



Stateless Encryption

GlobaLeaks

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



+25



ecuador
TRANSPARENTE



HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM

Spanish: Documentos filtrados revelan la maquinaria de censura en Ecuador

APRIL 14, 2016 | BY KATITZA RODRIGUEZ



Leaked Documents Confirm Ecuador's Internet Censorship Machine

Schedule 32. Chaos Communication Congress

lecture: Ecuador: how an authoritarian government is fooling the entire world

Version 1.5b Castle in the Sky

Index

Guess what? The Government of Rafael Correa actually is totally against free-speech and we got proofs on that

The whistleblower



Saw something wrong

Left the office

Connected with a browser 

Uploaded files

Filled out a form

Took a receipt

The organization follows up

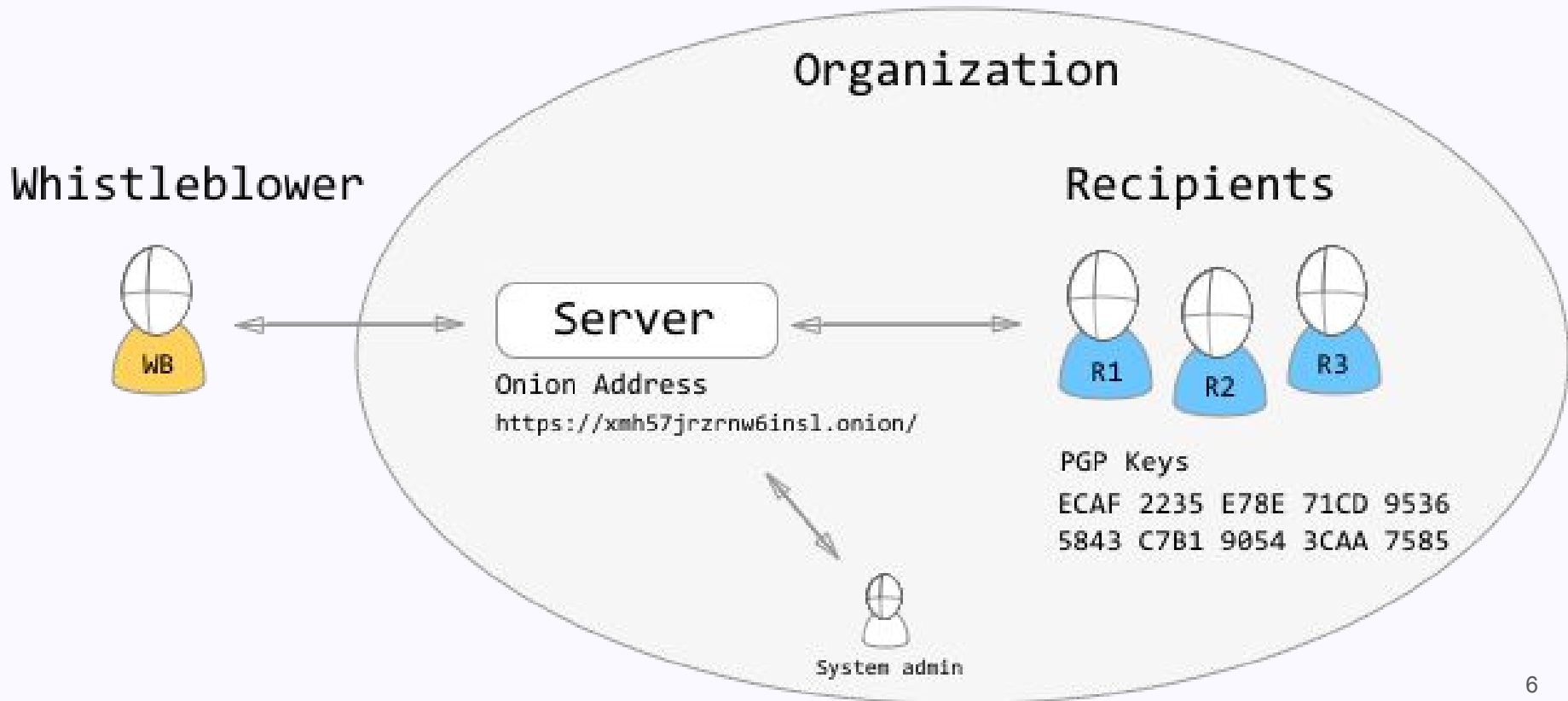
Asks whistleblower for more information

Organization acts

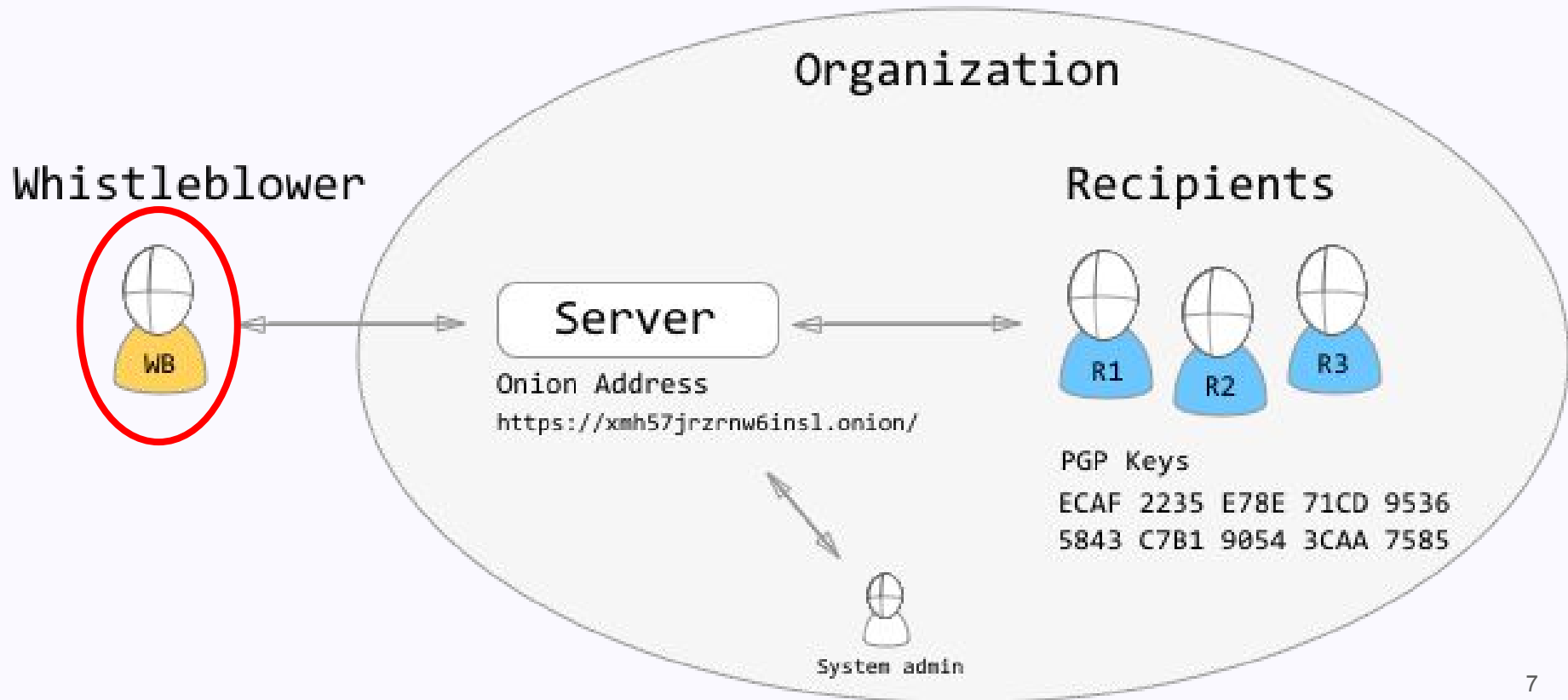
- Writes a story
- Starts a trial
- Publishes a leak



