



Theses and Dissertations

2014-08-08

Browser-Based Manual Encryption

Yuanzheng Song

Brigham Young University - Provo

Follow this and additional works at: <https://scholarsarchive.byu.edu/etd>



Part of the [Computer Sciences Commons](#)

BYU ScholarsArchive Citation

Song, Yuanzheng, "Browser-Based Manual Encryption" (2014). *Theses and Dissertations*. 4235.
<https://scholarsarchive.byu.edu/etd/4235>

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.

Browser-Based Manual Encryption

Yuanzheng Song

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of
Master of Science

Kent E. Seamons, Chair
Daniel Zappala
Christophe Giraud-Carrier

Department of Computer Science
Brigham Young University
August 2014

Copyright © 2014 Yuanzheng Song
All Rights Reserved

ABSTRACT

Browser-Based Manual Encryption

Yuanzheng Song

Department of Computer Science, BYU

Master of Science

Billions of web-based email and chat messages are sent over the Internet every day. However, very few service providers support end-to-end privacy protection. While providing security for these messages is technically feasible, usability remains a challenge in this field. Recent research attempts to hide security details like key management and encryption in order to make the system more usable. However usability studies demonstrated that hiding these details may confuse the user and contribute to mistakes (e.g., sending out an email in plaintext when the user thought it would be encrypted). In an effort to increase trust and eliminate mistakes, this thesis presents the design of a browser-based manual encryption mechanism that supports automatic key-management and manual encryption. It also describes the Message Protector (MP) prototype. An evaluations of MP is presented based on a user study conducted on the campus of BYU.

Keywords: usable security, secure email, manual encryption, end-to-end encryption

ACKNOWLEDGMENTS

I thank my parents for their support, patience, and encouragement through many years of graduate school at BYU. I also thank Dr. Kent Seamons for being a thoughtful advisor and for his guidance. I appreciate the many hours he spent editing my thesis. Without his contributions to the thesis, I would not have been able to complete it in time. I also appreciate Scott Ruoti for his valuable feedback on my thesis research. I would like to thank my colleagues in the Internet Security Research Lab for their helpful feedback while writing my thesis and preparing my presentation.

Table of Contents

1	Introduction	1
1.1	The Problems	2
1.2	Key Management	3
1.3	Automatic vs. Manual Encryption	3
1.4	Thesis Summary	4
2	Related Work	5
3	Message Protector Design	9
3.1	Transparent Key Management	10
3.2	Manual Encryption and Decryption	11
3.3	Tight integration with the web browser	11
4	Message Protector Implementation	12
4.1	User Interface	12
4.2	The Purpose for Authentication	18
4.3	Encryption and Decryption	18
5	MP Usability Study	24
5.1	Participants	24
5.2	Setup	25
5.3	Tasks	26
5.4	Results	27

5.4.1	Task 1	28
5.4.2	Task 2	28
5.4.3	Task 3	29
5.4.4	Task 4	30
5.5	SUS Evaluation	30
5.6	Lessons Learned	31
5.6.1	Recipient email address	31
5.6.2	Copy and Paste	33
5.7	User Feedback	33
5.7.1	Google OAuth	33
5.7.2	What users liked about MP	34
5.7.3	What users disliked about MP	35
5.7.4	Suggested improvements to MP	36
5.7.5	Browser extensions	37
5.8	Recommendations	38
5.9	Comparison	39
6	Conclusions and Future Work	41
6.1	Conclusions	41
6.2	Future Work	41
	References	43
A	User Study Survey	45
A.1	Introduction	45
A.2	Demographics	45
A.3	Tasks	47
A.3.1	Task 1	48
A.3.2	Task 2	48

A.3.3 Task 3	48
A.3.4 Task 4	49
A.4 User Reaction Survey	49
B Survey Results	53
B.1 Demographics Results	53
B.2 Computer Background Survey Results	54
B.3 MP Survey Results	55
B.4 General Security Questions	69

Chapter 1

Introduction

Email and online social networks are convenient and popular. They are the most common platforms for email and instant messaging currently in use on the Internet. As of December 2012, Email Marketing Reports announced that Microsoft's Hotmail, Yahoo! Mail and Gmail together accounted for well over 1 billion users¹. In 2013, 204 million emails were sent out every 60 seconds². Social networking popularity has increased at an amazing speed for the past 6 years. In 2010, Facebook's internal statistics showed that about 350 million Facebook users sent more than 4 billion personal messages every day³. A Gartner report forecasted that by 2014, social network messaging would be the primary communication method for 20 percent of business users in daily interpersonal business communications⁴.

The vast majority of users do not send encrypted messages through the Internet, even when their messages contain sensitive information. Some service provides encrypt data transmissions between clients and servers using SSL/TLS in order to prevent an attack from eavesdroppers. However, not all providers protect users' conversations. For example, Facebook transports instant messages in plain text by default. This allows eavesdroppers on the network to intercept Facebook Chat conversations. Users need to manually turn on HTTPS in Facebook's account settings in order to ensure that all traffic between the browser and Facebook is encrypted.

¹<http://www.email-marketing-reports.com/metrics/email-statistics.htm>

²<http://www.techspot.com/news/52011-one-minute-on-the-internet-640tb-data-transferred-100k-tweets-204-million-e-mails-sent.html>

³<http://techcrunch.com/2010/11/15/facebook-350m-people-using-messaging-more-than-4b-messages-sent-daily/>

⁴<http://www.gartner.com/newsroom/id/1467313>

Even if messages are transmitted over SSL/TLS to the service provider, they are not protected by encryption on the service provider's computers, storage devices, or during transmission between back-end servers. Google has recently started encrypting Gmail traffic between its data centers^{5,6}, but Google can still read the plain text messages on their servers.

Online messaging service providers (including webmail service providers) have been criticized for their lack of concern for service-side privacy protection. For example, Google recently claimed that people who use web-based email should not expect privacy because their emails will be subject to automated processing in the course of delivery⁷. Service providers might utilize collected information for business purposes (e.g., to determine what ads to serve based on the content), and therefore this poses the risk of unwanted disclosure of users' information [5].

Evidence suggests that some users desire that their sensitive messages be read only by the intended recipient, not the email service providers. Fahl et al. surveyed Facebook users to determine their level of interest in protecting their instant messages [6]. In total, 66.53% of the 514 people surveyed stated that they care or would care about Facebook being able to read Facebook conversations. Thus there is a significant need for usable and secure systems to protect personal messages.

1.1 The Problems

While many cryptographic mechanisms have been developed to meet the privacy needs of today's Internet users, none of these solutions has seen widespread use. This is primarily due to inadequacies in usability and portability. These systems are often compatible with only a single service, requiring a different product for each service the user wants to secure. Previous usability studies have shown that there are several problems surrounding usable

⁵<http://googleblog.blogspot.com/2014/03/staying-at-forefront-of-email-security.html>

⁶<http://www.dslreports.com/shownews/Google-Gmail-Now-Fully-Encrypted-Between-Data-Centers-Servers-128233>

⁷<http://www.dailymail.co.uk/sciencetech/article-2392773/Gmail-email-users-NOT-expect-privacy-Google-claims-stunning-admission.html>

secure communication. This thesis focuses on two of them: key management and automatic vs. manual encryption. Each of these problems must be addressed in order to create a system where the effort required of a user, whether money or time, is low enough to allow the system to become widely deployed.

1.2 Key Management

Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) are relatively mature and stable solutions for secure email messaging that require users to manage their own encryption keys. They have never been regarded as easy to use. PGP requires users to create key pairs using PGP software and to obtain a recipient's public key from a key server before they can send encrypted email. Since no central authority can validate a PGP public key, users need to verify a recipient's public key before sending secure communications. All of these steps cause PGP to be hard to use. S/MIME is much easier to use than PGP. Instead of relying on users' manually deployed key pairs, trusted certificate authorities (CA) handle public key verification and management for users. Users only need to obtain a certificate from a CA prior to sending secure communication. Unfortunately, the procedures for acquiring S/MIME certificates from a CA is difficult and can be costly, thwarting the efforts of non-technical users who wish to encrypt sensitive messages. Neither S/MIME nor PGP is user-friendly, and users avoid encrypted email for this reason.

1.3 Automatic vs. Manual Encryption

Manual encryption exposes ciphertext to the user in some fashion. It may even allow them to copy and paste it into a data sharing application. Automatic encryption usually hides all the encryption details from the user so that they are only exposed to the plaintext.

Traditionally, some researchers have believed that users will reject manual encryption as inefficient and confusing to use. Therefore automatic encryption has been considered as necessary for achieving the widespread deployment of secure online communication. However,

a recent study demonstrated that a system supporting automatic encryption has high usability, it can also lead to a lack of user confidence on whether outgoing messages are indeed encrypted [10]. The consequence is that some users do not trust the system and also that some users mistakenly send out sensitive messages without encryption. Manual encryption has been shown to eliminate mistakes and foster trust [10].

1.4 Thesis Summary

This thesis presents MP (Message Protector), a web browser extension designed to provide end-to-end security for web communications, such as Gmail and Facebook. MP was designed to leverage the strengths of two prior research efforts, Pwm [10] and MP-Original [9, 10], and avoid their weaknesses. The key features of MP include automatic key management, manual encryption, and a user interface integrated with the browser. The thesis presents the design and implementation of MP with a specific focus on usability for new users. It also presents the results of a user study and compares the results to earlier user studies involving Pwm and MP-Original. The user study shows that MP competes well with the two earlier studies based on a slightly higher usability score. The thesis concludes with lessons learned and plans for making future improvements to the system.

Chapter 2

Related Work

Whitten and Tygar [13] published one of the first papers that explored the usability of security software. It provides a definition of usability for security. It also enumerates five properties that make it difficult to design a user interface and poses essential questions for the correct use of PGP 5.0, the target for their evaluation. The evaluation consisted of two parts. First, an informal cognitive walkthrough was conducted to evaluate PGP's usability and identify specific items that failed to meet their definition of usability. Second, a laboratory user study with 12 participants was completed to see how well users could complete specific tasks without outside assistance. The participants were given the task of generating PGP key pairs, getting public keys from each other, and using keys to send signed and encrypted email messages. The results were unexpected. Although 10 of 12 participants successfully distributed their public keys, only 4 of 12 eventually sent correctly signed and encrypted email, and 3 of 12 accidentally emailed the confidential message without encryption. Only one was able to complete all the tasks. Even though PGP 5 has an attractive user interface, the results indicate it is usable enough to provide effective security only for those who already understand the model of public key cryptography.

Based on Whitten and Tygar's results, Garfinkel and Miller [8] conducted a usability experiment of CoPilot, a secure email system based on the key continuity management (KCM) model. The study was nearly identical to the methodology in Whitten and Tygar's study. The KCM model does not rely on a trusted third party to sign certificates. Instead, the KCM model is a trust-on-first-use model where each user generates their own self-signed

certificate that other users initially accept and use to verify that the key does not change in subsequent messages, just like the popular SSH remote access system. After verifying each incoming message using the public key corresponding to the senders' email address, CoPilot uses a colored border to notify users whether messages are signed and whether the sender should be trusted. Unfortunately, although the fundamental usability barriers that Whitten and Tygar identified could be overcome by using the KCM model, 60% of experimenters fell victim to a new identity attack, and 43% of experimenters fell victim to an unsigned message attack. Another disadvantage is that the user interface is too tightly integrated with Outlook Express, so that some participants failed to notice the new warning message displayed under the "To:" box in the user interface.

Fahl et al. [6] conducted a pilot study to determine how to design a usable Facebook message encryption mechanism. Based on the analysis of existing approaches (Encipher.it and uProtect.it), this paper focused on two key features for creating a usable security mechanism to protect social network conversations: automatic or manual key-management and encryption. The paper evaluated the four combinations of these features by using mockups and found that automatic key-management and automatic encryption have the highest preferences due to the user acceptance and usability scores. Based on the findings of the laboratory study, the paper describes the design and implementation of FBMCrypt, a usable service-based encryption mechanism to encrypt Facebook conversations. A usability study was conducted to determine whether automatic key-management and automatic encryption is usable. The study revealed that while all participants successfully encrypted their Facebook conversations, none of them would consider using FBMCrypt to protect their Facebook messages. They found that participants did not trust the automatic encryption mechanism, since it was too transparent to ascertain whether or not the solution indeed encrypted the outgoing messages. This is a strong indicator that an acceptable message encryption system should provide good usability characteristics while at the same time heightening users' perceived protection.

Ruoti et al. [10] conducted a series of user studies regarding how to design a secure webmail system that users would be willing to adopt. They created Private WebMail (Pwm). It uses security overlays to provide an encryption interface on top of the existing Gmail interface. While the usability study demonstrated significant improvements, it also identified problems surrounding the transparency of security details. One of major findings was that 12% (3/25) of the participants mistakenly sent out sensitive messages without encryption because the user interface in encryption mode and in non-encryption mode are so similar. Their work also demonstrated that hiding encryption details can cause some users to be reluctant to trust the system. Based on the lessons learned from Pwm, they built a mockup, Message Protector (MP-Original) [9, 10], which is a standalone application supporting manual encryption in order to study whether users could avoid the usability issues revealed in the Pwm user studies. They observed that exposing security details helped users to trust the system and avoid the mistake of sending out unencrypted messages. However, more users preferred Pwm compared to MP-Original because it is more convenient to have the user interface tightly integrated with Gmail.

In order to simplify the management of public keys, Shamir [11] proposed the idea of Identity-based Cryptography (IBC) where a user's public key can be their identity string (or any arbitrary string). The decryption key is obtained from a key escrow server that derives the key from the user's identity string and a master secret known only to the key escrow server. This approach can simplify key management at the expense of trusting the key escrow server. Boneh and Franklin [3] created Identity-Based Encryption (IBE), the first practical implementation of the idea. This allows Alice to send an email to Bob that she can encrypt using a public key like Bob's email address "bob@company.com" instead of obtaining Bob's public key certificate in advance. When Bob receives the encrypted email, he authenticates himself to a key escrow server with his email address "bob@company.com" and then obtains the associated private key that he can use to decrypt the message. The advantage of this scheme is that Alice can send an encrypted email to Bob before he sets up his key pairs. It

differs from traditional secure email schemes, such as RSA, that require additional effort by users to generate and share key pairs in advance of any secure communication.

