Browser Encryption

Nick Skelsey / The Hermes Center for Transparency and Digital Human Rights / 9.2016

GlobaLeaks

A platform that anonymizes Whistleblowers as they transmit information to an organization.

filtra.la

bez korupce

EDIƧOИ

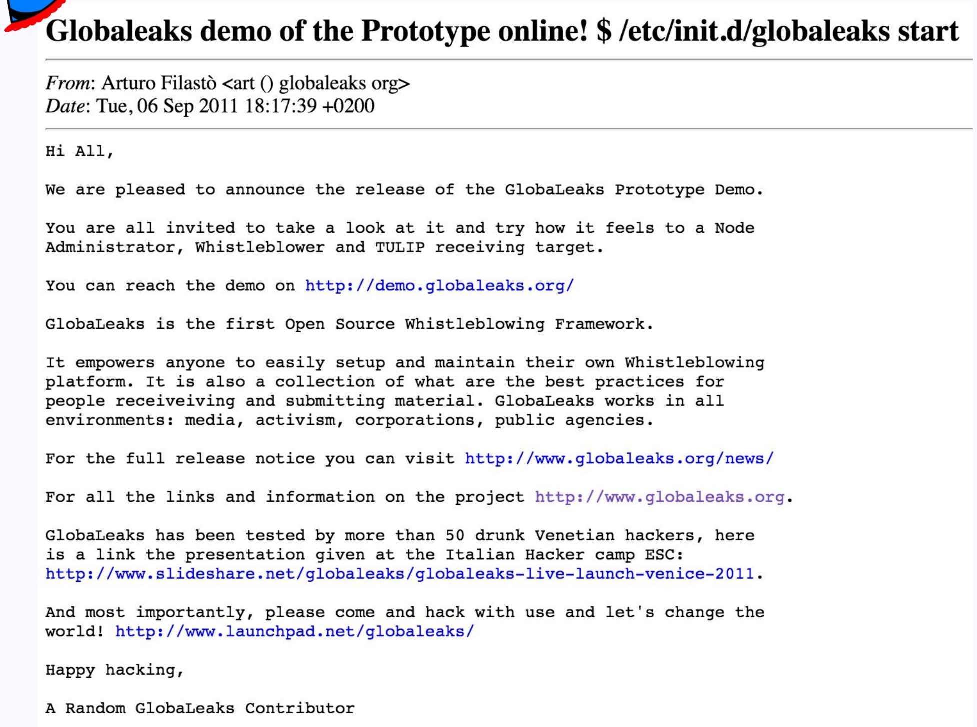
ecuador TRANSPARENTE

AMNESTY INTERNATIONAL

Leaks

+25

This project is 5



Globaleaks demo of the Prototype online! $ /etc/init.d/globaleaks start

From: Arturo Filastò <art () globaleaks org>
Date: Tue, 06 Sep 2011 18:17:39 +0200

Hi All,

We are pleased to announce the release of the GlobaLeaks Prototype Demo.

You are all invited to take a look at it and try how it feels to a Node Administrator, Whistleblower and TULIP receiving target.

You can reach the demo on http://demo.globaleaks.org/

GlobaLeaks is the first Open Source Whistleblowing Framework.

It empowers anyone to easily setup and maintain their own Whistleblowing platform. It is also a collection of what are the best practices for people receiveiving and submitting material. GlobaLeaks works in all environments: media, activism, corporations, public agencies.

For the full release notice you can visit http://www.globaleaks.org/news/

For all the links and information on the project http://www.globaleaks.org.

