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 25, 2022

Contents

1 Email - As a communication medium **2**

1.1 Strengths 2

1.2 Weaknesses 2

2 Email Client - Thunderbird **2**

2.1 Why Thunderbird? 2

2.2 WebExtensions 2

3 Cryptography **2**

3.1 Choosing Algorithm 2

4 Project Implementation?? **2**

4.1 Strengths 2

4.2 Weaknesses 2

4.2.1 Attack Vectors - Mitgation 2

5 Summary **2**

1 Specifications

1.1 Personas

This section defines the personas, the most likely and expected users, of the target system. Here are their stories and backgrounds.

1.1.1 Alice - Privacy Advocate

Alice values her online privacy above all. In an ideal world, everyone would use key exchanged based cryptography. But, we do not live in such a world. This frustrates Alice, and she often feels ostrasized that others do not feel the same way. Alice uses other means to try and maintain a level of privacy like sending cloud links to documents or media she would like or needs to share that are password protected - that she will then transmit those passwords through another channel. Usually this includes a additional phone call, or encrypted SMS program like Signal. These additional steps are a bother, but certainly the steps Alice is willing to take to ensure privacy. She will not, in any case, share or send delicate information through ″normal channels,″ i.e. unencrypted emails.

Alice is technically savvy, but she studied Economics. She is committed to privacy, and as an advocate she will do all she can to ensure it, but also she is technically limited, i.e. she's not a computer scientist, if that is a crime.

1.1.2 Bob - Technocrat

Bob values his time most of all. Privacy is not something he cares about. For Bob, ″privacy″ is only for those with something to hide, i.e. criminals, terrorist, etc. Bob is happy to send all correspondence through plaintext emails and attachments. This is how Bob has been doing it for years, and he is happy to continue to correspond this way.

Bob has been working in a corporate environment for years, and has corresponded with all his clients – thousands of emails – without issue. Bob sees no reason to be bothered with any encryption, privacy issues. Bob is annoyed when he has to deal with people like Alice, who do not wish to simply correspond ″like normal people″ via email. Even though Bob works in an environment where data is shared electronically that

might otherwise be considered sensitive, i.e. insurance, legal, medical, Bob still sees no reason to bother. This often leads to friction between the two. [1]

1.1.3 Carlos - Alice's father

Carlos should probably not even be allowed to use a computer. The depth of his skills include *only* the following:

1. Open a web brower
2. Barely enter a URL
3. Barely be able to search the internet
4. Check and Write Emails

That's it!

Anything beyond that is a challenge, and often requires additional support.

1.1.4 Mallory - Alice's evil sister-in-law

Mallory has a Ph.D. in Computer Science, and her competence is only matched by her maliciousness and hatred for her step-sister.

She will stop at nothing to intercept and read Alice's emails. To date, Mallory has had mixed results depending on Alice's diligence.

How can she intercept, decrypt, and read Alice's email in the future, if she uses the "super duper Thunderbird addon?"

1.2 Use Cases

1.3 Use Case Diagrams

1.4 Requirements

[1] Alice is smart enough to know there two types of Bob's. Those with free email services, and those that use more secure email servers. Alice just treats them the same - not secure.

2 Email - As a communication medium

2.1 Strengths

2.2 Weaknesses

3 Email Client - Thunderbird

3.1 Why Thunderbird?

3.2 WebExtensions

4 Cryptography

4.1 Choosing Algorithm

5 Project Implementation??

5.1 Strengths

5.2 Weaknesses

5.2.1 Attack Vectors - Mitgation

6 Summary