Chapter 3

Message Protector Design

This chapter describes the design of Message Protector (MP), a system supporting browser-based manual encryption. MP combines the strengths of two earlier systems, Pwm and MP-Original, while avoiding some of their weaknesses.

Like Pwm, MP is implemented in the browser. However, unlike Pwm it is not tightly-coupled to a specific webmail provider like Gmail. Instead, it is independent from any single web service so that encrypted messages created using MP can be sent and received within any web service used for communicating messages.

Like MP-Original, MP utilizes manual encryption to help users better understand how the system works and to avoid mistakes. Another purpose is to help the users trust the system and be more willing to use it. Unlike MP-Original, MP is tightly-coupled to the browser so that users do not need to exit the browser entirely in order to compose or read encrypted messages.

A primary goal of MP is that it be easy to use by those without a technical background. Any user can begin sending or receiving encrypted messages by simply installing MP and using it without the need for coordinating with the sender or recipient in advance. A sender can encrypt messages for anyone who has a valid email address. Also, a receiver can decrypt messages after receiving them even if they didn't have the software installed ahead of time.

The following are the primary design features of MP that help to meet its objective.

- Easy setup to avoid complicated configuration and prior communication,
- Transparent key management using key escrow,

- Manual encryption to help foster trust in the system and also prevent users from sending out sensitive messages without encryption by mistake, and
- Tight integration with the web browser that is web page-agnostic, enabling end-to-end encryption in any web-based communication system.

3.1 Transparent Key Management

MP supports automatic key management through a key escrow server in order to relieve users from the burden of managing their own encryption keys. A trusted third party hosts a key escrow server that generates encryption keys and delivers them to authorized users.

All secure email systems use a random locally generated key to encrypt each message using a symmetric encryption algorithm such as AES. This random key is also encrypted such that only the recipient can decrypt the key in order to decrypt the message. The key escrow system manages the keys used to encrypt the random symmetric key.

MP is designed to leverage Identity-based Cryptography so that users do not need to exchange keys prior to communicating securely. There are several existing approaches that support this design approach. IBE [3] permits any user to encrypt a message for another user based on the recipients identifier (e.g., email address). The recipient must retrieve their private key from the key server in order to decrypt the random key used to encrypt the message. There are also symmetric encryption schemes that provide similar functionality where the sender and receiver must contact the key escrow server to obtain symmetric keys used to encrypt the random key [6, 10].

The key escrow server must authenticate users to ensure that an encryption key is delivered only to the authorized user. To maximize usability, the key server adopts an approach that does not require the user to create a new account at the key escrow server. The server utilizes email-based authentication as the means to easily authenticate users [7, 12]. This authentication can be implemented to occur once per message, once per session, or once across multiple sessions.

3.2 Manual Encryption and Decryption

MP requires users to perform manual encryption and decryption. This means that the user sees the actual ciphertext during the process to give them greater assurance that the system is working correctly and protecting their message. The user creates their message in the MP compose window and explicitly indicates the message is to be encrypted. After encryption, users copy and paste the ciphertext back to the website application from which they wish to transmit the message, such as Gmail. Visual feedback that a message is protected may help users avoid mistakenly sending sensitive messages without encryption. It may also foster greater trust in the system.

3.3 Tight integration with the web browser

MP is a client-side applications that is integrated into the browser but it is independent from any single website. A message encrypted with MP can be incorporated into many web communication systems. This makes MP easier to deploy and maintain. For example, Pwm may need to be changed when Gmail changes its user interface, but MP requires no such changes.

Chapter 4

Message Protector Implementation

This chapter describes the prototype implementation of MP. It provides a detailed description of the interface that users interact with as they install the system and exchange secure messages.




MP is implemented as a Google Chrome browser extension. It utilizes HTML, CSS, JavaScript, JQuery, Bootstrap, tool libraries, and browser APIs. MP is a browser action¹ that consists of a **Lock** icon added to the Google Chrome toolbar once MP is installed, and a popup window that appears when the **Lock** icon is clicked. The popup window is a graphical user interface (GUI) that is used to compose and read encrypted messages.






A browser extension is essentially a web page. The MP extension was implemented primarily by using HTML and CSS. Bootstrap is a front-end framework for creating web applications that was used to create dropdown menus, tabs, modal dialogs, and progress bars. NicEdit JavaScript, an Inline Content Editor, provides the support for composing and reading sensitive messages. The Kiwi Encryption Library developed in the Internet Security Research Lab at BYU provides the encryption functionality.

4.1 User Interface

Suppose Alice uses MP to generate an encrypted message to Bob and sends it to him using Gmail as shown in Figure 4.1. Bob has not made any prior arrangements to receive the encrypted message. MP is designed to spread in a grassroots fashion, so each encrypted

¹<https://developer.chrome.com/extensions/overview>

Acme Offer (between Applicant and Acme) Inbox x   

 **Fake Company** <acme@isrl.byu.edu> May 16   
to me 

You have received a message that has been **encrypted** using Message Protector (MP).

Directions for decrypting and reading this message can be found at <https://mp.isrl.byu.edu>.

```
----- Begin Encrypted Message -----  
eyJFbmNyeXB0ZWRNZXNzYWdlIjpb7IkVuY3J5cHRpb25JbmZvIjo1U  
1VJSng1MEZpek91cyttTEgxMEtPUT09IiwVmfSdWUioiJFazhCYm  
81bXlCRDBLUjkhTlJ0dUdJODBKemVpMGFyVVNoNUxYFTRWbzVCYnp
```

Figure 4.1: An MP Encrypted Message Received in Gmail

message is accompanied with a plaintext explanation that includes a link to the MP website that provides the following instructions on how to install MP and decrypt the message:

You have received a message that has been encrypted using Message Protector (MP).
Directions for decrypting and reading this message can be found at <https://mp.isrl.byu.edu>.

When Bob clicks on the URL, he is taken to the MP homepage shown in Figure 4.2 that contains step-by-step instructions on how to install MP from the Chrome Web Store. Each step in the instructions has a screenshot to assist the user. Each action the user should select is circled in the screenshot to indicate what users should do in the Chrome Web Store if they do not already have experience installing an extension. Once the installation is finished, the MP Lock icon is displayed in the main Google Chrome toolbar to the right of the address bar. Publishing MP in the Chrome Web Store provides users with a standard, familiar way to easily install MP. Google validates each app before publishing it, so users can have greater confidence that MP is a legitimate application.

After Bob clicks the Lock icon on the Chrome browser toolbar to activate the MP popup window, he is presented with a tutorial that briefly explains how to use MP to decrypt

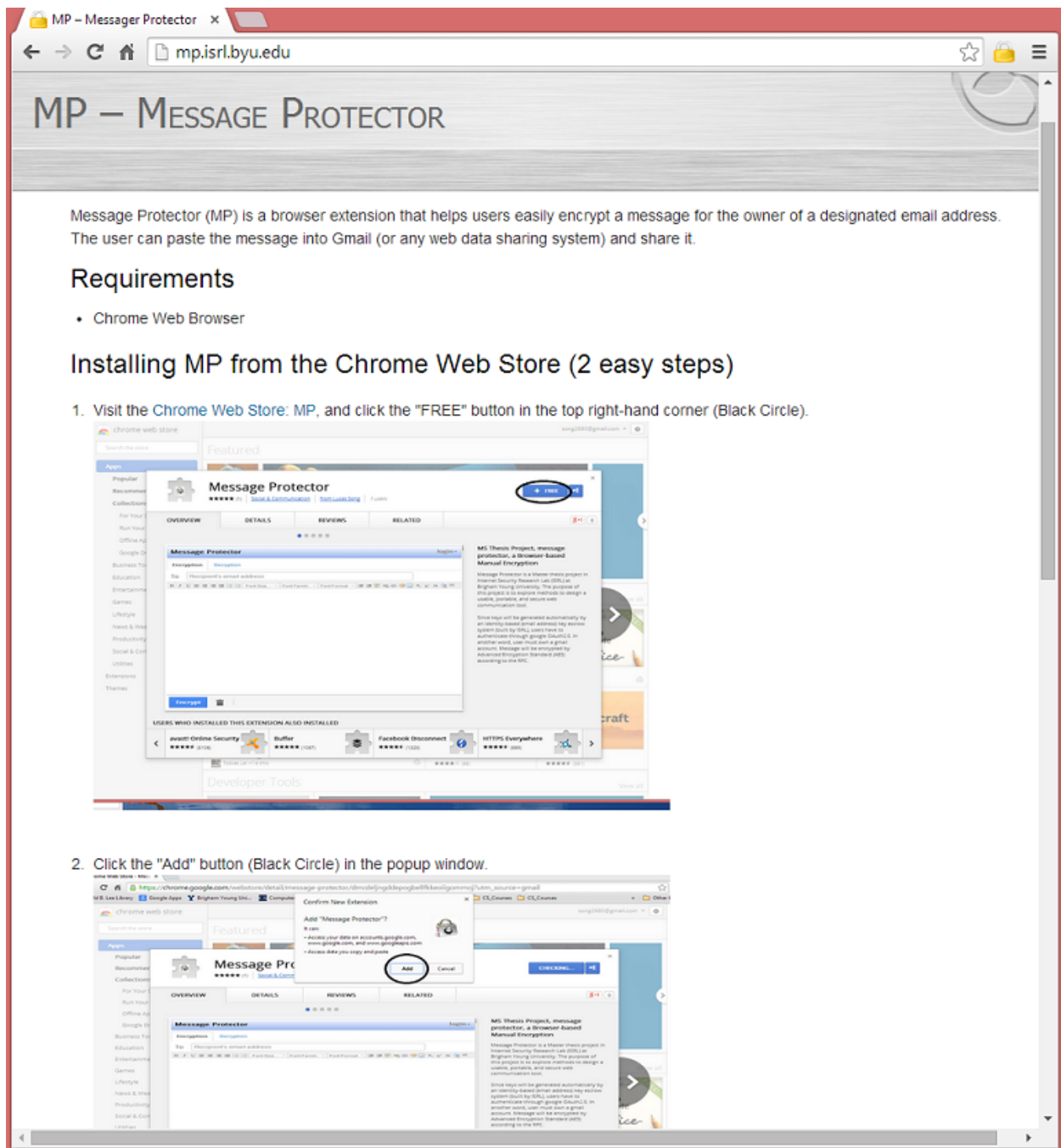


Figure 4.2: MP Homepage

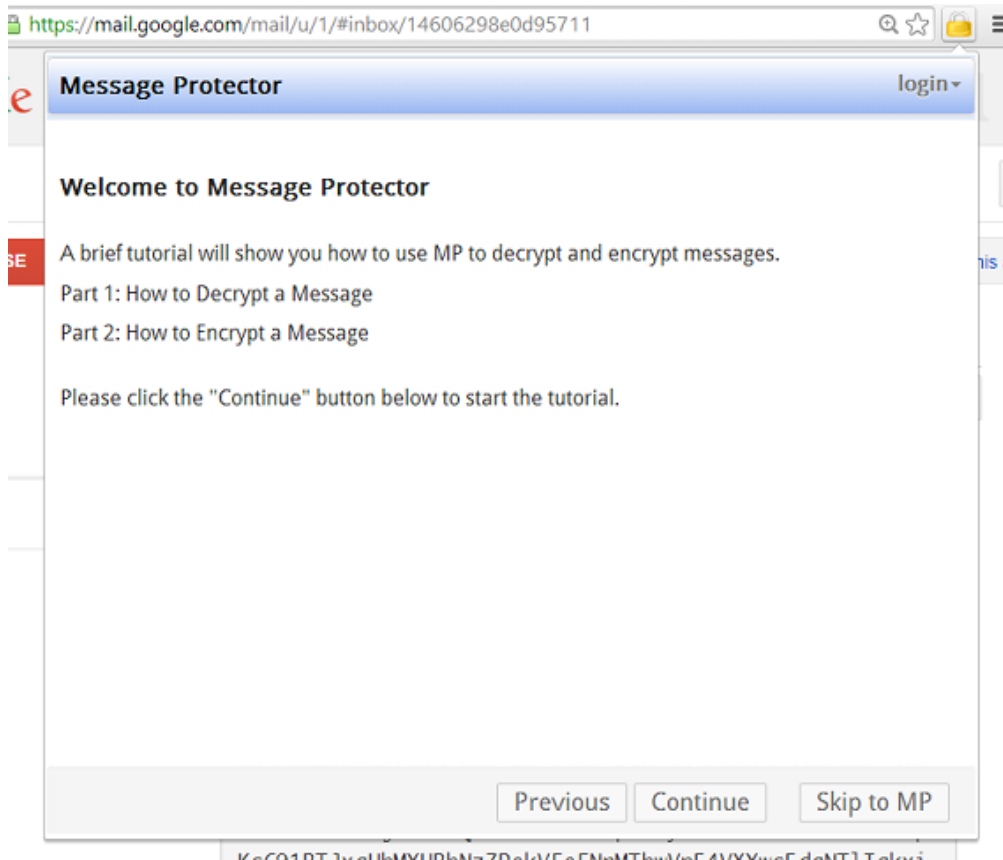


Figure 4.3: MP Tutorial

and encrypt messages (see Figure 4.3). Once the tutorial is completed, he is prompted to log in to his Google Account (see Figure 4.4). He may be prompted to select from among his Google accounts, or he will be prompted to provide a username and password for his Google account (see Figure 4.5). Once Bob supplies valid credentials, he will be prompted to grant MP permission for offline access (see Figure 4.6). After a successful login, Bob grants MP permission to retrieve his profile information (e.g., profile image, name, and email address).

