

combox

Siddharth Ravikumar

0x00B252AF

April 20, 2016

Acknowledgments

Dr. Robert C. Green II

(cons 'combox 'presentation)

Introduction

Problem

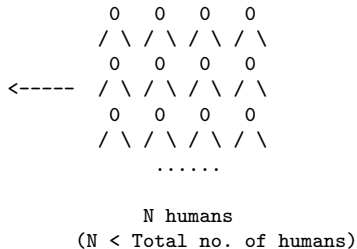
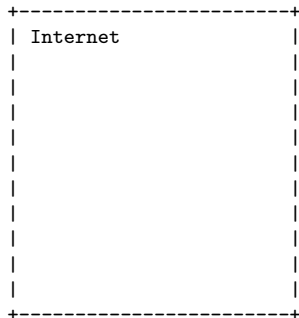
Proposed Solution

Benchmarks

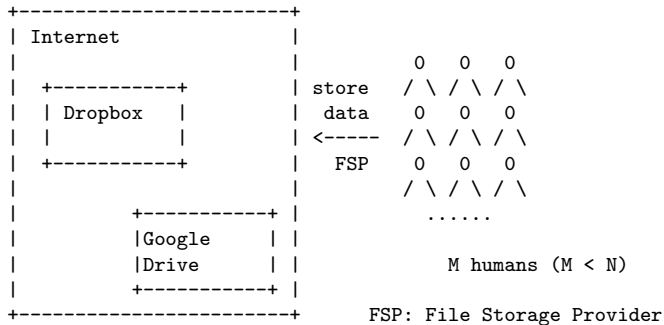
Testing

Conclusion

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

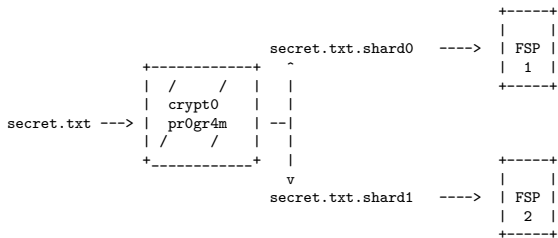
The last resort

Encrypt everything!

Not Enough

Our Adversaries are too powerful.

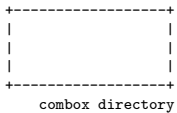
What if



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

Enter combox

combox



Computer I

combox

node directory 0
(dropbox)



combox directory

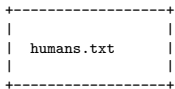


node directory 1
(google drive)

Computer I

combox

node directory 0
(dropbox)



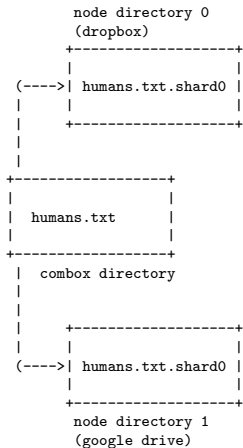
combox directory



node directory 1
(google drive)

