combox

Siddharth Ravikumar

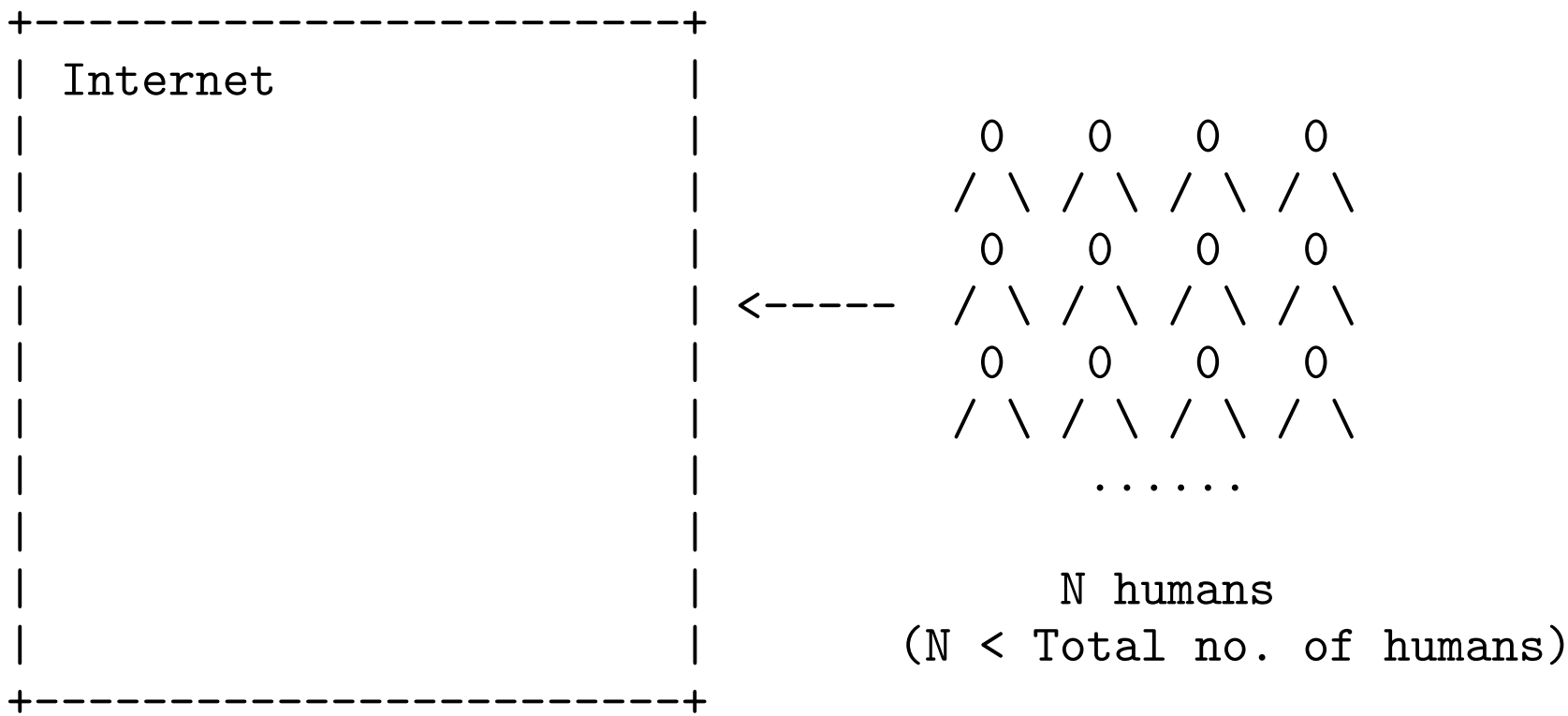
0x00B252AF

