

combox

siddharth ravikumar

0x00B252AF

April 20, 2016

acknowledgments

Dr. Robert C. Green II

introduction

problem

proposed solution

testing

- unit testing

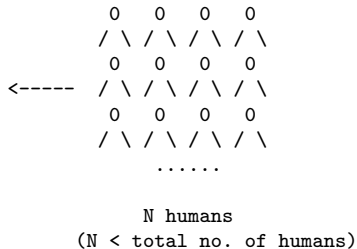
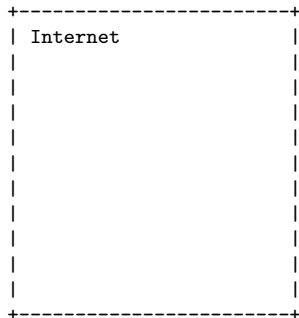
- manual testing

- stress testing

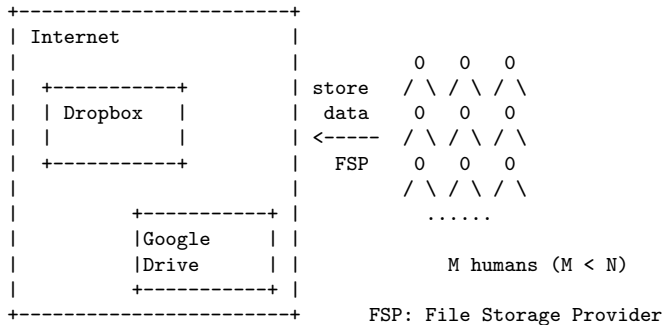
conclusion

pre-recorded demo

2016



2016



invariantly

Law & Order. We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights¹.

¹<https://www.dropbox.com/privacy>

2013

- ▶ ECHELON
- ▶ Carnivore
- ▶ XKeyscore
- ▶ Boundless Informant
- ▶ PRISM

problem

“L” folks are in trouble.

“L” are in trouble

data stored in FSP's² computers \neq private

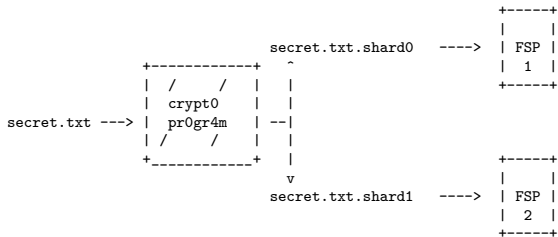
the last resort

encrypt everything!

not enough

our adversaries are too powerful.

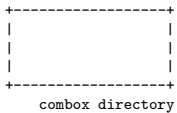
what if



FSP: File Storage Provider (Dropbox, Google Drive, etc).

enter combox

combox



computer i

combox

node directory 0
(dropbox)



combox directory

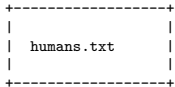


node directory 1
(google drive)

computer i

combox

node directory 0
(dropbox)



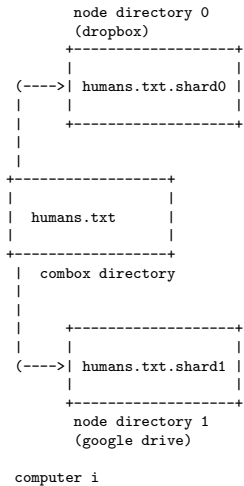
combox directory



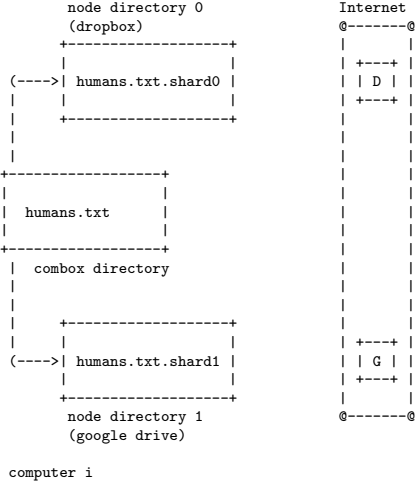
node directory 1
(google drive)

