Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

BACHELORARBEIT

FACHBEREICH 4: INTERNATIONALE MEDIENINFORMATIK

Abstract: Thunderbird Add-on, 'One Time Password' Encryption

Student
Esteban LICEA
Matr. Nr. 536206

Primary Mentor
Prof. Dr. Debora
WEBER-WULFF

Secondary Mentor
Prof. Dr Kai Uwe
BARTHEL

May 23, 2022

1 Introduction: Problem defined

The bachelor thesis candidate intends to research and develop a Thunderbird Add-on, that will allow Alice wants to send an encrypted message to Bob. Bob is not tech savvy and clueless about encryption technology, and so learning, installing, or setting up any type of keys is impossible. 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 could then use a Thunderbird add-on, that will allow her to encrypt the message with a 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 password" solution. The goal is for the best solution to the use case, while also providing the best possible security.

2 Context of the problem

While PGP has existed for years, it is predicated on the exchange of public keys. In clear text, there is a technical requirement to create and exchange keys, and installation of any additional required client software that most average users do not have the patience to complete. Originally, Thunderbird relied on an add-on, Enigmail, to create, manage, and exchange keys.

Starting with Thunderbird 78, Mozilla implemented OpenPGP as part of it's core client software, and dropped support for all add-ons not using MailExtensions (which includes Enigmail). However, the feature is disabled by default, and is still considered a work in progress. All other add-ons found on Thunderbird's extensions page or searching through Github were considered to be in a testing or experimental phase.

[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 Research concept

The researcher will seek to determine the best practices for encrypting email communications. Furthermore, the researcher will implement a ″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.

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.

Upon completion, the project will be submitted to Thunderbird.

4 Research methods employed

The methods and 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

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

5 Technical Implementation

*** More here after the research is complete. ***

6 Obstacles Encountered their and solutions and compromises

*** More here after the research is complete. ***

7 Outlook

*** More here after the research is complete. ***