 && cur_cmd.sector<48000)
    tamperdetected=true;
Never gonna let you down
Never gonna give you up
Never gonna let you down
Never gonna give you up
Beyond a PoC

- ACSAC 2014, Seagate Disk Backdoor
  - Talk to Aurélien Francillon. He’s here!
- Sprites Mods, Western Digital Reverse Engineering
  - He booted Linux on a WD hard disk!
Myron Aub’s PGP Matryoshka Doll

PoC||GTFO 2:3
PGP Matryoshka Doll

- RFC 4880, `OpenPGP Message Format’ by Phil Zimmerman
- Messages are compressed or encrypted.
  - These are just containers, and they can be nested!
  - You can required more than one key for decrypt.
  - You can compress more than once.
Lempel-Ziv (LZ) Compression

• A dictionary is used as shorthand for a larger file.

• The output of the decompression can be the same as the input.
PGP Quine

• Message, when decompressed, is itself.

• After decompression, the parser tries to go deeper.
  • And deeper.
    • And deeper.
      • And deeper!
• GnuPG fixed this bug.

• Symantec PGP didn’t fix this bug.
PDF that’s a ZIP File
PoC||GTFO 1:5

• Zip files begin with a footer near the end of a file.
• This makes them easy to combine with other files.
  • cat foo.gif foo.zip >zippgif.bin
• PDF also ends near the end.
%!PDF-1.etc in
%!PK/1003/004 etc... Not CR, LF, or NUL
2.zip metadata

1 0 obj << ...
Begin stream in
<< Lib
2 bytes
end stream
end obj
%!PK/1003/004 (see above)
(Repeat)


```
% PDF-1. etc
% PK\003\004 etc... Not CR, LF, or NUL

Zip metadata

TYPE LENGTH

1 0 obj << ... >>
Begin stream

% lil 2 bytes

Deflate stream

end stream
end obj

% PK\003\004 (See above)
(Repeat)
```
END

Probably

Best

OPTION 1

OPTION 2

Zip Dir

Zip Dir Rec

Zip Common

Trailer

XREF

%eof

% Zip Dir

Zip Dir Rec
cat foo.pdf bar.zip > buz.pdf
zip -A buz.pdf

or...

cat foo.pdf bar.zip foo.pdf > buz.pdf
zip -A buz.pdf

or...
echo -e "trailer << /Root ... >> /XRef /n 0 0 0 0 0 0 1... etc. % "EOF" >> comment.txt

cat foo.pdf bar.zip > buz.pdf
zip -2 comment.txt baz.zip Stuff
zip -A buz.pdf
PDF+ZIP

• For very small Zips, just
  cat foo.pdf foo.zip >bar.pdf

• For larger files, insert the zip just before the PDF’s closing xref table.

• This is reliable, and we’ve shipped it in every release since the first.
Angecryption
PoC||GTFO 3:11

Ange Albertini
Jean-Philippe Aumasson
Angecryption

• pocorgtfo03.pdf was a valid PDF file.

• Encrypt it with AES CBC to get a valid PNG file.
  key=“Manul Laphroaig!”
  IV=5B F0 15 E2 04 8C E3 D3 8C 3A 97 E7 8B 79 5B C1

• Ain’t that nifty?
Angecryption

• It’s easy to control ECB-mode data before or after encryption.
  
  • AES(controlled)=uncontrolled
  
  • controlled=AES(uncontrolled)
    AES^-1(controlled)=uncontrolled
  
• Angecryption lets us make a file valid before and after encryption, with different contents!
The Nifty Trick

• In ECB mode, we control each block before or after encryption.

• In CBC mode, the same is true, except

  • The very first block is XOR’ed with the IV,

  • and we control the IV, so

  • we control Block 0 before and after encryption!
Weird Python Encoding
PoC||GTFO 3:10
Frederik Baun
10.2 The PoC

Recognizing that `cevag` is the Rot13 encoding of Python's `print` command, it's easy to test this strange behavior.

```python
#! /usr/bin/python
#encoding: rot13
cevag 'Hello World'
```

10.3 Caveats

Sadly, this only works in Python versions 2.X, starting with 2.5. My current test with Python 3.3 yields first an unknown encoding error (the "rot13" alias has sadly been removed, so that only "rot-13" and "rot_13" could work). But Python 3 also distinguishes string from bytearray, which leads to type errors when trying this PoC in general. Perhaps `rot_13.py` in the python distribution might itself be broken?

There are numerous other formats to be found in the encodings directory, such as ZIP, BZip2 and Base64, but I've been unable to make them work. Most lead to padding and similar errors, but perhaps a clever reader can make them work.

And with this, I close the chapter of Python encoding stories. TGSB!
Proofs of Concept are Proofs by Construction
Proof of Concept is Proof by Construction

• A proof by construction is the best kind of proof.

  • See Euclid’s proof that there are infinitely many prime numbers.

• Stop calling them unscientific! Stop demanding statistics!

• “You can’t argue with a root shell.”
Go now in peace.

- Read your scripture.
  - PoC||GTFO, Phrack, and SSTIC proceedings!
- Preach the good news!
  - Conference talks, soap box.
  - "Hey, want to learn a cool trick?"
Credits

- Antiforensic iPod, PoC||GTFO 0:2
  Travis Goodspeed

- PGP Matryoshka, PoC||GTFO 2:3
  Myron Aub

- PDF Zip File, PoC||GTFO 1:5
  Julia Wolf

- Angecryption, PoC||GTFO 3:11
  Ange Albertini
  Jean-Philippe Aumasson

- Weird Python Encoding, PoC||GTFO 3:10
  Frederik Braun