Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

BACHELORARBEIT

FACHBEREICH 4: INTERNATIONALE MEDIENINFORMATIK

Thunderbird Add-on: 'One Time Password/Pad' Encryption

Student
Esteban LICEA

Mentor/Supervisor
Prof. Dr. Debora
WEBER-WULFF

April 11, 2022

1 Thesis Proposal

The bachelor thesis candidate intends to research and develop a Thunderbird Add-on, that will fulfill one specific use case. Namely, Alice wants to send an encrypted message to Bob, but Bob is clueless about encryption technology, and can't be bothered learning, installing, or setting up any type of keys. However, they communicate regularly, so Alice can just whisper a one time password to him, or even via a telephone conversation–for any important message she wants to send him. Alice then would like to use a Thunderbird add-on, that will allow her to encrypt the message with that password, that Bob can later open with that same password. The message will be encrypted point-to-point. [1]

Research will dictate the best implementation strategy with likely possibilities including a "one time pad" or "one time password" solution. The goal is for the best solution to the use case, while also providing the best possible security.

2 Methods

The methods and or tools used to solve this research inquiry will include:

1. Literature either in the form of online or paper publications, i.e. books
2. Online learning resources
3. Thunderbird and JS Encryption APIs
4. Guidance from Mentors
5. Visual Studio Code for code production
6. Github for Source Code and Thesis code management
7. Latex for writing the Thesis
8. Jira for project management, i.e. Kanban board, sprints, and road maps

[1] Alice and Bob are fictional characters commonly used as placeholders in discussions about cryptographic systems and protocols. https://en.wikipedia.org/wiki/Alice_and_Bob

3 Methodology

The researcher will seek to determine the best practices for encrypting email communications. Furthermore, the researcher will implement a ”one-time pad” or ”one time password” type encryption add-on to be used with the multi-platform email client Thunderbird. Research will guide the final implementation. The study will examine the different possible approaches to email encryption, the challenges and solutions to such goals.

Previous coursework in cryptography under the instruction of Prof. Dr. Weber-Wulff and Dr. Thiel has laid the foundation for my understanding the strengths of various methods, and equally, the possible pitfalls involved with various implementations – as the math is generally sound in perfect use cases.

The implementation foreseen by the author suggests that there will be challenges, and may not represent the ultimate solution, however, the goal is to reach a level of acceptability given the constraints of no key exchange. With this in mind, the author will highlight and spotlight vulnerabilities and attack vectors with this implementation. Not in an effort to break the system or limit culpability, but to be as informed as possible and reduce these weaknesses on the system.

After the research has been completed, all coding will proceed using a test driven development approach. Thunderbird Add-ons are based on MailExtension technology, which are created using the follow standard languages:

1. HTML
2. CSS
3. Javascript

Upon completion, the project will be submitted to Thunderbird.