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.
- I teach in the afternoons.
- Some of my background is at this link https://g.dev/franklin

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.

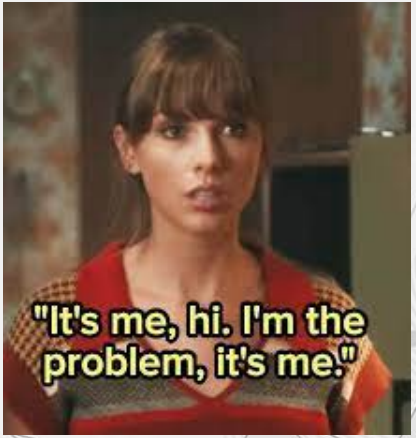

Figure 1: You

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.
- We gain the ability to use our encrypted secrets in our applications.

Setting Up your Haunted Stash House

These are the basic setup steps so you have a place to hide your secrets.

- Create a repository on GitHub or other revision control system.
- Install the framework (demo soon).
- 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.

Demo Script: Setup

- Here is a stash-house setup tool that you can use/modify for your system.
- “https://github.com/devsecfranklin/stash-house”

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

Hide Your Goodies

We found the secrets, now what?

Setting up GnuPG

- GPG key setup.
-

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 Simple Tokens

- Use the pass tool to encrypt the tokens and push them into Revision Control.

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

Using Tokens

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

Considerations

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

Other Cool Stuff

Where is all this going?

Keyringer

- I found a tool called “keyringer” that is supposed to do all this already.
- “Keyringer lets you manage and share secrets using GnuPG and Git in a distributed fashion.”
- I will incorporate it into this ...toolkit?

Nostr

- Been experimenting with the decentralized ideas from the coin mining world.
- There are all sorts of apps and clients out there.

Kerberos and OpenLDAP

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

demo container

- There is a container file in the project repo.

SSH Key Setup

-

Github Setup

-