

Data Hiding and Recovery

Jonathan C. Busey
busey@cs.fsu.edu

April 21, 2003

Overview

Began as review of **Linux Data Hiding and Recovery** by Anton Chuvakin

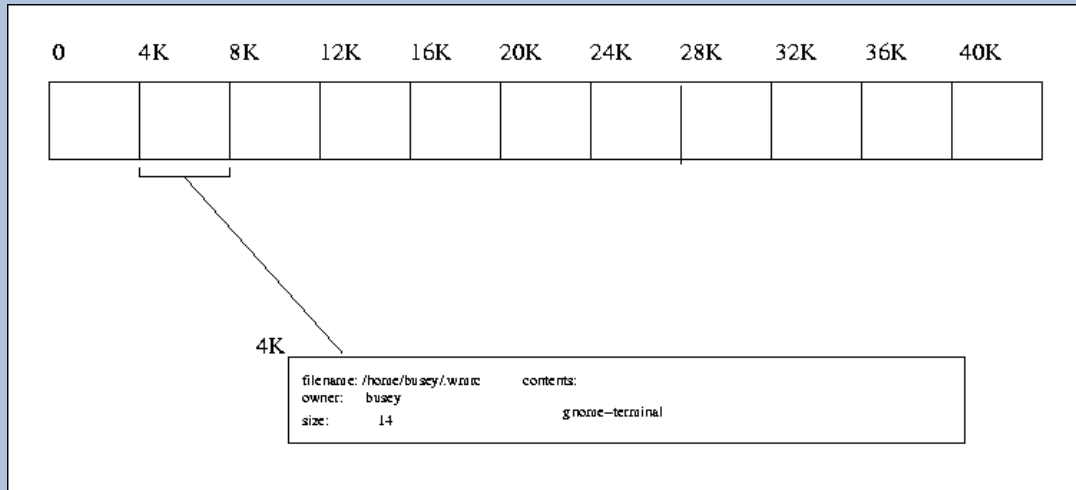
- hiding binaries
- hiding other files
- examples
- recovering data

Hiding binaries

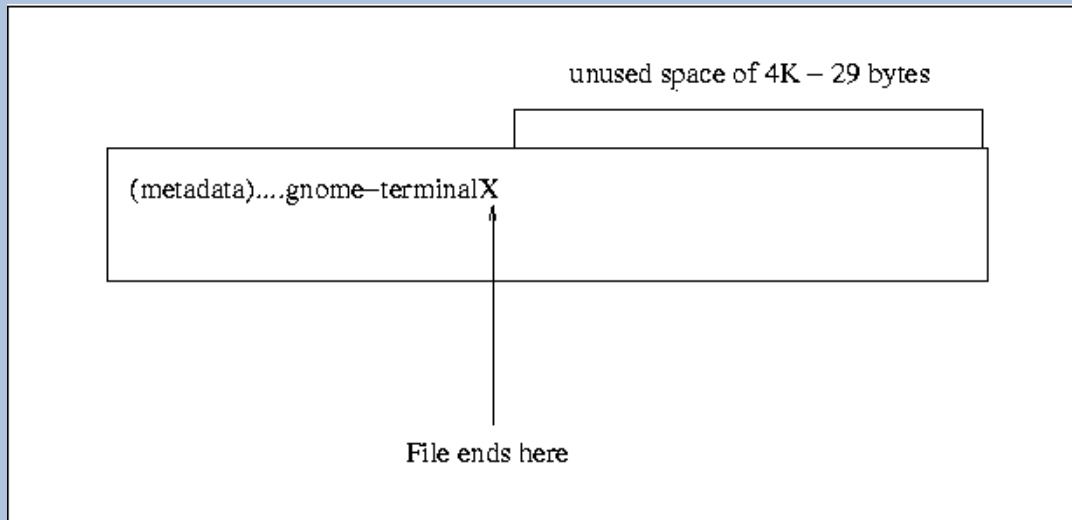
- unix-wide technique
- run process which keeps file open
- copy of binary in `/proc/$PID/exe`

Slack space

- data can be hidden in unused portion of block



Slack space



Slack space

- bigger the block and smaller the file stored in it, the more the slackspace
- “undetectable by file integrity checkers using file checksumming and MAC times” claims Chuvakin

bmap

- **bmap** is the tool which makes use of this slack space

```
$ echo "mQGiBDm+XgQRBACJALsgXC3ZL9TrJefYaHm5kZ4"  
| bmap -mode putslack /home/busey/.wmrc
```

will put the data in quotes in the slackspace on previous slide

- retrieving data

```
$ bmap -mode slack /home/busey/.wmrc  
getting from block 192288501  
file size was: 26  
slack size: 4070  
blocksize: 4096  
mQGiBDm+XgQRBACJALsgXC3ZL9TrJefYaHm5kZ4
```

- cleaning the data

```
$ bmap -mode wipeslack /home/busey/.wmrc
```

bmap

- need not be text files
- larger files can be split and spread over slack space of files
- automate splitting—integrity checkers can not find it
- bug or feature? now we can use that space!
- from: <http://en.tldp.org/HOWTO/mini/Partition/formatting.html>:

Files come in any size. They don't end on block boundaries. So with every file a part of the last block of every file is wasted. Assuming that file sizes are random, there is approximately a half block of waste for each file on your disk.

Recovering deleted files

- verified **ext2** only (and **not ext3**)

- using **mc** or underlying tool **debugfs**:

```
mount /dev/sdb5 /tmp/sdb5
```

```
rm thttpd.log.4
```

```
umount /tmp/sdb5
```

```
echo lsdel | debugfs /dev/sdb5 > lsdel.out
```

```
cut -c1-6 lsdel.out | grep "[0-9]" | tr -d " " > inodes
```

```
sed 's/^\.*$/stat <\0>/' inodes | debugfs /dev/sdb5 > stats
```

- often only filename and size are needed
- **fsgrab** or **debugfs dump** then **dd** to recover data

Regarding Computer Crime

Definition includes “using computers to commit crimes” Mon, Oct. 14, 2002 story:

FBI planning Bay Area computer forensics lab

By Sean Webby of **Mercury News**

“This is where everything in law enforcement is going,” said Randall Bolelli, director of the FBI’s regional forensic lab in San Diego. “Almost every case these days involves a computer in some way. And as hard drive space and capacity keeps increasing, we have more things to look at.”

<http://www.siliconvalley.com/mld/siliconvalley/4286982.htm>

Links

- www.vogon-international.com
- www.netsecurity.com
- Scientific evidence links:
www.law-forensic.com/cls_sci_evidence_links.htm
- **Design and implementation of the Second Extended Filesystem** e2fsprogs.sourceforge.net/ext2intro.html
- Digital Forensics Links: vip.poly.edu/kulesh/forensics/list.htm
- F.I.R.E: Forensic and Incidence Response Environment (Bootable CD) fire.dmzs.com
- other popular bootable cdroms for forensic purposes:
 - Knoppix www.knoppix.net
and www.knopper.net/knoppix/index-en.html
 - Trinux trinux.sourceforge.net
 - PLAC (Portable Linux Auditing CD)
sourceforge.net/projects/plac