Steganographic AVI Filesystems for fun and profit

Paul Sebastian Ziegler

HITB KL 2011

Introduction

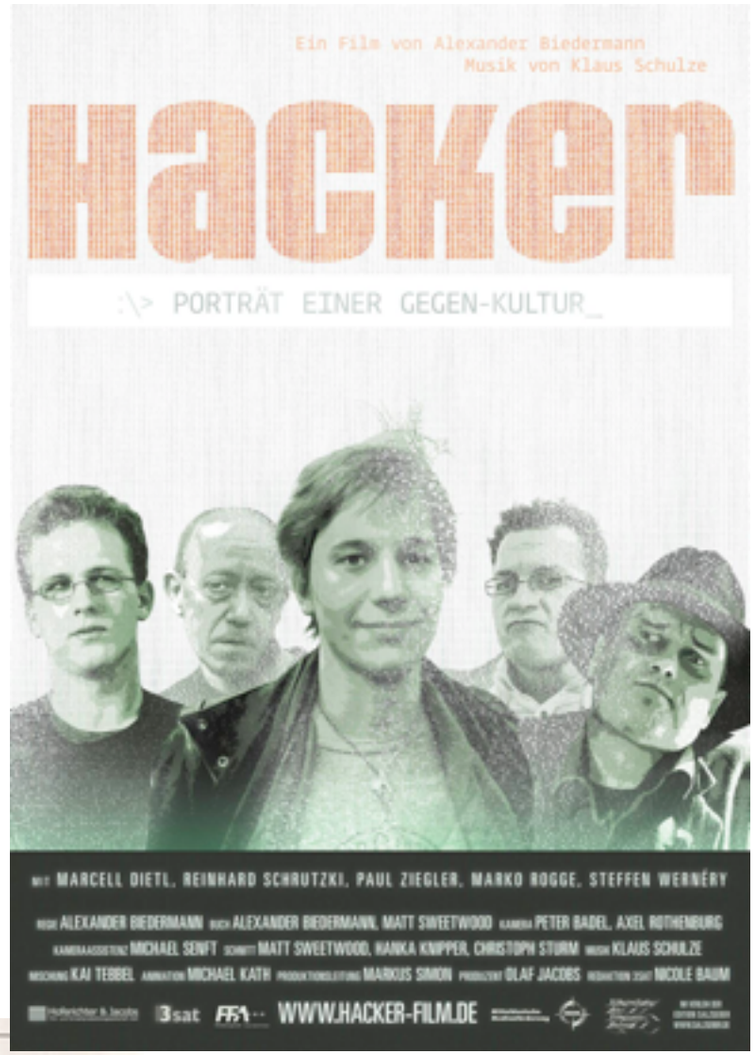
Introduction

In 30 seconds or less

Paul Sebastian Ziegler


rotring T 0.5
rotring isograph
.35
rotring isograph
.25
PILOT CROQUIS 6B
rotring rapidoliner

Pentester




Lokales

Kein System ist absolut sicher

20-jähriger Hacker gibt Einblick in seine Welt – Die größte Schwachstelle ist der Mensch

Heute bis 18 Uhr geöffnet
Wrede - die Servicegärtnerei

Cross-Site Scripting

Paul Sebastian Ziegler

Cross-Site Scripting (XSS) ist die Schwachstelle in Webanwendungen schlechthin. Wie kaum eine andere Technik kombiniert diese Technik einfache Methoden und Ansätze zu letztendlich verheerenden Angriffen. Jedoch ist das Wissen um diese Schwachstelle und die damit verbundenen Angriffe derzeitig lediglich Sicherheitsexperten vorbehalten. Es existieren zwar umfangreiche Berichte und Dokumentationen, aber diese können zumeist nur von Insidern verstanden werden. Der normale Programmierer oder Nutzer, der sich mit Cross-Site Scripting auseinandersetzen muss, bleibt in der Regel außen vor.
Dieses TecFeed ist bemüht, das zu ändern. In einfachen Schritten führt Sie der Autor in das komplexe Thema ein. Sie werden lernen, was Cross-Site Scripting ist und wie man mit seiner Hilfe Webanwendungen angreifen kann. Nach der Lektüre dieses TecFeeds werden Sie in der Lage sein, Schwachstellen zu erkennen und zu beheben.

O'REILLY®

INHALT

TecFeeds

www.tecfeeds.de

Ninja Penguin Limited

Chief Executive Penguin Trainer

Artificial

Intelligence

Make my computers act on their own.

