SecureDrop Workstation: Handling unsafe documents safely

LibrePlanet 2021
Conor Schaefer
Chief Technology Officer, Freedom of the Press Foundation
Overview

- Intro, about FPF
- SecureDrop
  - What it is
  - Who uses it
  - Motivations
  - How it works today
- Workstation
  - Qubes OS
  - How isolation works
  - Pilot program
- Security audit
- Next steps
Freedom of the Press Foundation protects, defends, and empowers public-interest journalism in the 21st century.

NEWS & ADVOCACY
Get the latest news on secrecy, surveillance, and whistleblowers.

PRESS FREEDOM TRACKER
Systematically documenting press freedom violations in the United States.

GUIDES & TRAINING
How-to guides on how to protect yourself in the age of mass surveillance.

SECUREDROP
Enabling secure communication between journalists and anonymous sources.
Guides & Training

Our training team delivers digital security trainings to news organizations, freelance and citizen journalists, and other at-risk groups. With education and advocacy, we aim to protect press freedoms through the adoption of the tools and practices included in our trainings.

FROM FPF

What to do if your phone is seized by police

So, you’ve been arrested at an event. You’re taken to the police station and your phone is confiscated. When you’re let out, you realize someone has gone through your digital belongings. What now?

FROM FPF

Everything you wanted to know about media metadata, but were afraid to ask

Take a crash course in some of the tools you can use to analyze, manipulate, and scrub media metadata.
SecureDrop is an online whistleblowing platform, hosted on-premise by news organizations. It uses Tor Onion services for anonymity and GPG for encryption. The code is free software, under the AGPL.
Some of the organizations that currently use SecureDrop
Why SecureDrop?
Journalists have an inherently risky job
Whistleblowing is an inherently risky act

Prognosis

Hospitals Tell Doctors They’ll Be Fired If They Speak Out About Lack of Gear

By Olivia Carville, Emma Court, and Kristen V Brown
March 31, 2020, 6:23 AM PDT

‘Hero who told the truth’: Chinese rage over coronavirus death of whistleblower doctor

The death of a whistleblowing Chinese doctor who was punished for trying to raise the alarm about coronavirus has sparked an explosion of anger, grief and demands for freedom of speech among ordinary Chinese.
Don’t roll your own implementation

- Security software must be audited, with results public
- Sources need assurances regarding communication
- Free software provides a stable, well-reviewed implementation
- Newsrooms can position themselves downstream from custom development
How it works
Application server: Runs two Python web applications (one for sources, one for journalists) exposed via Tor Onion Services.

Source Interface: Public v3 Onion URL, accessible by anyone in Tor Browser

Journalist Interface: Authenticated v3 Onion URL. Requires key-based auth to resolve. Only accessible to journalists.
What the source sees
Monitoring server: Runs a host-based IDS (OSSEC) to monitor the application server and send alerts to administrators.
Network firewall: pfSense used to isolate the SecureDrop area of the network from the rest of the news organization.

Drops all inbound traffic, except established/related. Tor Onions provide NAT-punching.
Documents stored encrypted to the instance’s public key
Journalists log in to Tails OS
What the journalist sees
The documents are stored encrypted for security. To read them, you will need to decrypt them using GPG.
Private key to decrypt documents only in the air-gap environment.
Legacy airgap architecture
SecureDrop Workstation
Motivations for SecureDrop Workstation

- Existing workflows are slow (~1 hour round-trip), and largely one-way
- It’s hard to patch an airgapped system
- Airgap is not perfect isolation
- Journalists need more tools than just viewing
Qubes OS

- Hypervisor-based isolation, via Xen
- Template & disposable environments to combat malware persistence
- Strict controls for inter-VM communication

https://qubes-os.org/
How Qubes OS works
Qubes OS: single-user desktop-based Xen distribution

xen

hardware
Qubes OS: single-user desktop-based Xen distribution

Dom0 (Fedora)

xen

hardware
Qubes OS: single-user desktop-based Xen distribution

- Dom0 (Fedora)
- TemplateVM (e.g. Debian Stable)
- xen
- hardware
Qubes OS: single-user desktop-based Xen distribution

Only /home, /usr/local, /rw/config will persist a reboot, otherwise state is reset to the base TemplateVM

Dom0 (Fedora)

TemplateVM (e.g. Debian Stable)

xen

hardware
Qubes OS: single-user desktop-based Xen distribution

Upon shutdown, VM is destroyed

Dom0 (Fedora)