computer i

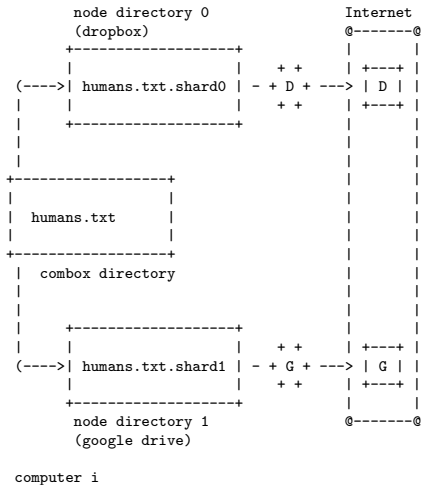
combox



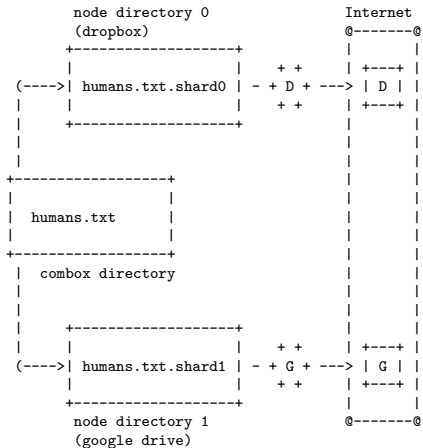
combox



combox



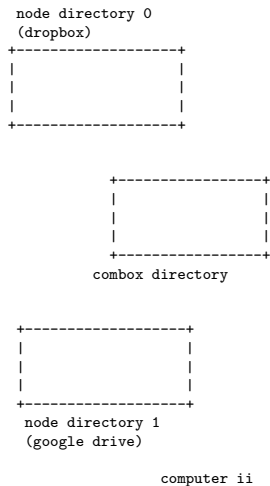
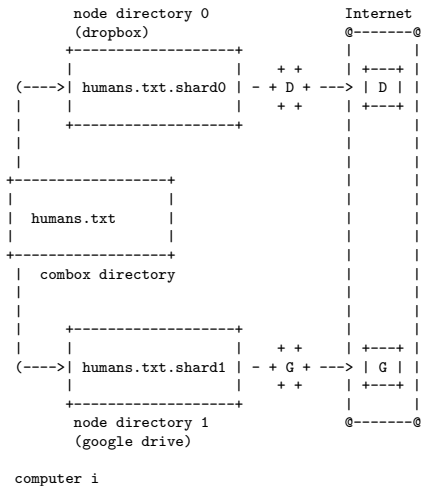
combox