That's what HE thinks!

Write code

Hack stuff

Things I do

Train ninja penguins

Write books & articles

Visit

observed.de

for more l33t-cred

Steganographic AVI File Systems

Securing your Data

“I don’t want anyone to be able to access my data!”

Great!

Cryptography!

Many algorithms
to choose from

Cryptography!

Many algorithms
to choose from

Variable strength
adapts to your
needs

Cryptography!

Many algorithms to choose from

Variable strength adapts to your needs

Cryptography!

Algorithms are rarely (*cough*) broken

Many algorithms to choose from

Variable strength adapts to your needs

Cryptography!

Algorithms are rarely (*cough*) broken

Crypto Cascade + Secure Passphrase = Secured data for 5 years

YOU

Me?

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

NO GOOD! IT'S 4096-BIT RSA!

BLAST! OUR EVIL PLAN IS FOILED!

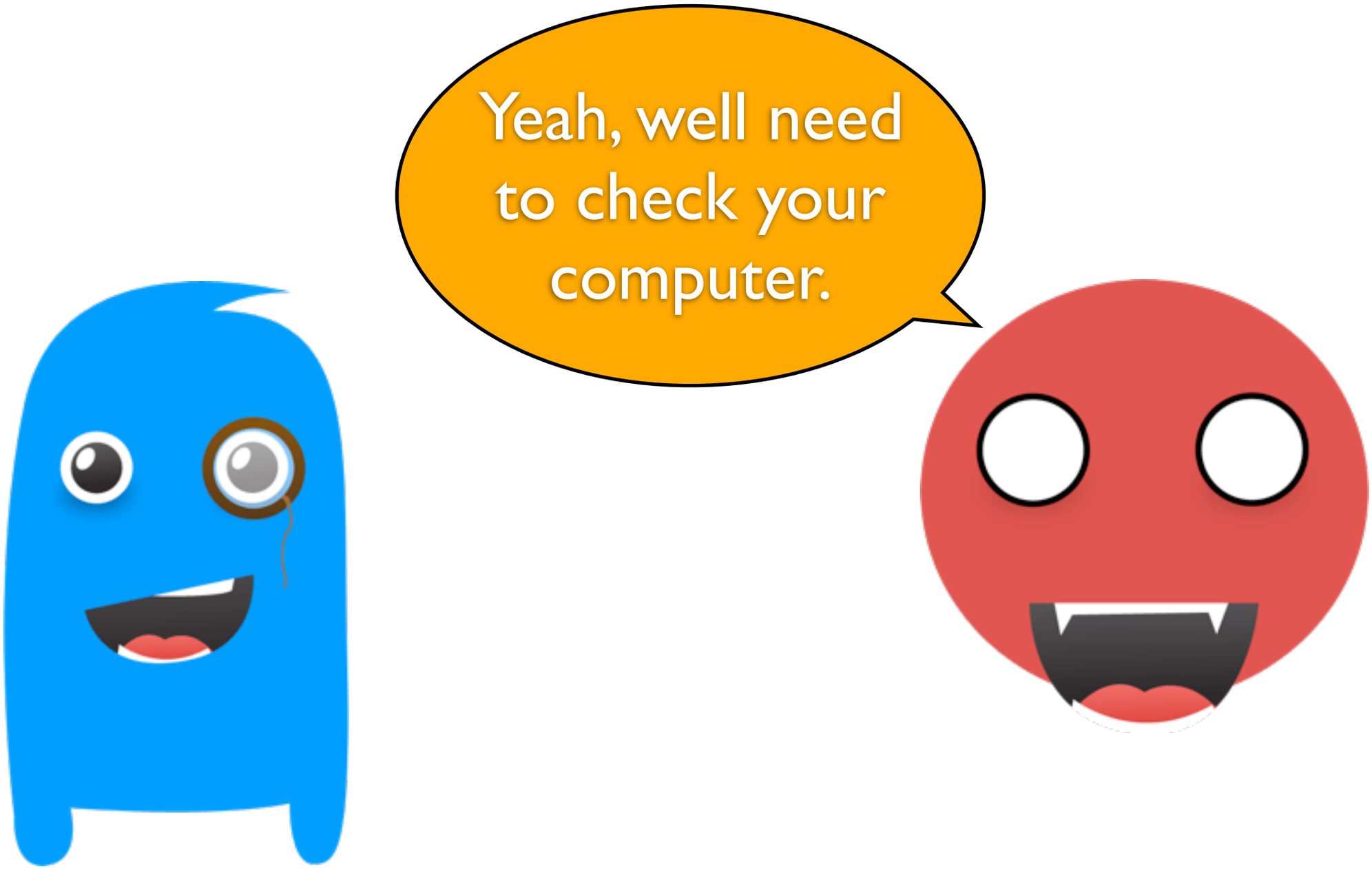
WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.

