Kyle Hagood, Zachary Conner, Syed Rizvi
CMSC 413 Project Report
Password Management System

Overview

Working together, we have created a simple password management system with capability to support multiple user accounts with little installation overhead. Our user interface design is built with the JavaFX library and presents a simple, intuitive, and easy-to-use interface for account creation and bound-to-account password management. Beneath the surface, an embedded H2 database is used for information storage. Sensitive information is protected through a combination of the Jasypt and BouncyCastle libraries, where BouncyCastle provides the implementation and Jasypt provides a high-level interface.

Security Measures

Our project hides all sensitive information before database storage, including account and managed passwords. Encryption is accomplished using a password based encryption scheme, where a symmetric private key is built from a pre-generated random 16-bit string. Upon successful key generation, the plaintext data is obfuscated using the SHA-256 hashing algorithm. The hashed data is then encrypted using 128 bit AES with the Cipher-Block-Chaining technique. Only after all sensitive data has been successfully encrypted is any of it stored.

JCE Unlimited Strength Jurisdiction Policy Files

Java behavior dictates that extension of the default cryptographic library requires special policy files to be added to the Java Virtual Machine installation. Required files are found within the project structure.

File name - “jce_policy-8.zip”
File Placement - %JAVA_HOME%/jre/lib/security *and* %JAVA_HOME%/jdk/jre/lib/security

Run Instruction

1. Install the latest version of Java
2. Install JCE Unlimited Strength Jurisdiction Policy Files into Java Installation
3. Download IntelliJ IDE
4. Open project in IntelliJ, and run