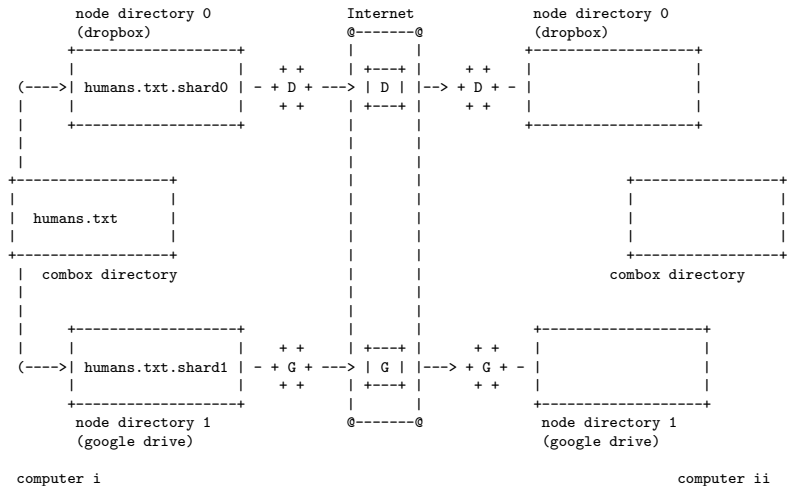
computer i

computer ii

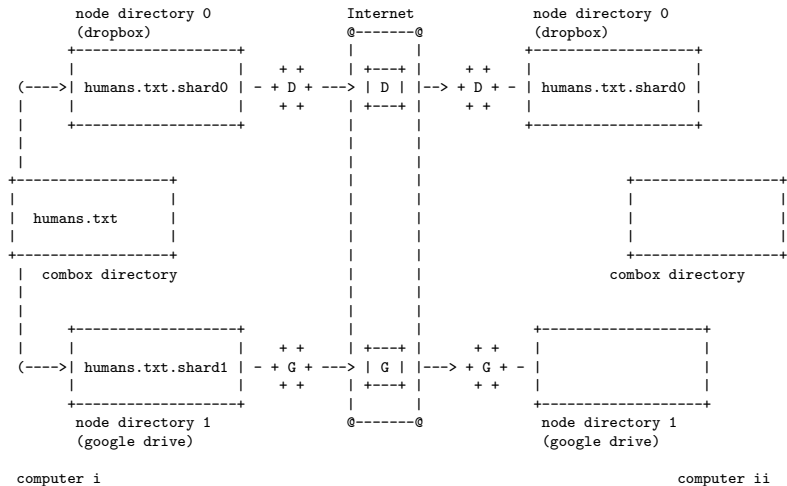
combox



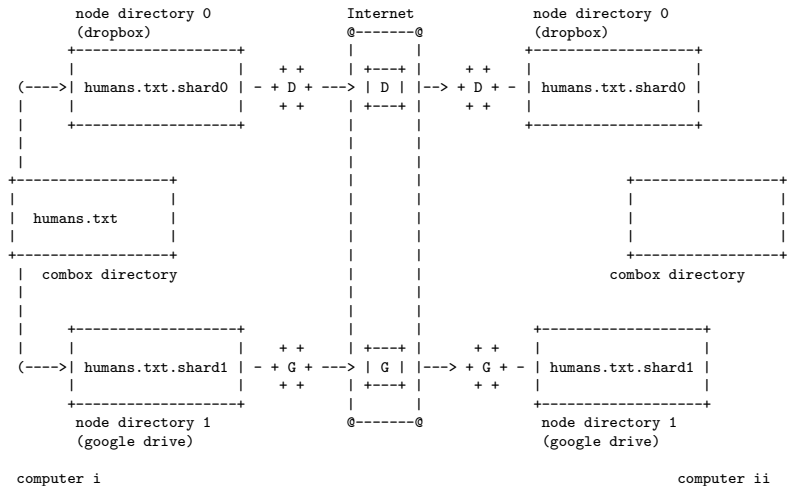
combox



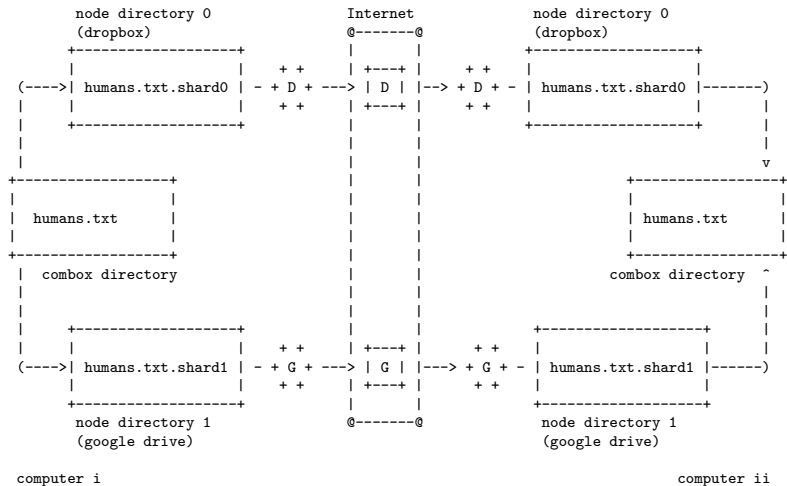
combox



combox



combox



Vollmar's Combo-Box

- ▶ C#

Vollmar's Combo-Box

- ▶ C#
- ▶ SQL for tracking files

Vollmar's Combo-Box

- ▶ C#
- ▶ SQL for tracking files
- ▶ Microsoft Windows program

combox

- ▶ python

combox

- ▶ python
- ▶ key-value data store for tracking files

combox

- ▶ python
- ▶ key-value data store for tracking files
- ▶ python package, runs on GNU/Linux and OS X

testing

testing

- ▶ unit testing
- ▶ manual testing
- ▶ stress testing

unit testing

unit testing

- ▶ nose testing frame work

unit testing