GOT IT.

Airport

Airport



Solutions

Don’t possess the passphrase

Transmit data through separate channel

Physically hide the data

Thou shall
not pass!

(That, or the wrench)

Introducing

Super Hero #1

Steganography

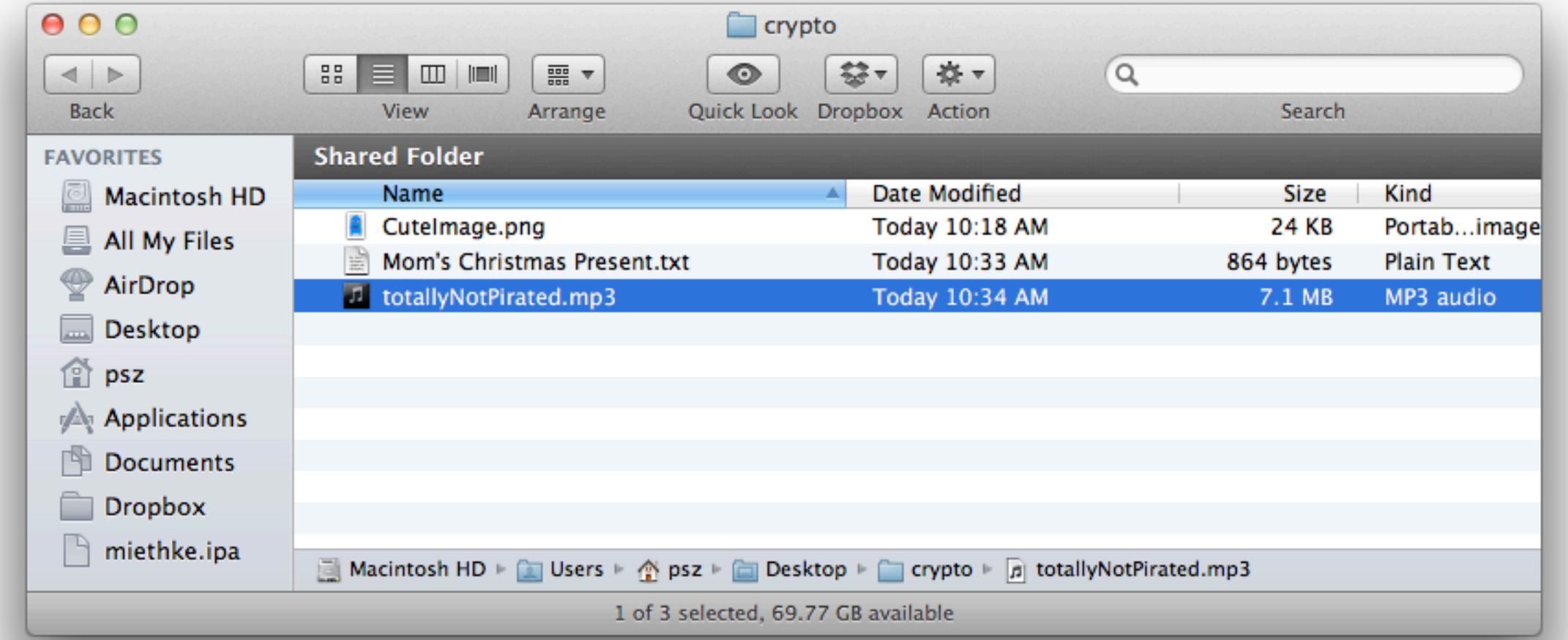
“Hey, Truecrypt does that!”

