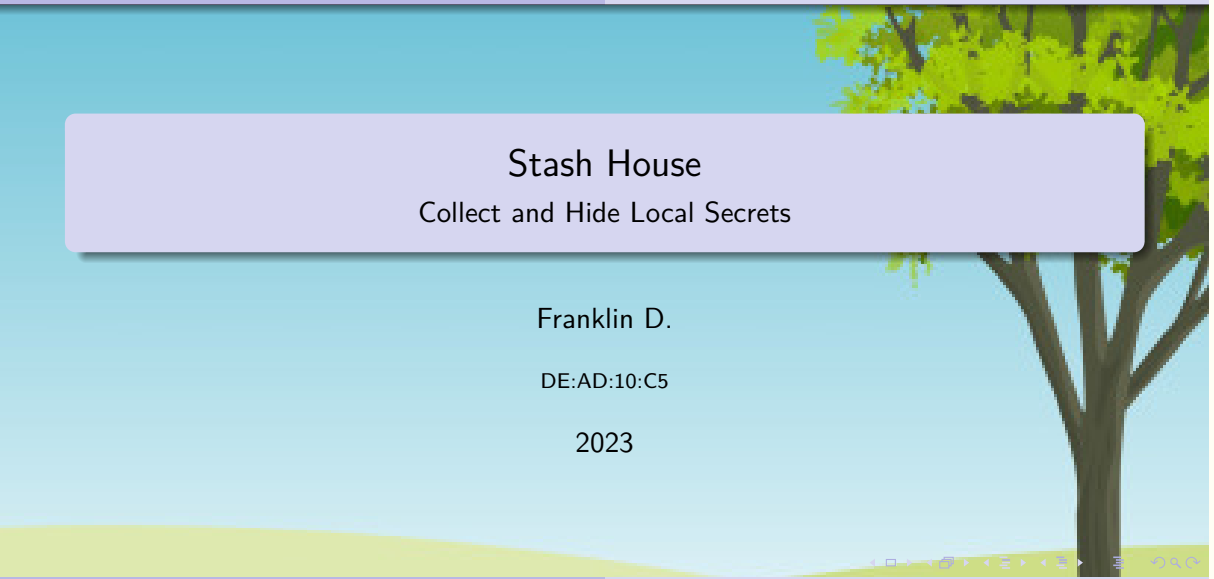

Stash House

Collect and Hide Local Secrets

Franklin D.

DE:AD:10:C5

2023

1. https://www.youtube.com/watch?v=DYDT165LGBY

Introduction

The Lost Art of Keeping a Secret

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

Step One: Admit That You Have a Problem

1. Yes you do this
2. No it's not good

Project Goals

- Locate unprotected credentials on the local host
- Encrypt and safely store these credentials and other secrets.
- Access to credential store from multiple locations.

Project Goals

1. Clean up the ones we know about
2. Of course there will always be gaps and edge cases, just try to improve over time
3. What prior art is out there

Finding Those Creds

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.

n my case I had a whole folder of text files that I'd collected of some time.

What Do We Mean by Secrets, Exactly

1. I

Finding Tokens

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

Finding Tokens

1. There are some known places we can look
2. Clean up the ones we know about

Demo Script

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

Demo Script

1. Do a small demo here

Hide Your Goodies

We found the secrets, now what?

Saving Simple Tokens

- Encrypt the tokens and push them into RCS.

Saving Simple Tokens

Setting Up the Stash House

- Create a repository on GitHub or other revision control system.
- Install the framework with shell script.
- Set up your GPG key.
- Add items to DB, remove plain text tokens and secrets.

Setting Up the Stash House

Saving Simple Tokens

- Encrypt the tokens and push them into RCS.

he first kind of secret we want to save is a "simple" password, basically a string.

Saving Simple Tokens

1. T

Saving Multi-line Tokens

- Encrypt the tokens and push them into RCS.

e can also save multi-line secrets, GCloud JSON for example.

Saving Multi-line Tokens

1. W

Backing up Tokens to RCS

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

Backing up Tokens to RCS

Using Your Stashed Tokens

How to Use What You Built

Using Tokens

- Now you can use the secrets in your project without exposing them.

Using Tokens

Considerations

- You need your GPG key on the local machine to encrypt, decrypt, and use the secrets.

Considerations

1. Don't be lazy, you still have to use a password manager