2022-10-27

Entrusted – A document Sanitization Tool
A Brief Introduction

https://github.com/rimerosolutions/entrusted

Agenda

- Introduction
- What is “Entrusted”?
- How does “Entrusted” work?
- Why does “Entrusted” exist?
- What is available with “Entrusted”?
- How to Use “Entrusted”?
- What is Next for Entrusted?

Introduction

When we’re online (using the internet), we exchange data with others all the time. *Someone that you trust can still send you malware, without even being aware of it.*

Internet hyperlinks to documents containing malware

Dangerous files downloaded from file sharing programs

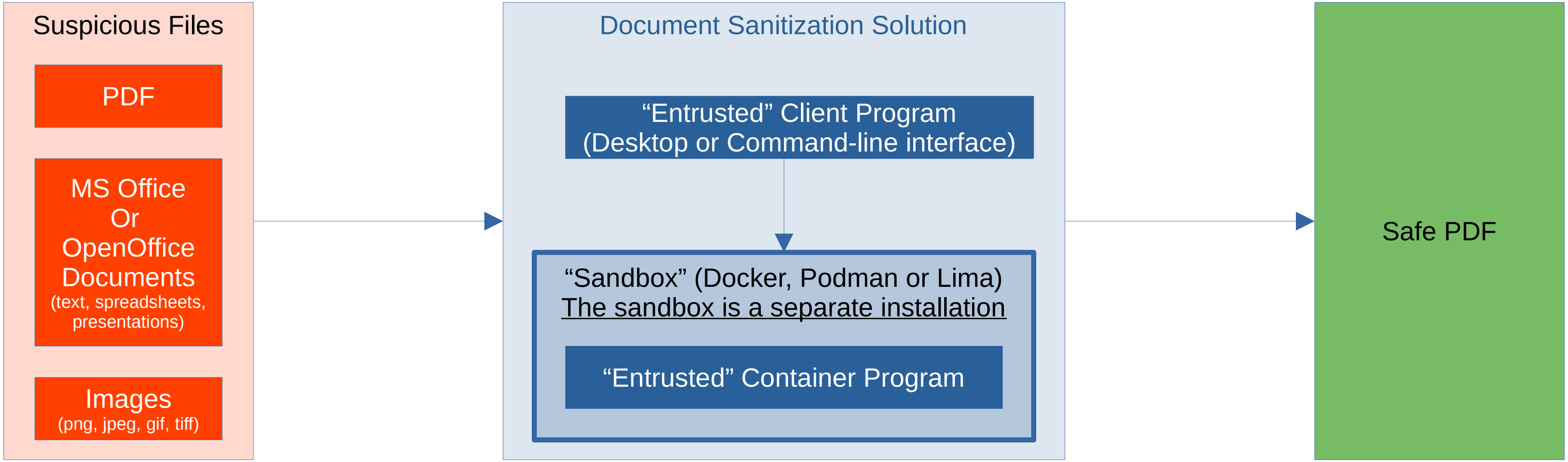
Email attachments with viruses

Suspicious files exchanged in instant messaging tools

Several other ways to receive malware

What is Entrusted?

“Entrusted” is a **document sanitization solution** that converts “**potentially suspicious files**” into **safe PDFs**. File processing happens inside a “sandbox”.



Suspicious Files

PDF

MS Office Or OpenOffice Documents (text, spreadsheets, presentations)

Images (png, jpeg, gif, tiff)

Document Sanitization Solution

“Entrusted” Client Program (Desktop or Command-line interface)