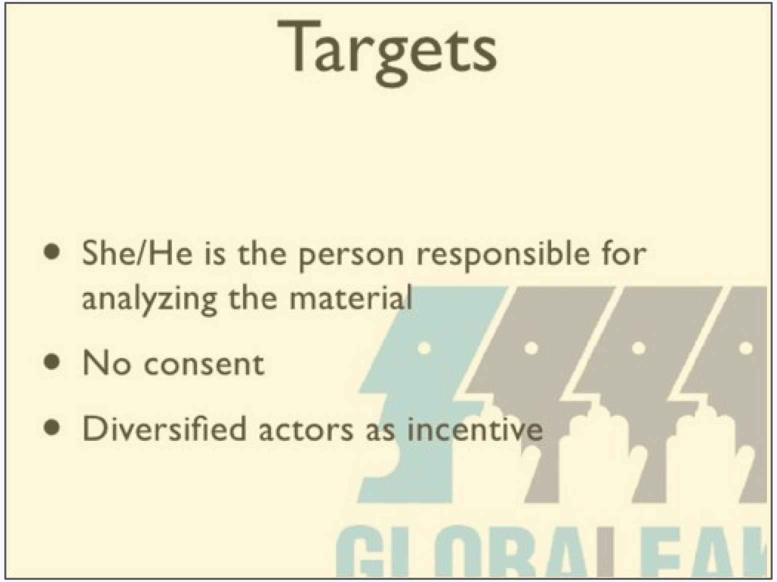
GlobaLeaks has been tested by more than 50 drunk Venetian hackers, here is a link the presentation given at the Italian Hacker camp ESC:
http://www.slideshare.net/globaleaks/globaleaks-live-launch-venice-2011.

And most importantly, please come and hack with use and let's change the world! http://www.launchpad.net/globaleaks/

Happy hacking,

A Random GlobaLeaks Contributor

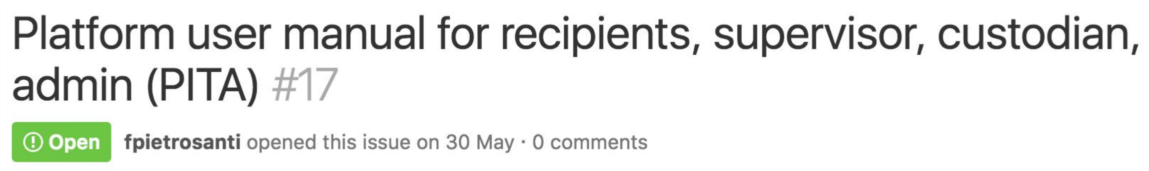
It has changed a lot…!



Targets

- She/He is the person responsible for analyzing the material
- No consent
- Diversified actors as incentive

It has changed a lot…!



Platform user manual for recipients, supervisor, custodian, admin (PITA) #17

fpietrosanti opened this issue on 30 May · 0 comments

More changes: A new goal

Encrypt data at rest without GPG or user input

Sub Reqs:

- Store nothing in whistleblower’s browser
- No required software
- Key escrow for submissions
- Upgrade existing GlobaLeaks sites