Truecrypt 7.0a

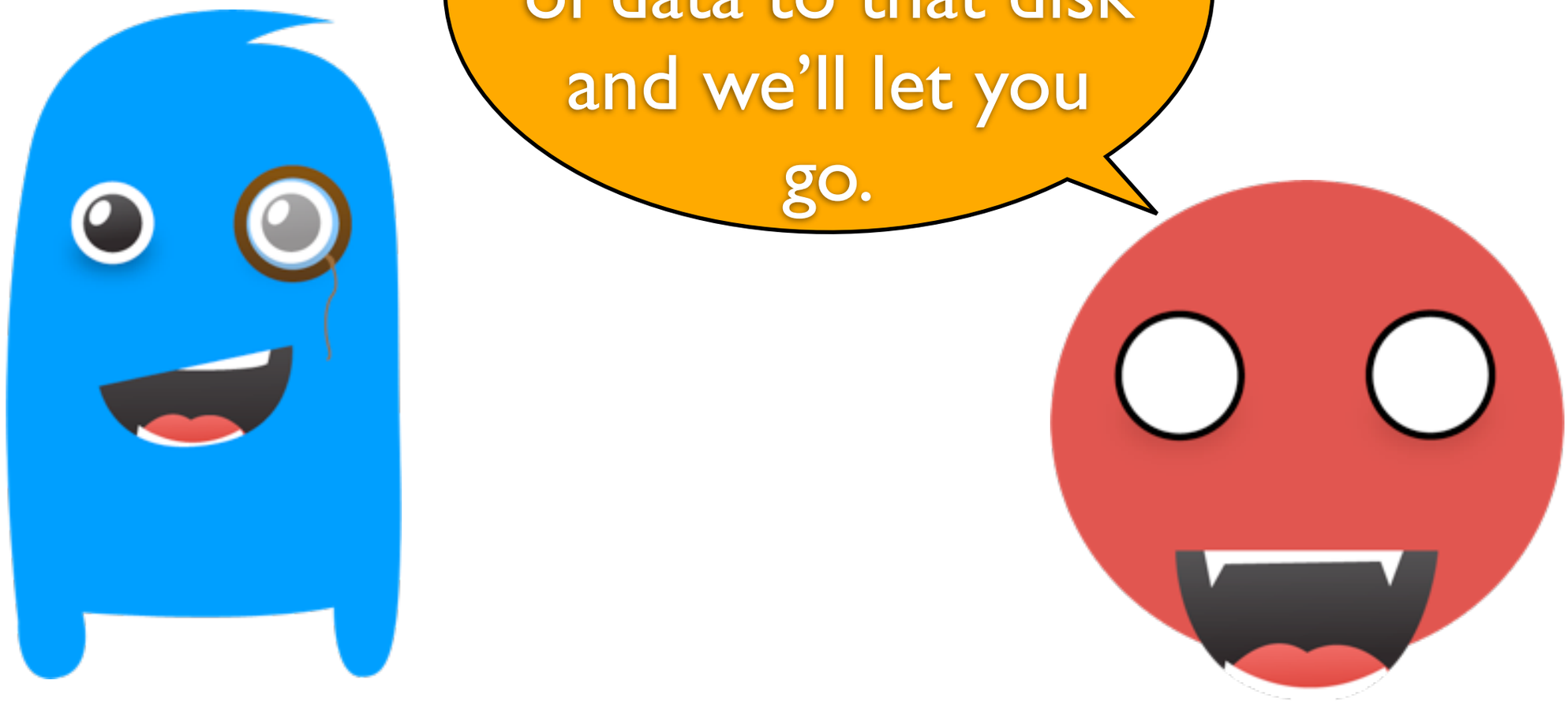
- Hidden partitions
- Hidden volume within crypto container
- Hidden OS

3 Problems

Need for fake outer partition


crypto
Back
View
Arrange
Quick Look
Dropbox
Action
Search
FAVORITES
Macintosh HD
All My Files
AirDrop
Desktop
psz
Applications
Documents
Dropbox
miethke.ipa
Shared Folder
Name
Date Modified
Size
Kind
CuteImage.png
Today 10:18 AM
24 KB
Portab...image
Mom's Christmas Present.txt
Today 10:33 AM
864 bytes
Plain Text
totallyNotPirated.mp3
Today 10:34 AM
7.1 MB
MP3 audio
Macintosh HD ▸ Users ▸ psz ▸ Desktop ▸ crypto ▸ totallyNotPirated.mp3
1 of 3 selected, 69.77 GB available

Partition Overwriting


Cool.
Just write one gig of data to that disk and we'll let you go.

Transporting lots of data

I always travel
with 5 1-terabyte-disks
containing only 15MB
each!

