# The Dissident File System

Aneesh Neelam<aneelam@ucsc.edu>

# Introduction and Background

- Protect data: Encryption
- Hide data: Steganography

Both?

Dissident in a totalitarian state?

- File encryption?
- Disk encryption?
- Steganography? Files in files?

Must also have plausible deniability.

# Overview

Innocent files already on native file system. Sensitive files will be XORed with these.

Innocent files specific to dissident. Preferably compressed data like media files.

Cryptographically secure random number generator for offsets. ‘/dev/random’ on FreeBSD, Linux and OS X.

Offsets stored in a file-based database (BerkeleyDB)

DB file also XORed the same way. DB’s offset determined from SHA512 of a passphrase.

Written using FUSE, for most Unix-like/Unix-based system (OS X, Linux and FreeBSD)

Must not change underlying native file system.

# Evaluation

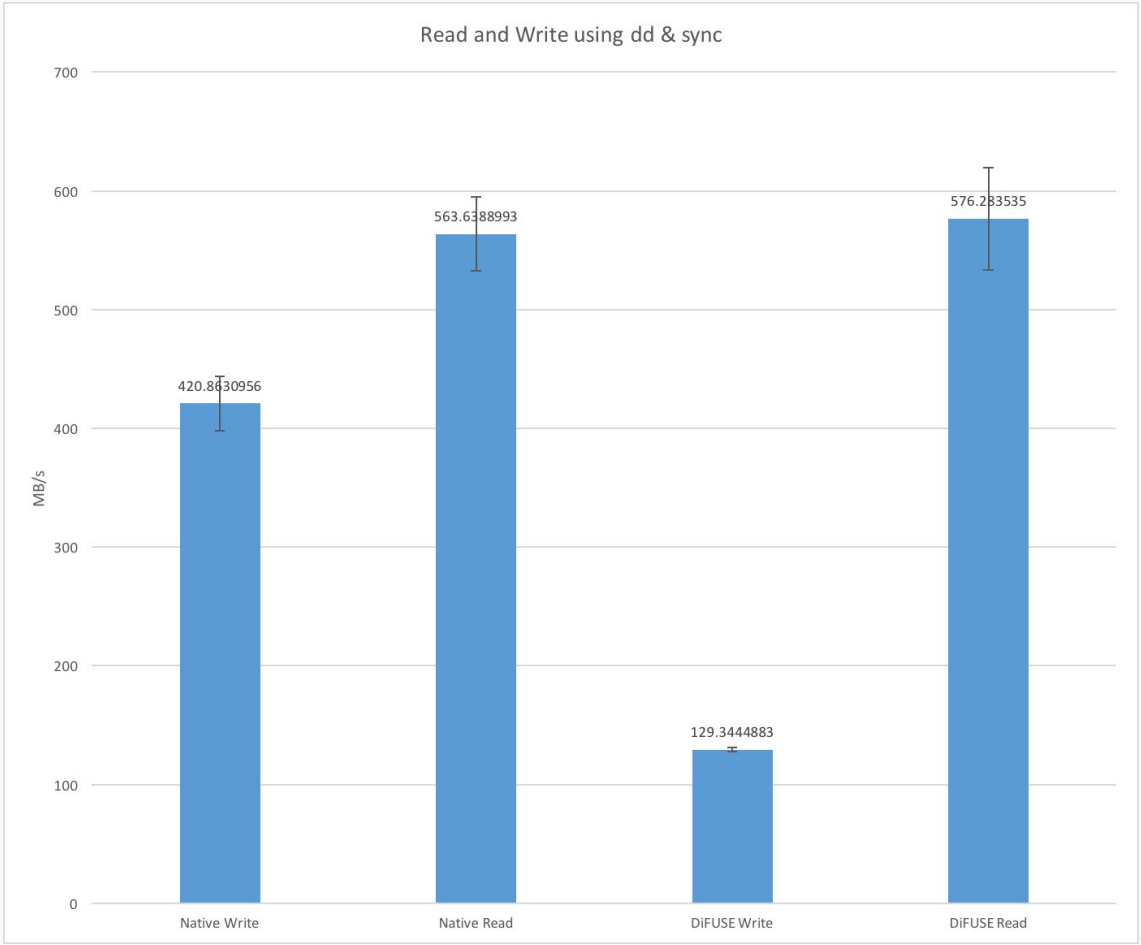
Performance

- dd & sync
- Bonnie++ (Preliminary results)

Analysis of Adversary and Threats

Some attack vectors

Tradeoffs




18 runs, dd & sync, 100k block size, 1000 blocks

# Adversary and Threats

Adversary? Government:

- Highly motivated
- Unlimited resources

Most powerful attack: Rubber hose.