The whistleblower

Sees something wrong

Wants to remain anonymous

Reads the man

Connects with a browser

Uploads files

Fills out a form

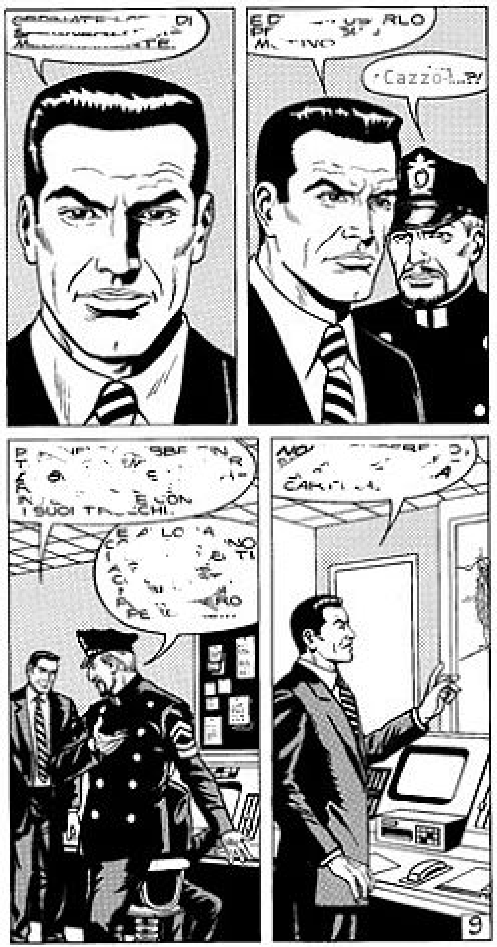
Given a receipt

