Improving the SecureDrop System Architecture

heartsucker
SecureDrop Maintainer

FOSDEM 2018

SecureDrop Release Signing Key Fingerprint:
2224 5C81 E3BA EB41 38B3 6061 310F 5612 00F4 AD77
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.
Threat Model
What are we trying to protect?

Source Anonymity  Document Confidentiality
Who do we want to protect it from?

Nation States
Large Corporations
Local Law Enforcement
& Government
EVERYONE
What are their capabilities?

- Intercept Network Traffic
- Hack Into the Servers
- Send Agents to Seize Hardware
- Submit Malware to Journalists via SecureDrop

EVERYTHING
Current State of SecureDrop
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
Failures and Fixes
Got a hot tip through my @SecureDrop that base64 decodes to a malicious Python executable. FYI, @DonnchaC, it phones home to your website.

```python
# Find the desktop file and replace it with the decoy
desktop_filename = os.environ['XDG_DATA_HOME'] + '/.local/share/applications/desktopeace.desktop'

# Extract the file name and decode file data from the desktop file
desktop_data = open(desktop_filedata, 'r').read()
decoy_data = open('key_file', 'r').read()
decoy_data_list = [item.strip() for item in decoy_data.split('
') if item.strip()]

# Create new QR code and replace image in decoy doc.
new_file_data = os.path.join(os.getcwd(), 'new_file.txt')
new_file_data = try_msg('Hello from the other side of the aligera', new_file_data)
new_file_data = get_message_data(new_file_data)

# Save the decoy file with the same name as the Desktop name
final_filename = os.path.join(os.path.dirname(desktop_filedata), 'new_file.desktop')
with open(final_file, 'w') as new_file:
    new_file.write(decoy_data)

# Remove the original desktop file
os.remove(desktop_filedata)
```

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
Internet-connected VM

Disposable VM not connected to the internet

Journalist Workstation

Journalist's smartphone w/ One-Time Password app

Internet-connected VM

Disposable VM not connected to the internet

Preparing of documents for publication to the Public Internet via Organization's website
Uses apt mirror for Tor via `securedrop-config` package

#2441

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

Conorsch commented on Oct 13, 2017 • edited by dachary

Status

Ready for review.

Description of Changes

Fixes #2106. Reimplements and supersedes #2113.
SUBMIT DOCUMENTS

Send inn Dokumenter

Envoyer des documents

Dokumente versenden

Documenten inzenden
def submit():
    if msg and not fh:
        things = 'message'
        html_contents = gettext('Thanks! We received your message. ')
    elif not msg and fh:
        things = 'document'
        html_contents = gettext('Thanks! We received your document. ')
    else:
        things = 'message and document'
        html_contents = gettext('Thanks! We received your message and ')
        html_contents += 'document. ')
    msg = render_templates('next_submission_flashed_message.html',
        things=things)
    html_contents=html_contents)
    flash(Markup(msg), "success")
    for frame in fnames:
Localization

- Code changes
- Dependency changes
- Build update to support translations
- Weblate for external translators
- String freezes in preparation for a release
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
App Server
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
marcjuares@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
Operating system and container binary deployment and upgrades  https://ostree.readthedocs.org/en/latest/
TODO SD is super boring to write and it’s bs grunt work but the end result is super important
can prevent press freedom violations.
Current SecureDrop Team

+ contributors

prototyping next generation SecureDrop workstation

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