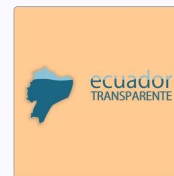
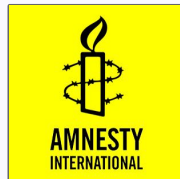
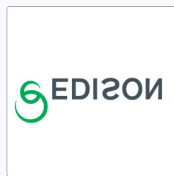




A source protection program

GlobaLeaks


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



+45



ecuador
TRANSPARENTE

 **ELECTRONIC FRONTIER FOUNDATION**
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

[HOME](#) [ABOUT](#) [OUR WORK](#) [DEEPLINKS BLOG](#) [PRESS ROOM](#)

Spanish: Documentos filtrados revelan la maquinaria de censura en Ecuador

APRIL 14, 2016 | BY [KATITZA RODRIGUEZ](#)

[Twitter](#) [Facebook](#) [Google+](#) [Print](#) [Email](#)

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

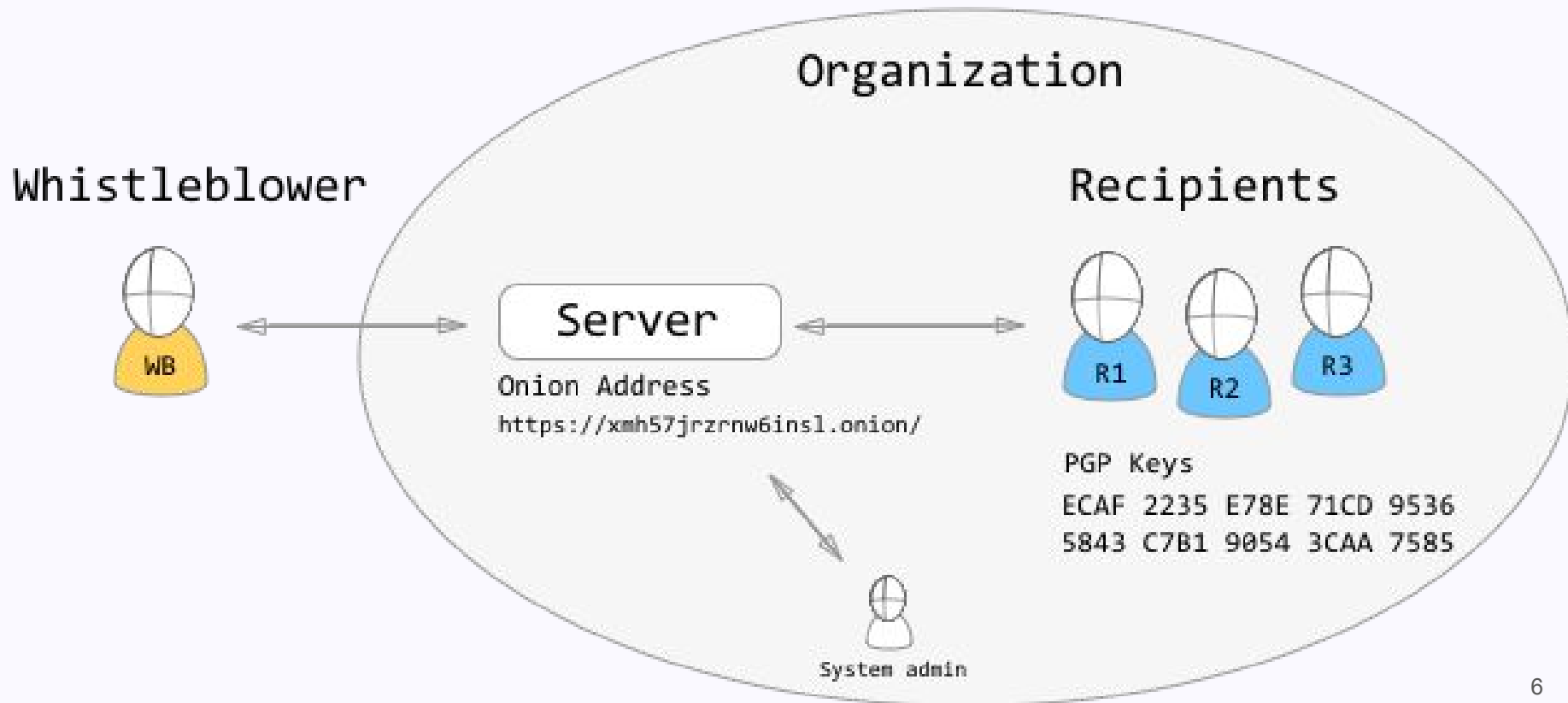
Asks whistleblower for more information

Organization responds

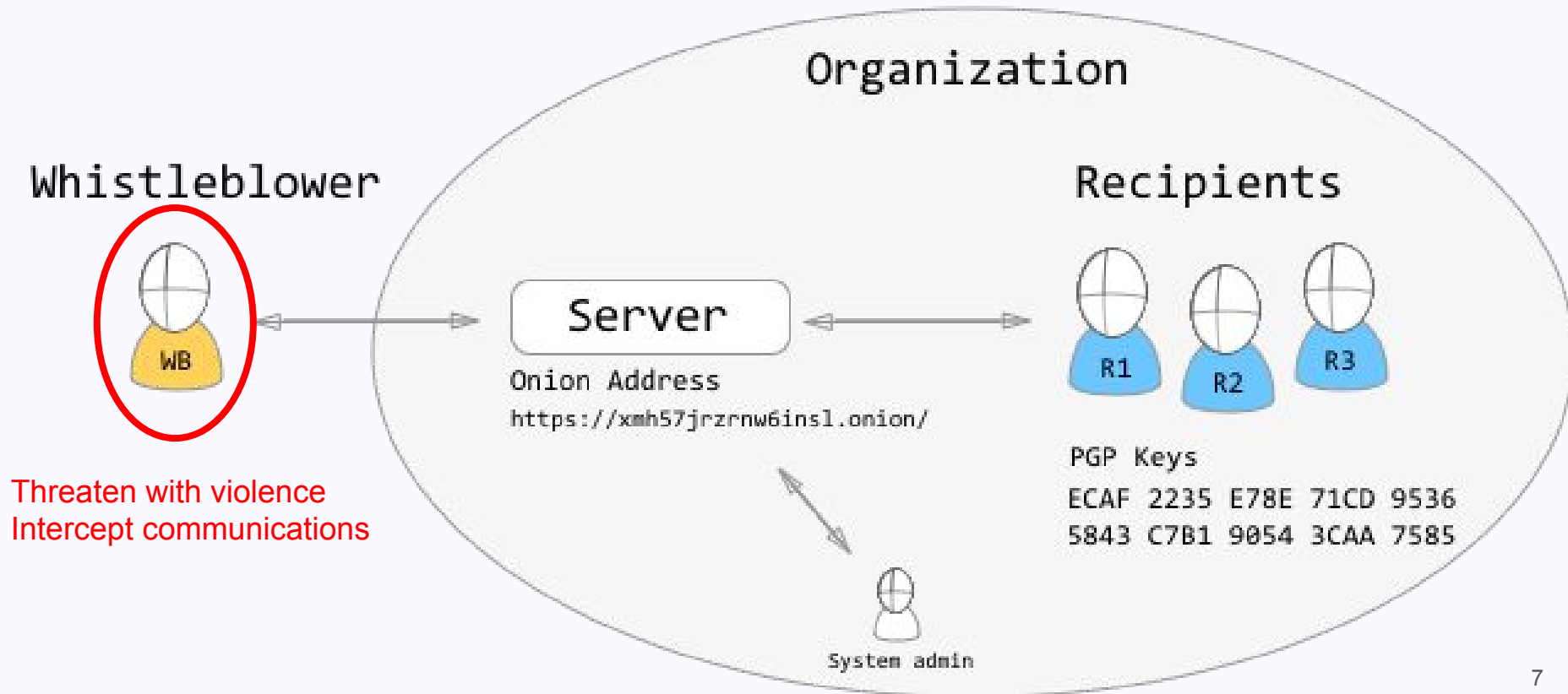
- Writes a story
- Starts a trial
- Publishes a leak