The organization follows up

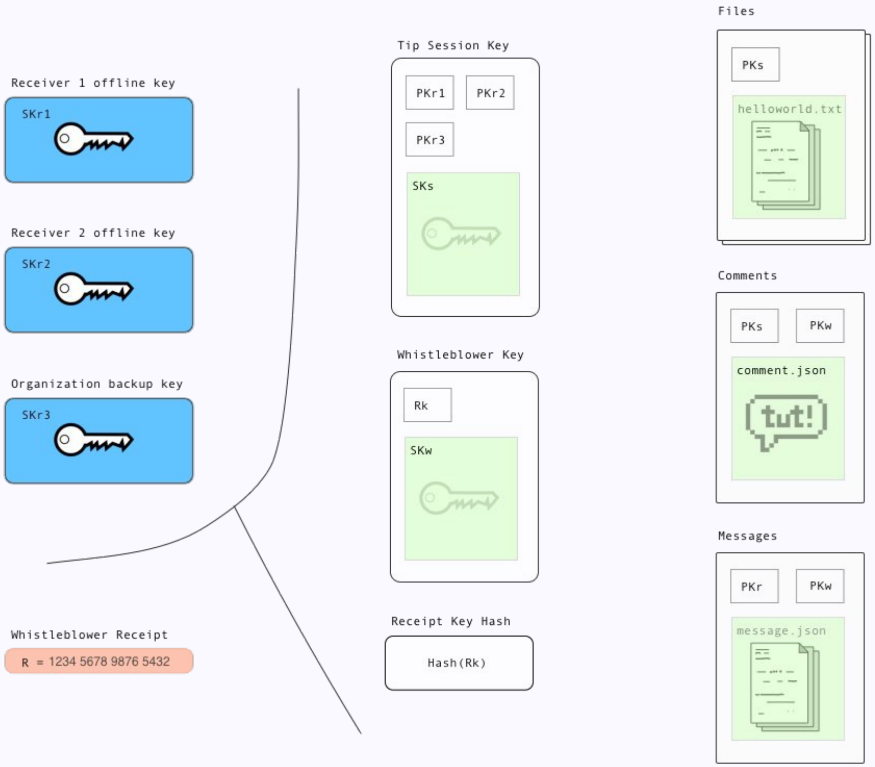
Asks whistleblower for more information

Organization acts

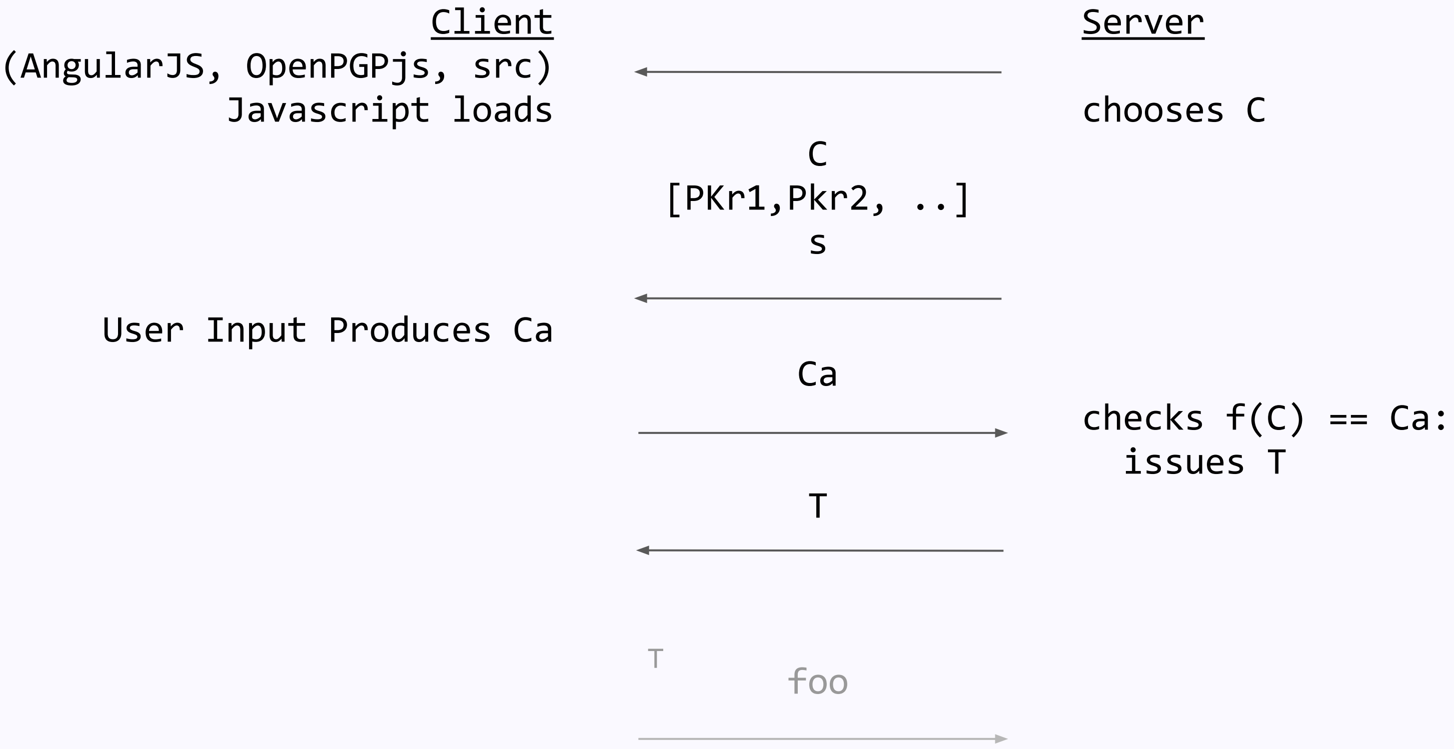
- Writes a story
- Starts a trial
- Publishes a leak



