Cloud Storage Security & Privacy

whoami

secure
sba-research.org

starWarsVI = return new Jedi();

2012
TROOPERS
MAKE THE WORLD A SAFER PLACE

WTF are we talking about?

Cloud Storage

Cloud Storage

Cloud Storage

Cloud Storage

"It was much nicer before people started storing all their personal information in the cloud."

Why cloud storage?

Price

Why cloud storage?

Scalable

Why cloud storage?

Access anywhere

Cool stuff

Delta sync
Sharing
LAN P2P

Skipping over details

…kinda the idea of cloud

Oh by the way…

APT DLP FBI CIA ANTIVIRUS CYBERWAR WIKILEAKS ANONYMOUS
CLOUD CLOUD CLOUD CLOUD CLOUD CLOUD CLOUD CLOUD CLOUD
memegenerator.net

Challenge: Crypto

Where can you encrypt?

Encryption on client

Pro: No key escrow
Contra: Sharing, recovery

Encryption by provider

Pro: Sharing, recovery
Contra: Escrow (MAFIAA)

Encryption by provider

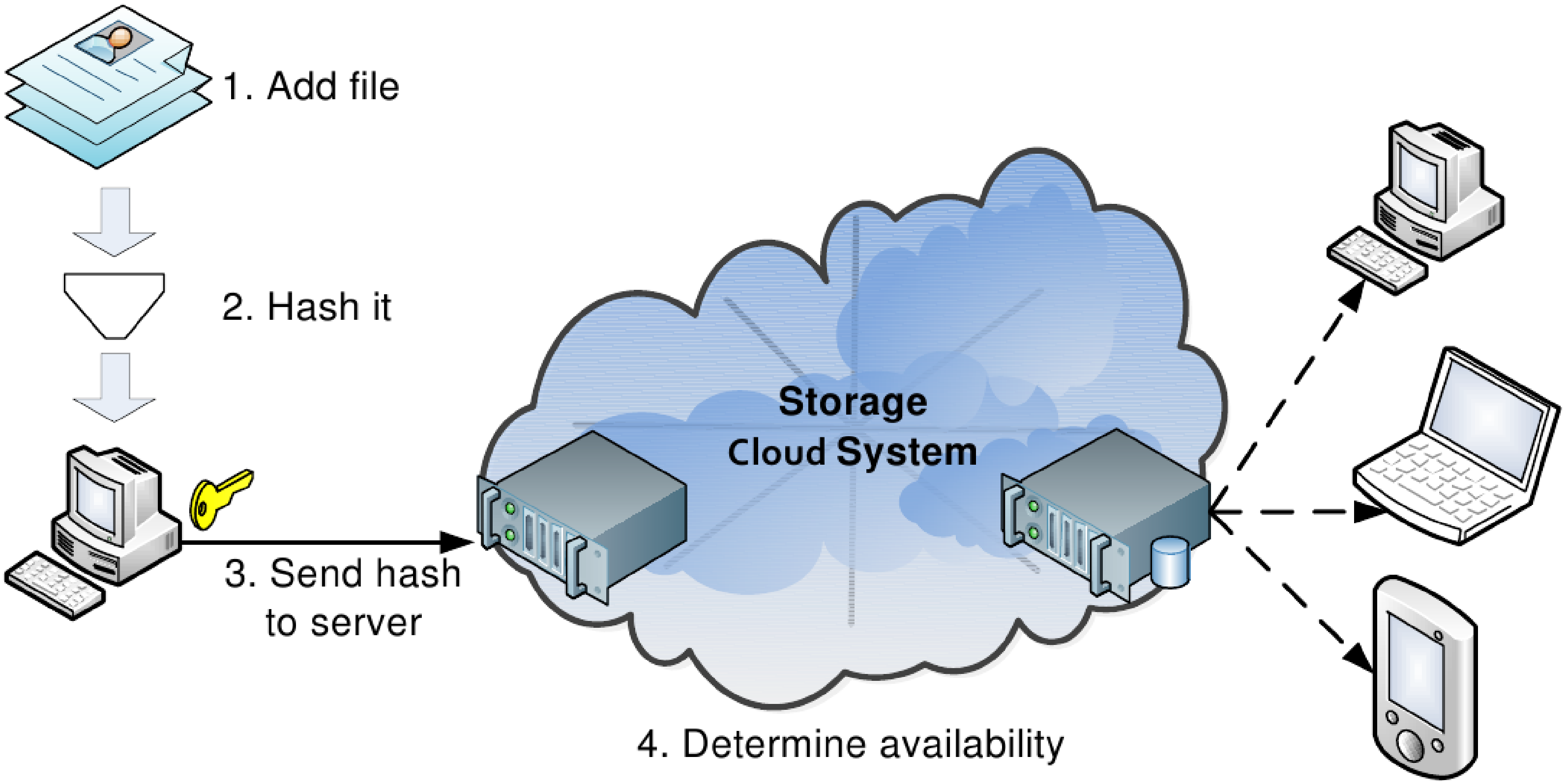
NOT SURE IF
SECURITY
OR COMPLIANCE
memegenerator.net