Introducing

Super Hero #2

File-Based Steganography!

Plausible Deniability

What? That picture
I got from flickr contained
a hidden message?
Great Scott!

Carrying lots of data

Scenario:

Male

18-30

3TB of data

Scenario A:

Male

18-30

3TB of data

5 1-terabyte-harddrives containing 150MB each

Scenario B:

Male

18-30

3TB of data

5 terabytes of “miscellaneous” video files

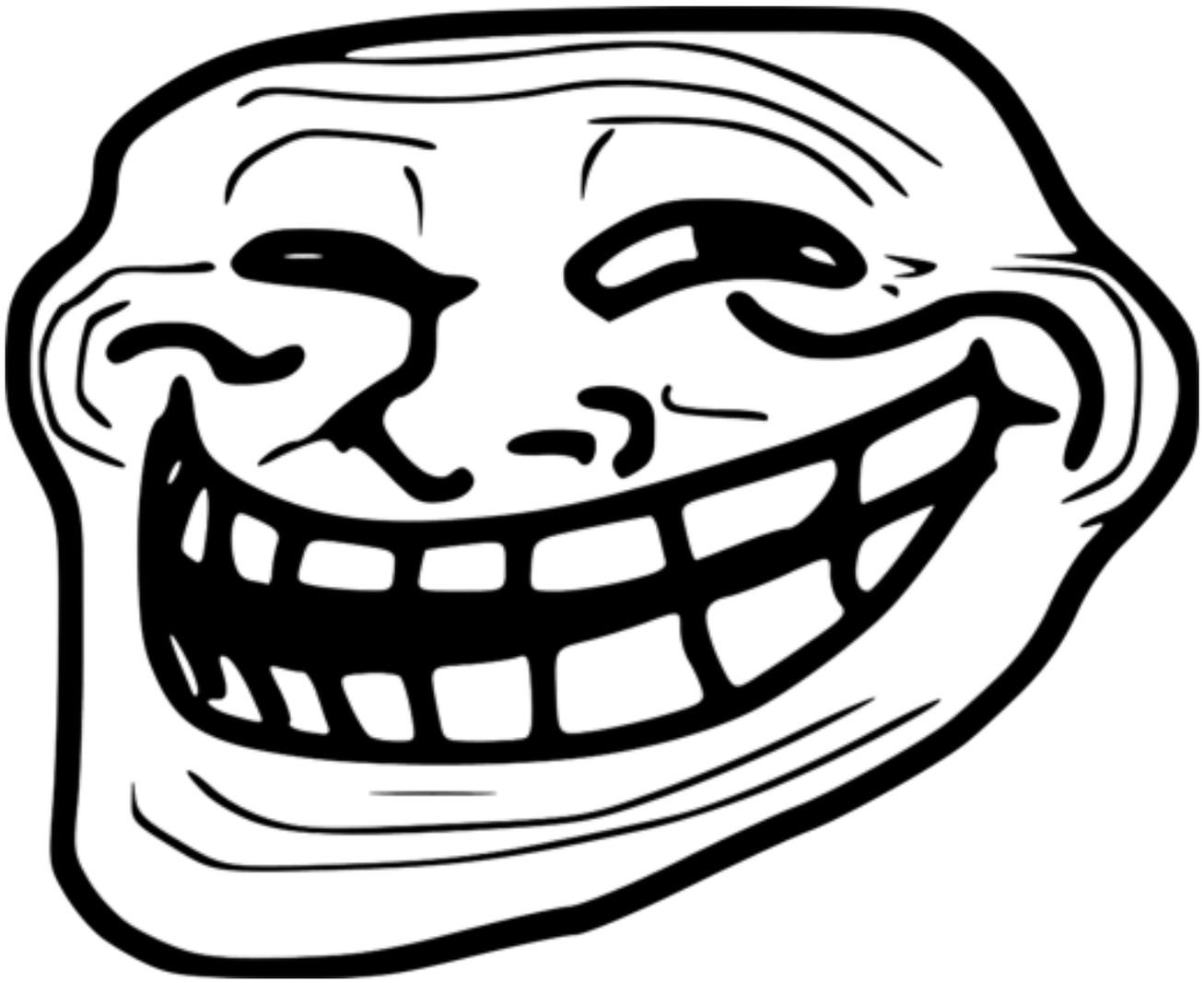
Sharing through open channels

flickr™

YouTube
Broadcast Yourself™

vimeo

RAPIDSHARE
EASY FILEHOSTING



Problem?