Throughout the remainder of the session, the dropdown component next to the email address of the user triggers a dropdown box for displaying the user's Google account information, such as the user's profile image, user's name, and email address (see Figure 4.7). The user can select to log out or change accounts.

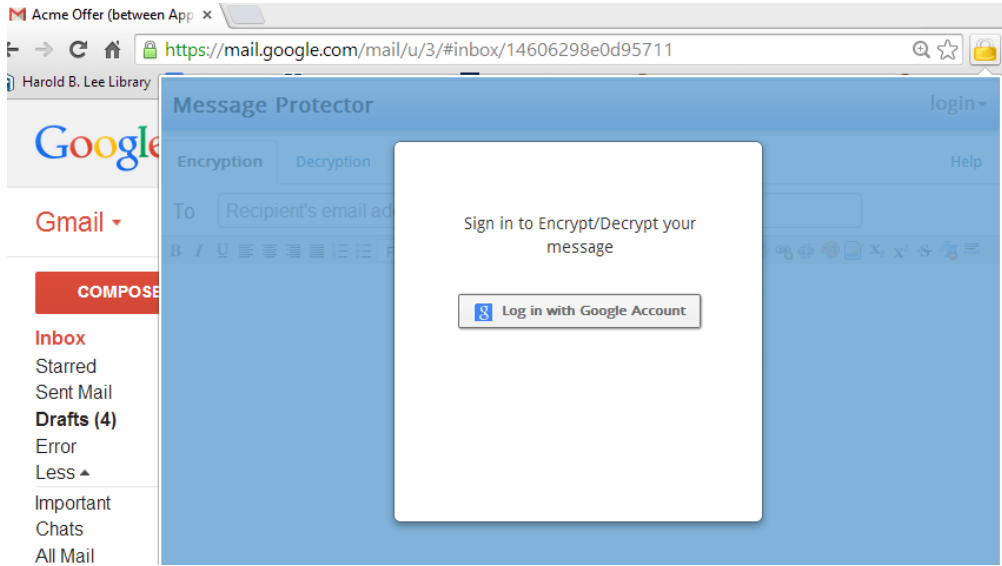


Figure 4.4: MP Login Prompt

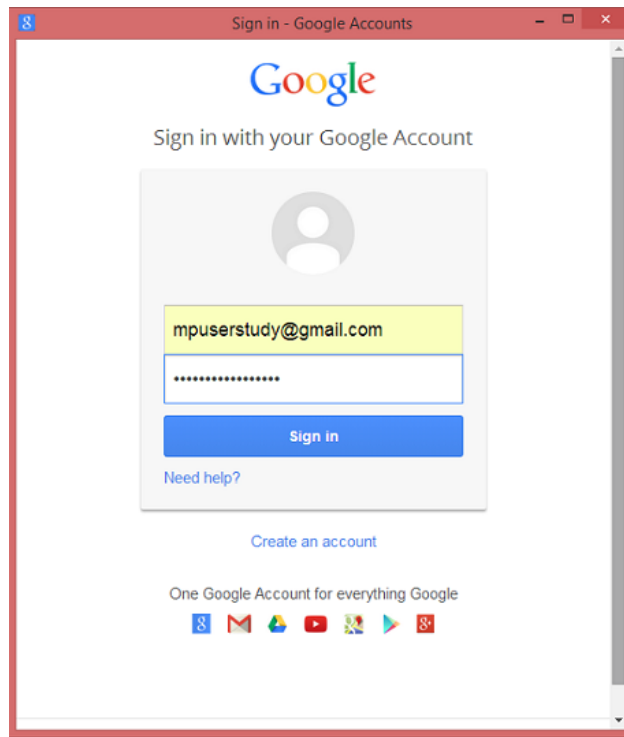


Figure 4.5: Google Account Login

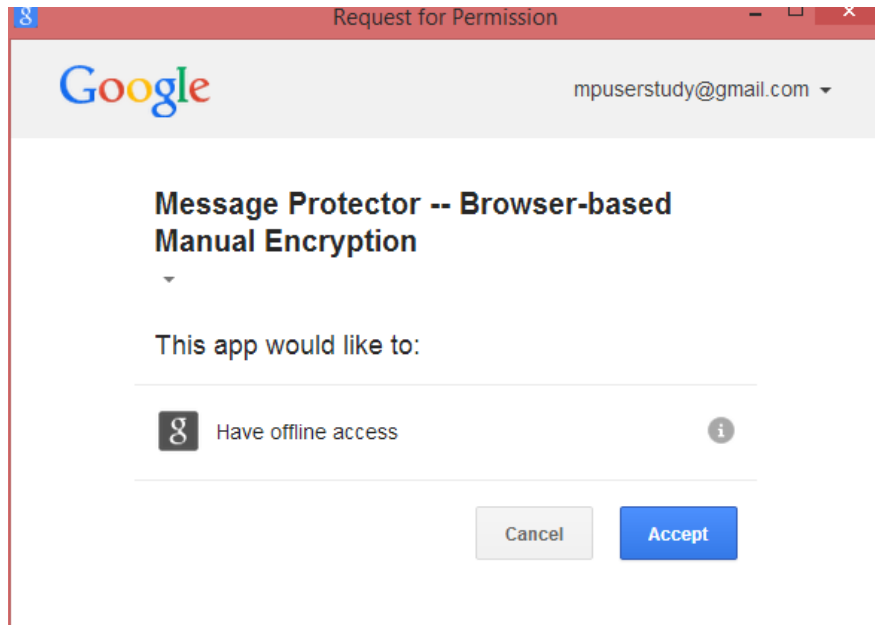


Figure 4.6: MP Request for Permission

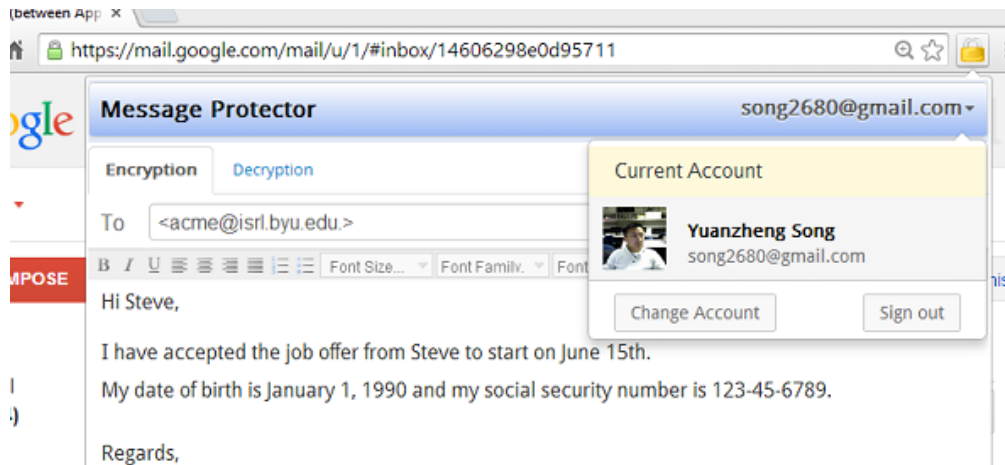


Figure 4.7: Dropdown Menu

4.2 The Purpose for Authentication

The reason the user needs to log in to MP is that MP supports automatic key management. This helps avoid the need for users to receive training prior to using the system.

MP is designed to use a key escrow server to handle automatic key management. The key escrow server is designed and implemented based on ideas from identity-based cryptography (IBC) [11]. The key escrow server generates symmetric keys based on the email addresses of the senders and receivers. A user can send an encrypted messages before the recipient has installed MP since the only information required for encryption is the recipient's email address. The recipient can obtain the decryption key after the fact by proving they own their email address to the key server.

In order to prove ownership of an email address, the MP prototype adopts Google OAuth 2.0. Currently, MP only works for users who have a Gmail account. OAuth is an authentication and authorization protocol. It allows users to authorize a third-party (e.g., MP) to access the key server without sharing their password with the key server. The advantages of Google OAuth are (1) a user doesn't need to create a new account, (2) no new password is required, (3) the well known service provider can be used to validate the user's email address. The disadvantages are (1) a user has to own a Gmail account in our implementation, and (2) a user has to grant MP the permission to access his Google profile information.

4.3 Encryption and Decryption

The main user interface for MP has two primary tabs for encryption and decryption. A help tab on the right side is also provided for the user to obtain help on how to use MP. When MP is activated, the popup window is opened on top of the current web page. MP was designed to be independent from any website so that users can encrypt messages for any service that supports online communication.

The current prototype supports encrypting a message for only one recipient since that was all that was necessary for the user study. A production implementation could support multiple recipients.

Once Bob completes the log in process, he selects the **Lock** icon and is shown the MP interface shown in Figure 4.8. In order to decrypt a message, he selects the **Decryption** tab shown in Figure 4.9. He then copies and pastes the ciphertext from his Gmail message into the text input area under the **Decryption** tab as shown in Figure 4.10. A progress bar (see Figure 4.11) is displayed while the decryption operation is being performed. Finally, the plaintext is displayed as shown in Figure 4.12.

If Bob wants to send an encrypted message to Alice, he selects the **Encryption** tab (see Figure 4.8). He first specifies the recipient's email address (i.e., Alice's email address) in the **To** input text box (see Figure 4.13). He then composes the sensitive message in the compose area. Finally, he clicks the **Encrypt** button to start encryption. The progress bar provides visual feedback to Bob informing the progress of encryption (see Figure 4.14). The encrypted message is displayed in the dialog window (see Figure 4.15). Bob clicks the **Copy to Clipboard** button to copy the encrypted message. He can paste the copied message into a Gmail message addressed to Alice.