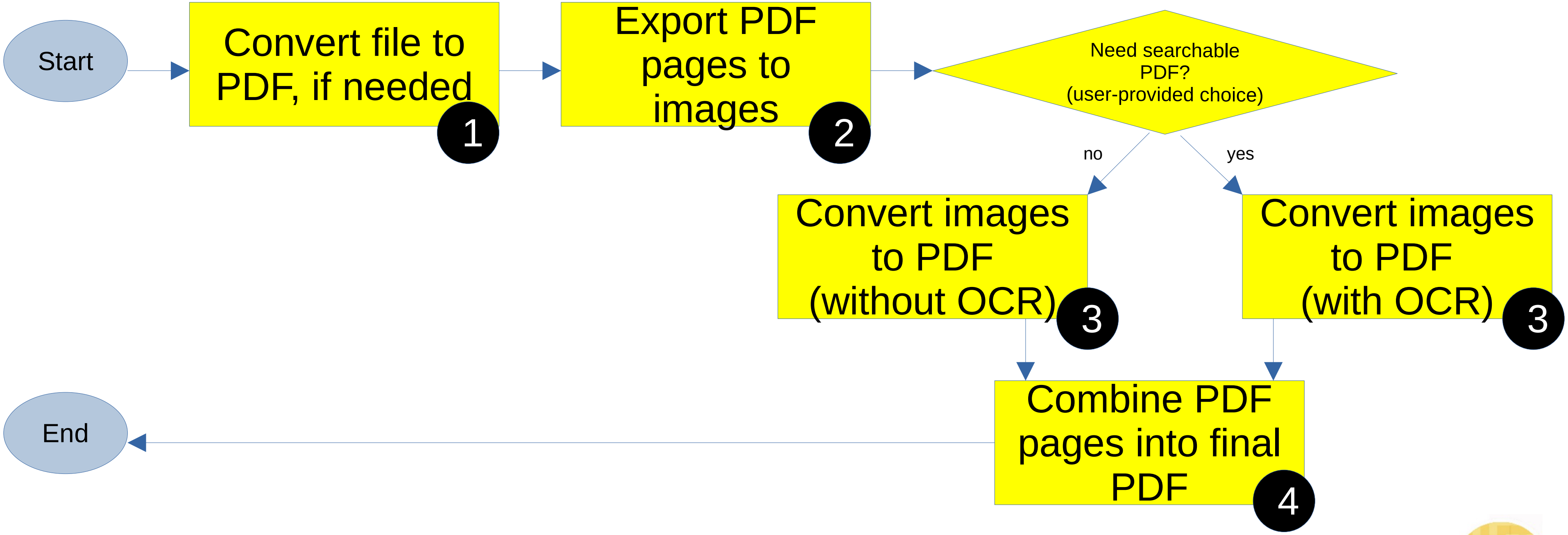
“Sandbox” (Docker, Podman or Lima)
The sandbox is a separate installation

“Entrusted” Container Program

Safe PDF

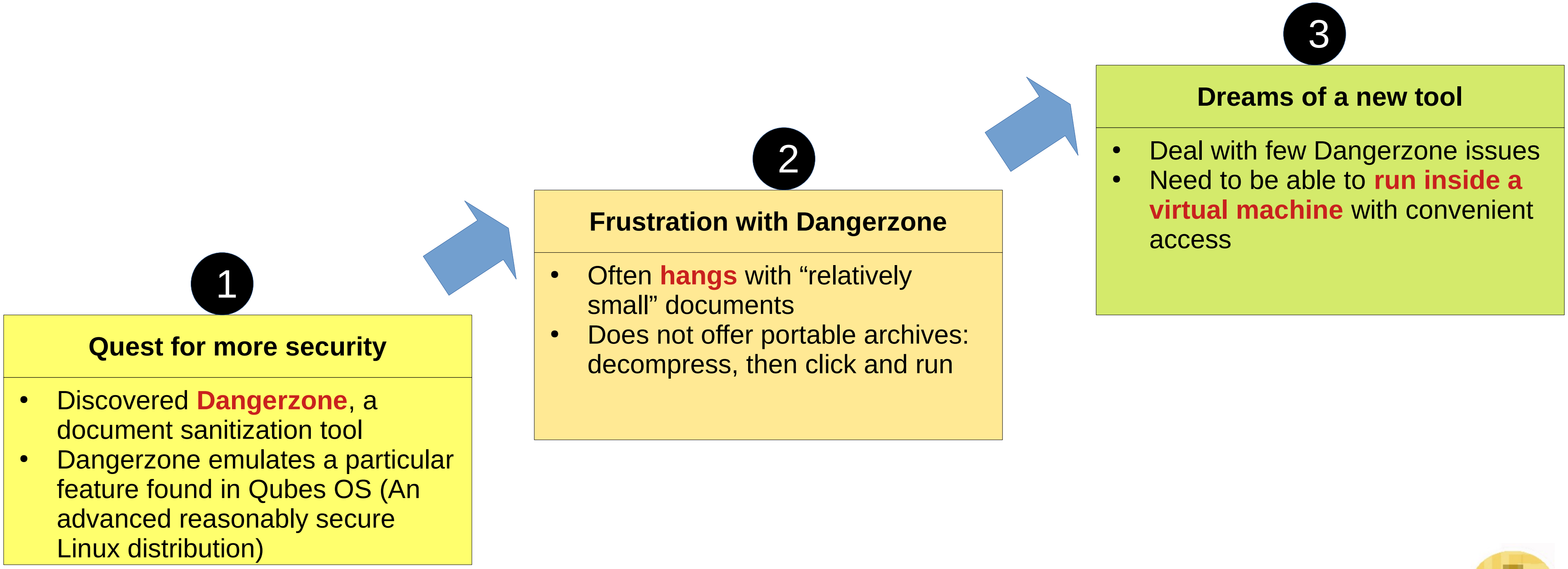
How Does "Entrusted" Work?