April 20, 2016

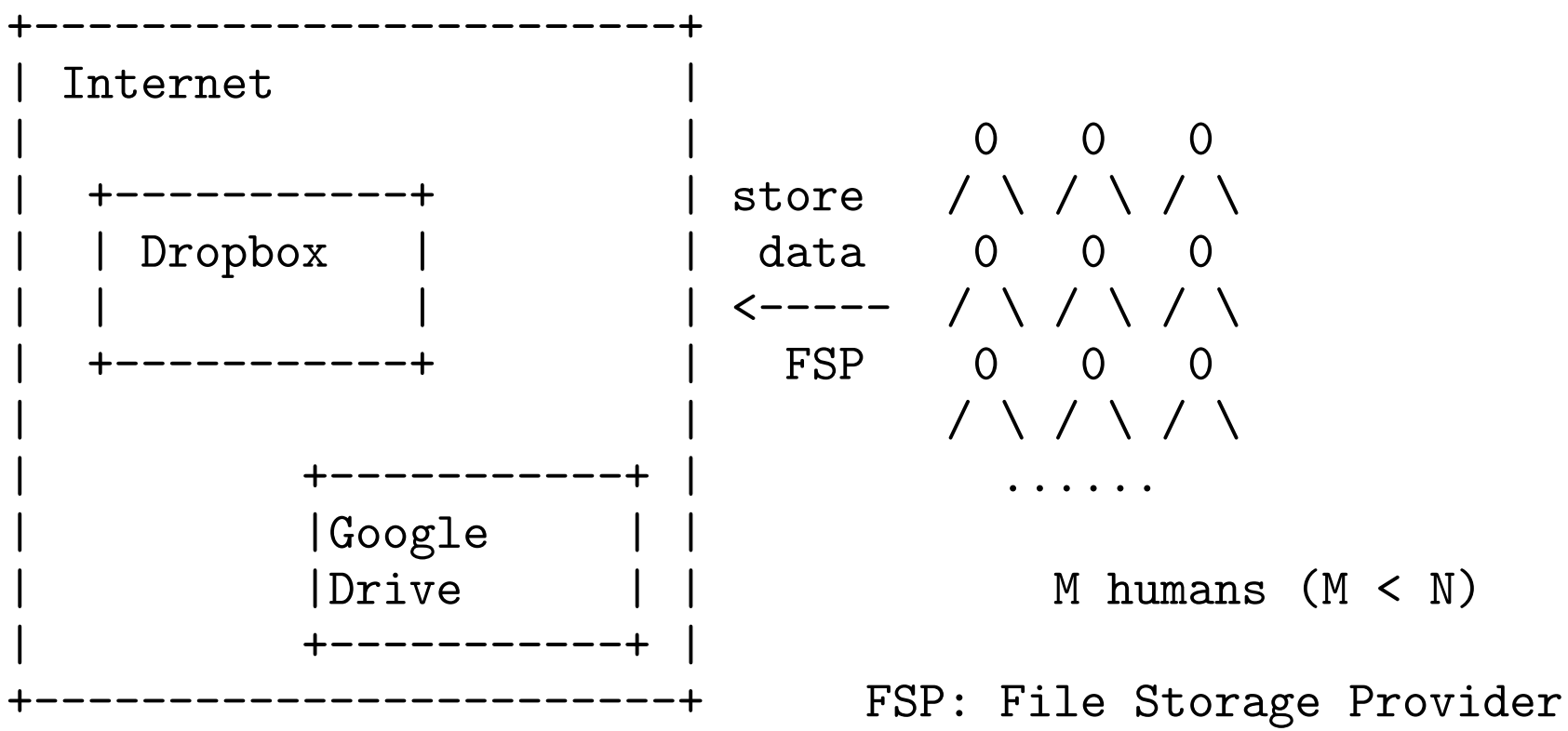
(cons 'combox 'presentation)