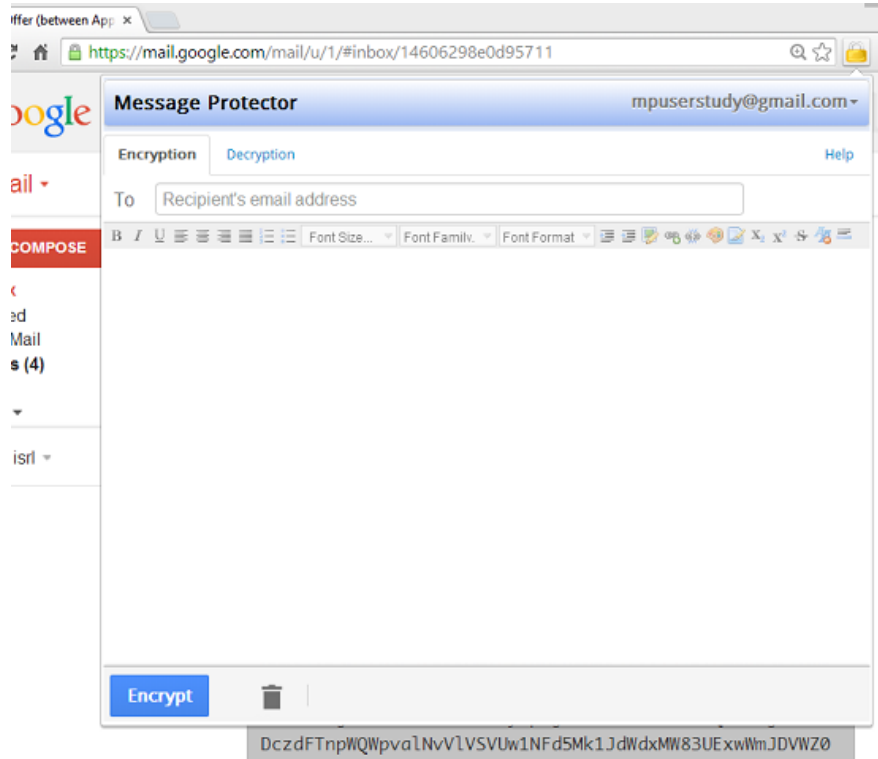


Figure 4.8: MP User Interface - Encryption

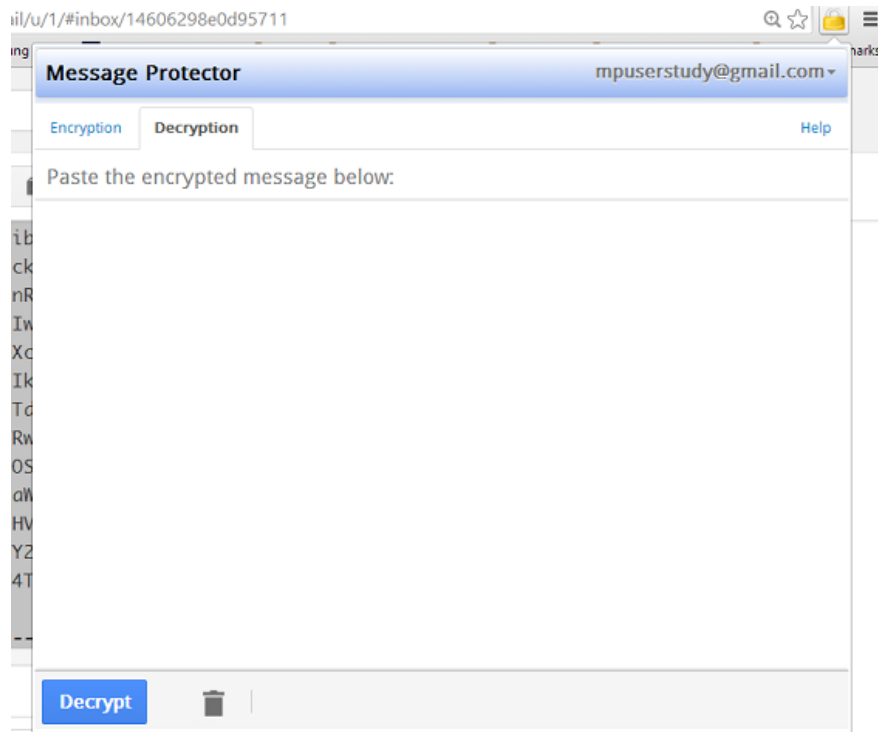


Figure 4.9: MP User Interface – Decryption

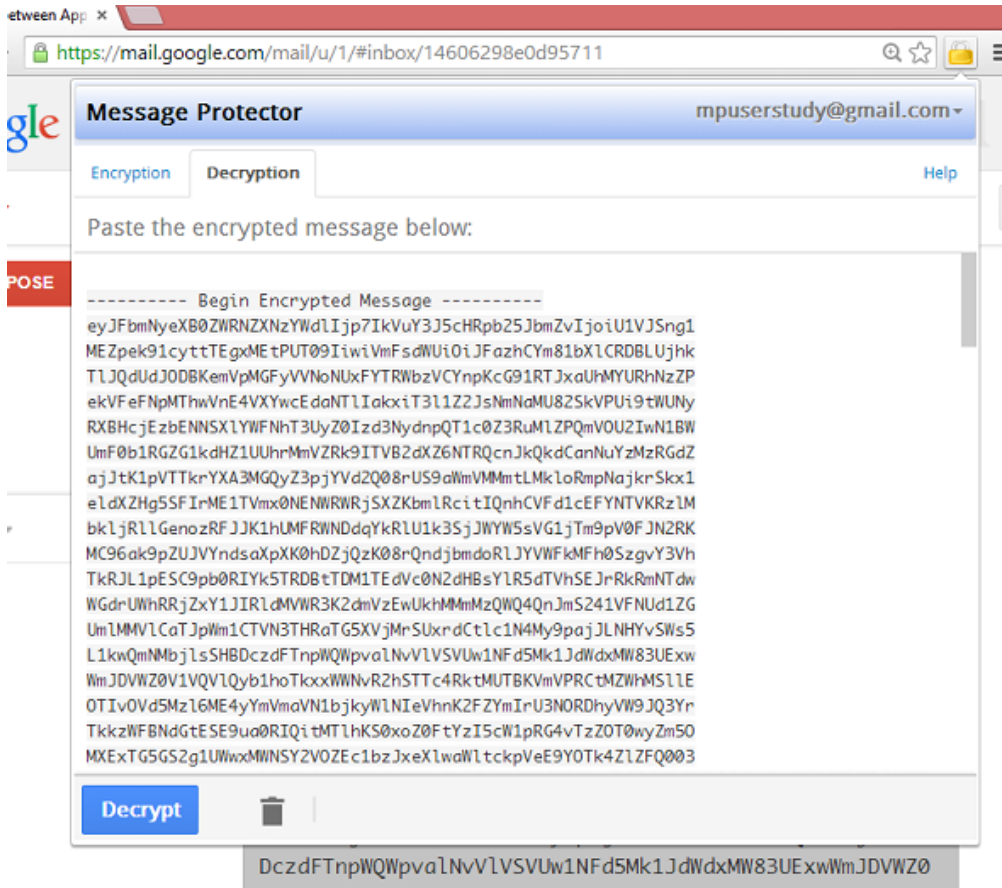


Figure 4.10: Encrypted Message Pasted into MP

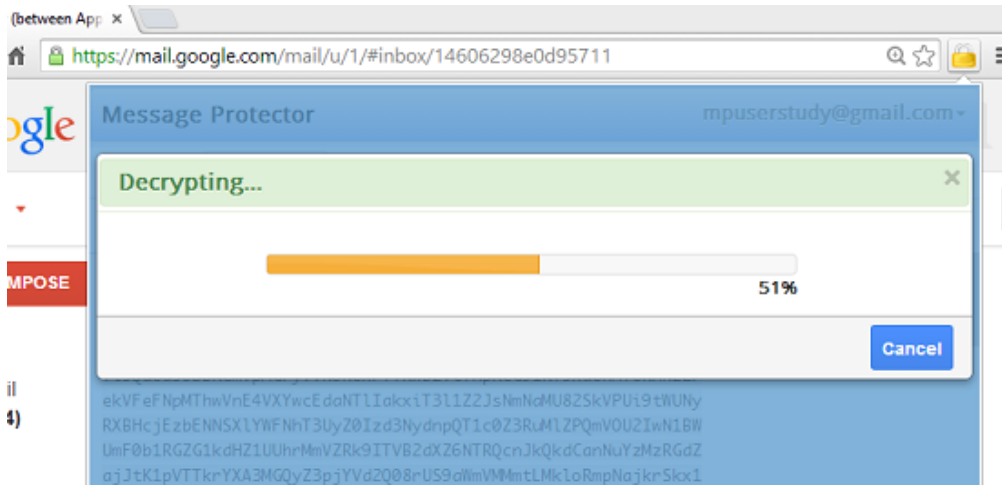


Figure 4.11: Decrypting a Message in MP

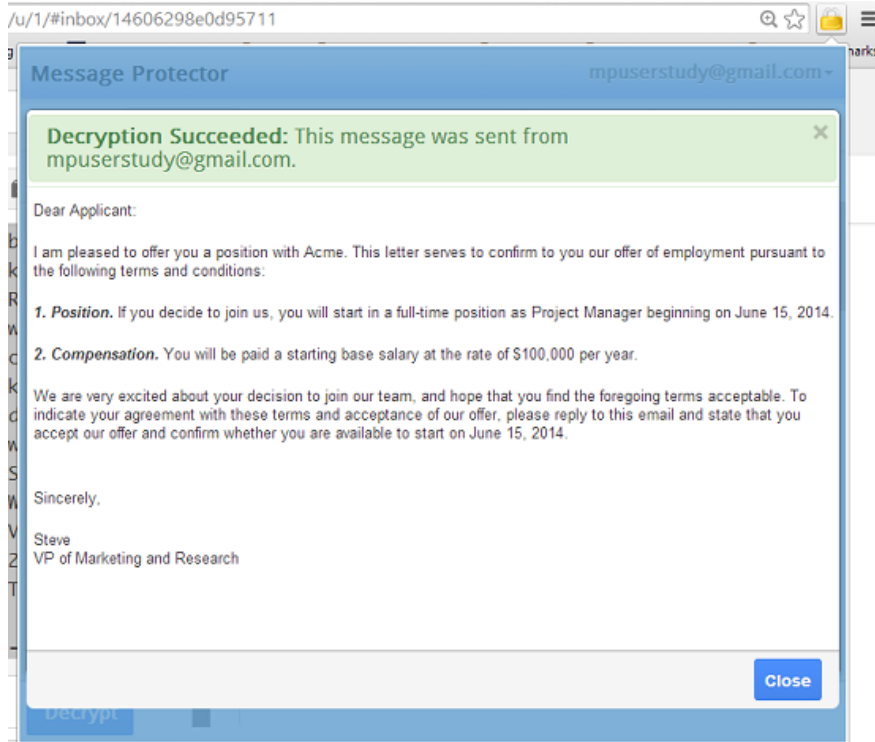


Figure 4.12: Decrypted Message Displayed in MP

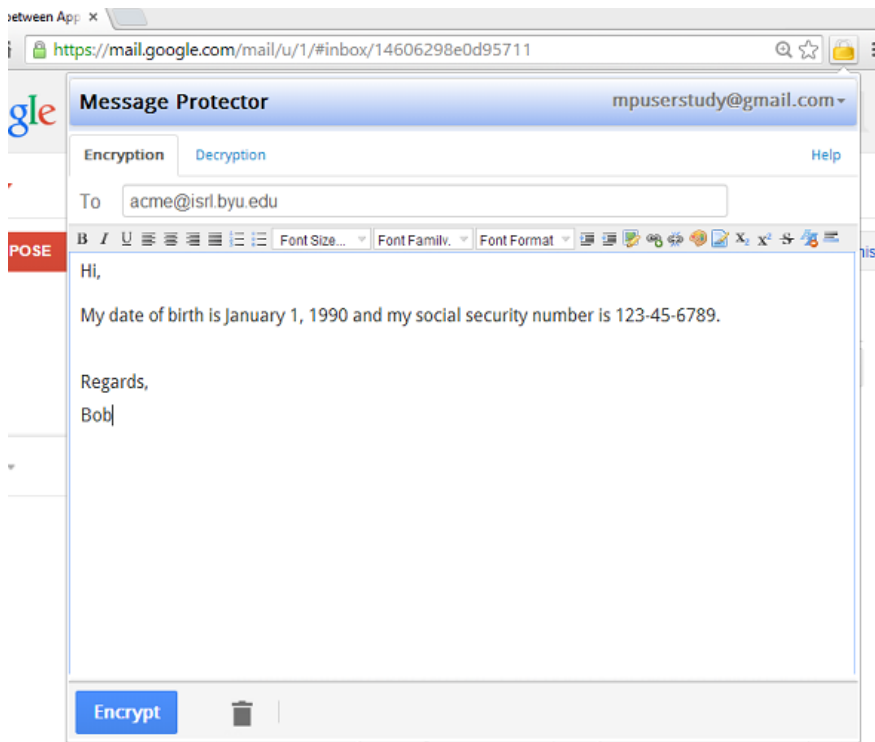


Figure 4.13: Composing a Message in MP

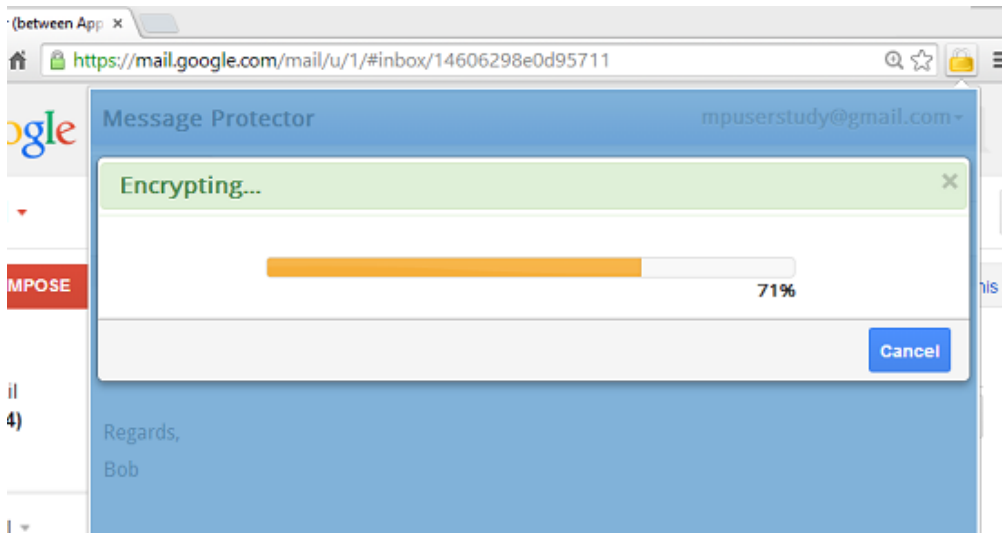


Figure 4.14: Encrypting a Message in MP

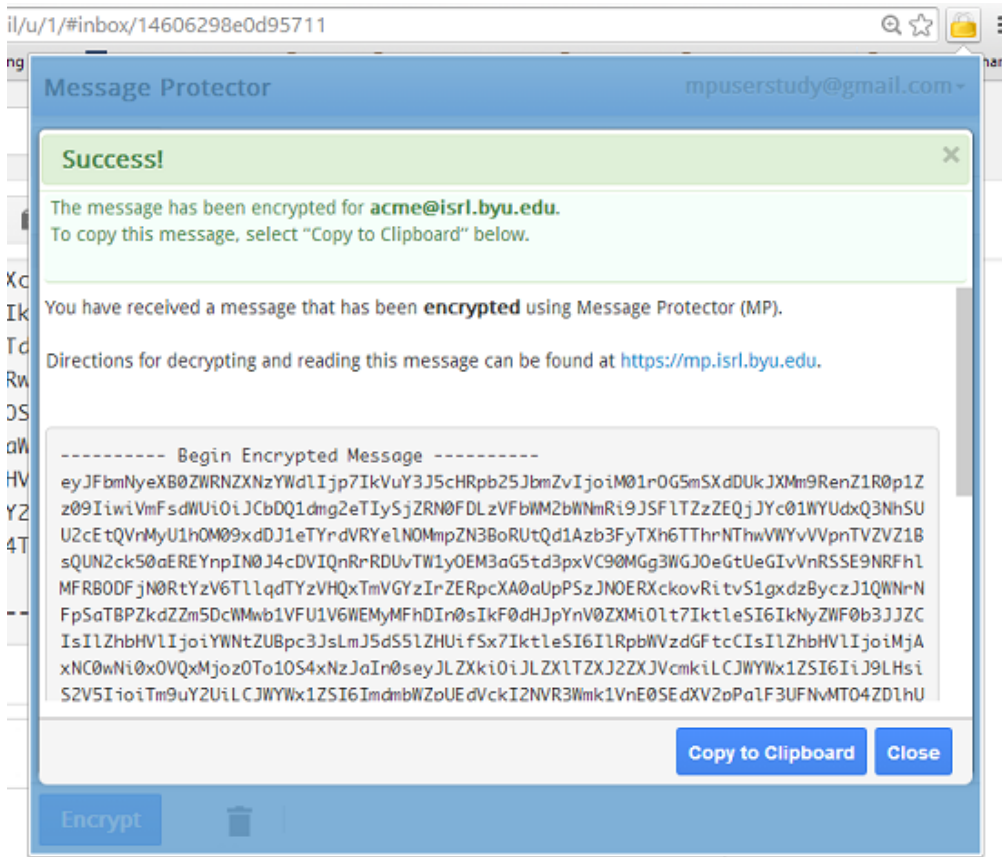


Figure 4.15: Encrypted Message Displayed in MP

Chapter 5

MP Usability Study

An IRB-approved laboratory usability study was conducted to measure the usability of MP and compare the results to previous usability studies of Pwm and MP-original. The study assessed whether MP achieved the following design goals.

- Determine whether an untrained user can setup and use MP
- Determine whether MP helps users avoid mistakenly sending out sensitive messages without encryption
- Determine whether users trust the system

5.1 Participants

Participants for the user study were recruited through flyers posted on the bulletin boards located in non-technical departments on the BYU-Provo campus. The posters invited students who were familiar with Gmail to participate in the usability study but did not alert them that the study pertained to encrypted webmail. All participants were paid \$10.00.