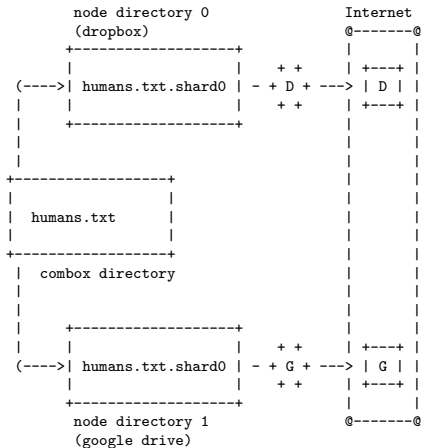
Computer I

combox



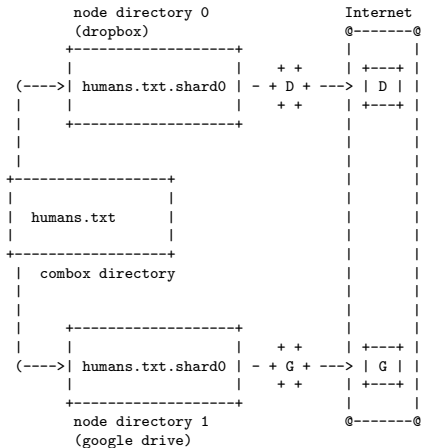
Computer I

combox



Computer I

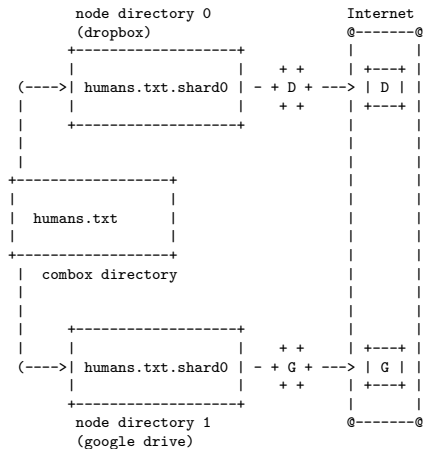
combox



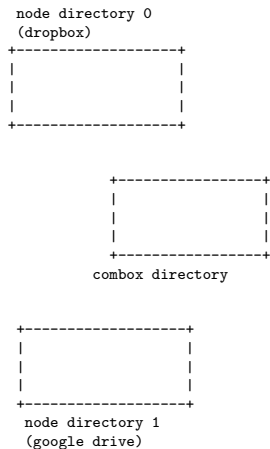
Computer I

Computer II

combox

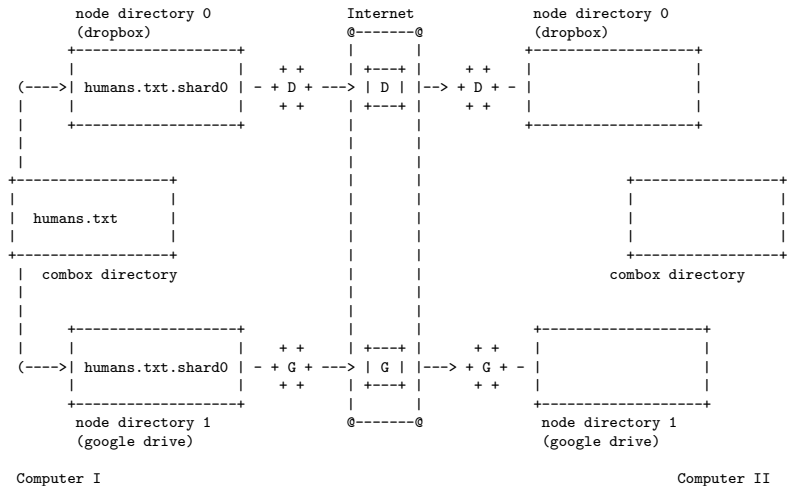


Computer I

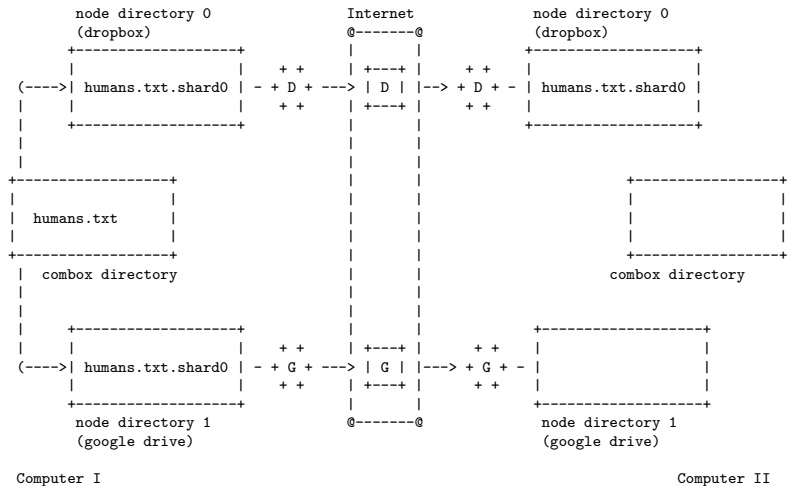


Computer II

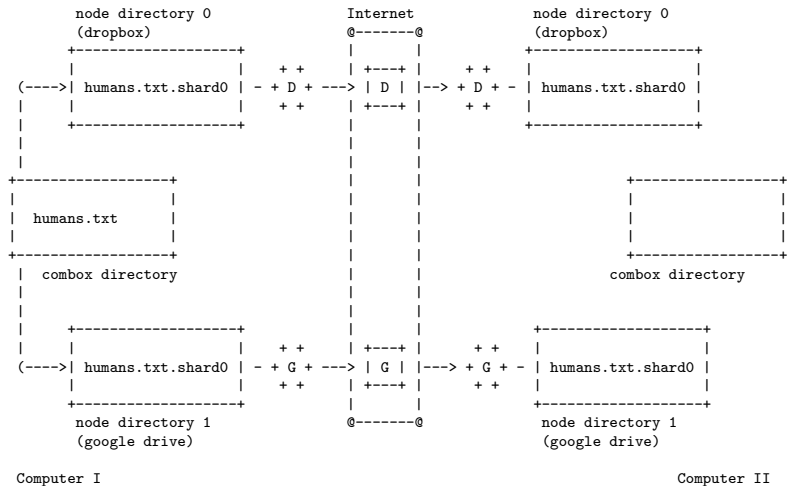
combox



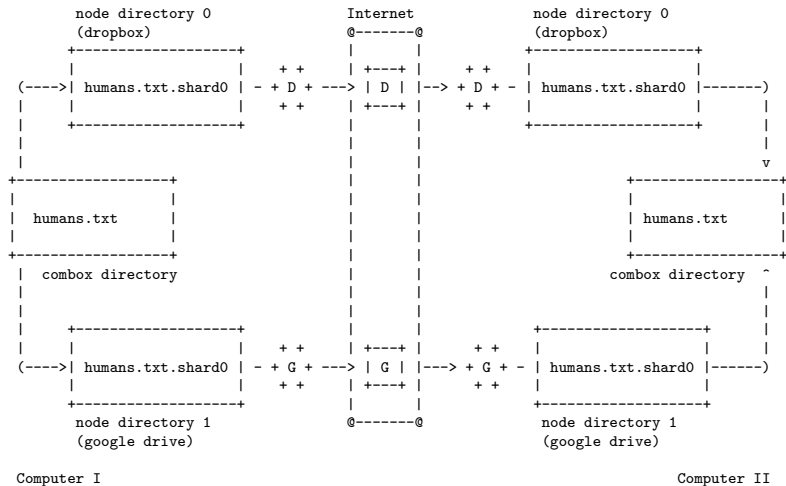
combox



combox



combox



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>