Deduplication

Save storage & traffic!

(at the cost of security)

Traffic deduplication



Storage deduplication

Same concept in storage

BROKE DROPBOX
BEFORE IT WAS COOL
memegenerator.net

Timeline

- 01. 10. 2010: CERT.fi contact
- 21. 10. 2010: Paper draft forwarded to Dropbox
- 27. 10. 2010: CERT.fi: Dropbox “is investigating”

----- March 2011: Hell breaks loose ---

- 12. 04. 2011: People send hashes & I DL stuff
- 13. 04. 2011: Dropbox mails us
- 24. 04. 2011: Temp fix in place
- [soon after]: All fixed, but PR damage done

Moral of the story:
Post exploits and startups listen.

Dropbox

S3 storage
EC2 transparent AES-256
Deduplication (SHA256)
4MB chunks

Our vectors

Hash Manipulation

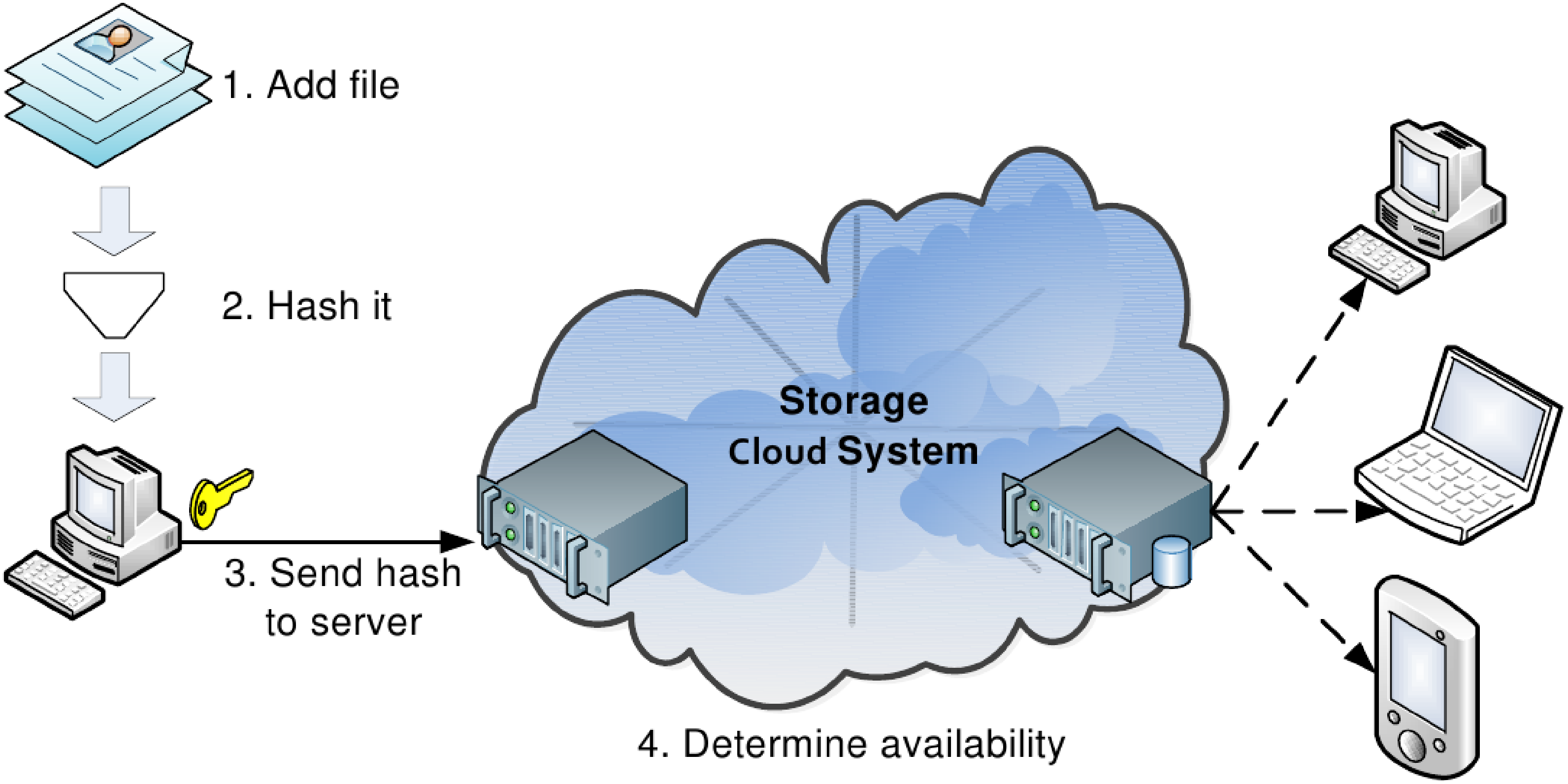
Stolen Host ID

“Cloud Slack Space”