- ▶ nose testing frame work
- ▶ not pure TDD

unit testing

- ▶ nose testing frame work
- ▶ not pure TDD
- ▶ benefits?

benefits

- ▶ immediatly verify correctness for “N” use cases.

benefits

- ▶ immediatly verify correctness for “N” use cases.
- ▶ was useful when testing compatibility on OS X.

benefits

- ▶ immediatly verify correctness for “N” use cases.
- ▶ was useful when testing compatibility on OS X.

```
$ nosetests
```

```
.....
```

```
-----  
Ran 35 tests in 62.159s
```

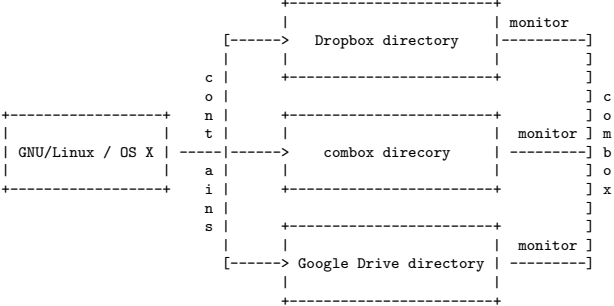
```
OK
```

manual testing

manual testing

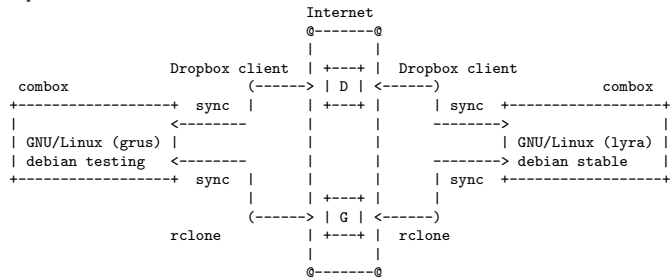
- ▶ combox on two GNU/Linux machines.
- ▶ combox on GNU/Linux and OS X
- ▶ combox on GNU/Linux and OS X with USB stick as the third node.