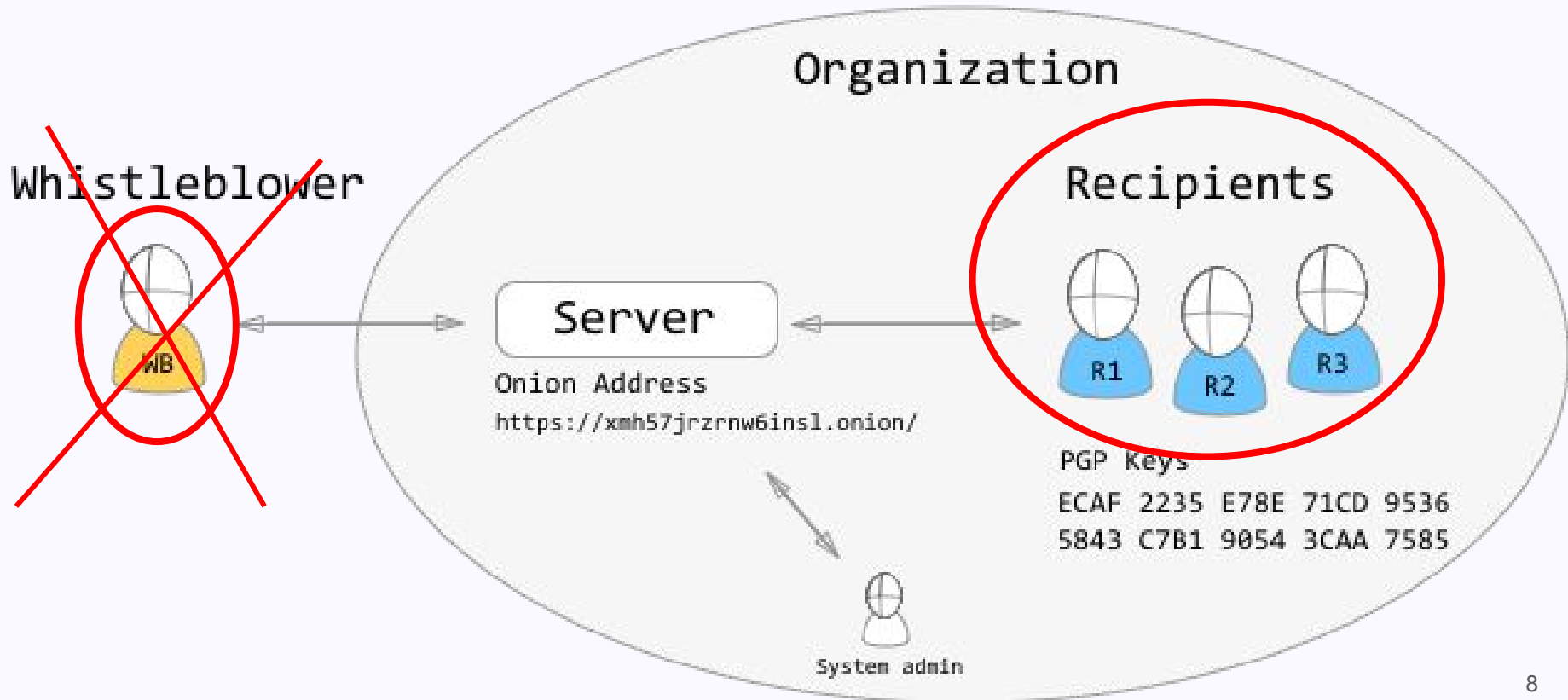
The big picture



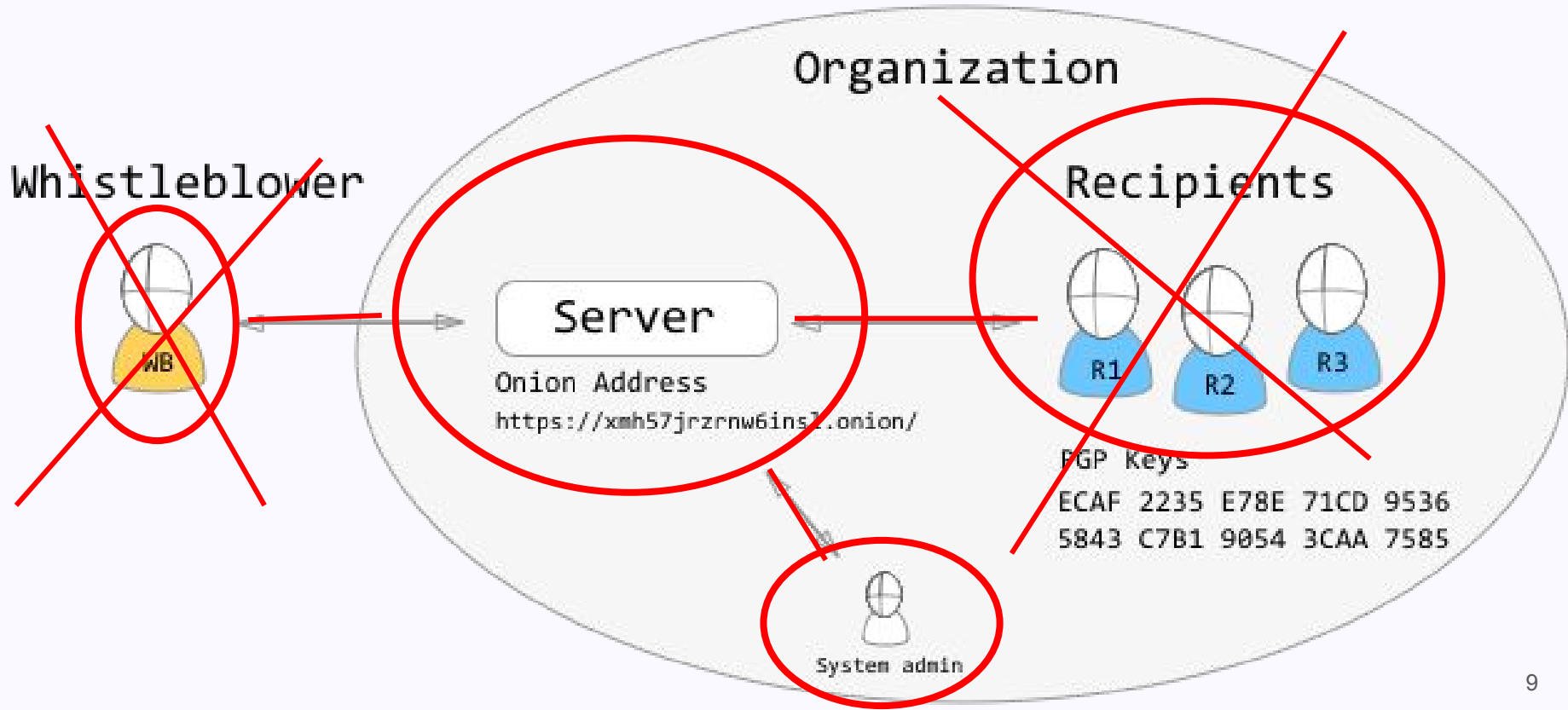
Go after the whistleblower



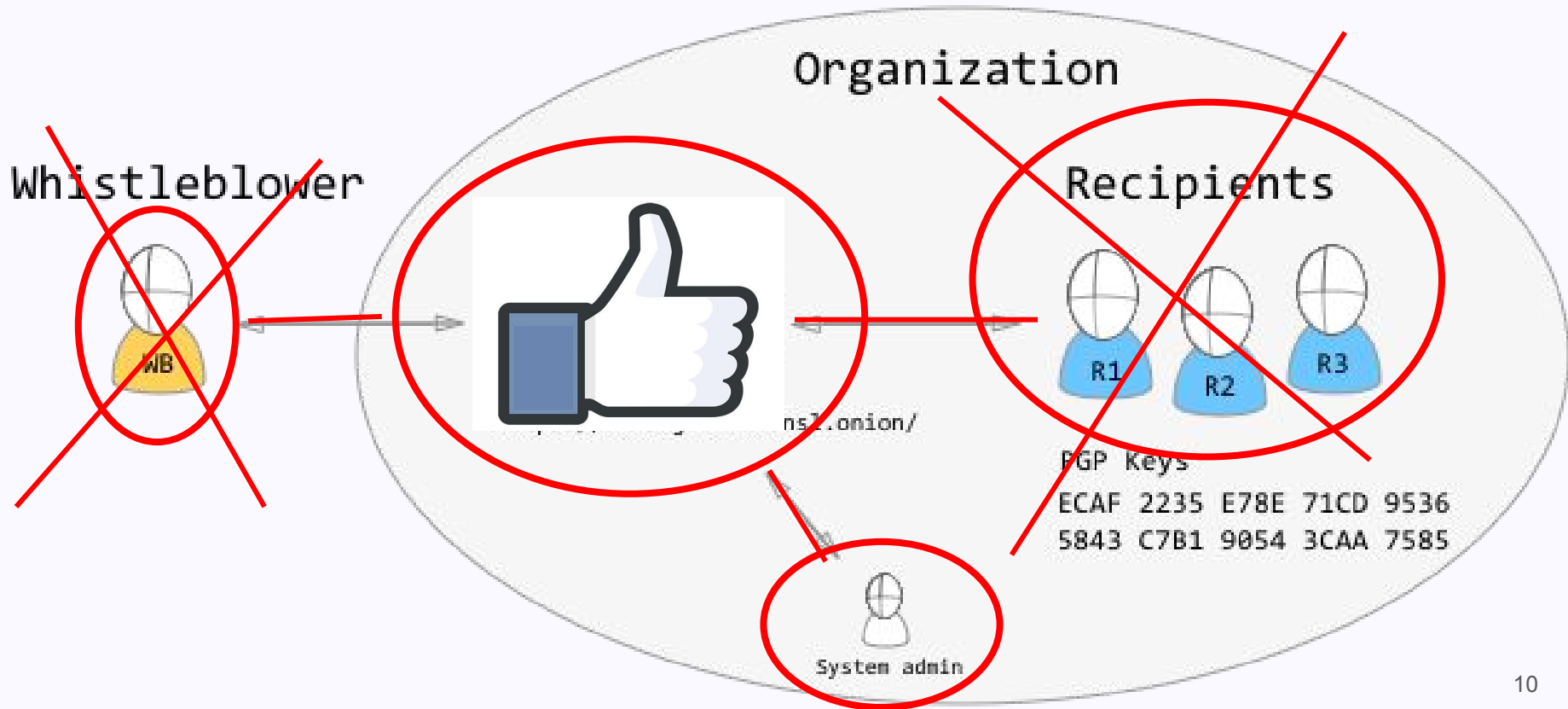
Go after the journalists



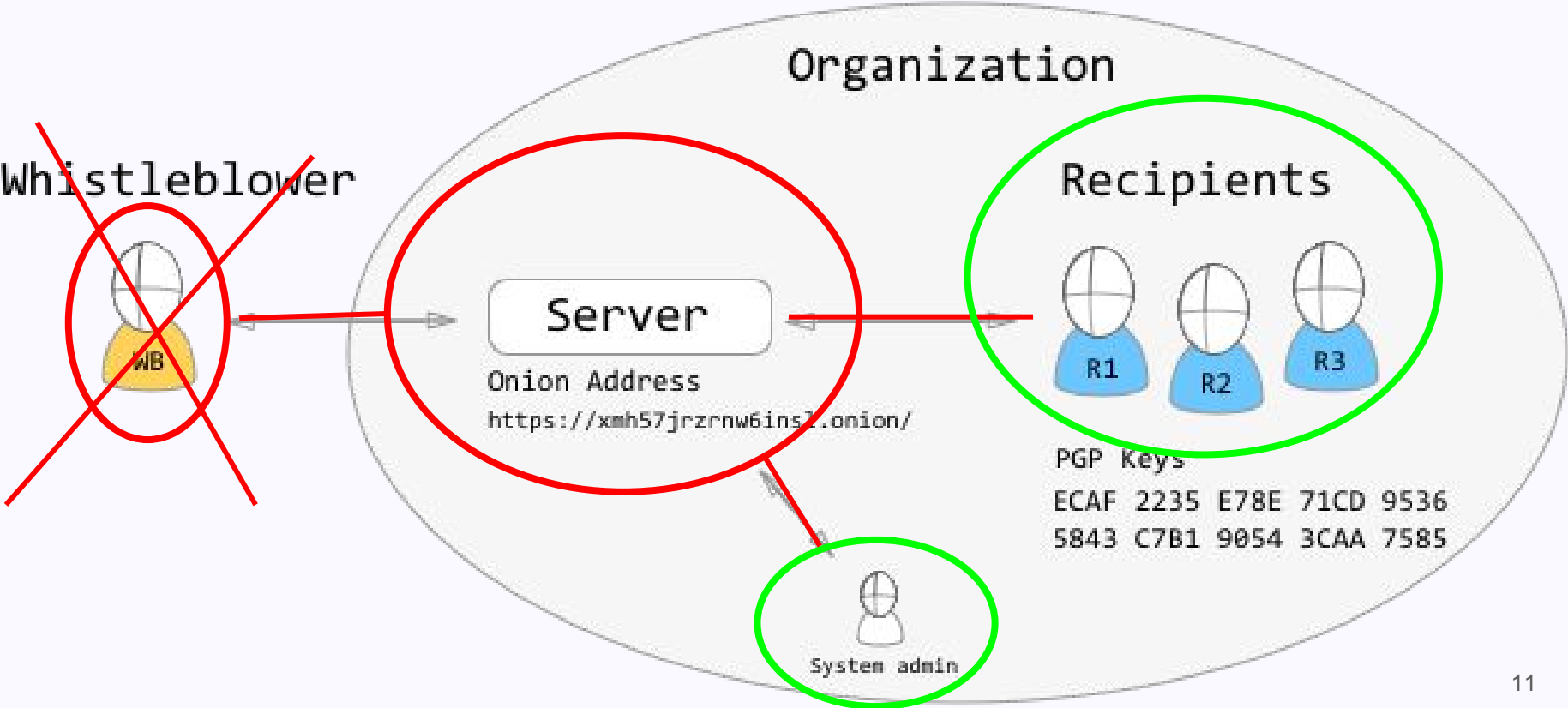
Go after the system



This works for the committed



Improvements can be made



Data stored by server for each submission

Offline

Receiver 1 key
prvR1



Receiver 2 key
