Free space file system

Sai Emrys

ccc@saizai.com
GPG: D6D408A9
DECT 4724 (4-SAI)
AIM, IRC, LJ, Skype etc: saizai

It's just a proposal

No code yet, sorry. Just an idea.

Feel free to use however you want.

The problem

All crypto and steganographic file systems:

- leave suspiciously “random” chunks of “empty” disk,
  - TrueCrypt partition
- create large and suspiciously random files,
  - TrueCrypt file data store
- modify data in detectable and hackish ways, or
  - media steganography, slack space, etc
- require difficult & suspicious setups
  - LVM, RHFS, etc

The usual answer

- “Rubber hose” plausible deniability
  - 2+ working passwords
  - Not very plausible in practice
    - Old files
    - Not much data
  - Not fully deniable
    - Cops know about hidden partitions
    - Cryptostore is easily detectable
      - Provably? No. But what would you think if someone had 50 GB of “random”, “unpartitioned” data at the end of their HD?
    - Cruft left behind unless explicitly wiped
      - Cruft = forensics data

Free space file system

- Disk 100% accounted for by legit partitions
  - Perfectly normal, stock file system
- Every disk has free space
  - Nothing suspicious about it...
- We live there.
  - Use only what the host doesn't want

Benefits

Nothing to deny

- No detected cryptostore = no talking to feds

Automatically destroyed if not maintained

- “Wipe” your cryptostore by downloading a big file

Zero “used” space

- Host gets to use all its resources, we defer

No messing with host FS's files

- ... just its “free” space

No special setup (*VM, reformatting, unmounting, RO, etc)

Blackhat benefits

- Can be run without user knowledge
  - Doesn't use up their resources
    - Bots less likely to be detected / resented
- Not seen on any file or partition scans
  - Nothing obvious to delete
  - But any free space wiper will do it
- Disappears if you get cut off
  - No evidence left behind to worry about

Drawbacks

- Higher disk use
  - Shorter disk life
  - Will be slower if competing with host
- Data store is volatile
  - Host file system may allocate away “your” space
- Not for heavily used disks
  - High disk usage
  - Low free space
  - Defraggers, disk wipers, etc

Partial fixes

- Store redundantly
  - No chunk is critical - like RAID
  - Maintenance utility required
- Don't rely on it
  - Distribute data across computers - like Tahoe, Freenet
- Make the host try not to allocate “your” space
  - Drastically reduces volatility
  - Requires deeper hooks into host FS

Vulnerabilities

Utility may be a real file in host FS

- Could be stored on flash drive, loaded in RAM only

Free space is suspiciously “random”

- Many tools do “secure erase”; looks the same

Crypto layer still required

- This is just steganography

Disk is suspiciously busy when “not in use”

- Only if the maintenance utility is running…

Summary

A hidden data store that is:

- Unsuspicious
- Undetectable unless running
- Self-wiping if unused
- Compatible with vanilla partition setup
- Deferential to host

Let's talk

Sai Emrys ccc@saizai.com
GPG: D6D408A9
DECT 4724 (4-SAI)
AIM, IRC, LJ, Skype etc: saizai

https://www.noisebridge.net/wiki/FSFS

Shameless plug

18:30 Day 2, here – Make a language!
19:30, B04 – workshop

16:00 Day 4, C04 – Meditation workshop & Scientology inoculation