Hash Manipulation

Attack on traffic deduplication

Traffic deduplication



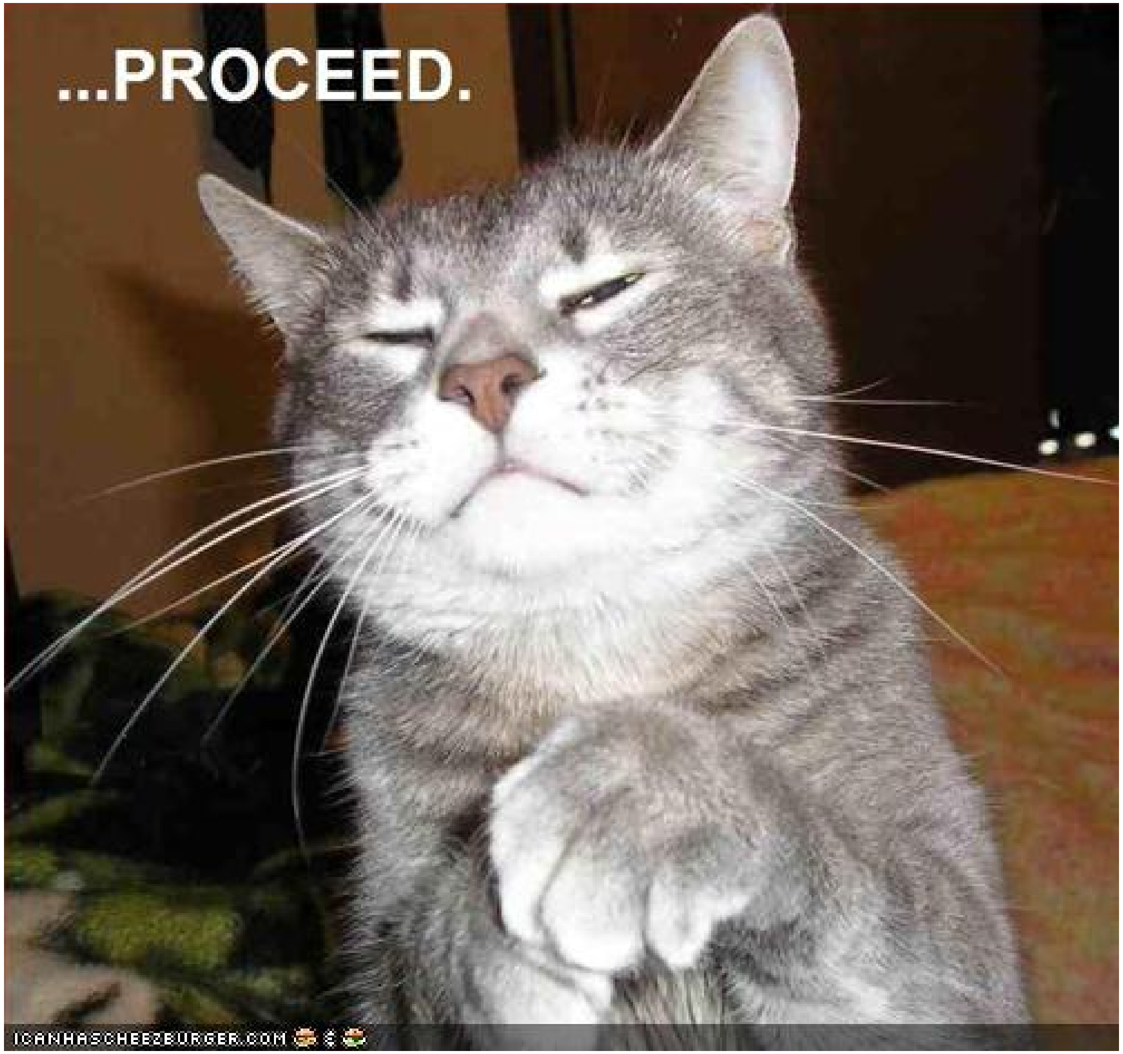
Attack

Client computes SHA256

Attack

Client ~~computes~~ SHA256 fakes

...got data we don't actually own...



More effective

https://dl-clientXX.dropbox.com/retrieve
hash=46983468573180109806

Side notes…

2^256 is HUGE

