MSCS 630L – Spring 2022 – Prof. Aaron Kippins

Project Writeup – Citrus Digital Journal

Christopher Ravosa
christopher.ravosa1@marist.edu

May 15, 2022

I. Abstract

This writeup discusses the technical and design details behind Citrus Digital Journal, an electronic journaling application. It provides context to the inspiration for the application and overviews its internal and external design. The application was developed by Christopher Ravosa to demonstrate a competency in cryptography for the course MSCS 630N Security Algorithms and Protocols.

II. Introduction

Citrus Digital Journal is a desktop application created with Python. The application functions as a private journal, taking care to encrypt journal entries using the *Advanced Encryption Standard* (AES). Entries can be decrypted by reversing the order of the rounds' state transformations in the AES algorithm and replacing each transformation by its inverse transformation. Decryption only occurs on journal entries given a user's unique key (Stanoyevitch 439).

The use of AES to encrypt and decrypt journal entries negates the requirement of user accounts and passwords. Any instance of Citrus Digital Journal can be run with full confidence that a user cannot decrypt another user's entries without the secret key used when the entry was created. Additionally, entries are stored locally via a SQLite database embedded directly into each instance of the application. This means that user data is stored only on their own devices, never in a remote location accessible by anyone other than the device owner. Entries are stored in their encrypted state on the database.

Due to the limited scope of the project, Citrus Digital Journal will only support one user per device. This is subject to change as the project expands, but the application will only support one user by the end of the Spring 2022 semester.

III. Background & Related Work

Some background in cryptography and computer science is recommended to adequately analyze this project. The concepts which were used to conceive, design, and develop Citrus Digital Journal are discussed here.

The purpose of Citrus Digital Journal is to demonstrate the developer's understanding of cryptography fundamentals. To do this, the developer decided to demonstrate the effectiveness of the AES encryption algorithm via the application. The AES is based on the Rijndael encryption algorithm developed by Belgian cryptographers, Joan Daemen and Vincent Rijmen (Stanoyevitch 418). The pair's algorithm was selected by the U.S. *National Institute of Standards and Technology* (NIST) to form the basis of the AES which is now used by the United States government to encrypt top secret documents. The intricacies of the AES will not be discussed in this writeup, but readers are expected to have a firm understanding of the subject. In addition to a basic understanding of cryptography, readers should be familiar with modern programming practices. Citrus Digital Journal was developed using the Python scripting language.

Lastly, readers should have a working knowledge of databases and their implementation. The embedded database used for Citrus Digital Journal is very simple and leverages only one table. If one is to review the code used to create the database, they should still understand how relational databases are constructed and maintained. The internal design of the application will be discussed in the next section.

IV. Methodology

Inspiration for the application came from Christopher Ravosa's tendency to scribble thoughts down in a moleskin journal. Upon further investigation, it became apparent that digital journals exist in abundance in marketplaces like Apple's App Store. Christopher concluded that this type of application is functional and would be a great way to demonstrate encryption with AES. Furthermore, it adds meaning to the demonstration by placing it in a context which consumers are actually interested in.

Given that the project doesn't require an immense amount of computing power, it was decided that Python would be a reliable language to develop it with. Python has an abundance of libraries available for small desktop applications. Additionally, the availability of frontend frameworks for Python will allow Citrus Digital Journal to be presented in a user-friendly manner. The graphical user interface (GUI) for the application was developed with the DearPyGui API. DearPyGUI is a cross-platform, graphical user interface toolkit for Python (Hoffstadt 1). The GUI had previously been in development using the cross-platform GUI API, PyGUI, which allows the construction of GUIs for Python applications running on Unix, Mac, and Windows (Ewing 1). However, the documentation for PyGUI proved to be less informative than DearPyGui's. The developer decided to switch frameworks to reduce the amount of time required to develop the frontend.

Since the application must store user entries, it requires a database. Each instance of the application assumes it is being used by a single user (thought multiple users can share an instance securely). So, a database is embedded directly into Citrus Digital Journal. This was done with SQLite. SQLite is a library which provides a self-contained, relational database management system (DBMS) (SQLite Tutorial 1).

Lastly, unit tests were used to validate the execution and return values of every method used for encryption and decryption with AES. Failure to validate the successful implementation of these methods could lead to errors in the decryption of user entries. Worse, it could lead to the data being compromised by attackers. Test cases for AES methods can be found in the *test_aes.py* file in the Citrus Digital Journal source code repository.

For version control, the developer used GitHub. The Citrus Digital Journal repository exists at *https://github.com/crav12345/Citrus-Digital-Journal*. Citrus Digital Journal is being developed solely by Christopher Ravosa.

V. Experiments

The amount of experimentation required to develop Citrus Digital Journal was very limited. Apart from research to find a suitable GUI framework, the application's requirements were very clear.

The most difficult part of developing this application was the implementation of AES in Python. The majority of "experimentation" done on this project was through test cases. These test cases exist to verify that the results of various AES functions return correct values. Past this, the application required no experimentation.

VI. Discussion & Analysis

The minimum requirements of this application are that it be able to encrypt, store, and decrypt user journal entries. However, part of the decision to create this type of application is that it lends itself to expansion. One journaling app with many more features than those required for Citrus Digital Journal's minimum requirements is Day One Journal: Private Diary. This application is an Editor's Choice on Apple's App Store and offers a daily prompt, tips for mental health, and a calendar to help users decide what to write about on a given day (Bloom Built Inc. 1).

As stated previously, little experimentation was required to conceive and develop Citrus Digital Journal (at this point in time). The application employs tested, reliable encryption methods. Its development also follows programming best practices to the best abilities of the sole developer. However, as the developer completes the first version of the application, more experiments may be done. These experiments would be done to determine which features might be realistic to add in the near future.

VII. Conclusion

Citrus Digital Journal meets the minimum requirements of the project prompt. Furthermore, it lends itself to expansion. Its architecture is lightweight making it easy to iterate on. It will be made available publicly on Christopher Ravosa's GitHub. Citrus Digital Journal should serve as both a great portfolio piece and a simple demonstration of the power of AES.

VIII. References

"Advanced Encryption Standard." *Wikipedia*, Wikimedia Foundation, 6 Apr. 2022, https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Bloom Built Inc. "Day One Journal: Private Diary." *App Store*, Apple, 9 July. 2021, https://apps.apple.com/us/app/day-one-journal-private-diary/id1044867788.

Ewing, Gregory. "The Python GUI Project." *University of Canterbury*, University of Canterbury, https://www.csse.canterbury.ac.nz/greg.ewing/python_gui.

Hoffstadt, Jonathan & Preston Cothren. "Dear PyGui's Documentation." DearPyGui, https://dearpygui.readthedocs.io/en/latest/index.html#:~:text=Dear%20PyGui's%20Documentation-,About%20DPG,to%20create%20a%20functional%20layout.

"SQLite Tutorial." SQLite Tutorial, 2022, https://www.sqlitetutorial.net/

Stanoyevitch, Alexander. "Introduction to Cryptography." *California State University*, Contemporary Scientific Press, 2020.