The big picture



Go after the whistleblower



Go after the journalists

Threaten with violence
Intercept communications
Deliver malware
Attack contacts and sources

Whistleblower



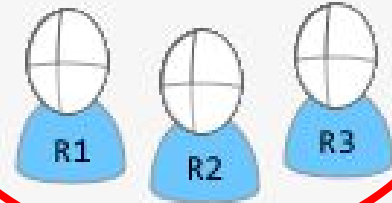
Organization

Server

Onion Address

<https://xmh57jrznw6insl.onion/>

Recipients



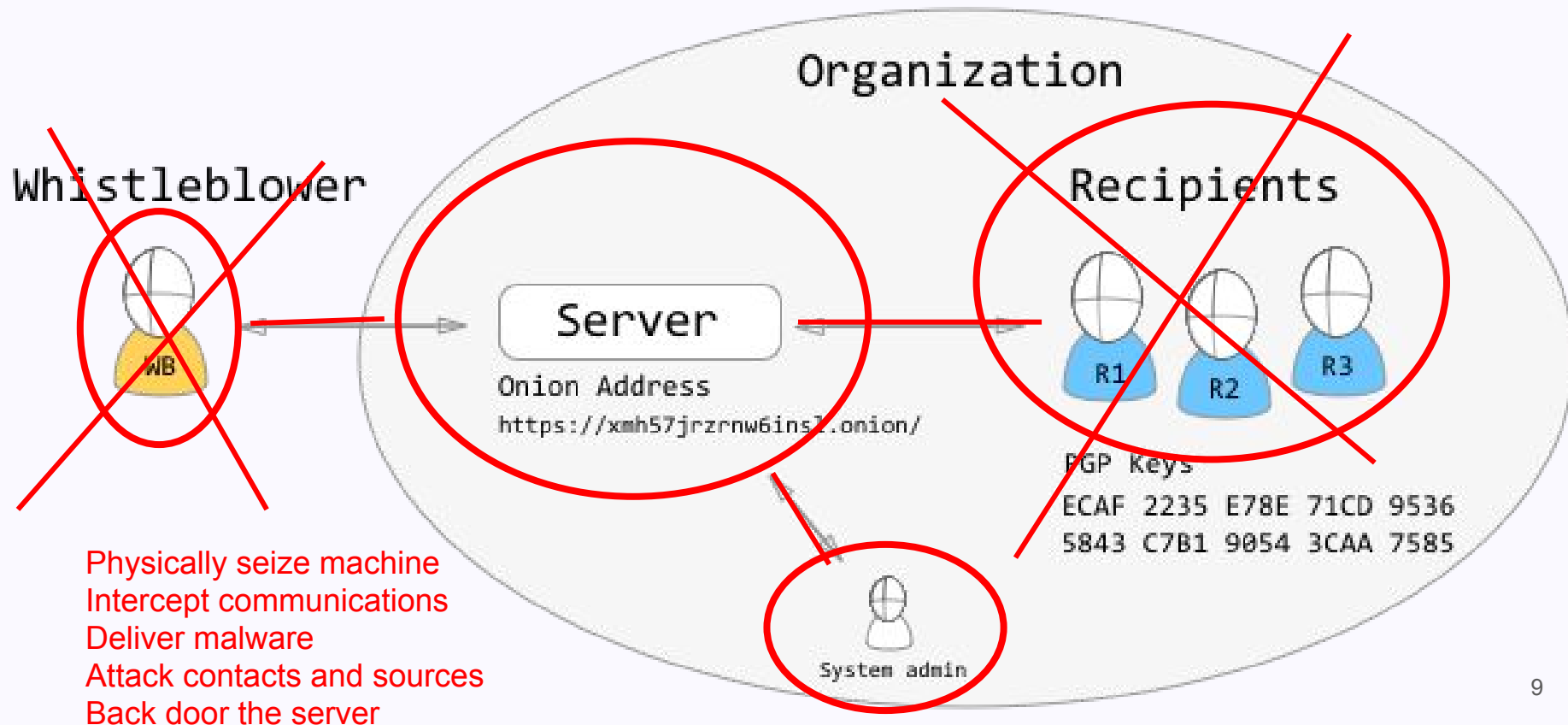
PGP Keys

ECAF 2235 E78E 71CD 9536
5843 C7B1 9054 3CAA 7585

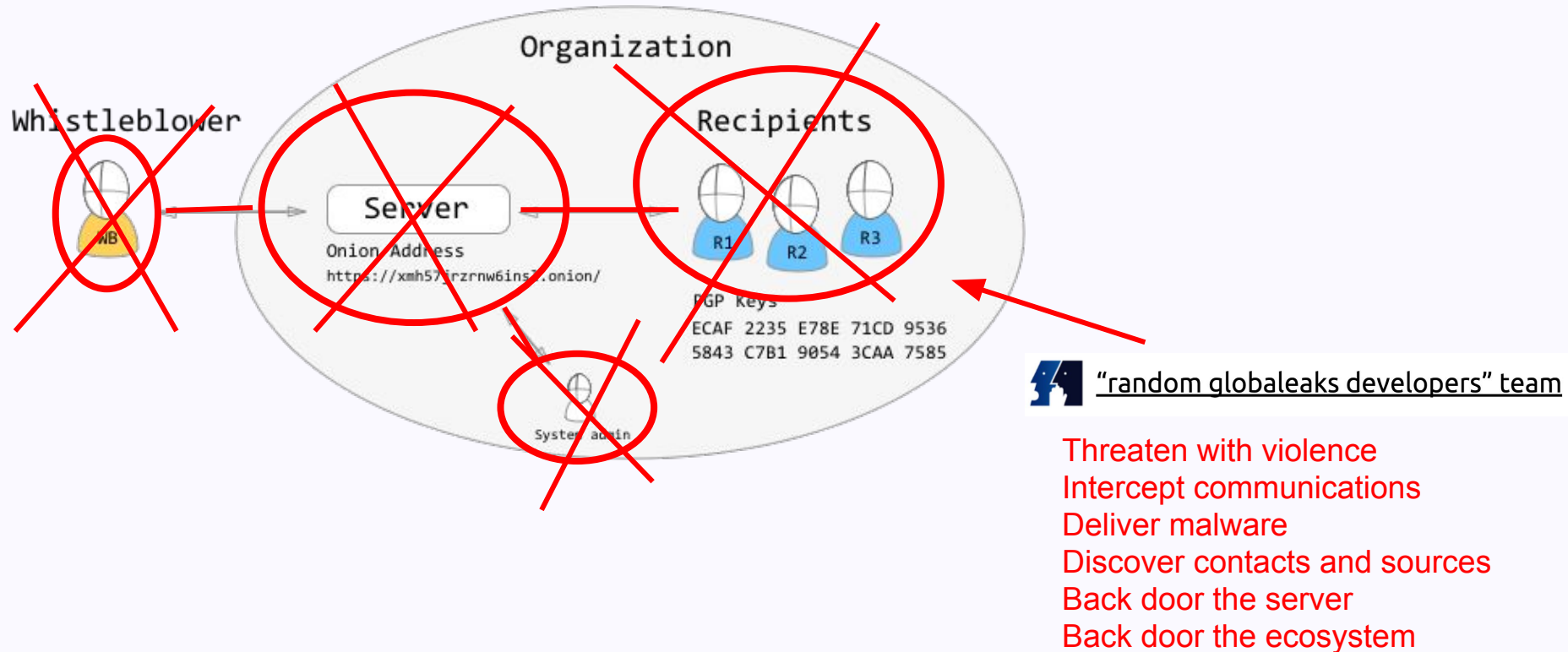


System admin

Go after the server

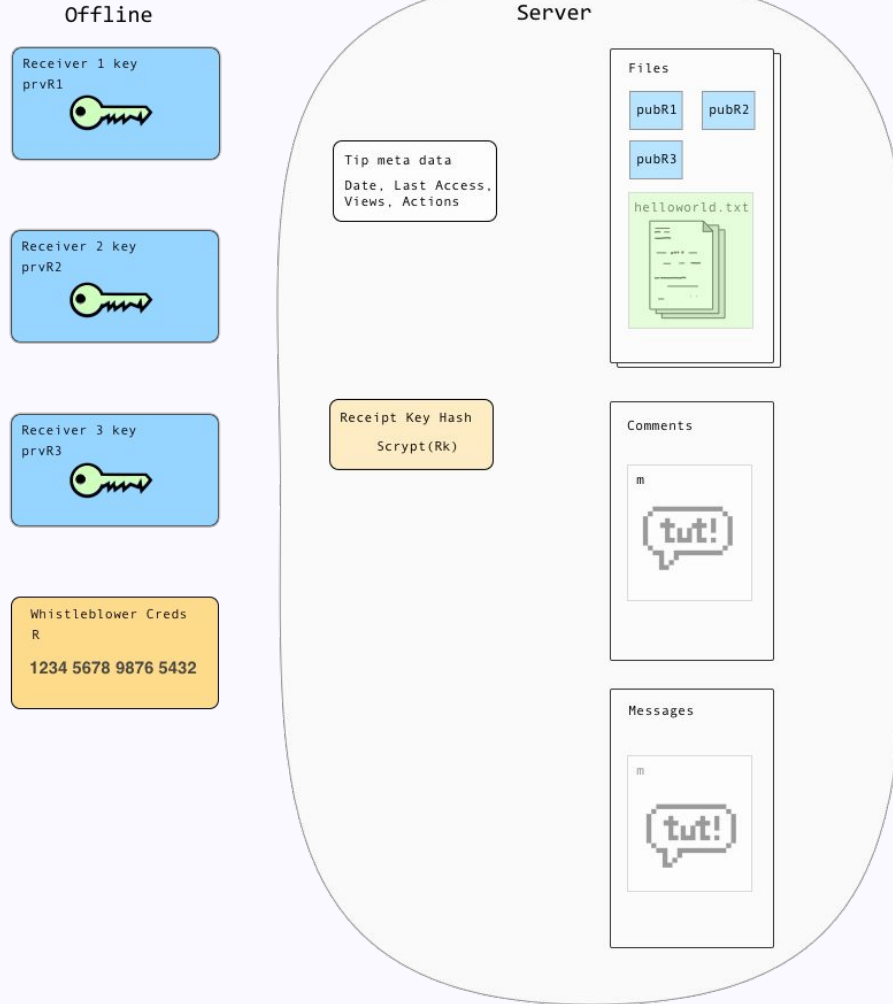


Go after the developers



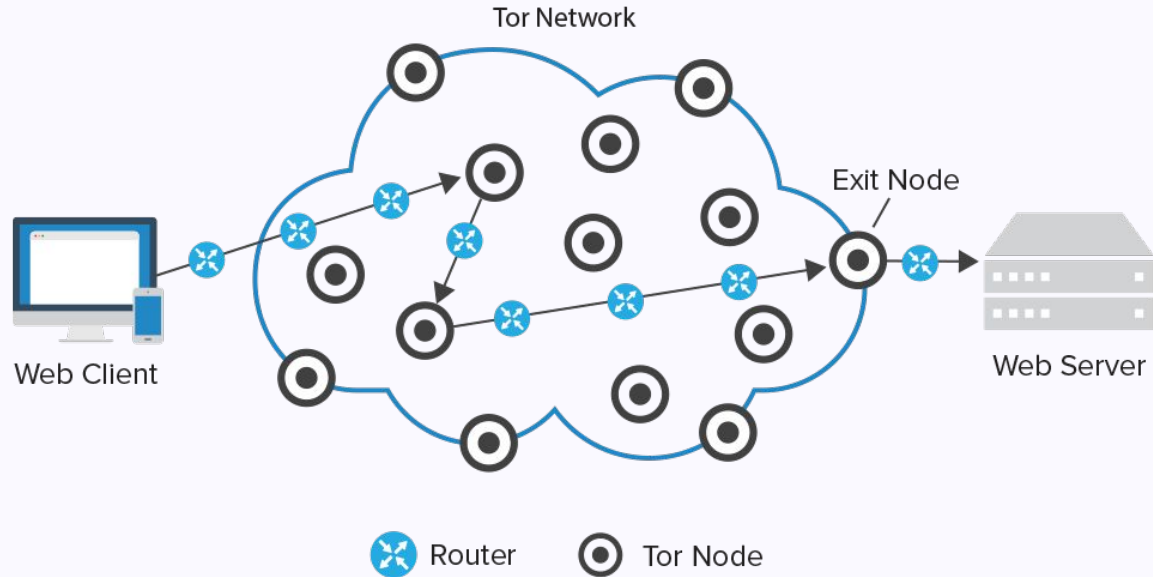
What information is in on the service?

- Encrypted Files
- Meta-data
- Logs
- Public Keys



Connecting to the service?

A network on top of the Internet