Torrents use SHA1

Rapidshare-over-Dropbox!

Host ID

512 bit string
Credentials after setup

Problems

Stored unencrypted etc
Grab & impersonate

Side notes…

Not transferred in clear (*cough*NDSS*cough*)

Dropbox file upload (2010)

“I wanna upload XX!”

“Give me chunks XXY and XXZ.”

[store]

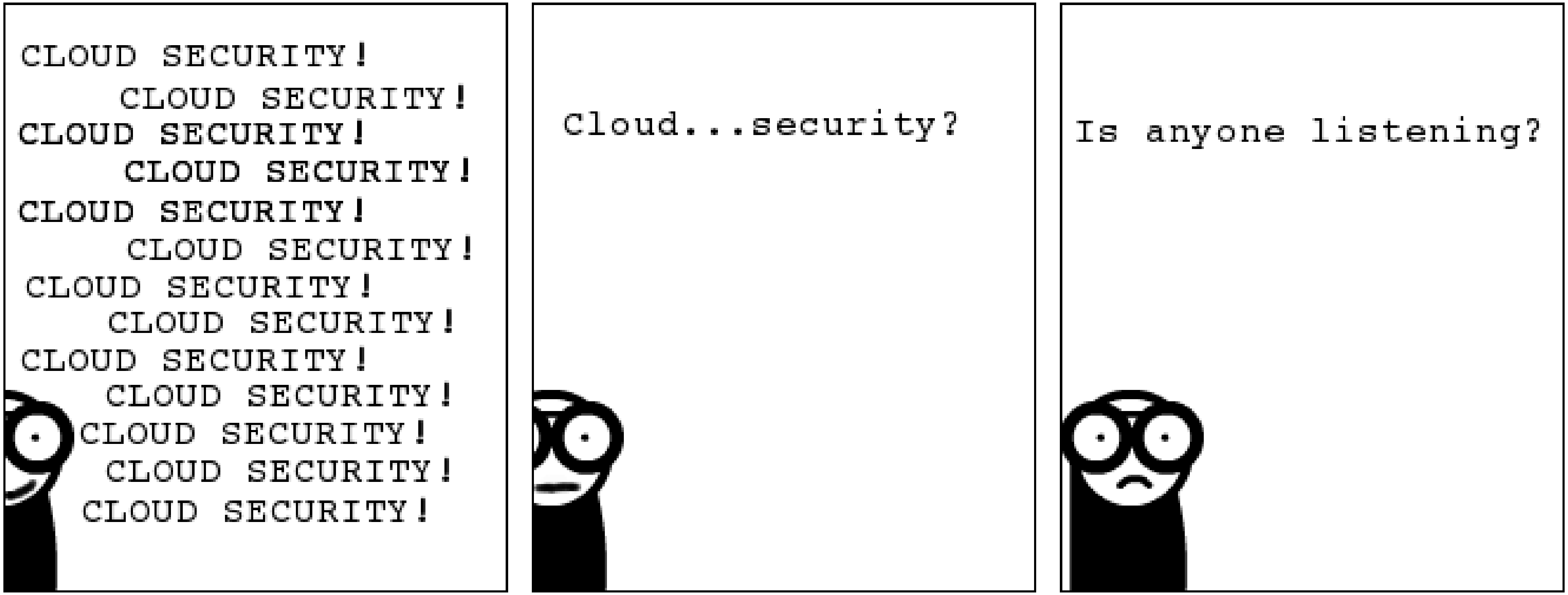
“I wanna upload XX!”