The diagram below describes the sanitization process inside "the sandbox".


Start
Convert file to PDF, if needed
1
Export PDF pages to images
2
Need searchable PDF? (user-provided choice)
no
yes
Convert images to PDF (without OCR)
3
Convert images to PDF (with OCR)
3
Combine PDF pages into final PDF
4
End

Why does “Entrusted” exist?

Entrusted exists because of limitations found in a tool called Dangerzone.



1

Quest for more security

- Discovered **Dangerzone**, a document sanitization tool
- Dangerzone emulates a particular feature found in Qubes OS (An advanced reasonably secure Linux distribution)

2

Frustration with Dangerzone

- Often **hangs** with “relatively small” documents
- Does not offer portable archives: decompress, then click and run

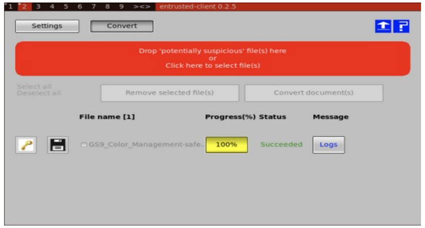
3

Dreams of a new tool

- Deal with few Dangerzone issues
- Need to be able to **run inside a virtual machine** with convenient access

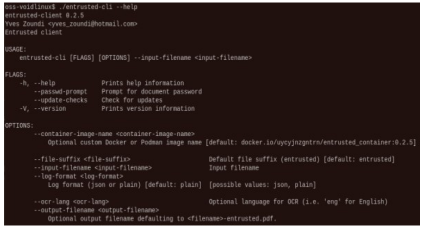
What is Available with “Entrusted”?

Available User Interfaces



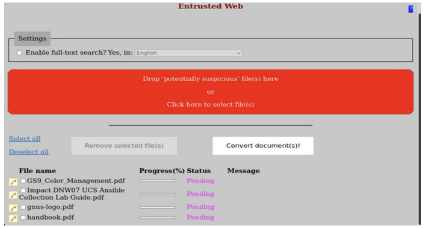
File name [1]	Progress(%)	Status	Message
□ GS9_Color_Management-safe...	100%	Succeeded	Logs