A total of 33 participants came into the Internet Security Research Lab at BYU to complete the study. Each participant was scheduled for thirty minutes. The study required participants to accomplish 4 tasks designed to experience the full range of MP features for encrypting and decrypting messages as well as answering some questions in an online survey.

Of the 33 participants who completed the study, 30 (90%) were current BYU students, the remaining 3 participants were BYU alumni. Most of the participants were from non-technical majors, while 4 participants (12%) were engineering students. None of the

participants had any prior experience encrypting messages. 14 participants (42%) were male and 19 (58%) were female.

In terms of computer expertise, 12 participants (36%) rated themselves as beginners, and the remaining 21 participants (64%) rated themselves as intermediate. All of the participants had experience using Google Chrome.

The participants were also asked how often they send messages using email, Facebook Chat, etc., and 27 participants (82%) reported that they send messages every day, 5 (15%) send messages 2 or 3 times a week, and 1 (3%) sends messages once each week.

Participants reported that they use the following technologies on a regular basis to send messages: 25 (76%) use webmail to send message, 29 (88%) use Facebook Chat, 5 (15%) use Twitter, 6 (18%) uses Skype, 33 (100%) use text messaging, and 5 (15%) use other technologies (e.g., Wechat, QQ, or Whatsapp).

5.2 Setup

The study was conducted on a computer that had a 3.4 GHz Intel Core i7 processor with 16 GB of RAM. It had a Windows 7 Enterprise operating system and the Google Chrome web browser installed. All participants were required to complete the study using the Chrome web browser on this computer. The MP browser extension was removed from the browser before each test so that each participant would have to install it prior to using it.

The tasks for the study were based on a hypothetical scenario involving sensitive information in order to observe how well new users with no training would be able to use MP. The scenario had the participants receive a job offer from a company named ACME, and it required them to send several emails containing sensitive information in order to complete the hiring process.

Participants used a Gmail account that was created for testing purposes to complete this study instead of using their own Gmail account in order to protect their private infor-

mation. Two additional Gmail accounts were created for the study coordinator to receive participants' responses during the study.

Participants began the study by completing demographic questions (see Appendix A.2). Then they completed the 4 tasks using MP (see Appendix A.3). After completing the tasks, participants were given a survey about their experience using MP (see Appendix A.4). Following the survey, participants were interviewed about their experience and noted any difficulties in using MP. Those participants who failed to complete a task were asked to explain the reasons for their actions.

5.3 Tasks

The study required that each participant complete 4 tasks using MP. These tasks were designed to simulate what a user would experience if they received an encrypted email and began using MP.

The first task required that the participant log in to a Gmail account with a given username and password and check for a new incoming email. A single message in the inbox contained an encrypted message sent from Steve at ACME that informed the participant that ACME was extending them an offer of employment. Since participants were not informed in advance that this email would be encrypted using MP, they had to rely on the plaintext instructions located just above the encrypted message that directed them to the MP website containing step-by-step instructions for installing MP from the Chrome Web Store. Once installed, a tutorial instructed participants on how to encrypt and decrypt messages using MP. The purpose of this task was to observe whether MP was easy to install and whether untrained users could successfully decrypt messages with only a brief tutorial and no other outside help.

For the second task, participants were asked to send a secure reply to Steve (the study coordinator) in response to the email message in Task 1. Participants needed to click on the Lock icon and select the Encryption tab in order to compose the reply message in the

editing area. The recipient's email address also needed to be entered. If participants did not provide the recipient's email address before clicking on the **Encrypt** button, an error popup message would remind them that the recipient email address is required before the message can be encrypted. Once the message was successfully encrypted, participants copied the ciphertext and returned to Gmail to paste the ciphertext into a Gmail reply message. The purpose of this task was to determine whether participants could compose an encrypted reply message in MP and send it using Gmail.

For task 3, participants were asked to compose and encrypt a new message containing the text "I have accepted the job offer from Steve to start on June 15th. My date of birth is January 1, 1990 and my social security number is 123-45-6789." The ciphertext was copied into a new Gmail message that was sent to a HR staff member at ACME (study coordinator). Once participants successfully sent the encrypted email, they were required to log out of MP. The primary purpose of this task was to determine whether participants could compose a new message compared to replying to a message in task 2.

Task 4 informed the participants that Steve needed them to send a bank account number to human resources for the direct deposit of their signing bonus. In order to accomplish this task, participants needed to first log in to MP and encrypt a new message containing the text "Please deposit my signing bonus into my Chase savings account at 12345-67890." Next, they copied the ciphertext and sent it to an HR staff member at ACME (the study coordinator). Once the message was sent, participants logged out of MP and closed Gmail. The primary purpose of this task was to determine whether participants were able to log in to MP and encrypt a new message.

5.4 Results

All participants successfully installed MP and were able to use it.

5.4.1 Task 1

For task 1, 33 participants (100%) successfully installed MP in the Chrome web browser and decrypted the message. Only one participant moved on to the second task without providing the requested information (i.e., the salary from the job offer) from the decrypted email. In the post interview, the user said that they didn't notice the second question on the same page of the survey.

5.4.2 Task 2

After decrypting the email in the first task, 24 out of 33 participants (73%) successfully completed the task and sent an encrypted reply. The remaining 9 participants had various reasons for not completing the task that reveal weaknesses in MP and the user study.

Two participants (6%) failed to send any reply. The first actually composed the reply message, but didn't send it out. When asked about this, she reported that she wasn't sure about what she should do, therefore she chose to skip that step. However she realized that the task was quite easy after the explanation from the study coordinator, and said that she could complete this task without a mistake if asked to try again. The second participant who failed to reply stated that she thought MP would reply automatically immediately after the encryption. A brief explanation by the study coordinator helped these two users succeed at the remaining two tasks. These failures represents an important misunderstanding of the tool for these two users. MP needs to do more to help all users complete these tasks.

Two participants (6%) sent encrypted replies that could not be read by the study coordinator. The first participant didn't correctly distinguish between the sender's address and recipient's address in the Gmail message received in task 1. Consequently, she selected the incorrect address from the prior message to encrypt the outgoing message. In this case, the user encrypted the message for her own email address. MP can help prevent this error in the future by notifying the user when they attempt to encrypt a message for their own address to confirm whether that is the user's intent. The second participant copied the

sender's email address surrounded by angle brackets. The MP prototype did not ignore the angle brackets during the encryption process, therefore, the study coordinator could not successfully decrypt the reply. MP can be enhanced to help prevent this error in the future with stronger validation of a correctly formatted email address. It should ignore the angle brackets surrounding the email address.

Finally, 5 participants (15%) sent a reply without any encryption. One design goal of MP is to eliminate the mistakes that occurred in the prior Pwm studies when users mistakenly sent out a sensitive message in plaintext. In the Pwm study, 3 participants (9%) mistakenly sent out the plaintext message. However, the users in the Pwm study thought the message they sent was encrypted when it was not. In contrast, all the MP users intended to send a plaintext message. They each missed the detail in the instructions that the reply should be encrypted. Since the reply included information that did not appear to be especially sensitive, the users did not pick up on the detail that the intent of the task was to test their ability to send an encrypted reply. This represents a flaw in the study design instead of indicating that the tool is confusing about when data is and is not encrypted. This inadvertent error may have been prevented if the task had included some obviously sensitive information in the reply along with some kind of forcing function to help the users understand clearly that the reply should be protected using encryption.

5.4.3 Task 3

On the third task, 30 participants (91%) sent an encrypted email. However, 3 participants (9%) used the wrong email address for the recipient causing the study coordinator to be unable to decrypt the message. The participants incorrectly used the same recipient used in Task 2, and didn't notice that Task 3 required them to send the message to a different email address. MP may need to do more to inform the user which email address will be able to read the encrypted message. The failure may be influenced by the task design that used unfamiliar email addresses. All three of these users successfully completed task 4.

5.4.4 Task 4

On the fourth task, 32 participants (97%) sent an encrypted message. However, 1 participant (3%) copied the email address from the task instructions and included a trailing period that is not part of the email address (“acme-human-resources@isrl.byu.edu.”). This also caused the recipient to fail to decrypt the message. MP failed to detect that this was an invalid email address. It can be extended to help prevent this kind of error.

5.5 SUS Evaluation

The System Usability Scale (SUS) [4] is a general-purpose usability evaluation metric for rating software usability. It provides a standard method to measure and compare the usability of software products. SUS consists of ten questions using a 5-point Likert scale. Users respond to each question with a rating from *Strongly Disagree* to *Strongly Agree*. The questions alternate between negative and positive statements. For example, positive statements like *I think that I would like to use this system frequently*, and negative statements like *I found the system unnecessarily complex*. A single SUS score on a scale between 0 and 100 is calculated for each user based on that user’s rating of each statement. The final overall SUS score for the system is the mean of the individual user scores.

Bangor et al. [2] collected the results of SUS evaluations from previous research on hundreds of systems and compared them. The results of their study are illustrated in Figure 5.1 that presents several interpretations of the numeric SUS scores. The quartile ranges are listed to show the distribution of SUS scores across all the systems they analyzed. The Figure also shows the correlation between SUS scores and subjective ratings about whether the systems were acceptable, not acceptable, or marginal. For instance, if a SUS score is higher than 70, the system is considered acceptable. Finally, an adjective rating is given to provide additional meaning to each scalar value. For example, if a SUS score is between 73 and 85, the adjective rating is excellent.

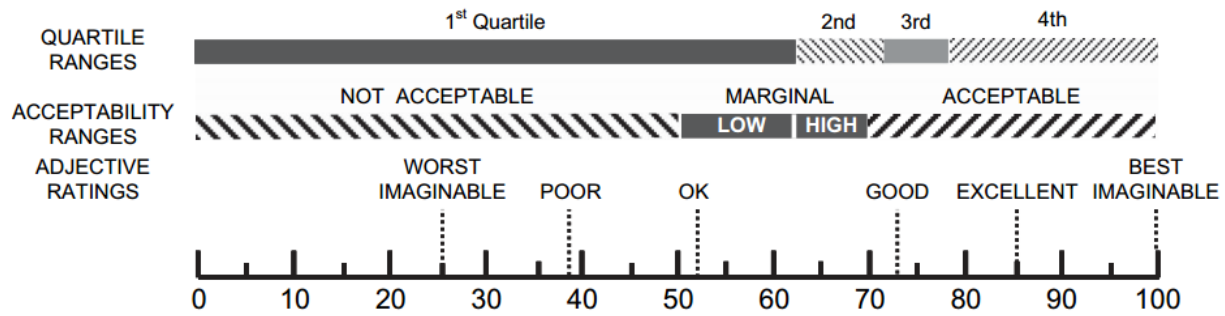


Figure 5.1: An adjective-based interpretation of SUS scores [1]

To assess the usability of MP, the ten SUS questions were included as part of the survey. The participants responses are shown in Table 5.1. The participant’s responses resulted in an overall SUS score of 77.35 with a standard deviation of 13.96 and a 95% confidence interval of ± 4.76 . According to Bangor’s research, a score of 77.35 falls in the top of the third quartile (70.5 - 77.8) and above the mean score of 69.69. This score places MP within the *Acceptable* range and qualifies for an adjective rating of *Excellent*. MP’s SUS score of 77.35 compares favorably to recent studies of Pwm with a SUS score of 75.69 and MP-Original with a SUS score of 72.23 [10]. This provides empirical evidence that MP succeeds in maintaining the usability of these two earlier systems while avoiding their drawbacks.

5.6 Lessons Learned

Even though the SUS score for MP is on par with earlier studies, the user study provides valuable feedback for improvements that can be made to both the user study itself as well as the MP implementation.

5.6.1 Recipient email address

In task 3, three users correctly sent an encrypted reply but directed it to the wrong recipient. This could be considered a simple failure of the users to follow directions and not a weakness with MP. The study design may have contributed to the problem with its use of unfamiliar

Question	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I think that I would like to use this system frequently	0	5	14	12	2
I found the system unnecessarily complex	9	16	8	0	0
I thought the system was easy to use	0	1	1	15	16
I think that I would need the support of a technical person to be able to use this system	17	10	5	1	0
I found the various functions in this system were well integrated	0	4	5	17	7
I thought there was too much inconsistency in this system	13	17	3	0	0
I would imagine that most people would learn to use this system very quickly	0	1	2	17	13
I found the system very cumbersome to use	11	14	8	0	0
I felt very confident using the system	1	0	2	20	10
I needed to learn a lot of things before I could get going with this system	17	10	5	1	0

Table 5.1: Message Protector SUS Survey Responses

email addresses as part of the hypothetical scenario along with the introduction of a new recipient email address between tasks 2 and 3 instead of a single recipient across all tasks.

There is one aspect of the design that may have contributed to the error. After an encrypted email is generated, the plaintext contents of the recipient email address and message are not deleted from the text entry boxes in case the user needs to return in order to edit the message or repeat the encryption due to a cut and paste error. It would be very annoying to users to lose the message contents and have to re-enter it. However, this means that when the user goes to create a second message, they have to explicitly delete the contents of the prior message. The three users in the study may have overlooked updating the recipient for the next message because the box already had a valid-looking email address. If the box had been empty, the user may have been more likely to enter the correct recipient for the task. An open question is how to better design the system to prevent the loss of plaintext contents that would force a user to re-enter the message and make it harder to inadvertently encrypt the message for the wrong user.