[link to account]

Hackers are lazy

[store]

m-(


CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
CLOUD SECURITY!
Cloud...security?
Is anyone listening?

Effects

Unlimited space
Push data to other accounts

Billy is here!

Deletion

When are chunks deleted?

Deletion

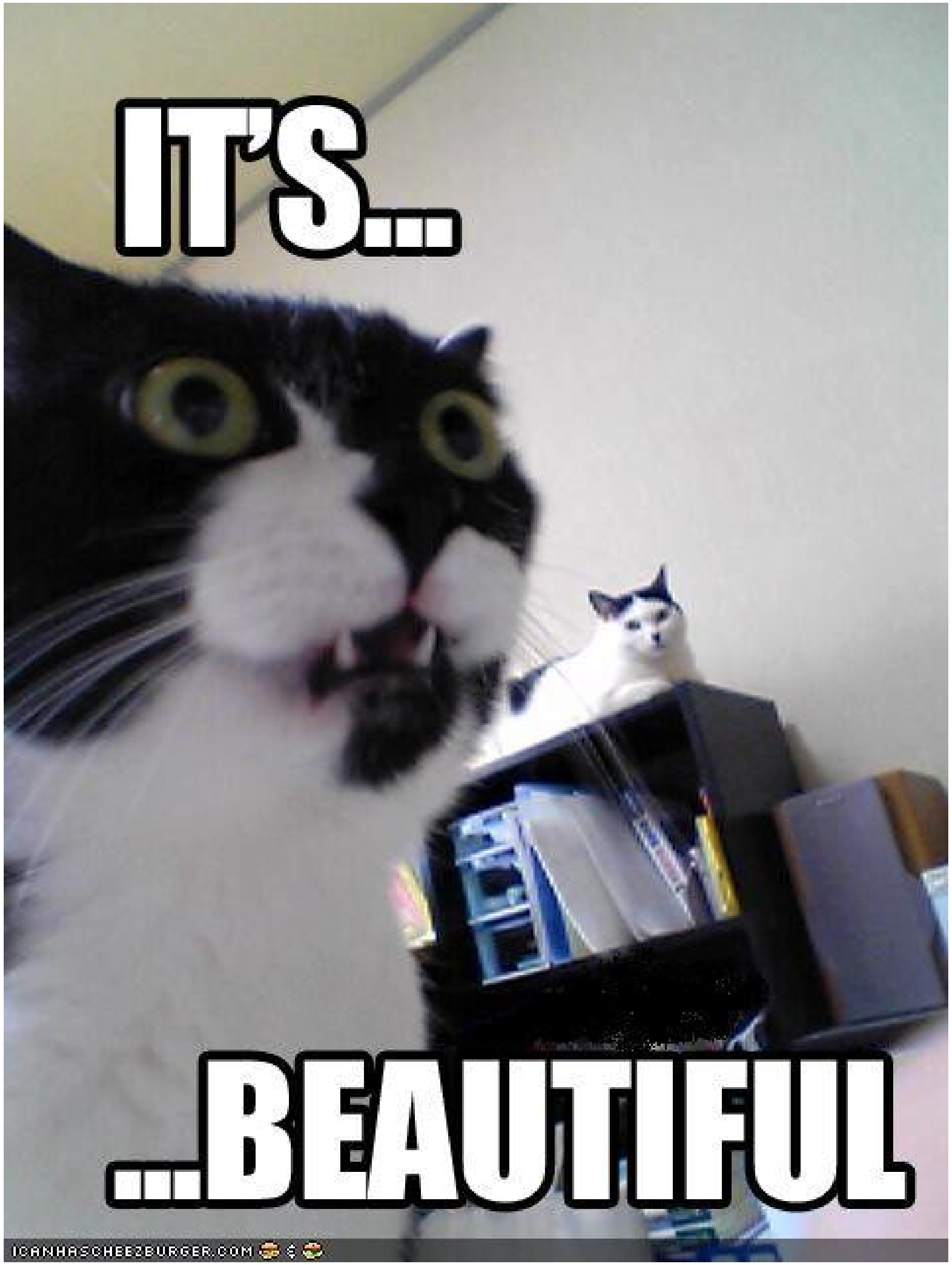
Piracy, yarr!