Where data is stored



First Connection



Client

(AngularJS, OpenPGPjs, src)
Javascript loads

Server

chooses C

C
[PKr1,Pkr2, ..]
s

User Input Produces Ca

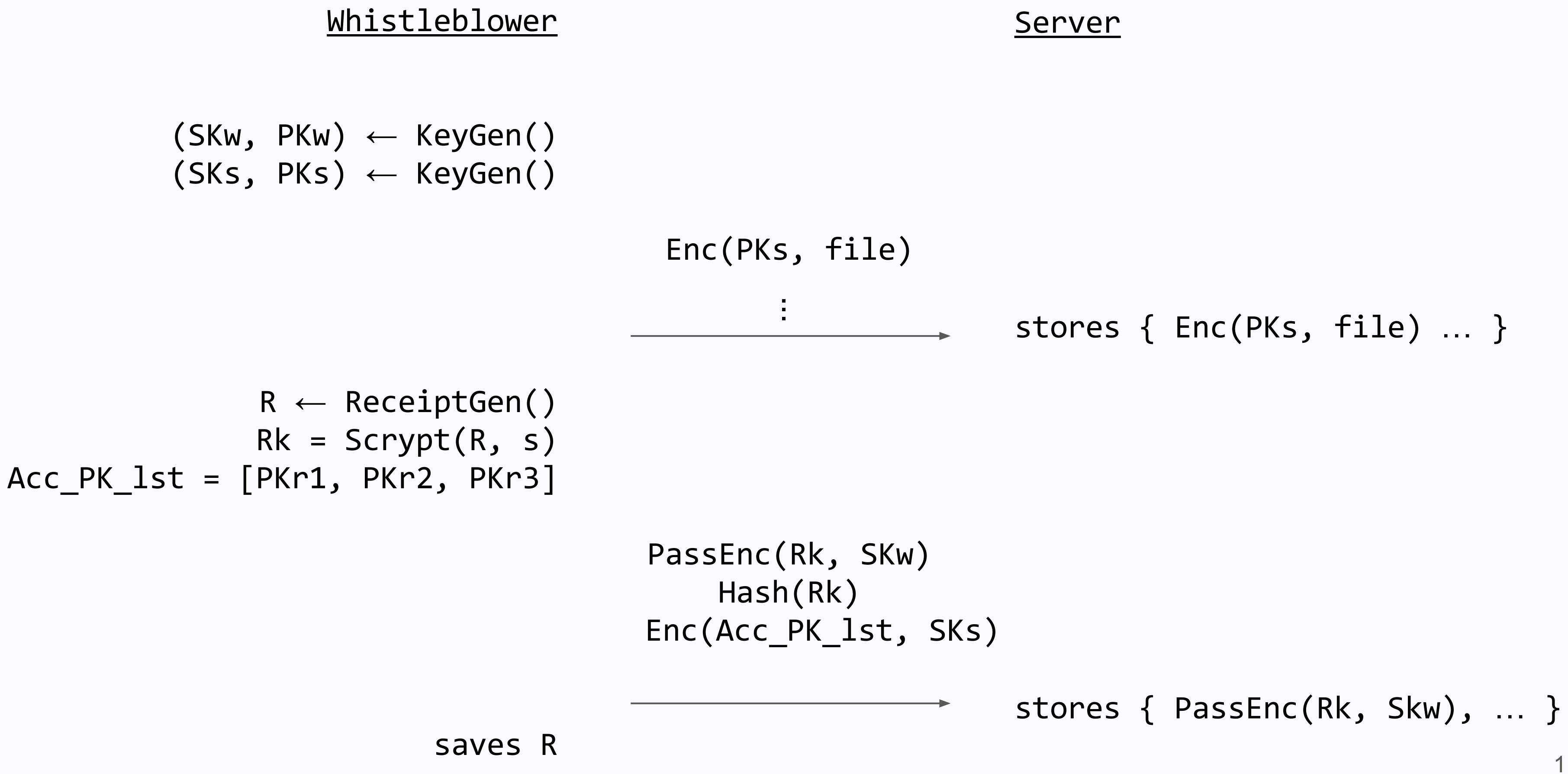
Ca

checks f(C) == Ca:
issues T

T

T
foo

Whistleblower creates Submission



Whistleblower

Server

(SKw, PKw) ← KeyGen()

(SKs, PKs) ← KeyGen()

Enc(PKs, file)

⋮

stores { Enc(PKs, file) … }

R ← ReceiptGen()

Rk = Scrypt(R, s)

Acc_PK_lst = [PKr1, PKr2, PKr3]

PassEnc(Rk, SKw)

Hash(Rk)

Enc(Acc_PK_lst, SKs)