- Introduction
- Problem
- Proposed Solution
- Benchmarks
- Testing
- Conclusion

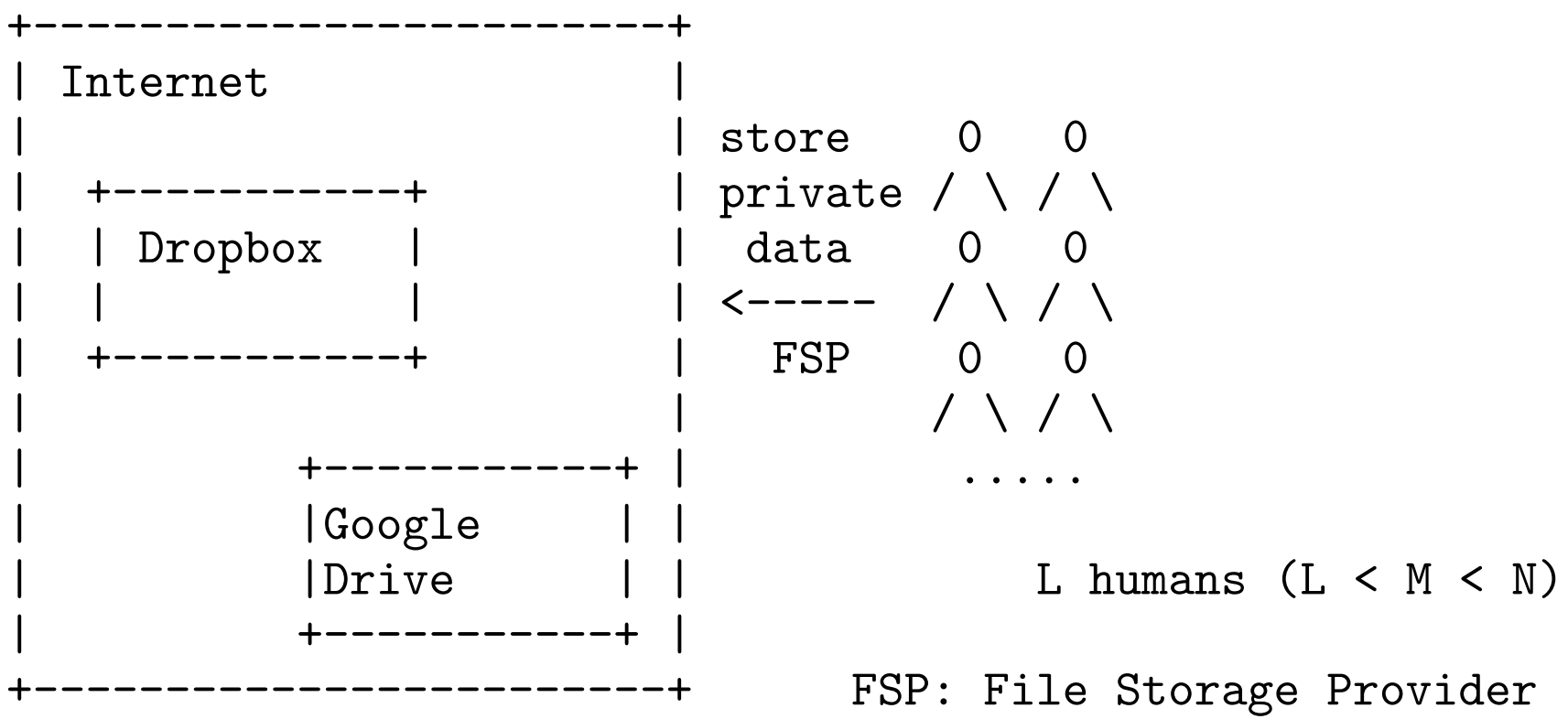
2016



2016


Internet
Dropbox
Google
Drive
store
data
<-----
FSP
M humans (M < N)
FSP: File Storage Provider

2016


Internet
Dropbox
Google
Drive
store
private
data
<-----
FSP
0 0
/ \ / \
.....
L humans (L < M < N)
FSP: File Storage Provider

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 rights[1].

[1] https://www.dropbox.com/privacy

2013

- ECHELON
- Carnivore
- XKeyscore
- Boundless Informant
- PRISM

Problem

"L" folks are in trouble.