Yes, actually.

Storing and accessing data is tiresome

Carrying specialized tools for access

Don’t mind my
400GB picture collection
and the folder labeled
“steganographic imaging
toolset”

Can’t be modified while hidden

Files need to be de-

cloaked to be accessed

Let's address **some** of these issues

Introducing

MariaFS

Put your money where your mouth is!

-- Cut at the perforated line --

-- Cut at the perforated line --

Goals

Goals

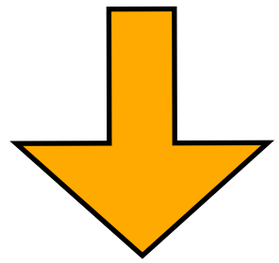
- Easy to use
- Reasonably fast
- Unsuspicious in airport setting
- Clear language

Problem	Solution
Hiding Files	Steganography
Carrying Lots of Files	File Based Steganography
Specialized Toolset	
Hard to use	
Needs to decrypt to alter	
Hard to alter, adapt, extend	

Problem	Solution
Hiding Files	Steganography
Carrying Lots of Files	Steganography in AVI Containers
Specialized Toolset	File System Driver (1 file)
Hard to use	Simple CLI usage (once, when mounting)
Needs to decrypt to alter	Steganography hidden from user
Hard to alter, adapt, extend	Python

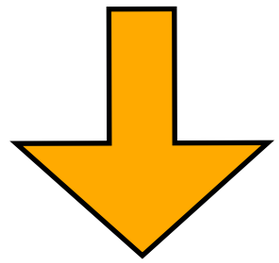
PornFS

PornFS



MariaFS

PornFS

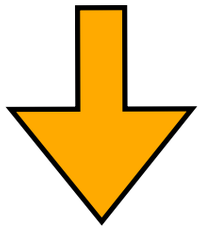


MariaFS

(Ask someone Japanese if you don't get the joke)

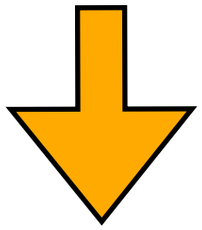
2_cups_1_girl_starbucks_commercial.avi

2_cups_1_girl_starbucks_commercial.avi

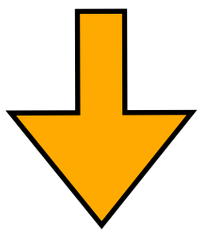


Mount using custom FUSE driver

2_cups_1_girl_starbucks_commercial.avi



Mount using custom FUSE driver



Provide data to user abstracted as FS

FUSE?

FUSE?

Filesystem in User Space

FUSE?

Filesystem in User Space

Allows fast FS implementation

FUSE?

Filesystem in User Space

Allows fast FS implementation

Supports many languages

Implemented in FUSE

- ntfs-3g
- GmailFS
- sshFS
- GVFS (Gnome)
- s3FS

Ideas for Infosec

- Write custom FS to nail down access policies, log, etc
- Specialized FS for honeypots
- Extend existing FS
- Write custom FS that returns the complete lyrics to Rick Astley's "Never gonna give you up" for every file read

Thursday, October 13, 2011

AVI?

Very common

AVI?

Very common

AVI?

Large size differences

Gap between data and index

Very common

AVI?

Large size differences

Very common

Gap between data and index

AVI?