“Backups”

Pirate Bay's Top 100 on Dropbox?

“Backups”

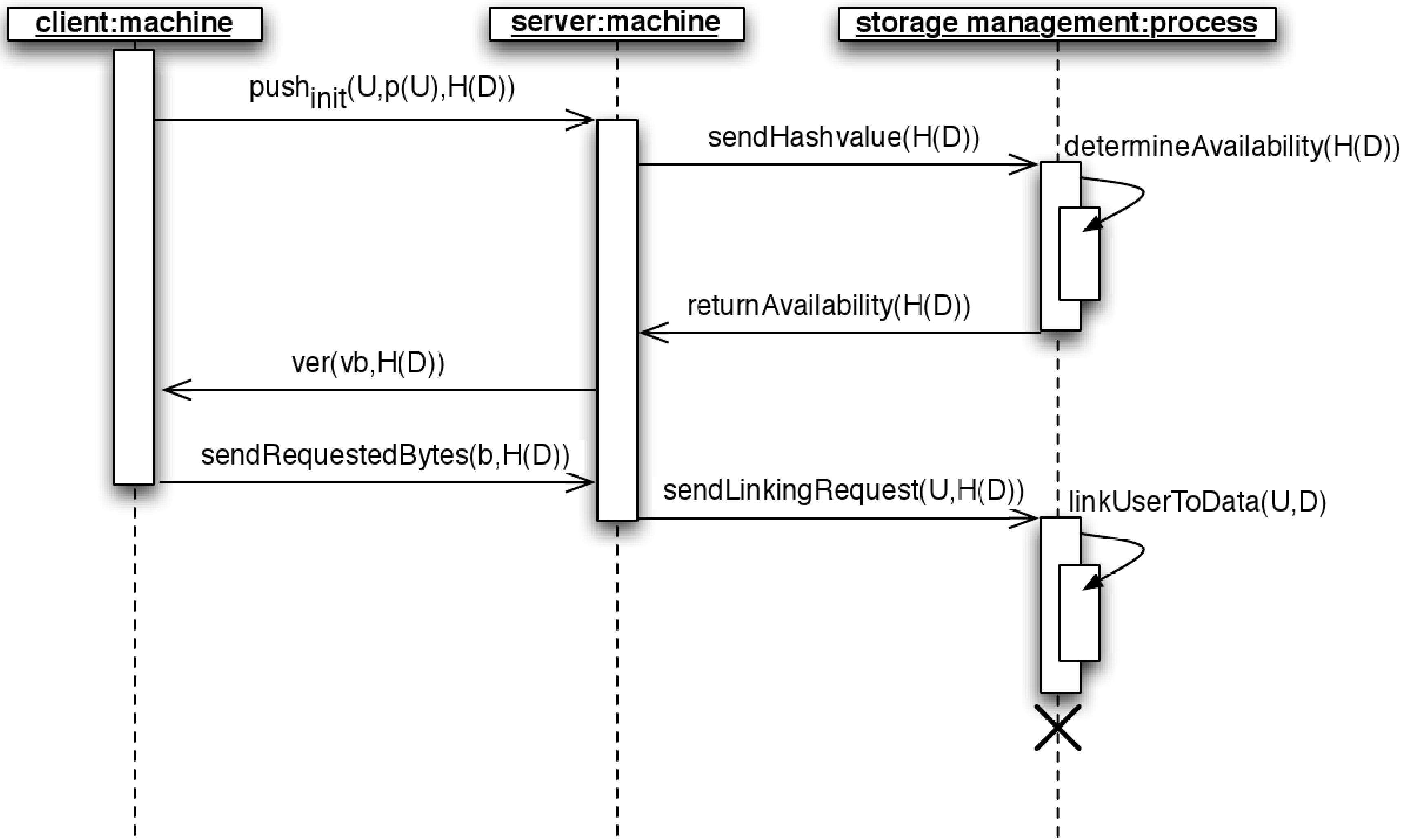
Yep, 97%


IT'S...
...BEAUTIFUL
ICANHASCHEEZBURGER.COM

Getting deduplication right

Data possession protocol

Data possession protocol



Confusing graphs suck

Verify ownership:
Sending a few bytes

What Dropbox did

Encrypted host_id
Disabled traffic deduplication
Removed unlinked file vuln