5.6.2 Copy and Paste

Once a message is encrypted, MP includes a **Copy to Clipboard** button to provide an easy, foolproof mechanism to copy the entire encrypted message along with the decryption instructions for the recipient. Four users in Tasks 2–4 copied the ciphertext manually and omitted these instructions. In practice, this could lead to a situation where a recipient is unaware of what steps they should take to read the message unless they are already familiar with MP. There were seven separate instances where users copied the plaintext without the instructions. User #27 repeated this during tasks 2, 3, and 4. For task 2 they only copied the base64 encoded ciphertext, leaving off the **Begin Encrypted Message** and **End Encrypted Message** designators. They did include these designators in tasks 3 and 4. User #31 left off the plaintext instructions during tasks 3 and 4. Finally, users #19 and #15 left off the plaintext instructions during tasks 2 and 3, respectively. The user comments indicated that some users were not familiar with the term **Clipboard**. The resulting uncertainty may have caused them to copy the ciphertext manually. MP could either prevent manual copying or alert the user to be certain that they include the plaintext instructions when they attempt to perform a manual copy.

5.7 User Feedback

This section summarizes the written comments users provided during the survey. It includes direct quotes from some users to illustrate some of the trends that were observed in the data. All of the user comments are included in Appendix B.

5.7.1 Google OAuth

The survey asked users whether they preferred using their Google account to login to MP or if they would prefer to create a new username and password to use with MP. A high percentage, 27 out of 33 users (82%), preferred using their Google login because it was convenient. Some example comments from users who preferred using their Google login include:

- *I don't like creating new passwords or usernames, already too many.*
- *It would be one less username and password to remember.*
- *Convenience. It is related to emails, therefore it makes sense to use the same information as your email (gmail) account.*
- *less password to remember. Also when I have my gmail open is probably the only time I would really need to use this.*

A few users recognized the added security that a new account would provide.

- *I like to keep my login information for various websites, e-mails, applications, etc. separate from each other/compartmentalized.*
- *If someone else broke into my computer my gmail would already be signed in and therefore they could sign into MP and discover all my private information I was trying to hide.*
- *Just because if I would use this gmail account for important information, I would like to keep it separate from school and other unimportant task that I already manage from my gmail account.*

5.7.2 What users liked about MP

The survey asked the users what they liked about MP, and most of the responses centered around how easy it was to use. Some users commented specifically about how manual encryption gave them a feeling of security.

- *I like that It is a chrome extension and uses my google account. I also like that there is a button to copy the encrypted message easily. I like that the button to encrypt and decrypt a message are very clear. I liked that MP was simple to download.*
- *It is easy to use.*
- *It was easy and makes me feel like my information was safe*

- *It is very intuitive and easy to use.*
- *I knew for a fact that my message was being encrypted, and therefore protected.*
- *This program was really easy to use. I was simple and well organized so even a beginner like me can use it!*
- *Very easy and intuitive to use. It was simple and straightforward.*
- *I liked that it was simple. It didn't take a long time to learn. Yet I felt more secure sending private information through email knowing that not everyone who read the email would be able to have my information.*
- *It was easy to use and it made me feel more comfortable about sending important information over email.*

5.7.3 What users disliked about MP

The survey also asked users what they disliked about MP.

Three users commented about the clipboard, and this indicates that some users are not comfortable with that terminology.

- *I'm not really sure what clipboard is so when it saved there I was lost and just copied and pasted manually but I don't know PCs very well...*
- *When encrypting a message it was confusing on how to send it. I encrypted it but I felt like the "Copy to Clipboard" button did nothing. I had to copy and paste the whole thing into a new message myself and re-enter to recipient address.*
- *I didnt know what clipboard was, the message looked the same every single time, so I couldn't tell the difference. I needed to ask in order to understand if I was doing it write*

A few user's comments reveal a preference to have the tool more tightly integrated with Gmail. This illustrates the tension to create a tool that is easy to deploy and maintain by being loosely integrated with websites such as Gmail, and yet still create a tool that has high usability.

- *I dislike that I have to copy the encrypted message into my webmail instead of sending directly from MP.*
- *The copy and paste method is cumbersome. It would be cool if MP was just a button that automatically changed the message within Google. I also have a love hate relationship with the idea that you have to type in the email address in both the MP app and the email message. It would be cool if that only had to happen once.*
- *I wish it was more integrated with Gmail.*
- *Having to do a separate step outside of gmail to encrypt it.*
- *I didn't like having to copy and paste the message; it should just be able to send an email automatically within MP.*

Some users do not understand who can read the encrypted message. This may indicate that more work can be done to help non-technical users understand how the tool works.

- *I feel like it was a little too easy? If the email fell into the wrong hands, it seems like the encryption would be easy to figure out because the messages also tell you how to use MP.*
- *Uh... I wasn't sure if anyone who gets the encrypted message will be able to somehow decrypt it.*
- *I didn't like that the program did not explain fully who would have access to be able to decrypt my information. If a hacker found the email would he be able to use MP to decrypt the email? I am not sure.*

5.7.4 Suggested improvements to MP

The user's suggestions for improving MP followed from some of the things they disliked in the previous sections.

- *It would be nice to have a little explanation of how it works but that's all*

- *Make different texts so they look similar but not equal. Just say: Your message is ready to be pasted into your email. Instead of saying Clipboard.*
- *improve it so people can send a message directly through MP.*
- *Integrate it more with Gmail and make it easier to use.*
- *It would be more convenient just to type the message into gmail directly and having it be encrypted when I hit send.*
- *Honestly I think that it is pretty easy to use, the only thing I didn't understand was the saving to clipboard part of the encryption process so I just copied and pasted it. Other than that I think that it is well put together.*
- *allow for an easier way to copy and paste*

5.7.5 Browser extensions

The survey asked users what has prevented them from installing browser extensions in the past. Seven users specifically mentions concerns about security and trust. Three users had concerns that extensions will slow down their computer. Finally, seven users mentioned that extensions introduce clutter to their browsers. Here is a sample of some of the user comments.

- *Worried that they would slow down my usage. Not sure if they work (can access my information) for all of my internet activity or just certain websites. Don't want to clutter up my taskbar.*
- *I don't trust them or they seem gimmicky. They have bad reviews or don't work properly.*
- *they don't look legitimate. They look sketchy like they will give me a virus.*
- *Sometimes it slows down my computer too much. -Sometimes I am worried that the extension/plugin is just malware or a worm or a virus trying to gain access to my computer.*
- *Scared about them giving my computer viruses.*

- *They usually slow down the browser, constantly updating*
- *I feel psychologically they clutter things. Since I don't know much about computers, I feel like they would clutter up "space." (whatever that means- space, memory, etc.) I also worry about getting too much. But other than that weird thought, I download the necessary ones and use them when needed*
- *Clutter and security issues*

The survey also asked users what would influence them to trust an extension. The most common answers focused on reputation, reviews, trusted companies, and trusted friends/co-workers.

5.8 Recommendations

The following are recommended changes to the MP prototype based on the experiences reported and observed during the user study.

- Add an alert message after selecting the encrypt button to verify that the recipient email address is correct and that only that recipient will be able to view the message. This will also serve a teaching role to inform users about who is able to decrypt a message.
- Add the plaintext instructions for decryption to the gray box used to display the encrypted contents so that more users will also copy these instructions along with the ciphertext as they cut and paste the data into another email message. Including all of the content in the gray box may help users understand that the data all belongs together.
- Validate the recipient email address to reject any that are syntactically incorrect and canonicalize them so that the same email address string is used for encryption and decryption.

- Modify the scenario so that the same recipient email address is used across all tasks to help the users avoid mistakes using email addresses that are not already familiar to them. Alert the user when they encrypt a message for their own address and confirm that this is the intended action.

There are several recommended changes to the survey that will help avoid some problems and confusion in the future.

- Modify the instructions in Task 2 to make it more clear that the reply must be encrypted.
- Improve Task 2 instructions to include data that obviously would benefit from encryption.

5.9 Comparison

A goal of the MP prototype was to combine the strengths of Pwm and MP-Original and avoid their weaknesses. Table 5.2 contains a comparison of these three systems in terms of usability, deployability, and security.

In terms of usability, all three systems were easy for new users to use correctly. MP-Original did not provide any initial training instructions for first-time users like MP and Pwm do, but MP-Original was not designed for the IBC grass roots adoption model where users receive an encrypted email without any taking any prior action. MP and MP-Original utilize manual encryption, and user studies illustrate this encourages greater trust in the system compared to systems like Pwm with automatic encryption. MP-Original was effective at preventing user errors during its user study. MP shows signs that it improves on Pwm's tendency for users to assume a message was encrypted when it was not.

In terms of deployability, MP and Pwm are designed to encrypt Gmail messages within the Chrome web browser Pwm is tightly coupled to Gmail. MP-Original runs on the Windows operating system and can be used by any messaging application. MP represents a compromise between MP and Pwm. MP is designed to support any web service, although the current

		MP	MP-Original	Pwm
Usability:	Easy-to-Learn	tutorial/help tab in system	no tutorial	video tutorial
	Login	Gmail account	any email account	Gmail account
	Cut and Paste	manual encryption	manual Encryption	automatic encryption
	Trust	high	high	low
	Mistakes	wrong recipient	no mistakes	sent plaintext
Deployability:	Installation	Chrome Web Store	O/S program	drag/drop bookmarklet
	Compatibility	Chrome	Windows	Chrome
	Email provider	Gmail-specific	independent	Gmail-specific
Security:	Authentication	Google OAuth	no trusted 3rd party	SAW

Table 5.2: Comparison of MP, MP-Original, and Pwm

prototype supports only Gmail. Unlike Pwm, MP won't break when Google changes the interface. All three systems require user installation, although Pwm's bookmarklet permits installation from a user without admin privileges.

In terms of security, all three systems are designed to support end-to-end encryption. The current implementations use different authentication methods. MP-Original is not tied to any third-party provider but leaves it to the users to identify which of their contacts require security communication. Pwm and MP both rely on email-based authentication. Pwm uses SAW, while MP is based on OAuth.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

This thesis presents the first design and implementation of browser-based manual encryption. It also presents the first user study to analyze browser-based manual encryption. The user study resulted in a SUS score for MP that is slightly higher than both Pwm and MP-Original, showing that MP has usability that compares favorably with these earlier systems, while avoiding the significant drawbacks of each. Users experience and comments provide valuable feedback for new ideas to improve the usability of the system. MP provides evidence that a browser-based manual encryption mechanism is both usable and deployable.

6.2 Future Work

The current MP prototype uses an email-based access control system so that the only person able to decrypt a message is the owner of the recipient email address that was used during encryption. In practice, this may lead to a decryption failure when an email is sent to a different address than the one that was used for encryption, or when the recipient is trying to decrypt a message sent to a different account than the one they used to sign in to MP. A user study that focuses on how recipients respond to these errors and whether the senders and recipients can effectively troubleshoot them without assistance is needed.

The MP prototype simulated the key server by hard-coding the server master key in the client implementation. A long-term user study with a full-functional key escrow server would be a valuable extension to this thesis research.

The survey results indicate some reluctance from users to install browser extensions. This is a barrier to wide-spread adoption of the system. An alternative implementation architecture is to provide the extension functionality as a web service so that users will move to another tab in the browser and access a website that provides the encryption functionality. The website can support client-side encryption and decryption so that the plaintext is never disclosed to the website. This approach requires no software installation at the client. A user study is needed to determine how users will react to this service and whether they can use it correctly. Another question is whether users will trust that the website is not accessing their sensitive data.

References

- [1] A. Bangor, P. Kortum, and J. Miller. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of Usability Studies*, 4(3):114–123, 2009.
- [2] A. Bangor, P.T. Kortum, and J.T. Miller. An empirical evaluation of the system usability scale. *International Journal of Human–Computer Interaction*, 24(6):574–594, 2008.
- [3] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '01, pages 213–229, London, UK, 2001. Springer-Verlag.
- [4] J. Brooke. SUS- A quick and dirty usability scale. *Usability Evaluation in Industry*, 189:194, 1996.
- [5] Sascha Fahl, Marian Harbach, Thomas Muders, and Matthew Smith. Trustsplit: Usable confidentiality for social network messaging. In *Proceedings of the 23rd ACM Conference on Hypertext and Social Media*, HT '12, pages 145–154, New York, NY, USA, 2012. ACM.
- [6] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. Helping Johnny 2.0 to encrypt his facebook conversations. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 11:1–11:17, Washington, D.C., 2012. ACM.
- [7] Simson L. Garfinkel. Email-based Identification and Authentication: An Alternative to PKI? *IEEE Security & Privacy*, pages 20–26, 2003.
- [8] Simson L. Garfinkel and Robert C. Miller. Johnny 2: A user test of key continuity management with s/mime and outlook express. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, pages 13–24, New York, NY, USA, 2005. ACM.
- [9] Nathan I. Kim. Message Protector - Demonstrating that manual encryption improves usability. Master's thesis, Brigham Young University, May 2013.

- [10] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy van der Horst, and Kent Seamons. Confused Johnny: When automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS '13*, pages 5:1–5:12, New York, NY, USA, 2013. ACM.
- [11] Adi Shamir. Identity-based cryptosystems and signature schemes. In George Blakley and David Chaum, editors, *Advances in Cryptology*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer Berlin / Heidelberg, 1985. 10.1007/3-540-39568-7_5.
- [12] Timothy W. van der Horst and Kent E. Seamons. Simple authentication for the web. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, pages 473 –482, sept. 2007.
- [13] A. Whitten and J.D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, volume 99, pages 169–183, 1999.

Appendix A

User Study Survey

The appendix contains the user study survey to assess users attitudes about secure communication and their experience using MP.

A.1 Introduction

Thank you for your participation. During this study you will be asked to send email messages to the study coordinator using Gmail. At the conclusion of the study you will answer questions in a survey in order to help us learn whether or not our software is easy to use.

- None of the results published as part of this research will personally identify you as a participant.
- You will have a temporary Gmail account to use during this study.
- You will not be required to use your own Gmail account or password at any time.
- If you have questions, please ask.
- If you need to take a break for any reason, please notify the coordinator.

You will receive \$10.00 as compensation for your participation in this study. The expected time commitment is 20-30 minutes. If you feel uncomfortable with any aspect of this study you may quit at any time.

Please read all task instructions before beginning each task.

A.2 Demographics

Please provide some basic information about yourself. This information will not be used to personally identify you.

Are you a student?