Graphical Desktop Interface



```
oss-voidlinux$ ./entrusted-cli --help
entrusted-client 0.2.5
Yves Zoundi <yves_zoundi@hotmail.com>
Entrusted client

USAGE:
    entrusted-cli [FLAGS] [OPTIONS] --input-filename <input-filename>

FLAGS:
    -h, --help            Prints help information
        --passwd-prompt   Prompt for document password
        --update-checks   Check for updates
    -V, --version         Prints version information

OPTIONS:
        --container-image-name <container-image-name>
            Optional custom Docker or Podman image name [default: docker.io/uycyjnzgntrn/entrusted_container:0.2.5]

        --file-suffix <file-suffix>                      Default file suffix (entrusted) [default: entrusted]
        --input-filename <input-filename>                Input filename
        --log-format <log-format>
            Log format (json or plain) [default: plain]  [possible values: json, plain]

        --ocr-lang <ocr-lang>                            Optional language for OCR (i.e. 'eng' for English)
        --output-filename <output-filename>
            Optional output filename defaulting to <filename>-entrusted.pdf.
```

Command-line Interface



□ Enable full-text search? Yes, in: English

File name	Progress(%)	Status	Message
□ GS9_Color_Management.pdf		Pending	
□ Impact DNW07 UCS Ansible Collection Lab Guide.pdf		Pending	
□ gnus-logo.pdf		Pending	
□ handbook.pdf		Pending	

Web Interface

Key Features

- Supported document types and images are converted inside a “sandbox” (network access disabled)
- Files can be processed in batch (sequentially)
- Sanitization of big documents is frictionless
- Password-protected documents are handled (PDF files or Office documents)
- A live CD provides additional security and convenience (Web interface and pre-installed container solution)

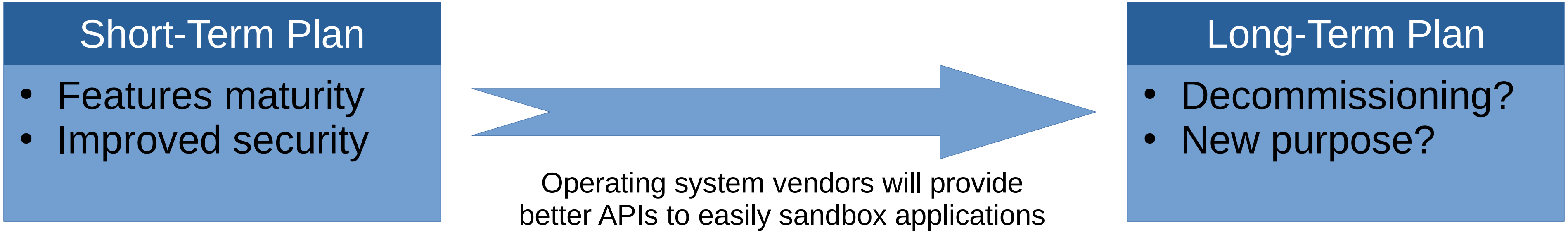
How to Use “Entrusted”?

- **Live Demo**
  - See the graphical Desktop interface in action (development build)
  - The application is running inside an Ubuntu Linux virtual machine
- **Pre-Requisite**
  - First, you’ll need to install a “sandbox solution” (“container engine”):
    - Docker (Linux, Mac OS or Windows)
    - Podman (Linux)
    - Lima (Mac OS)
  - Then you can grab “Entrusted” binaries from the project releases page on GitHub

What Is Next for “Entrusted”?

Entrusted is still a fairly new tool with a small user base, it hasn’t been battle-tested in the wild.

- The application seems to handle well common use-cases so far
- Community involvement is crucial to help the application grow and mature



Short-Term Plan

- Features maturity
- Improved security

Operating system vendors will provide better APIs to easily sandbox applications

Long-Term Plan

- Decommissioning?
- New purpose?

Few References

- Entrusted and Some Related Projects
  - Entrusted project page (github.com)
  - Qubes OS Linux Distribution website (qubes-os.org)
  - Dangerzone project page (github.com)
- Optical Character Recognition (wiki.beparanoid.de)
- Containers
  - General Information
    - Sandbox minimal definition (wiki.beparanoid.de)
    - Introduction to containers (digitalocean.com)
  - Container Security
    - Basic security principles for containers and container runtimes (redhat.com)
    - Docker vulnerabilities (opencve.io)
    - Podman vulnerabilities (opencve.io)