- File on your computer I cannot read? Hit you until you give me a satisfactory explanation.

Reverse-engineer passphrase? Break SHA512.

Reverse-engineer offsets? Break Cryptographically Secure Random Number Generators (/dev/random)

Brute-force offsets? Maybe… depends on how many innocent files and how many sensitive files there are.

# Tradeoffs and Future Work

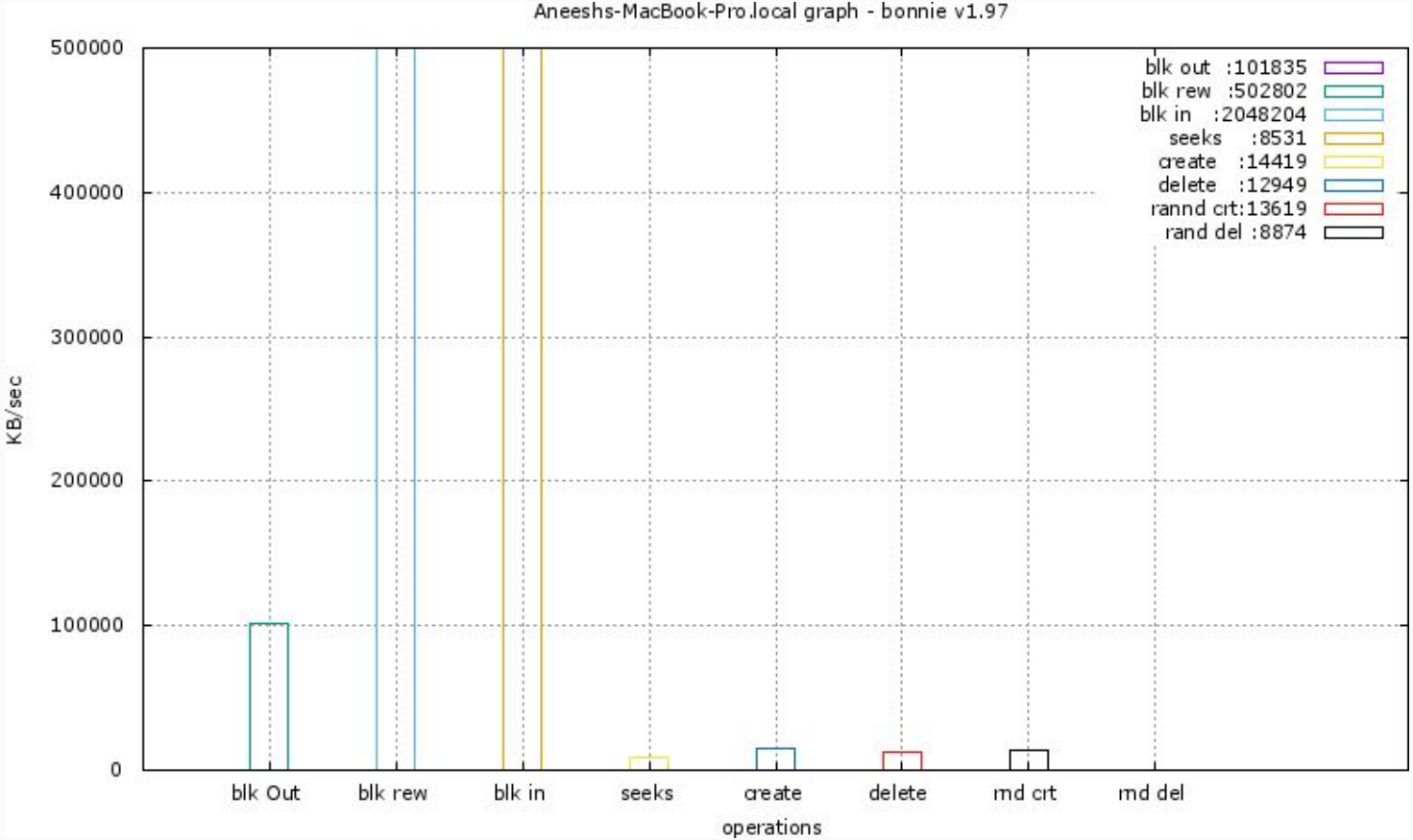
- XORed sensitive files still stored as files on the native file system.
- Data XORed with random data is also random, no matter what it is.
- Innocent files may not be truly random.