- Yes
- No

What is your major?

What is your occupation?

What is your Gender?

- Male
- Female

What is your approximate age?

- 18-25
- 26-35
- 36-45
- 46-55
- 56-65
- Over 65

How would you rate your level of computer expertise?

- Beginner
- Intermediate
- Advanced

Approximately how often do you send messages online (email, facebook chat, etc.)?

- Daily
- 2-3 Times a Week
- Once a Week

- 2-3 Times a Month
- Once a Month
- Less than Once a Month

Have you ever used Google Chrome in the past?

- Yes
- No

What devices do you regularly use to send messages? (Mark all that apply)

- Smartphone
- Tablet
- Laptop computer
- Desktop computer
- Other

What technologies do you regularly use to send messages? (Mark all that apply)

- Facebook
- Webmail
- Twitter
- Skype
- Text Messaging
- Other

A.3 Tasks

Please complete the following four tasks. You will assume the role of a job applicant in a hypothetical scenario. Pretend that you have interviewed for an exciting new job with Steve at Acme. You are eagerly waiting to hear back from Steve to find out if you will receive a job offer.

After completing these tasks, there will be a brief survey about your experience.

A.3.1 Task 1

Please launch a Chrome browser and sign-in to a temporary Gmail account with the username and password shown below:

Username: mpuserstudy@gmail.com

Password: ****

Read the first message and follow the instructions given in the message.

Once you have successfully completed task 1, please enter the salary from the job offer:

A.3.2 Task 2

Send a secure reply to the email message you received from Steve in Task 1. In your reply, tell Steve that you accept his offer and are available to start on June 15th.

A.3.3 Task 3

You receive a phone call from Steve congratulating you on accepting your new position with Acme. Steve asks you to send some personal information to human resources so they can start the formal hiring process.

Please use MP to encrypt the following hypothetical message for acme-human-resources@isrl.byu.edu

I have accepted the job offer from Steve to start on June 15th. My date of birth is January 1, 1990 and my social security number is 123-45-6789.

Use gmail to send the encrypted message using the following address and subject:

To: acme-human-resources@isrl.byu.edu

Subject: Personal information you requested

Sign out of MP when you are finished.

A.3.4 Task 4

You receive another phone call from Steve asking you to send your bank account number to human resources so that they can deposit your signing bonus.

Please use MP to encrypt the following hypothetical message for acme-human-resources@isrl.byu.edu

Please deposit my signing bonus into my Chase savings account at 12345-67890

Use gmail to send the encrypted message using the following address and subject:

To: acme-human-resources@isrl.byu.edu

Subject: Bank account #

Please sign out of MP and then sign out of Gmail.

A.4 User Reaction Survey

You have finished all of the tasks for this study. Please answer a few questions about your experience.

Please give your response to the following statements about using MP for securing Gmail messages. Ignore any issues with Gmail itself. Try to give your immediate reaction to each statement without pausing to think for a long time.

Choices presented:

Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, and Strongly Agree

1. I think that I would like to use this system frequently
2. I found the system unnecessarily complex
3. I thought the system was easy to use
4. I think that I would need the support of a technical person to be able to use this system
5. I found the various functions in this system were well integrated
6. I thought there was too much inconsistency in this system
7. I would imagine that most people would learn to use this system very quickly
8. I found the system very cumbersome to use

9. I felt very confident using the system
10. I needed to learn a lot of things before I could get going with this system

How confident are you that you used MP correctly to protect the message?

- Not at all confident
- Not very confident
- Somewhat confident
- Very confident

Would you prefer to use Gmail to login to MP as you did in the study or would you rather create a new username and password with the MP website?

- I prefer using my Gmail login
- Not very confident

Please explain why:

How often would you use MP to protect your email messages?

- Always
- Very Often
- Occasionally
- Rarely
- Very Rarely
- Never

Alice uses MP to encrypt a message for Bob. She pastes the encrypted message into Gmail and sends it to Bob. She also accidentally sends the same encrypted message to Cindy. Who can read the message? (check all that apply)

- Alice
- Bob
- Cindy
- Email server (Google)
- Company the owns MP

- An attacker that steals the encrypted message
- Other

What did you like about MP?

What did you dislike about MP?

What suggestions do you have to improve MP and make it easier to use?

Any other comments?

Have you ever installed browser extensions, add-ons or plugins before today?

- Yes
- No

What has prevented you from installing browser extensions, add-ons or plugins in the past?

When deciding whether you will trust a browser extension, add-on or plugin, what influences your decision?

Have you ever sent an encrypted email message?

- Yes
- No

Have you ever been asked to send sensitive information you were not comfortable sending through email?

- Yes
- No

What type of sensitive information were you asked to send? (Check all that apply)

- Passwords
- Social Security Number
- Medical Information

- Credit Card or Banking Information
- Other (Please specify)

Did you send the requested information?

- Yes
- No

Have you ever received information you were not comfortable receiving through email?

- Yes
- No

What type of sensitive information did you receive? (Check all that apply)

- Passwords
- Social Security Number
- Medical Information
- Credit Card or Banking Information
- Other (Please specify)

General Security Questions *Choices presented:*

Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, and Strongly Agree

- I trust Gmail with my sensitive email messages
- I am concerned about Gmail scanning my messages
- I worry that some messages aren't really from who they say they are from
- I feel safe sending important information through email
- I feel safe creating accounts with usernames and passwords on new sites
- I feel safe installing browser extensions or plugins
- Creating accounts for new websites is easy
- Installing browser extensions is easy
- I feel safe clicking on links in email messages
- I feel safe clicking on links in email messages from people I know
- I never click on links in email messages

Appendix B

Survey Results

This appendix contains the MP user study survey results.

B.1 Demographics Results

Student

- Yes: 30
- No: 3

College Majors: Public Relations; Statistics; Theatre Arts Education; Advertising; Computer Engineering; Mechanical Engineer; Psychology; Nursing; Public Health; Business Management; Accounting; Civil Engineering; Pre-management; Exercise and Wellness; Nursing; Economics; Accounting; Environmental Science; Pre-management; Microbiology; Chemical Engineering; Recreation Management; Social Work; Sociology; Environmental Science; Communication Disorders; Psychology; Special Education; Recreation Management; Finance;

Occupation: Writing Fellow; Student; Student; Tutor; Lighting Electrician Helper; N/A; Student; N/A; Student; Student; MTC Teacher; Student; Student; Student; Health Coach; Registered Nurse; Financial Analyst; Student; Student; Student; Student; Lab Assistant; Student; Student; Student; Student; TA; Student; Student; Customer Service Representative; Accountant;

Gender

- Male: 14
- Female: 19

Age

- 18-25: 32
- 26-35: 1
- 36-45: 0
- 46-55: 0
- 55+: 0

B.2 Computer Background Survey Results

Computer Expertise

- Beginner: 12
- Intermediate: 21
- Advanced: 0

Email, Facebook Chat, etc. Use

- Daily : 27
- 2-3 Times a Week : 5
- Once a Week: 1
- 2-3 Times a Month: 0
- Less than Once a Month:
- Never: 0

Google Chrome Use

- Yes: 33
- No: 0

Devices Used to Send Message

- Smartphone: 25
- Tablet: 6
- Laptop Computer: 30
- Desktop Computer: 17
- Other: 2 (Cell phone)

Technologies Used

- **Facebook:** 29
- **Webmail:** 25
- **Twitter:** 5
- **Skype:** 6
- **Text Messaging:** 33
- **Other:**5 (Wechat, QQ, Whatsapp)

B.3 MP Survey Results

The Message Protector SUS survey results were presented in Table 5.1 This section contains the remaining survey data that was collected during the user study.

How confident are you that you used MP correctly to protect the message?

- **Not at all confident :** 0
- **Not very confident :** 2
- **Somewhat confident :** 15
- **Very confident :** 16

Would you prefer to use Gmail to login to MP as you did in the study or would you rather create a new username and password with the MP website?

- **I prefer using my Gmail login :** 27
- **I prefer creating a new username and password for MP :** 6

Please explain why:

1. I would rather use an existing account that I would typically use MP with than to create a new MP account. If I created a new MP username and password, I would probably make it my gmail login info for simplicity rather than create a brand new username and password, which I think would not be very secure anyway.
2. It is more convenient as I already have a Gmail account.
3. Google owns too many of my passwords. I don't need to give them another one. It is also nice to be a little more hands on with your own security.

4. I like to keep my login information for various websites, e-mails, applications, etc. separate from each other/compartmentalized.
5. It's a lot easier and faster that way
6. So it's easily connected to my email which is probably the only time I would use it.
7. I don't like creating new accounts. and I don't even have a gmail account...
8. It would be easier and i would not have to create another account
9. If someone else broke into my computer my gmail would already be signed in and therefore they could sign into MP and discover all my private information I was trying to hide.
10. That way you are already connected to your mail when sending messages. It would make it easier to log into for both MP and mail and easier to send messages.
11. Just because if I would use this gmail account for important information, I would like to keep it separate from school and other unimportant task that I already manage from my gmail account.
12. I dont like creating new passwords or usernames, already tooo many.
13. I don't like having multiple accounts to access multiple things because then I have to remember more passwords. It is easier to access everything with my gmail account.
14. I would prefer using my gmail login in case I forget my MP user or password
15. So I can access different things using one account.
16. It would be one less username and password to remember.
17. If I use my Gmail login, it is one less password to have to remember.
18. It will make it more secure.
19. Convenience. It is related to emails, therefore it makes sense to use the same information as your email (gmail) account.
20. Because it reduces the number of steps to use MP. I already use Gmail daily.
21. It is a lot more convenient since you can just click the button to allow MP using you gmail account info, instead of having to input everything again.
22. I don't use Gmail so I would prefer another method.
23. less password to remember. Also when I have my gmail open is probably the only time I would really need to use this.

24. Mostly because the more accounts I make, the more passwords I have to remember. Rarely do I need to send such confidential information that I would need to use a different Gmail account.
25. I have a lot of passwords and user id's already to remember, so this would make it a lot easier to remember and use.
26. I think that it is just more convenient than having to remember more usernames and passwords. This is how I do most of my other online stuff as well.
27. It seems redundant to create a new username and password for MP if you can already use your own Gmail login information to use it. I feel it would seem more accessible to people who already have a Gmail account.
28. Easier to remember name and password.
29. I would like to have them connected because I would generally only use this program when sending emails. It would be easier and more convenient to have them connected as one account than to have two accounts to log into to send one email.
30. It is one less username and password to remember.
31. Seems easier
32. I already use Gmail, so it would be easier to use just one account rather than to use a new account.
33. I like to log into things once and not have to log in to a bunch of sites.

How often would you use MP to protect your email messages

- Always: 0
- Very Often: 4
- Occasionally: 15
- Rarely: 12
- Very Rarely: 2
- Never: 0

Alice uses MP to encrypt a message for Bob. She pastes the encrypted message into Gmail and sends it to Bob. She also accidentally sends the same encrypted message to Cindy. Who can read the message? (check all that apply)

- Alice: 12

- **Bob:** 33
- **Cindy:** 11
- **Email server (Google):** 3
- **Company the owns MP:**7
- **An attacker that steals the encrypted message:**3
- **Other:**0

What did you like about MP?

1. I like that It is a chrome extension and uses my google account. I also like that there is a button to copy the encrypted message easily. I like that the button to encrypt and decrypt a message are very clear. I liked that MP was simple to download.
2. It is easy to use.
3. It allows an encryption specifically for the person you are sending the message too. It also allows you to see that the message is encrypted which I like.
4. Seems like it could be useful for people who have sensitive information (bank account numbers, SSN, passport info, etc.).
5. It was easy and makes me feel like my information was safe
6. The encryption and decryption buttons did it all. Like a translator.
7. It secures information, and it's on Chrome, easier to use; and I assume it only allows one recipient to decrypt the message, which is relatively safer.
8. It is safer than just sending the email
9. I liked that it was easy and the directions were clear. I liked the idea being able to send an email with private information instead of texting half of my bank account numbers and emailing the other half to avoid it getting stolen (which I usually do). The buttons were big and obvious which ones to use which was helpful.
10. It was user friendly. Easy to follow instructions for the average or beginner user.
11. It helps you to maintain privacy
12. Cool idea to send personal information, but I am unsure if people are going to figure this out pretty soon. The instructions are on the email anyway.
13. It is very intuitive and easy to use.
14. That protects your emails

15. Secure
16. It seems like it is a good way to send confidential information.
17. The interface is user-friendly, very straight forward. I like that I can click the picture of the lock in the upper right corner of my screen/toolbar and immediately access MP
18. It seems to make your messages safe.
19. I knew for a fact that my message was being encrypted, and therefore protected.
20. It was very easy to use because of the instructions. I felt safer sending personal information. It was a Chrome extension using Gmail and I am already familiar with both of those systems.
21. I like how it protects your info and make it safe to send our personal info.
22. Very simple, looks like a complex code
23. It is quick and easy assuming that it translated my message correctly.
24. This program was really easy to use. I was simple and well organized so even a beginner like me can use it!
25. It was quite easy to use and to get the hang of. It also already used gmail, which is something that I am really familiar with already. I don't have to learn a lot of other things in order to be able to use it.
26. I think that it is an interesting idea to having an encryption service for sending confidential information, I could see that being very important for people that send messages with sensitive information regularly.
27. I don't really understand much about computer programming and encryption and so on so I found this program very easy to use. It was quick and simple.
28. Very easy and intuitive to use. It was simple and straightforward.
29. I liked that it was simple. It didn't take a long time to learn. Yet I felt more secure sending private information through email knowing that not everyone who read the email would be able to have my information.
30. It was easy to use and it made me feel more comfortable about sending important information over email.
31. It was very simple to use
32. I liked how easy it was to encrypt a message. I don't have to do any of the work; MP does it all for me.

33. It was easy to use.

What did you dislike about MP?