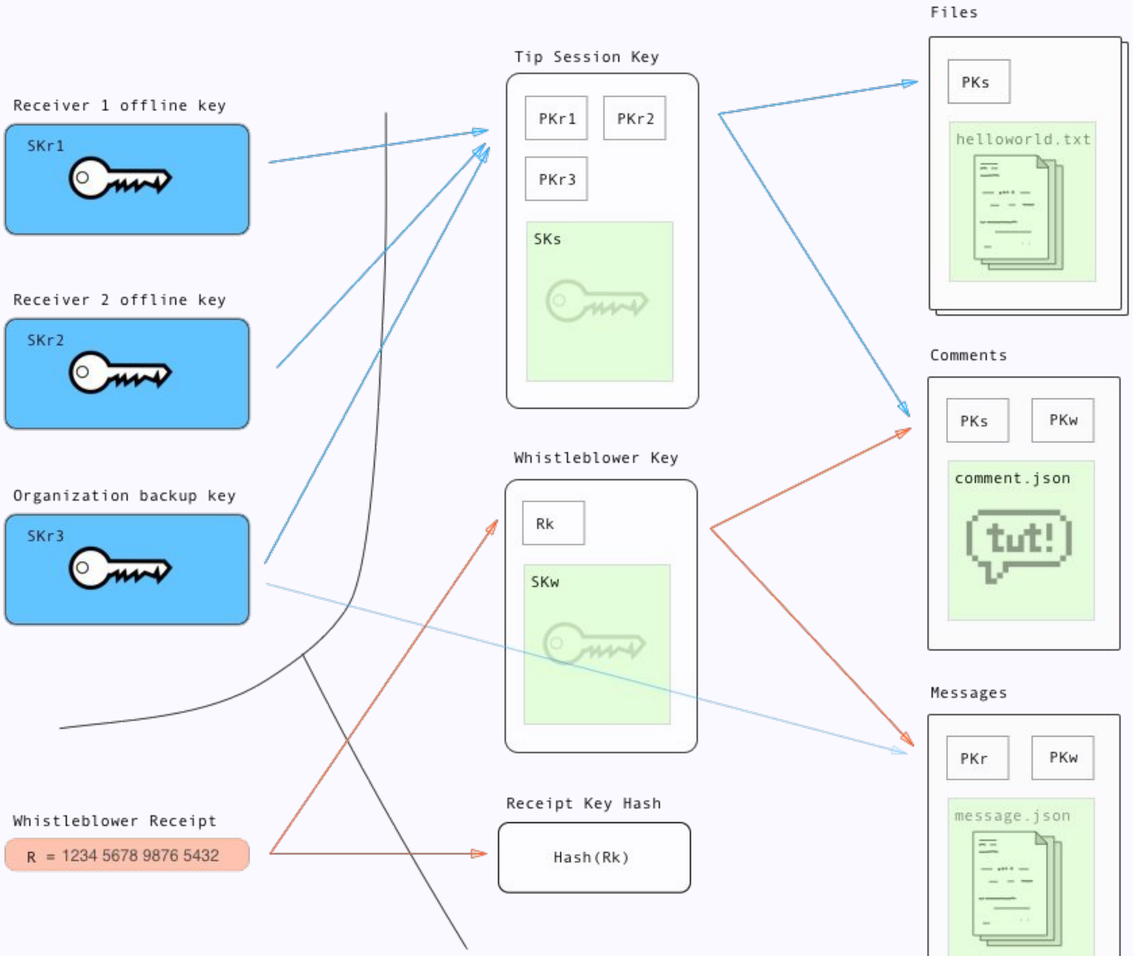
stores { PassEnc(Rk, Skw), … }

saves R

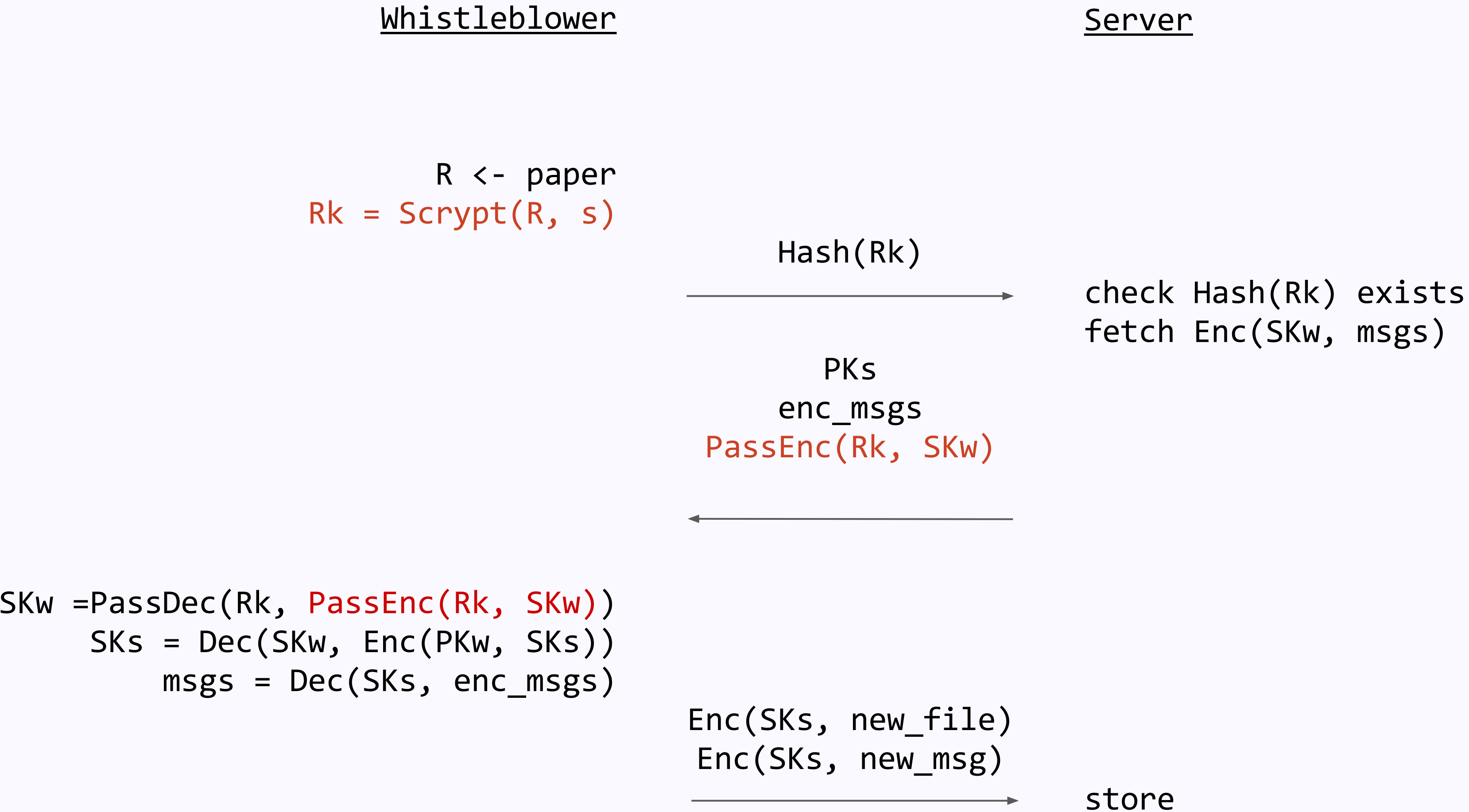
Who can read what

```
Hash(Scrypt(R, s) => {
  PassEnc(Rk, SKw),
  Enc(PKs, file),
  Enc(Acc_PK_lst, SKs),

}
```



Whistleblower receipt authentication



Whistleblower

Server

R <- paper

Rk = Scrypt(R, s)

Hash(Rk)

check Hash(Rk) exists

fetch Enc(SKw, msgs)

PKs

enc_msgs

PassEnc(Rk, SKw)

SKw =PassDec(Rk, PassEnc(Rk, SKw))

SKs = Dec(SKw, Enc(PKw, SKs))