“L” are in trouble

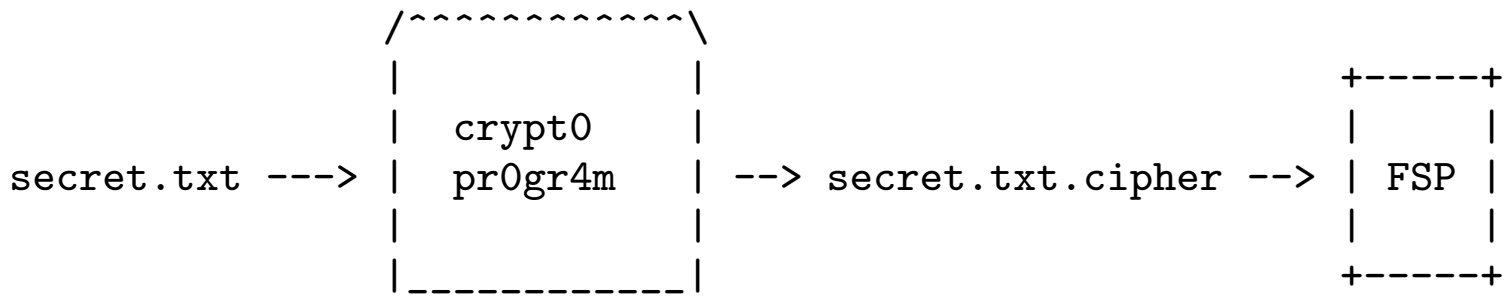
Data stored in FSP’s[2] computers $\neq$ Private

[2]FSP: File Storage Provider

The last resort

Encrypt everything!

Encrypt everthing

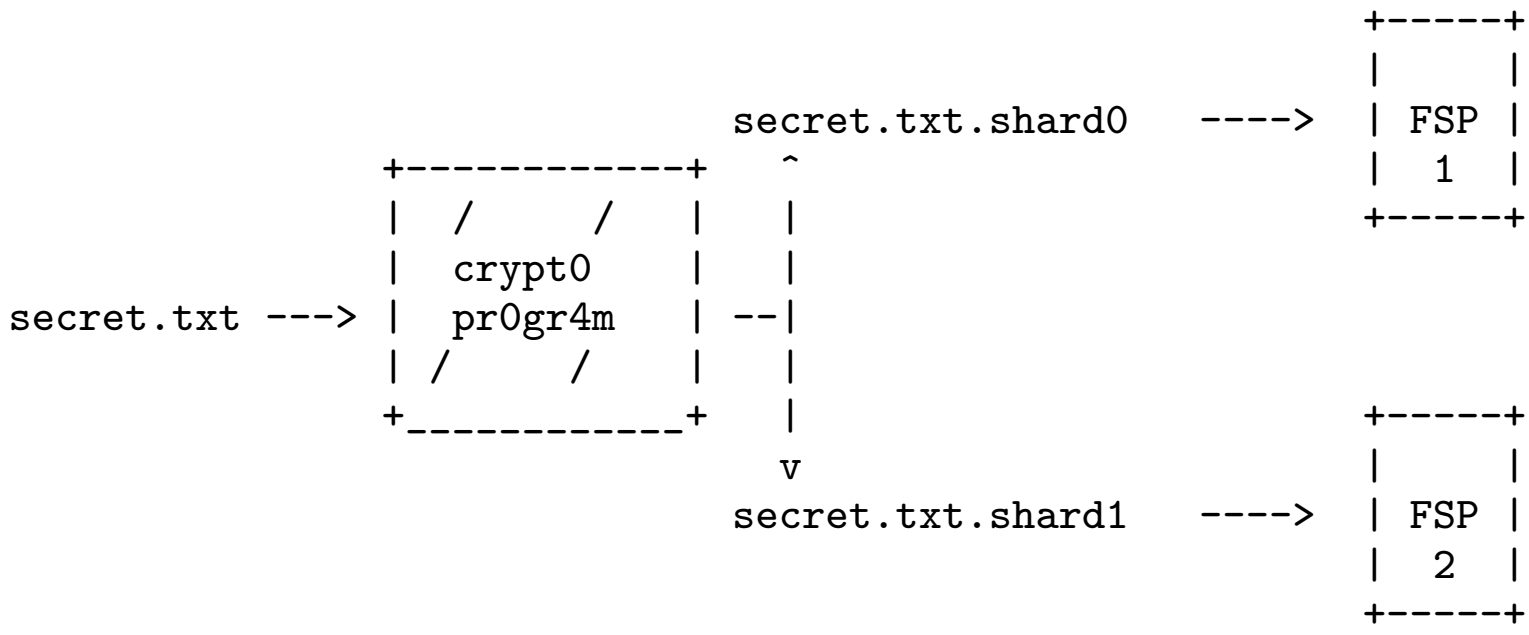


FSP: File Storage Provider (Dropbox, Google Drive, etc).

Not Enough

Our Adversaries are too powerful.

What if



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

Enter combox.

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