Also…

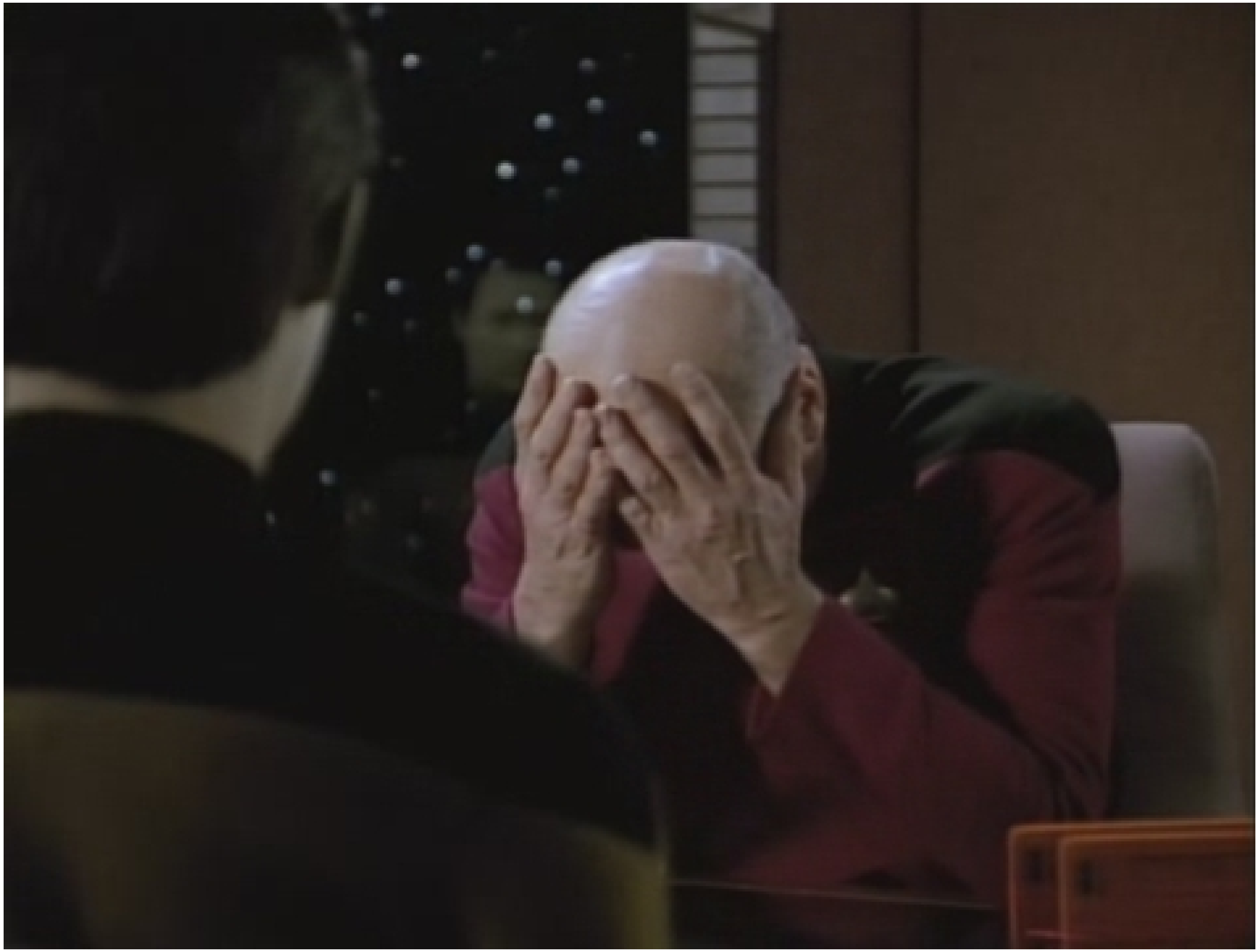
Do what you say
Be transparent
Don't kill useful bugs ;)

OMG the shouty man again!

QUBE Mini Wall of Sheep

fgj-87HJ
Titona12
Enorm2009

The FAIL is so strong



FIN

mleithner@sba-research.org

"Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space”

"Guess Who Is Texting You? Evaluating the Security of Smartphone Messaging Applications"