Does not hide usage

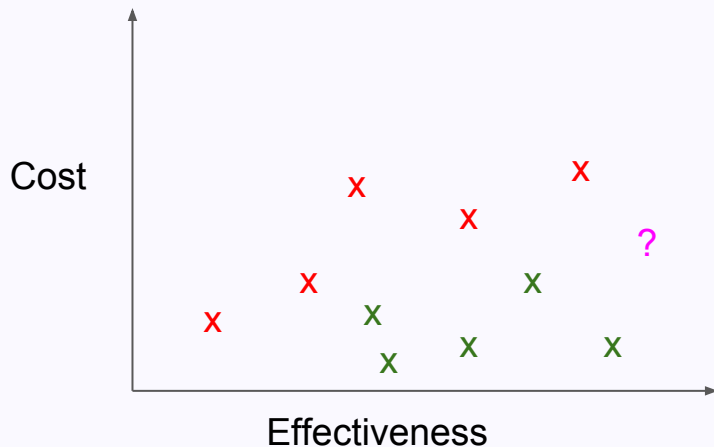


What is active on the network

```
nskelsey @ Trisong ~ master
[> cat ~/Desktop/demo-netstat]
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 demo.globaleaks.or:http *:.*                     LISTEN      24975/python
tcp        0      0 localhost.localdom:9040 *:.*                     LISTEN      556/tor
tcp        0      0 demo.globaleaks.or:8082 *:.*                     LISTEN      1260/python
tcp        0      0 localhost.localdom:8082 *:.*                     LISTEN      1260/python
tcp        0      0 *:9267                *:.*                     LISTEN      482/master
tcp        0      0 *:ssh                  *:.*                     LISTEN      249/sshd
tcp        0      0 localhost.localdom:9050 *:.*                     LISTEN      556/tor
tcp        0      0 demo.globaleaks.o:https *:.*                     LISTEN      24975/python
tcp        0      0 demo.globaleaks.or:http xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 24982/python
tcp        0      0 localhost.localdo:33362 xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 556/tor
tcp        0      0 demo.globaleaks.o:https xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 24979/python
tcp        0      0 demo.globaleaks.o:57009 xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 556/tor
tcp        0      0 demo.globaleaks.o:59215 xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 642/znc
tcp        0      0 demo.globaleaks.or:http xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 24979/python
tcp        0      0 demo.globaleaks.or:http xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 24979/python
tcp        0      0 localhost.localdom:8082 xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 1260/python
tcp        0      0 demo.globaleaks.or:http xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 24978/python
tcp        0      0 demo.globaleaks.o:43406 xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 382/python
tcp        0      0 demo.globaleaks.or:http xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 24980/python
tcp        0      0 demo.globaleaks.o:45081 xxxx.xxxxxx.xxxxxx.xxx ESTABLISHED 556/tor
```