prvR2



Receiver 3 key
prvR3



Whistleblower Creds
R
1234 5678 9876 5432

Server

Tip meta data
Date, Last Access,
Views, Actions


Receipt Key Hash
Script(Rk)

Files

pubR1 pubR2

pubR3

helloworld.txt



Comments

m



Messages

m



Requirements

Decrypt data at rest without client-side software

Admin reqs:

- Add new recipients to existing submissions

- Upgrade existing GlobaLeaks sites


Whistleblower Req:

- Store nothing in the browser


New scheme

Offline


Receiver 1 key
prvR1



Receiver 2 key
prvR2



Receiver 3 key
prvR3



Whistleblower Creds
pass || R
password
1234 5678 9876 5432

Server


Tip meta data
Date, Last Access,
Views, Actions

Tip Session Key

pubR1 pubR2

pubR3


prvS



Whistleblower Key

Rk

prvW




Receipt Key Hash
Hash (Rk)

Files

pubS

helloworld.txt



Comments

pubS pubW

msg



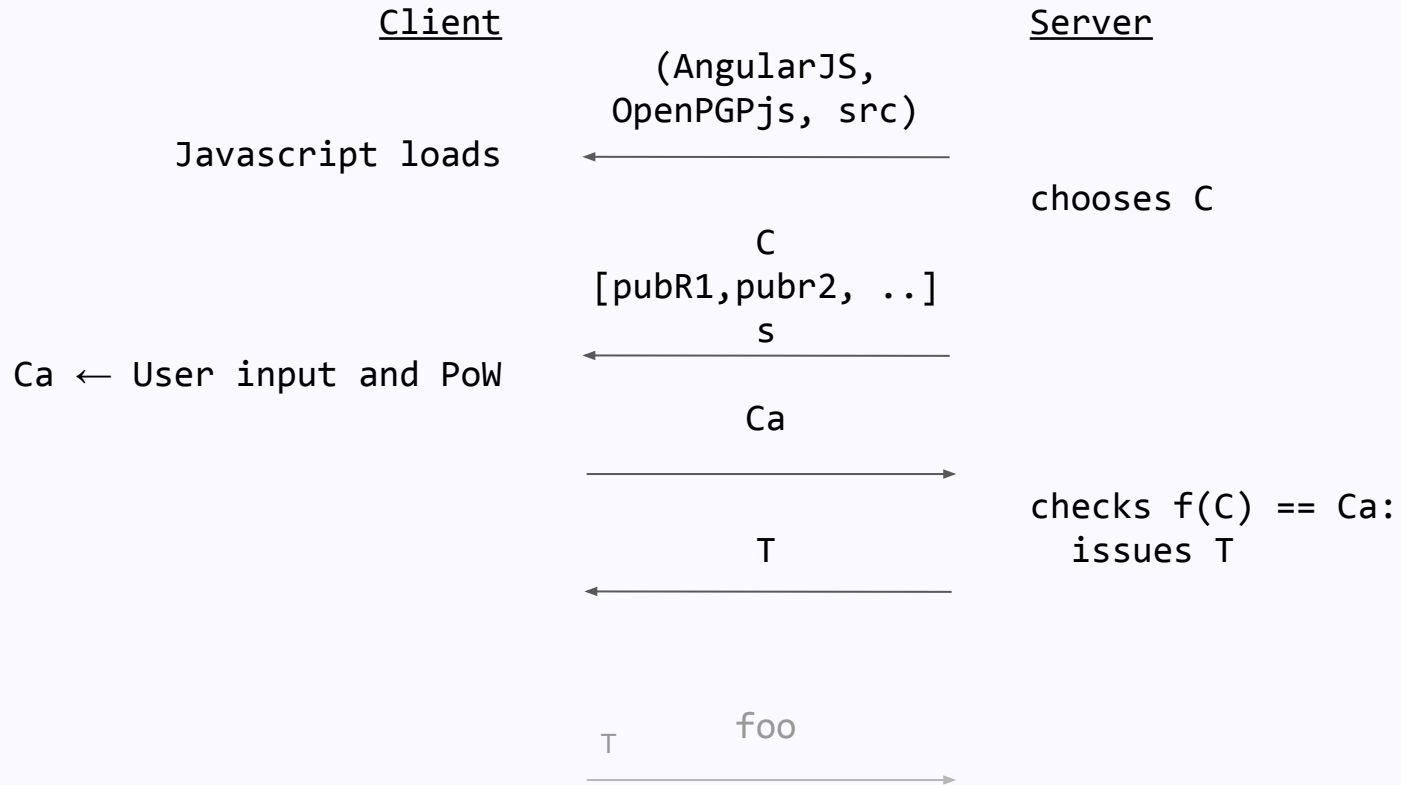
Messages

pubR1 pubW

msg



Whistleblower's initial connection



Whistleblower creates submission

Whistleblower

```
(prvW, pubW) ← KeyGen()  
(prvS, pubS) ← KeyGen()
```

```
Pass ← MakePassword()  
R ← ReceiptGen()  
Rk = Scrypt(R||Pass, s)  
pub_lst = [pubR1, pubR2, pubR3]
```

saves R

Server

```
Enc(pubS, file)
```

```
τ  
----->
```

```
stores { Enc(pubS, file) ... }
```

