

Introduction

The Lost Art of Keeping a Secret

Requisite Bio Slide

- I have been doing things to computers for a long time.
- During the day I am a computer security consultant at a big company.
- teach in the afternoons.
- ► Some of my background is at this link https://g.dev/franklin

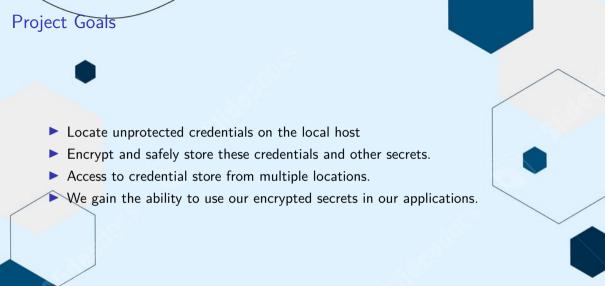


Step One: Admit That You Have a Problem

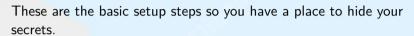
Most of us have a (reasonable?) expectation of trust for the files on our local machine. And so, we leave things like saved passwords and other credentials and secrets pasted into text files for quick access.



Figure 1: You



Setting Up your Stash



- Create a repository on FOKS or other revision control system.
- ► Install the framework (demo coming up).
- Set up your GPG key.
- Add items to DB, remove plain text tokens and secrets.

In the following slides we will break each of these items down.



FOKS Backend

► The backend revision control system for this project is Federated Open Key Service.





Video: Setup



Figure 2: Video: Setup





Video: Install Client



Figure 3: Local Client Installation

Finding and Protecting Secrets

What is it you want to protect?

What Do We Mean by Secrets, Exactly

- Credentials for example a username/password for that lab host that you only need for a couple weeks.
- ► Text files that are used as keys.

The Process of Finding Secrets

- ▶ Look around your local machines for tokens and credentials.
- Use some automation to help you find them.

Demo Script: Scanning Your Local System

Here is a small tool that you can use/modify for your system



Demo Script: Scan Local System



Figure 4: Setup Video Two

Hide Your Goodies

We found the secrets, now what?



Storing Tokens at Rest

We will use a tool called pass in combination with out GnuPG key to encrypt the secrets we found.

- Okay we found some, now what?
- ▶ Encrypt the tokens and push them into a Revision Control System.
- ► Could be a "private repo" but it doesn't have to.





Saving Multi-line Tokens Use pass to encrypt a multi-line secret and push it into Revision Control.

Backing up Tokens to RCS

- ► Encrypt the tokens and secrets
- Push everything into revision control.

Using Your Stashed Tokens

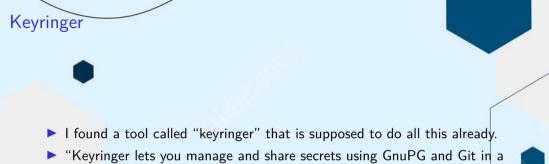
How to Use What You Built





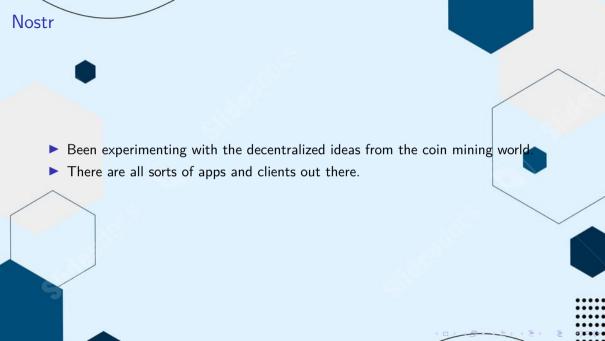
Other Cool Stuff

Where is all this going?



- "Keyringer lets you manage and share secrets using GnuPG and Git in distributed fashion."
- ► will incorporate it into this tool set if that makes sense.





Kerberos and OpenLDAP Research if there is any possible overlap. Integration with Kerberos on a LAN?