Hardening an instance of GlobaLeaks

Reduce number of ways an attacker can disable the service, execute code execution, or leak information.



✗ Compile Kernel:
Gentoo
Debian

Extend Kernel:
GRSecurity
SELinux

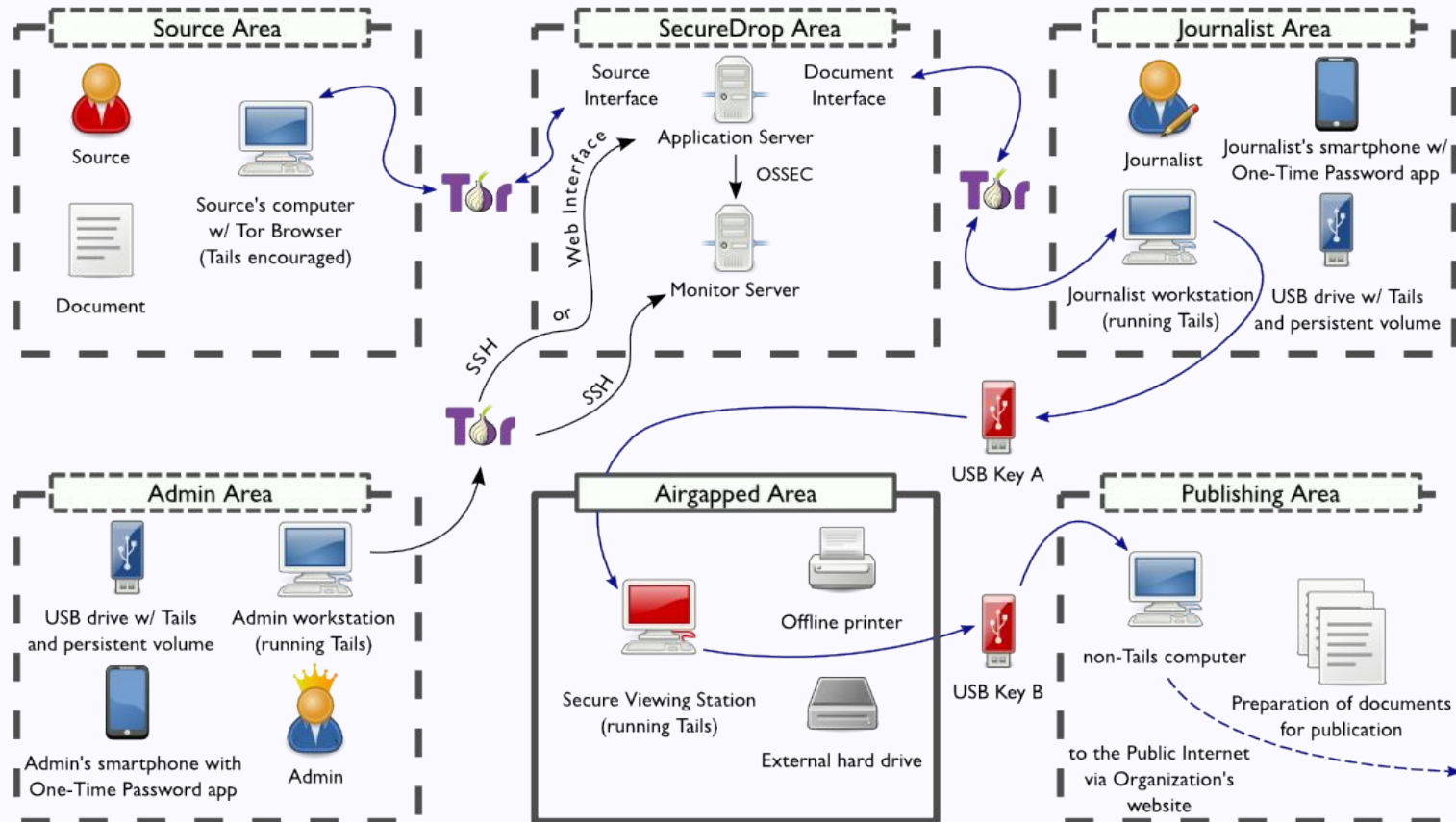
Defend Userspace:

- ✗ Virtualization
- ✗ Application sand box
- ✗ Firewall
- ✗ User isolation

Configure applications

- ✗ Force PGP
- ✗ Minimize logging
- ✗ Require HTTPS for landing page

As safe as you can make the process

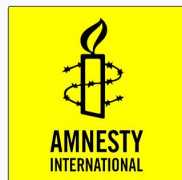


Research/Build/Deploy with us

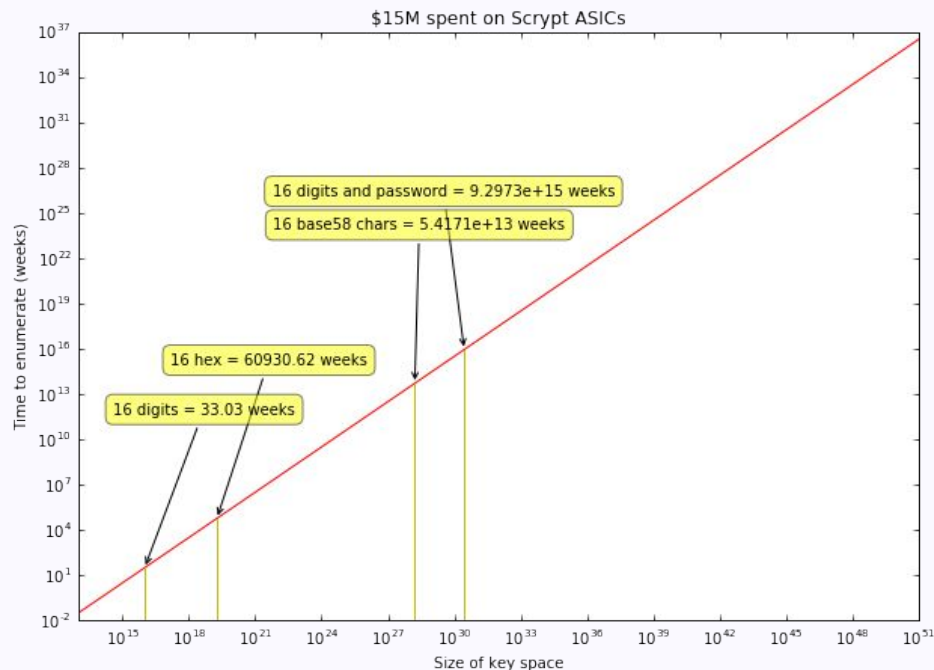
Implement new standards cryptographic



Create systems to protect people who are vulnerable



Analyze and author original research



Questions, Queries, Quandaries?

OFTC #globaleaks

contact@logioshermes.org

www.globaleaks.org

www.github.com/globaleaks

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