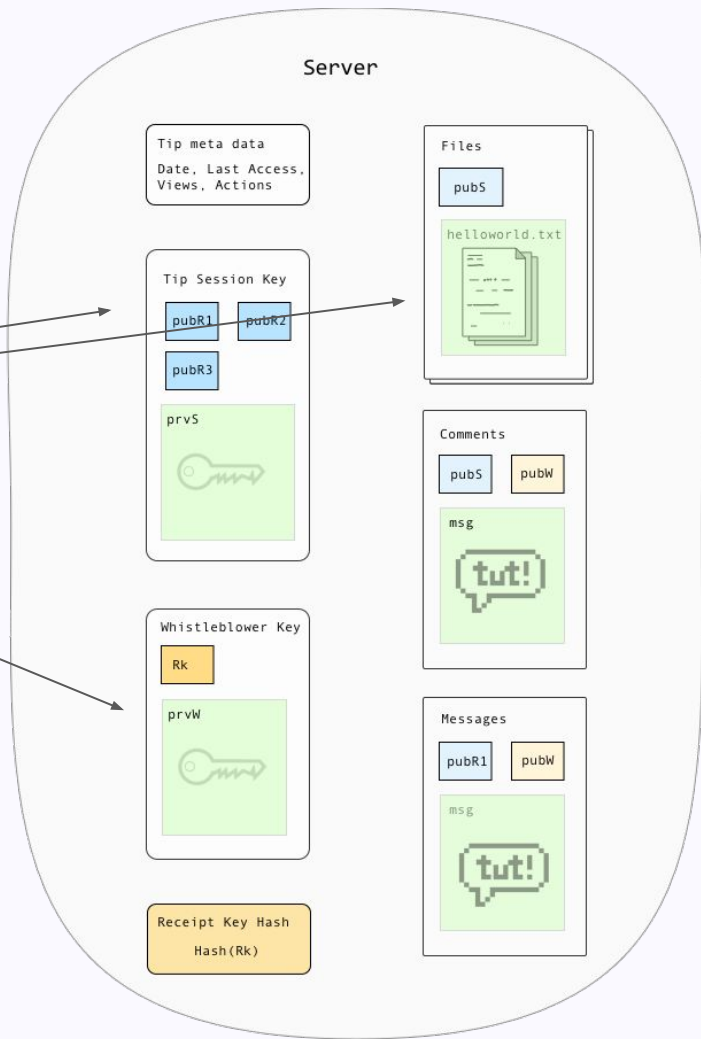
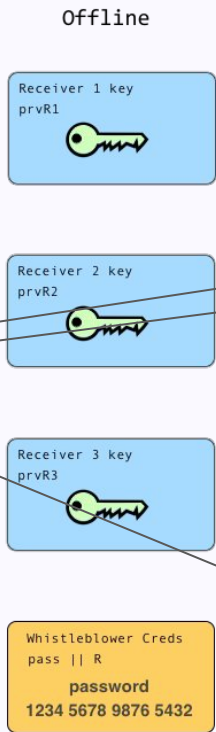
```
PassEnc(Rk, prvW)  
Hash(Rk)  
Enc(pub_lst, prvS)
```

```
τ  
----->
```

```
stores { PassEnc(Rk, prvW), ...  
}
```

