Steganographic AVI Filesystems for fun and profit

Paul Sebastian Ziegler
HITB KL 2011
Introduction
Introduction

In 30 seconds or less
Paul Sebastian Ziegler
Cross-Site Scripting

Paul Sebastian Ziegler


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.

INHALT
Einleitung | 2
Aufbau eines XSS-Angriffs gegen eine ungesicherte Webanwendung | 2
Effekte, die ein Angreifer durch XSS hervorrufen kann | 8
Schutzmechanismen, die zu kurz greifen | 9
Der Aufbau starker Schutzmechanismen – Escapen und listenbasiertes Filtern | 16
Das Gefahrenpotenzial von XSS heute und in naher Zukunft | 47
Zusammenfassung | 52
Anhang A – Liste verschiedener Angriffsvektoren | 53
Anhang B – safehtml | 54
Über den Autor | 72
Danksagung | 72

O'REILLY®

www.oreilly.de
Chief Executive Penguin Trainer
Artificial Intelligence
Make my computers act on their own.
That’s what HE thinks!
Things I do

- Write code
- Hack stuff
- 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!
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

Thursday, October 13, 2011
Me?
A CRYPTO NERD'S IMAGINATION:
His laptop's encrypted. Let's build a million-dollar cluster to crack it.

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

Yeah, well need to check your computer.
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
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
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
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiding Files</td>
<td>Steganography</td>
</tr>
<tr>
<td>Carrying Lots of Files</td>
<td>File Based Steganography</td>
</tr>
<tr>
<td>Specialized Toolset</td>
<td></td>
</tr>
<tr>
<td>Hard to use</td>
<td></td>
</tr>
<tr>
<td>Needs to decrypt to</td>
<td></td>
</tr>
<tr>
<td>alter</td>
<td></td>
</tr>
<tr>
<td>Hard to alter, adapt,</td>
<td></td>
</tr>
<tr>
<td>extend</td>
<td></td>
</tr>
<tr>
<td><strong>Problem</strong></td>
<td><strong>Solution</strong></td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Hiding Files</td>
<td>Steganography</td>
</tr>
<tr>
<td>Carrying Lots of Files</td>
<td>Steganography in AVI Containers</td>
</tr>
<tr>
<td>Specialized Toolset</td>
<td>File System Driver (1 file)</td>
</tr>
<tr>
<td>Hard to use</td>
<td>Simple CLI usage (once, when mounting)</td>
</tr>
<tr>
<td>Needs to decrypt to alter</td>
<td>Steganography hidden from user</td>
</tr>
<tr>
<td>Hard to alter, adapt, extend</td>
<td>Python</td>
</tr>
</tbody>
</table>
PornFS
PornFS

MariaFS
PornFS

↓

MariaFS

(Ask someone Japanese if you don’t get the joke)
2_cups_l_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

Thursday, October 13, 2011
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
AVI?
Very common

AVI?
Very common

AVI?

Large size differences
AVI?

Large size differences

Very common

Gap between data and index
AVI?

Very common

Gap between data and index

Large size differences

Easy Structure

Thursday, October 13, 2011
AVI File Structure
RIFF

Resource Interchange File Format
RIFF

Length

AVI

LIST

hdrl

hdrl data

movi

movi data

idx1

idx1 data
Internals
Requirements
Requirements
Requirements

FUSE
OSXFuse
macFUSE

Python 2.6+
Requirements

FUSE
OSXFuse
macFUSE

Python 2.6+

FUSE-Python bindings

+ PyCrypto
Requirements

FUSE
OSXFuse
macFUSE
PyCrypto
Python 2.6+

FUSE-Python bindings  +  Tons o’ RAM
creating

python mariaFS.py -c somefile.avi
mounting

```python
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"
<table>
<thead>
<tr>
<th>atime</th>
<th>mtime</th>
<th>ctime</th>
<th>size</th>
<th>uid</th>
<th>gid</th>
</tr>
</thead>
</table>

Stats
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  

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

Rebuild mmap  

Return  

Writing Data
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
Scalability

Maximum Number of Files
Maxmum Number of Files

Scalability

RAM Usage
Non-implemented FS Features
Simultaneous Access

Non-implemented FS Features
Simultaneous Access

Non-implemented FS Features

Access Controls
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!