AppVM

DispVM

TemplateVM (e.g. Debian Stable)

xen

hardware
Qubes OS: single-user desktop-based Xen distribution

- Dom0 (Fedora)
- TemplateVM (e.g. Debian Stable)
- AppVM
- DispVM
- Vault VM

An AppVM with no network

xen

hardware

https://securedrop.org
Qubes OS: single-user desktop-based Xen distribution

- Dom0 (Fedora)
- AppVM
- DispVM
- Vault VM
- TemplateVM (e.g. Debian Stable)
- sys-net

Networking stack runs in sys-net

xen

hardware
Qubes OS: single-user desktop-based Xen distribution

Dom0 (Fedora)

AppVM

DispVM

Vault VM

TemplateVM (e.g. Debian Stable)

sys-firewall

sys-net

Firewall rules applied

xen

hardware
Qubes OS: single-user desktop-based Xen distribution

- Dom0 (Fedora)
- AppVM
- DispVM
- Vault VM
- TemplateVM (e.g. Debian Stable)
- sys-net
- sys-firewall
- sys-usb

Handles USB controllers

- xen
- hardware
Qubes OS: single-user desktop-based Xen distribution

Inter-VM communication via qexec, based on Xen’s vchan

Dom0 (Fedora)
AppVM
DispVM
Vault VM
templateVM (e.g. Debian Stable)
xen
hardware
SecureDrop Workstation architecture
New consolidated architecture
to internet

sys-net

sys-firewall

tor

ProxyVM

qreexec
- Vault (non-networked)
- Disposable vault
- Networked AppVM
- System VM
sys-net

sys-firewall

tor

ProxyVM

User GUI application, displays conversations

Vault (non-networked)
Disposable vault
Networked AppVM
System VM

qrelec

to internet
User GUI application, displays conversations

Private key material

sys-net

sys-firewall

tor

ProxyVM

Vault (non-networked)
Disposable vault
Networked AppVM
System VM
Use a hardened template with grsecurity-patched kernel to provide additional generalized exploit mitigations for memory corruption vulnerabilities.
What the journalist sees
SecureDrop Workstation: Journalist perspective
SecureDrop Workstation: Journalist perspective

Select a source from the list, to:

- Read a conversation
- View or retrieve files
- Send a response
Reflective hygiene

See attached document. Parts are redacted, and I'm not confident about its authenticity. Still, it matches the research you've been doing, so thought I'd pass it along and provide more if you deem it worthwhile for reporting.

Interesting. Skills indeed be difficult to confirm, let me confer with the tech team here and follow up with you. If you have others that you can re-session, that would be helpful!

Sure, happy to help. Here's the only other document from that cache that I've access to. Again, parts are redacted, but the meaning is clear. Let me know if you think the reporting team deserves in terms of reliability.

Compose a reply to "reflective hygiene"
SecureDrop Workstation: Journalist perspective
Hardening, beyond VM isolation

- Code execution confined by AppArmor
- VMs use a custom kernel, with the Grsecurity patch set, to guard against memory corruption attacks
- Minimal templates suited to trust model in architecture, with common software excluded when appropriate
“Overall, the SecureDrop Workstation system represents a complex but well researched product that has been thoughtfully designed.”

- Trail of Bits, 2020
What’s next?
Pilot program, ongoing

- Small set of news organizations running the Workstation
- Gathering user experience to inform design
- Aiming for general availability in the near future
Future work

- Additional export tooling (e.g. Signal, Onionshare)
- Metadata redaction
- Research use
- Malware detection
- Localization
The team

100% of time on SecureDrop

Mickael Engineering
Kushal Engineering
Kevin Support, Engineering
Allie Engineering
John Engineering
Rowen Support

>= 50% of time on SecureDrop

Conor Engineering
Erik Project Manager
Jen Engineering
Nina UX

>= 25% of time on SecureDrop

Harlo Training
Olivia Training
David Training
Takeaways

● Investigative journalism can be dangerous
● Whistleblowers deserve protection
● Technology can reinforce cultural norms about privacy
Questions?

Get involved:

- SecureDrop: https://securedrop.org/contribute/
- Qubes OS: https://qubes-os.org/
- Tor: https://torproject.org/
- Want to donate? https://freedom.press/donate/

Contact:

Conor Schaefer
Chief Technology Officer
conor@freedom.press