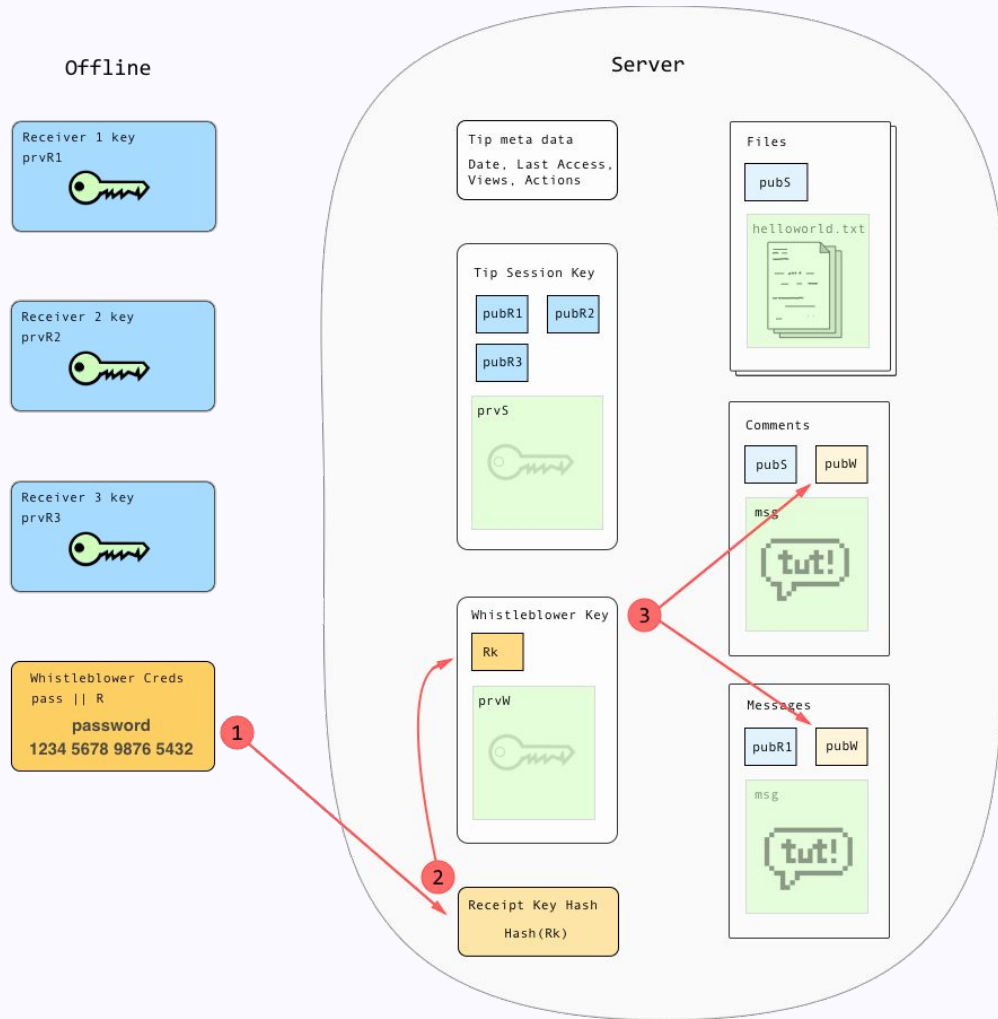

After creation of submission

```
Hash(Scrypt(R, s) => {  
  Enc(pub_lst, prvS),  
  Enc(pubS, file),  
  PassEnc(Rk, prvW),  
  ...  
  ...  
})
```



Whistleblower Access

- 1) Uses Credentials to authenticate
- 2) Decrypts prvW
- 3) Decrypts comments and messages



Whistleblower receipt authentication

Whistleblower

$R \leftarrow \text{paper}$
 $\text{pass} \leftarrow \text{brain}$
 $Rk = \text{Scrypt}(R || \text{pass}, s)$

$\xrightarrow{\text{Hash}(Rk)}$

Server

check Hash(Rk) exists
fetch Enc(prvW, msgs)

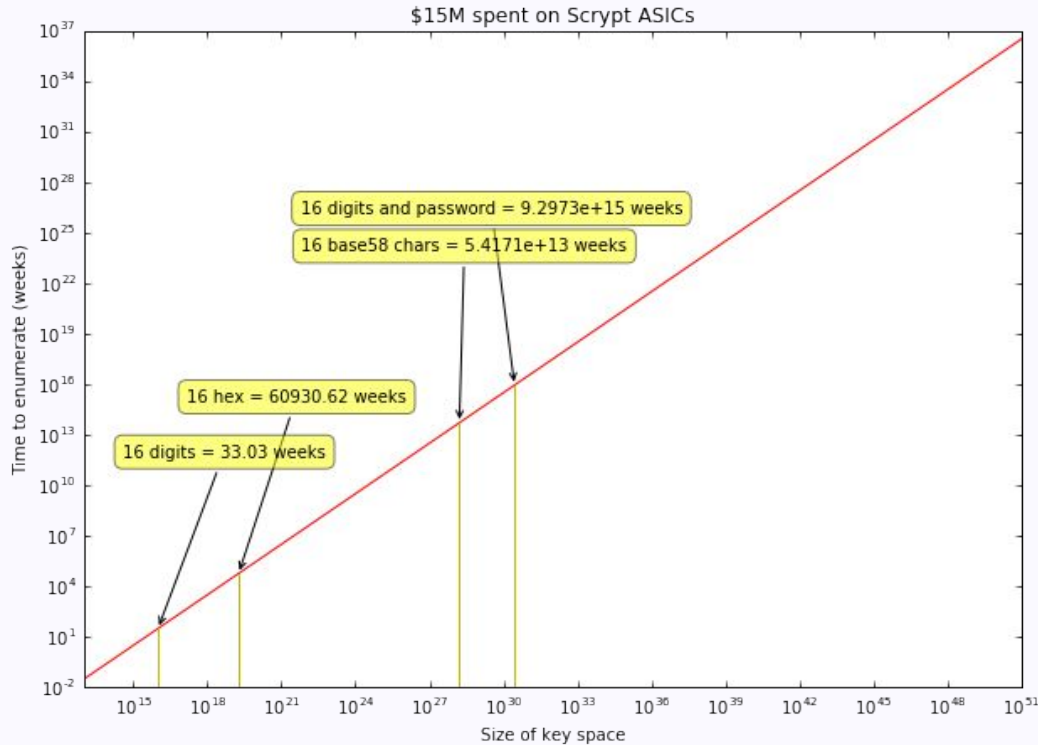
pubS
enc_msgs
 $\text{PassEnc}(Rk, \text{prvW})$
 $\xleftarrow{\hspace{10em}}$

$\text{prvW} = \text{PassDec}(Rk, \text{PassEnc}(Rk, \text{prvW}))$
 $\text{msgs} = \text{Dec}(\text{prvS}, \text{enc_msgs})$

Enc(pubS, new_file)
Enc(pubS, new_msg)
 $\xrightarrow{\hspace{10em}}$

store

Bad Case time



Script($n=14, r=8$)