manual testing



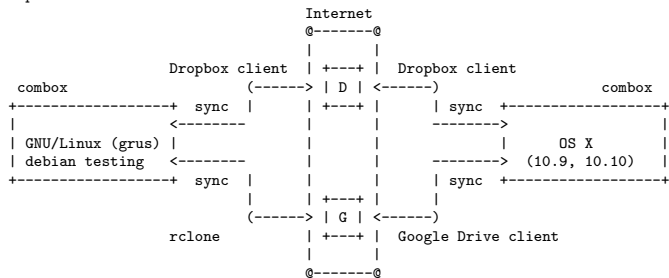
manual testing

setup i



manual testing

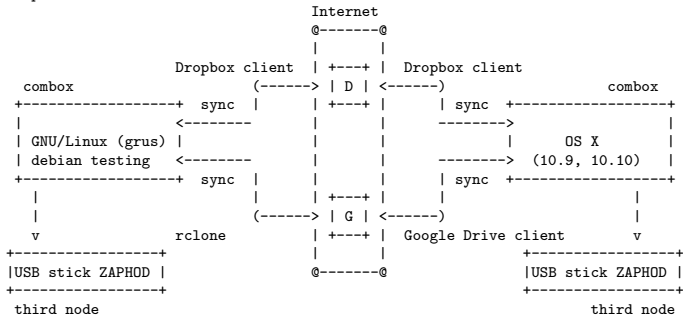
```
setup ii
```



```
found bugs #5, #6, #7, #10, #11
(git.ricketyspace.net/combox/plain/TODO.org)
```

manual testing

setup iii



- modified shard on usb stick must be "touch".
- file rename/move does not work.

stress testing

stress testing

```
1 second delay
  +----+
  |    |
  v    v
- F - -1s- - F - -1s- - F - -1s- - F -
  -     -     -     -     -     -     -1s-
----->----->----->----->
dump script

-
- F - 20MiB - 90MiB file
-
avg. file size 60MiB

-
- F -
-
|
| - - - - |
| - F - - F - |
| - - - - |
+-----+
combox directory
```

git.ricketyspace.net/combox-paper/tree/dumper/dump

1620MiB dump - 27 files

1620MiB dump - 27 files

avg. time to split and encrypt → 2670.59ms

1620MiB dump - 27 files

avg. time to split and encrypt → 2670.59ms

total time to process all files → 02m:22s

5940MiB dump - 99 files

5940MiB dump - 99 files

avg. time to split and encrypt → 2979.64ms (↑ 309.049ms)

5940MiB dump - 99 files

avg. time to split and encrypt → 2979.64ms (↑ 309.049ms)

total time to process all files → 09m:10s (↑ 6m:48s)

10800MiB dump - 180 files

10800MiB dump - 180 files

avg. time to split and encrypt → 3423.08ms (↑ 443.440ms)

10800MiB dump - 180 files

avg. time to split and encrypt → 3423.08ms (↑ 443.440ms)

total time to process all files → 18m:04s (↑ 8m:54s)

conclusion

conclusion

- ▶ combox v0.2.3

conclusion

- ▶ combox v0.2.3
- ▶ python package (python.org/pypi/combox)

conclusion

- ▶ combox v0.2.3
- ▶ python package (python.org/pypi/combox)
- ▶ licensed under GNU General Public license version 3 or later

conclusion

- ▶ combox v0.2.3
- ▶ python package (python.org/pypi/combox)
- ▶ licensed under GNU General Public license version 3 or later
- ▶ compatible with GNU/Linux and OS X

conclusion

- ▶ combox v0.2.3
- ▶ python package (python.org/pypi/combox)
- ▶ licensed under GNU General Public license version 3 or later
- ▶ compatible with GNU/Linux and OS X
- ▶ in “alpha” stage

conclusion

- ▶ combox v0.2.3
- ▶ python package (python.org/pypi/combox)
- ▶ licensed under GNU General Public license version 3 or later
- ▶ compatible with GNU/Linux and OS X
- ▶ in “alpha” stage
- ▶ rickety.space.net/combox

conclusion

- ▶ combox v0.2.3
- ▶ python package (python.org/pypi/combox)
- ▶ licensed under GNU General Public license version 3 or later
- ▶ compatible with GNU/Linux and OS X
- ▶ in “alpha” stage
- ▶ ricketyspace.net/combox
- ▶ git.ricketyspace.net/combox

pre-recorded demo

rickety.space.net/combox/demo.webm

Slides under public domain. No rights reserved. See
<https://creativecommons.org/publicdomain/zero/1.0/> for full
legal verbiage.

Source at <https://git.ricketyspace.net/combox-paper/tree/presentation>