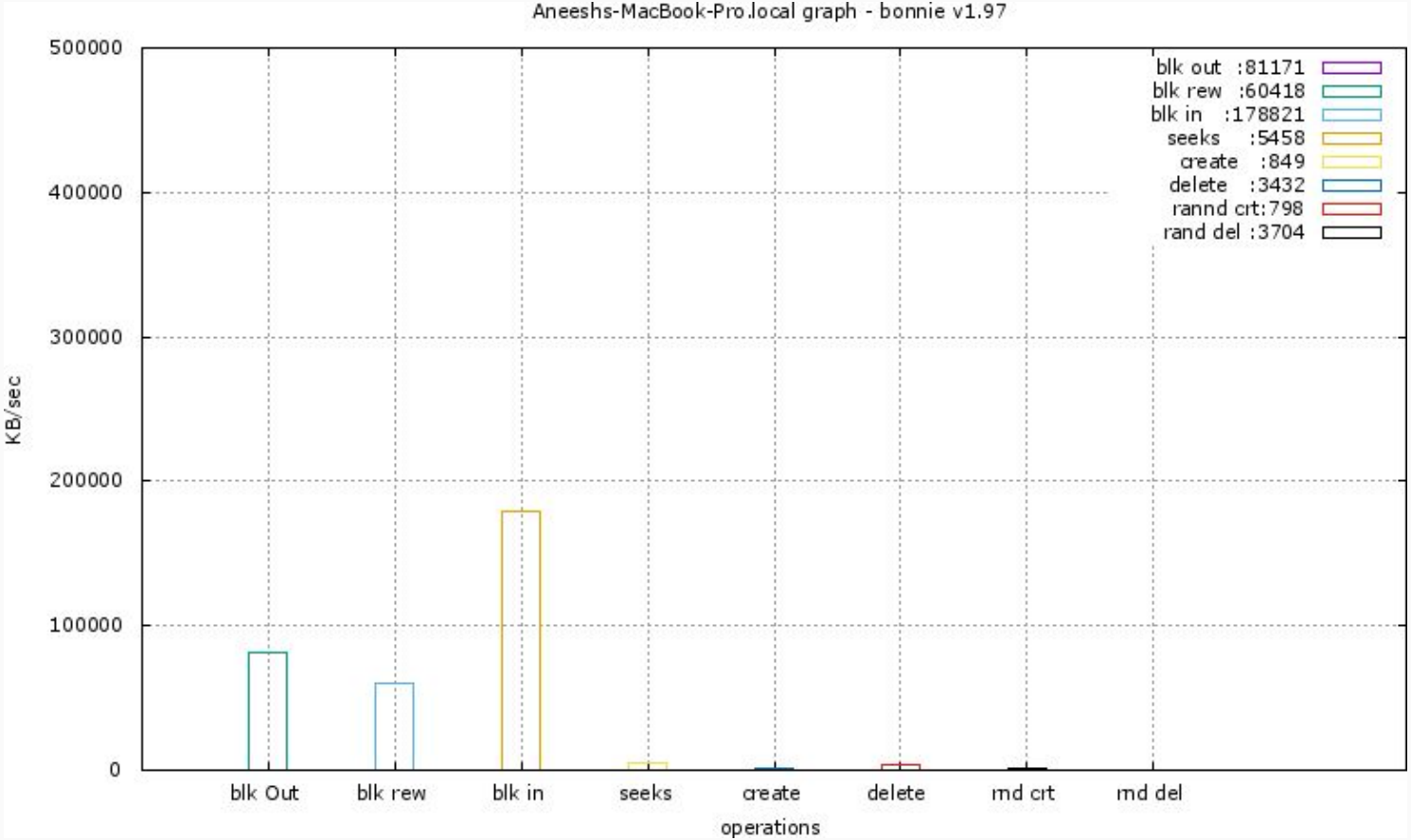
## What could be done?

- Store sensitive data in free space? Error correcting codes to prevent native file system from destroying data.
- Mark bad sectors, underlying file system won't touch those.
- Generate random data on the fly?

# Thank you

Questions?


Aneeshs-MacBook-Pro.local graph - bonnie v1.97
500000
400000
300000
200000
100000
0
KB/sec
blk out :101835
blk rew :502802
blk in :2048204
seeks :8531
create :14419
delete :12949
rannd crt:13619
rand del :8874
blk Out
blk rew
blk in
seeks
create
delete
md crt
md del
operations


Aneeshs-MacBook-Pro.local graph - bonnie v1.97
500000
400000
300000
200000
100000
0
KB/sec
blk out :81171
blk rew :60418
blk in :178821
seeks :5458
create :849
delete :3432
rannd crt:798
rand del :3704
blk Out
blk rew
blk in
seeks
create
delete
rnd crt
rnd del
operations