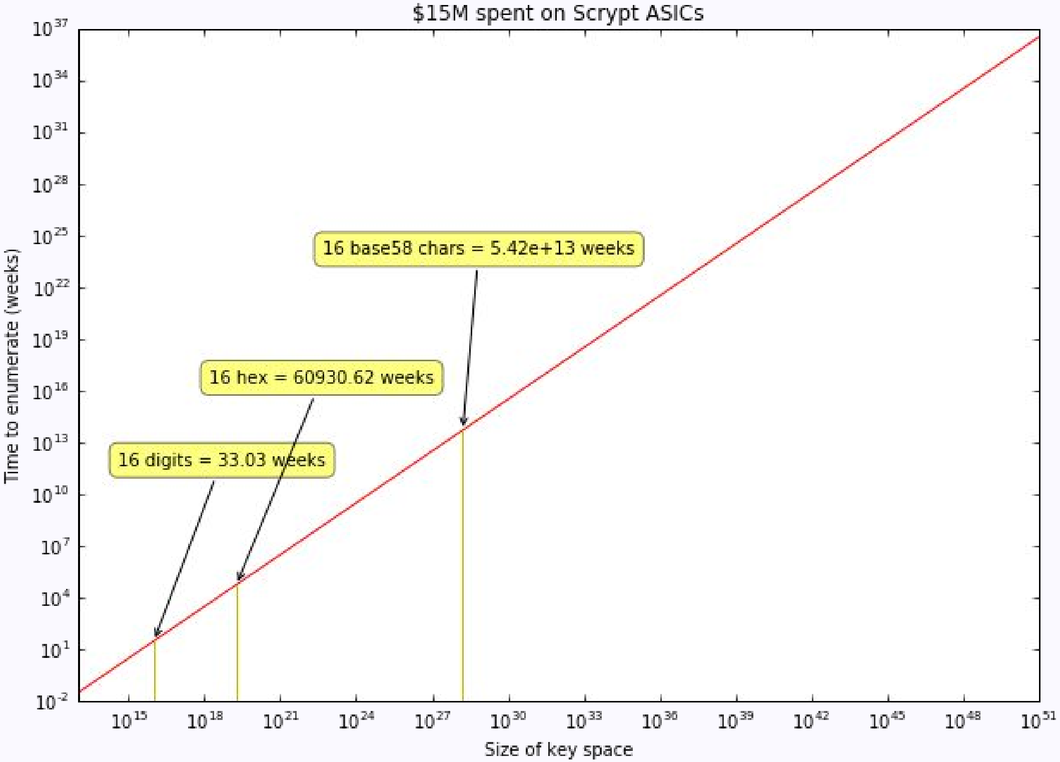
msgs = Dec(SKs, enc_msgs)

Enc(SKs, new_file)

Enc(SKs, new_msg)

store

Bad Case time



Scrypt(n=14, r=8)

- Uses 256 MB memory
- 17 H/s in python on laptop
- ~250 ms in JS

ASIC speed: 10 KH/s

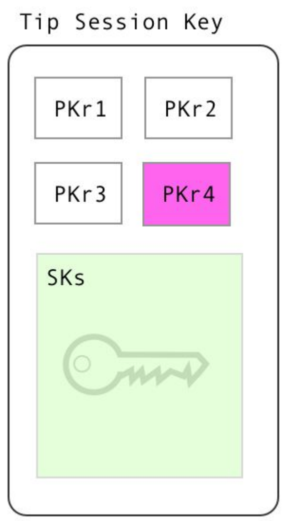
Number of asics manufactured 50000.0

Attacker scrypt rate: 0.5 GH/s

0-9	4532 6980 2034 4294
Hex	3de5 12a9 b443 6ff1
Base 58	CNbt MDqc w6o5 GNn4

Side Notes

Adding new users



Recipient Environment

ELECTRON

WebCrypto Standards

WC3 Candidate Rec
Native AES, SHA2, etc

Questions, Queries, Quandaries?

OFTC #globaleaks

contact@logioshermes.org

www.globaleaks.org

www.github.com/globaleaks

synnick: A6BD 2D38 7F39 236C A9CB 0F86 DD77 3D6D 7326 078E

Sources

This presentation: http://nskelsey.com/glbc-2016.pdf

GLBC spec: https://docs.google.com/document/d/1ShdxubexlFPKedhO28i0RvnjHSiQU4lma5B0DSs2xsQ/pub

GL launch: http://www.slideshare.net/globaleaks/globaleaks-live-launch-venice-2011

ASIC fab quotes: http://asic-cost-calculator.sigenics.com/

ver1-rev1