Large size differences

Easy Structure

AVI File Structure

RIFF

Resource Interchange File Format

RIFF

Length

AVI

LIST

hdrl

hdrl data

movi

movi data

idx1

idx1 data

RIFF

Length

AVI

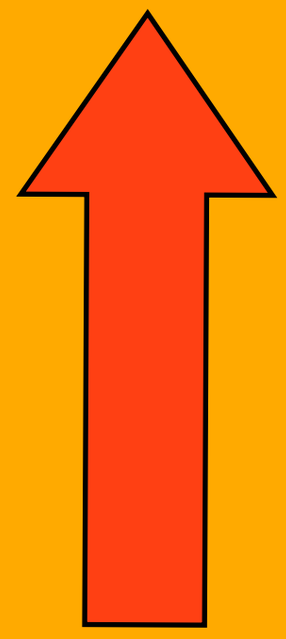
LIST

hdrl

hdrl data

movi

movi data



idx1

idx1 data

RIFF

Length

AVI

LIST

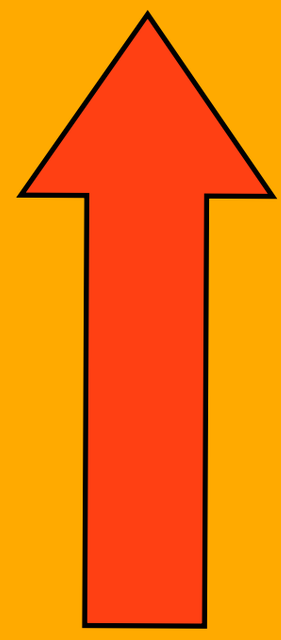
hdrl

hdrl data

movi

movi data

MariaFS Data



idx1

idx1 data

Internals

Requirements

FUSE

OSXFuse

~~macFUSE~~

Requirements

FUSE

OSXFuse

~~macFUSE~~

Python 2.6+

Requirements

FUSE

OSXFuse

~~macFUSE~~

Python 2.6+

Requirements

FUSE-Python bindings

+

PyCrypto

FUSE

OSXFuse

~~macFUSE~~

Python 2.6+

Requirements

FUSE-Python bindings

+

PyCrypto

Tons o' RAM

creating

```
python mariaFS.py -c somefile.avi
```

FS Markers
"VIDFSBEGIN"
"VIDFSEND"

Passphrase

AES

Encrypted
Markers

Insert before
IDX

mounting

```
python mariaFS.py somefile.avi \
mountpoint/ -o allow_other
```

FS Markers
"VIDFSBEGIN"
"VIDFSEND"

Passphrase

AES

Encrypted
Markers

Encrypted
Markers in File?

deleting

python mariaFS.py -x somefile.avi

FS Markers
"VIDFSBEGIN"
"VIDFSEND"

Passphrase

AES

Encrypted
Markers

Delete everything
between markers

Markers

BEGINNING_MARKER_PLAIN = "VIDFSBEGIN"
END_MARKER_PLAIN = "VIDFSEND"
FILE_NAME_MARKER_PLAIN = "FILENAME"
FILE_STATS_MARKER_PLAIN = "FILESTATS"
FILE_DATA_MARKER_PLAIN = "FILEDATA"

FILENAMEDATADATADATA
FILESTATSDATADATADATA
FILEDATADATADATADATA

FILENAMEDATADATADATA
FILESTATSDATADATADATA
FILEDATADATADATADATA
FILENAMEDATADATADATA
FILESTATSDATADATADATA
FILEDATADATADATADATA
FILENAMEDATADATADATA
FILESTATSDATADATADATA
FILEDATADATADATADATA

VIDFSBEGIN

FILENAMEDATADATADATA

FILESTATSDATADATADATA

FILEDATADATADATADATA

FILENAMEDATADATADATA

FILESTATSDATADATADATA

FILEDATADATADATADATA

FILENAMEDATADATADATA

FILESTATSDATADATADATA

FILEDATADATADATADATA

VIDFSEND

Stats

atime|mtime|ctime|size|uid|gid

Detectability

Writing Data

File is mmaped

Writing Data

File is mmaped

Writing Data

New file created or old one
updated with fresh data / stats

File is mmaped

Writing Data

Rebuild mmap

New file created or old one
updated with fresh data / stats

File is mmaped

Return

Writing Data

Rebuild mmap

New file created or old one
updated with fresh data / stats

Speed

Read: 0.01 MB/s

Write: 0.2 MB/s


CACHE ALL THE THINGS!

Speed

Read: 0.3 MB/s

Write: 2.5 MB/s

Main Demonstration

Limitations

Scalability

Maximum Number of Files

Scalability

Maximum Number of Files

Scalability

RAM Usage

Maximum Number of Files

Scalability

RAM Usage

Maximum File Size

Non-implemented FS Features

Simultaneous Access

Non-implemented FS Features

Simultaneous Access

Non-implemented FS Features

Access Controls

Simultaneous Access

Non-implemented FS Features

Access Controls

Devices

Code:

http://observed.de/conferences/mariaFS.tgz

Image Attributions

- pigpogm (page 4)
- xkcd (page 10)
- djwundi (page 34)
- skampy (page 45)
- logos of respective companies (page 54)
- steffenz (page 62)
- 60 in 3 (page 84)
- Hyperbole and a half (page 118)

Questions?
Ideas?
Bacon?

Thank you for listening!