BACHELORARBEIT

FACHBEREICH 4: INTERNATIONALE MEDIENINFORMATIK

Thunderbird: One Time Password

Student
Esteban LICEA
Matr. Nr. 536206

Primary Mentor
Prof. Dr. Debora
WEBER-WULFF

Secondary Mentor
Prof. Dr Kai Uwe
BARTHEL

June 27, 2022

0.1 Abstract

The developer describes the steps in researching and developing a Thunderbird Add-on that offers E2EE, without the need for key changes, i.e. without PGP. The developed software will allow one user to exchange a keyword/password with another user, encipher a message with that keyword/password, and the other user will be able to decipher to message with that password.

Contents

Chapter 1

Introduction

The digital age has fully absorbed our societies. We do everything in some form or another of digital media: create art, science, communicate, create and share memories, play games, and write thesis reports with our computers. There is basically no limit to what people do with their computers.

Proportional to this growth, the internet's influence on our lives has also ballooned. Our activities have been pushed more and more online, onto the cloud. Originally, few bothered to think about privacy. Most damaging, perhaps, was the erroneous expectation of private communication. Edward Snowden's revelations about the "Five Eyes" intelligence alliance, and cooperation in the collection of all online communication, social media, and phone data. No online communication has been considered safe ever since.

1.1 Problem

Mozilla has tried to support end-to-end encryption (E2EE? for a long time, it has been faced with a major obstacles:

- Setting the PGP add-on Enigmail was too technical
- Generating keys was too technical
- Even if conditions 1. & 2. were fulfilled, it was especially uncommon that anyone else you would want to converse with would have gone through the trouble to setup a client or keys for themselves

- Mozilla is in the process of using OpenPGP build-in to the client, but that also has problems, most obviously, you again need new keys (granted easier to setup this time)
- and, again, both people must have generated keys (again

Thus, the problem: How can Alice send an encrypted email to someone that does not have any type of public key available?

1.2 Context

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.

1.3 My solution to the problem

This project will implement of an Email Add-on that will allow end-to-end encrypted (E2EE) communication. More specifically, it will focus on the Mozilla Thunderbird client, for the simple fact that I have personally used it for over ten years, it's free, open-source, and cross platform. While I grant that not everyone uses Thunderbird, at least there should be no shortage of users, and theoretically anyone can get it easily, for free.

Ultimately, this project aims to offer a simple, albeit *not* perfect solution for those interested in privacy, that don't have the technical expertise to engage in key creation, exchanges or have zero knowledge about encryption. The will demonstrate the advantages and disadvantages

of various implementations strategies, and implement a solution that offers, hopefully, a viable encryption option that will fulfill some use cases.

1.4 Methods applied

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, and fellow Thunderbird add-on developers
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

Bibliography

[Shirey, 2007] Shirey, R., *"RFC 4949 - Internet Security Glossary, Version 2."*, Document Search and Retrieval Page, Aug. 2007, https://datatracker.ietf.org/doc/html/rfc4949.

[Delfs and Knebl, 2002] Delfs, Hans, and Helmut Knebl, *Introduction to Cryptography: Principles and Applications*, p. 12, Springer Verlag, Berlin, 2002.

[Schneier, 2015] Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, p. 155, Wiley, Indianapolis, IN, 2015.

[Nirula, 2022] Nirula, Urvashi, *Block Cipher — Purpose, Applications & Examples*, Document Search and Retrieval Page, https://study.com/learn/lesson/block-cipher-purpose-applications.html

[Aumasson, 2017] Aumasson, Jean-Philippe, *Serious cryptography: A practical introduction to modern encryption*, p. 107, No Starch Press Inc, San Francisco, CA, 2017

[Delfs & Knebl, 2007] Delfs, H., & Knebl, H., *Introduction to cryptography: Principles and applications*, Springer. Berlin, 2007

[Paar & Pelzl, 2009] Paar, Christof., & Pelzl, J., *Understanding cryptography: A textbook for students and practitioners.*, Springer Science & Business Media, 2009

[Dooley, 2008] Dooley, J. F., *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*, Springer, 2008

[Kahate, 2008] Kahate, A., *Cryptography and network security*, Tata McGraw-Hill Education, 2008

[Katz & Lindell, 2007] Katz, J., & Lindell, Y., *Introduction to modern cryptography: Principles and protocols*, CRC Press, 2007

[Martin, 2017] Martin, K., *Everyday cryptography: Fundamental principles and applications*, Oxford University Press, 2017