- 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 script rate: 0.5 GH/s

0-9 4532 6980 2034 4294

Hex 3de5 12a9 b443 6ff1

Base 58 CNbt MDqc w6o5 GNn4

Keys on system

Offline


Receiver 1 pass
password

Receiver 2 pass
password

Receiver 3 pass
password

Whistleblower Creds
pass || R
password
1234 5678 9876 5432


Server


Receiver 1 key
prvR1


Receiver 2 key
prvR2



Receiver 3 key
prvR3



Tip meta data
Date, Last Access,
Views, Actions

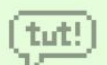
Tip Session Key
pubR1 pubR2
pubR3
prv5


Whistleblower Key
Rk
prvW


Receipt Key Hash
Hash (Rk)

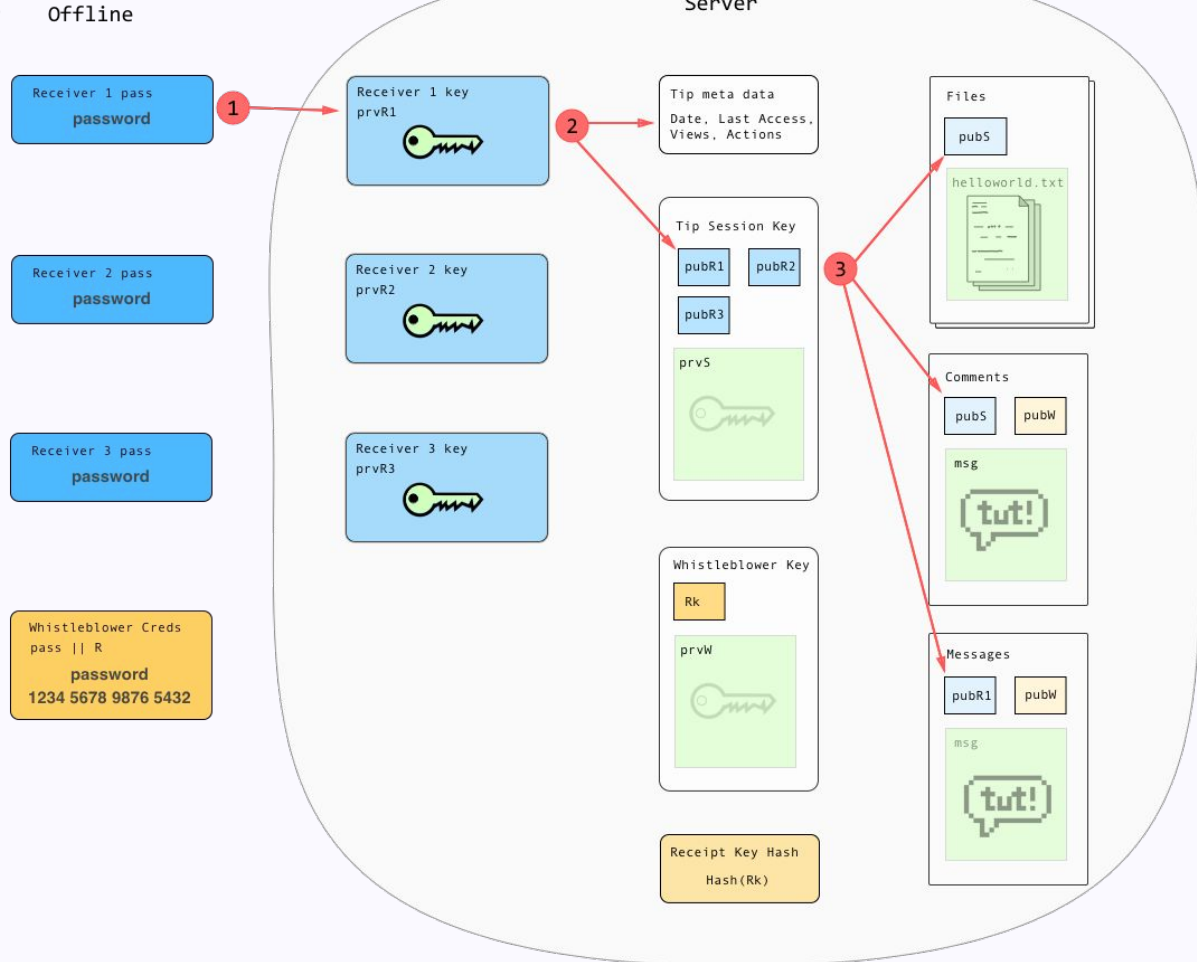
Files
pubS
helloworld.txt


Comments
pubS pubW
msg


Messages
pubR1 pubW
msg


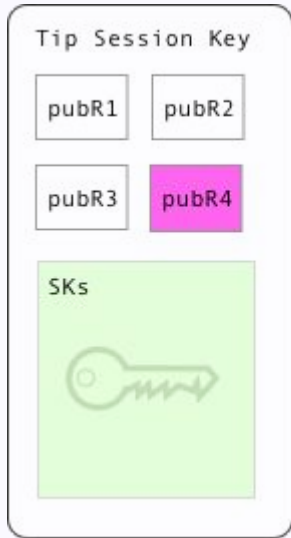
Recipient Access

- 1) Authenticate and decrypt prvR1
- 2) Decrypt prvS
- 3) Decrypt files, comments, msgs



Side Notes

Adding new users



Recipient Environment



PassEnc()

Receipt size

Script limits

Argon2

Questions, 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

ver2-rev1

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

GLBC spec: <https://docs.google.com/document/d/1ShdxubexlFPKedh028i0RvnjHSiQU4lma5B0DSs2xs0/pub>

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

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

Ecuador announcement: <https://events.ccc.de/congress/2015/Fahrplan/events/7134.html>