1. I dislike that I have to copy the encrypted message into my webmail instead of sending directly from MP.
2. I have to encrypt the message again once I visited other pages.
3. The copy and paste method is cumbersome. It would be cool if MP was just a button that automatically changed the message within Google. I also have a love hate relationship with the idea that you have to type in the email address in both the MP app and the email message. It would be cool if that only had to happen once.
4. I'm not a fan of forced integration. I would prefer the program to be completely separate from Google.
5. I'm not really sure what clipboard is so when it saved there I was lost and just copied and pasted manually but I don't know PCs very well...
6. When encrypting a message it was confusing on how to send it. I encrypted it but I felt like the "Copy to Clipboard" button did nothing. I had to copy and paste the whole thing into a new message myself and re-enter to recipient address.
7. Nothing really.
8. nothing really
9. I was annoyed that I had to delete the message I previously encrypted or decrypted last to do another one. (but I also liked that I didn't have to start over when I clicked out and went back).
10. Nothing I can think of.
11. that is uses a very long text to encrypt a message of one sentence.
12. I didn't know what clipboard was, the message looked the same every single time, so I couldn't tell the difference. I needed to ask in order to understand if I was doing it right
13. I couldn't go back and access the instructions once I was through them.
14. All the steps to encrypt the messages.
15. not at all
16. At first it seemed a little difficult but once I figured it out it was okay.

17. When I was trying to enter messages in MP, and go back and forth between reading the message in gmail and enter information in MP, it seemed like the MP application would close. I would like it if the MP application had an "X" in the top right corner, and it wouldn't close until I clicked that x. That way, I would know I wouldn't lose any work.
18. I wish it was more integrated with Gmail.
19. Having to do a separate step outside of gmail to encrypt it.
20. I feel like it was a little too easy? If the email fell into the wrong hands, it seems like the encryption would be easy to figure out because the messages also tell you how to use MP.
21. Uh... I wasn't sure if anyone who gets the encrypted message will be able to somehow decrypt it.
22. Needed a Gmail login
23. I didn't dislike anything. I don't think my experience with it was long enough to make rational assumption on any defects or annoyances.
24. Um... nothing really. I would assume if that person had never used MP before, it may be useful to include instructions of how to download it so they aren't on a wild goose chase looking. But if the recipient gets instructions or something, then I don't dislike anything about it!
25. I didn't like how it automatically closed when I switched between window tabs and I would have to relick on the lock to open it up. It would be nice if it could just stay open. But that really is a little extra perk, not really a major flaw or anything.
26. I just don't think that I would use it all that often. I don't generally send messages with bank info or other sensitive information, and for regular messages i wouldn't want to encrypt it in the first place because I think that that would be inconvenient and unnecessary.
27. I liked pretty much everything. I found the instructions easy to follow and the program itself workable and simple.
28. I didn't dislike anything about MP. I'm not sure how often I personally would use it, but I think for certain purposes it would be very useful.
29. I didn't like that the program did not explain fully who would have access to be able to decrypt my information. If a hacker found the email would he be able to use MP to decrypt the email? I am not sure.

30. I can't think of anything.
31. Seems vaguely unnecessary
32. I didn't like having to copy and paste the message; it should just be able to send an email automatically within MP.
33. Everything was fine

What suggestions do you have to improve MP and make it easier to use?

1. I do not really understand how MP works but I imagine that I can take that encrypted message and send it to anyone and they could decrypt it. I do not understand why MP has a field for the recipient. If that is so only that particular recipient can read that particular encrypted message, I would like some assurance that that is the case. I think in the section about how to download MP, there should maybe be more explanation for how the encryption works for the average user.
2. It is already very easy to use
3. If someone is worried about an email and is encrypting it, it might be cool to figure out how to "follow" that email, see when someone opened it and where it was opened and on what kind of device. Simplifying the copy and paste method to just a simple button that automatically encrypts the message within gmail would be pretty awesome.
4. I'm not entirely sure how MP operates, so I'm not sure how it could be improved. It is already easy to use.
5. It would be nice to have a little explanation of how it works but that's all
6. When you try to copy the encrypted message you are trying to send to clipboard that it automatically creates a new message and puts your encrypted message into it.
7. Does it only work for gmail? If it does, I hope it also works for other email accounts such as hotmail, etc. If it does only work on gmail, maybe just add it as another option on the email page instead of a lock on the top-right corner.
8. maybe send the email directly from the program so you dont have to copy and paste a lot. Also be able to open the emails there
9. if it is going to be connected with gmail maybe the contacts should also be connected so you don't have to leave the page to find the email you want.
10. Nothing.
11. I like it so far. I do not have any recommendations

12. Make different texts so they look similar but not equal. Just say: Your message is ready to be pasted into your email. Instead of saying Clipboard.
13. Let the user access the instructions if he/she wants to reference them.
14. I think it was easy to use. And it explained you very well what to do.
15. improve it so people can send a message directly through MP.
16. I can't think of anything. I was able to figure it all out without difficulty.
17. (See above comment about having an x button to close)
18. Integrate it more with Gmail and make it easier to use.
19. It would be more convenient just to type the message into gmail directly and having it be encrypted when I hit send.
20. None, it is already easy to use.
21. Maybe add a button or something that you can just use one click to decrypt or encrypt the message instead of having to copy and paste?
22. I really think it works well as it is. Maybe have it open in its own tab.
23. Make sure to explain that MP does not send the email for you but you must copy and paste it yourself than make your own email.
24. I think the layout is simple and the instructions are easy. I like it and found it easy to use.
25. See previous comment.
26. Honestly I think that it is pretty easy to use, the only thing I didn't understand was the saving to clipboard part of the encryption process so I just copied and pasted it. Other than that I think that it is well put together.
27. I really have no expertise at all with encryption or technology and I found this system extremely easy to use. I really did. I don't really think there can be much done to the current setup to further enhance it.
28. I can't think of anything to make it easier to use!
29. It is pretty easy to use already. I would just add more information about the security. I assume the security is high but I would feel better knowing more in depth information about it and how it works and who has access to it.
30. None. It was very easy to use. The instructions were very clear and it was simple.
31. allow for an easier way to copy and paste

32. I would suggest making it so MP can send emails automatically to people after encrypting, so I don't have to copy and paste the message.
33. Not applicable

Have you ever installed browser extensions, add-ons or plugins before today?

- Yes: 26
- No: 7

What has prevented you from installing browser extensions, add-ons or plugins in the past?

1. Worried that they would slow down my usage. Not sure if they work (can access my information) for all of my internet activity or just certain websites. Don't want to clutter up my taskbar.
2. I didn't really know the functions of extensions, add-ons or plugins.
3. I don't trust them or they seem gimmicky. They have bad reviews or don't work properly.
4. I don't like them. I only install ad blockers.
5. I don't know how
6. No need for them or not knowing what they did so I didn't even know if i had a need for them or not.
7. No need.
8. they are not that useful
9. they don't look legitimate. They look sketchy like they will give me a virus.
10. I don't want unnecessary programs running in the background.
11. I think most of the browser extension and add-ons are spam. They add so many things in the computer that are unnecessary.
12. I really dont know how they work
13. Sometimes they are hard to find.
14. I dont remember
15. when it has a terrible feedback from the users
16. I haven't needed to or known I needed to for anything. If I have done so, I don't remember.

17. Sometimes it slows down my computer too much. -Sometimes I am worried that the extension/plugin is just malware or a worm or a virus trying to gain access to my computer.
18. Not knowing about them.
19. Not seeing the usefulness/necessity
20. Scared about them giving my computer viruses.
21. I didn't really need to use those. It hasn't been a necessity for me.
22. They usually slow down the browser, constantly updating
23. They get annoying to manage since I don't know how to get some to work sometimes.
24. I feel psychologically they clutter things. Since I don't know much about computers, I feel like they would clutter up "space." (whatever that means- space, memory, etc.) I also worry about getting too much. But other than that weird thought, I download the necessary ones and use them when needed
25. I think knowing what their purpose was and not wanting to have a bunch of extras clogging up my computer.
26. If I feel that the extension or plug in is unnecessary than I don't install them.
27. Ignorance has mostly prevented me from using them. I know nothing about these things even though I am on my computer a fair amount of my day.
28. I think the only thing that has prevented me from installing anything is that my browser or operating system was not up to date (not sure though).
29. Clutter and security issues
30. Nothing.
31. Hassle
32. Sometimes firewalls have prevented me from doing it, especially on BYU Campus.
33. Not applicable

When deciding whether you will trust a browser extension, add-on or plugin, what influences your decision?

1. Friends also use it and haven't had complications. The benefits that the add-on brings far outweigh the perceived costs of possibly slowing down my usage or cluttering up my taskbar. Knowing that I will also use the extension often and make it part of my internet routine.

2. The reviews from previous users, and also reviews from online forum.
3. Review and whether or not friends and trusted them before.
4. If I know the company that created the extension.
5. Whether or not someone else I know has used it safely...
6. If it's popular and common. Trusted by the general public. Or people I know.
7. If it's introduced by sources that I trust.
8. the company that made it mostly
9. ratings, comments, I want to make sure it isn't a scam or giving me a virus
10. If I have heard of the name or if a friend has recommended it I will trust it. Often I like to read user reviews to see if I can trust it and how well it works.
11. ratings, I'll ask someone who know or who has use it before to see how it is.
12. It wasnt my gmail account.
13. I don't often install plugins, but so I rarely have to make that decision. I think who it is made by influences me.
14. How the website looks.
15. I'd google people's respond to that add-on, and reconsider.
16. I would trust it if it is coming from a website I recognize (like Google or something)
17. If it comes from a company or organization I trust. -If it clearly states the purpose or reason why I should get it.
18. Reviews and references from others.
19. Reputation
20. Well known company, user reviews, number of downloads, recommendation by someone I trust.
21. Maybe from what company, and if a lot of people around me use it?
22. If other people I know have used it before
23. I never thought of that. Maybe I should wonder if I should trust an extension or not now.
24. Word of mouth mostly.
25. Where it comes from and who recommended it. If my computer smart friends recommend it, I am a lot more likely to try it.

26. Whether or not it comes from a reputable source, and whether I know other people that use it and have not had problems with it.
27. I would honestly want to know how it is going to help me and if it is going to give my computer a virus later on down the road. That is something that I have found frustrating since lots of downloadable programs slow my computer down and put pop ups all over the place.
28. Where I download it from, the appearance of it, whether someone recommended it.
29. I do some research myself before deciding to install anything on to my personal computer. I research the products online and read customer reviews and information from the company's website. I also place a lot of trust on what my friends and family have to say. If they feel a product is secure I am more likely to trust it. Also, if we use the program at work I am more likely to trust it because I know that my boss at BYU is thorough in his research of every program he installs on our computers.
30. I look at the reviews.
31. If other people are using it
32. I usually will trust it if it is widely-used or well-known. If it is something a small group are using, I am generally more skeptical about using it.
33. If it looks safe or not

Have you ever sent an encrypted email message?

- Yes: 3
- No: 30

Have you ever been asked to send sensitive information you were not comfortable sending through email?

- Yes: 25
- No: 8

What type of sensitive information were you asked to send? (Check all that apply)

- Password(s): 18
- Social Security Number : 15
- Medical Information : 9

- **Credit Card or Banking Information** : 21
- **Other (Please specify)** : 8 (Passport information, Transcript)

Did you send the requested information?

- **Yes:** 23
- **No:** 10

Have you ever received information you were not comfortable receiving through email?

- **Yes:** 24
- **No:** 9

What type of sensitive information did you receive? (Check all that apply)

- **Password(s):** 21
- **Social Security Number** : 8
- **Medical Information** : 9
- **Credit Card or Banking Information** : 15
- **Other (Please specify)** : 11 (Never receive sensitive messages)

Any other comments?

1. If MP was produced by a company with a good history of providing internet security, or if it had been on the market for about a year and had good reviews, I would consider using it (if it were completely independent from any e-mail provider or browser). Can MP encrypt documents (such as those you would normally fax)? That could be very useful. If it did that, I would be much more interested in using it, because it could eliminate the need for a fax machine.
2. Nope
3. No
4. I really like it and do feel I would use it!
5. Even though I was unfamiliar with the MP program, I felt confident in my ability to successfully use it. Instructions were easy to follow.
6. I just want to know if other people can follow the instructions the same way and see my message?

7. N/A
8. Nope!
9. When I was going through the brief tutorial, I didn't see any information on how the encryption works, who can and cannot see my message, and if it protects from NSA surveillance. It would be good to know this information, or at least have a link that I can click on to learn this information.
10. No.
11. In the past, I have felt unsafe sending personal information over message, so I've had to call the other person. Using encrypted messages would be a very useful alternative.
12. Excellent product
13. That will do.
14. No. Thank you letting me participate in the study!
15. Will this cost money? If it were free or inexpensive I would definitely consider using it. However, right now in my life, I don't have a lot of reasons to encrypt messages. In the future it would probably be beneficial.
16. The comment about Bob and Alice confused me a little bit, because I understand that Alice and Bob are the two people who recognize what to do with the encrypted message, but it is to my understanding that if anyone receiving said message knows what to do with the encrypted message, they would in turn be able to read it. Also, I don't think I personally would use MP to encrypt my emails because I don't necessarily send information over email that could be used against me in any way. At least not yet. Maybe further down the road I will need to send bank account information or social security numbers over the internet. In that case, I probably would use encrypted messages.
17. I think this is awesome! I want it!

B.4 General Security Questions

The Message Protector survey results are presented in table B.1

Question	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
I trust Gmail with my sensitive email messages	1	5	15	11	1
I am concerned about Gmail scanning my messages	0	12	6	10	5
I worry that some messages aren't really from who they say they are from	3	6	5	16	3
I feel safe sending important information through email	3	8	12	10	0
I feel safe creating accounts with usernames and passwords on new sites	0	6	8	14	5
I feel safe installing browser extensions or plugins	1	4	10	16	2
Creating accounts for new websites is easy	0	3	2	17	11
Installing browser extensions is easy	0	0	7	20	6
I feel safe clicking on links in email messages	3	13	11	6	0
I feel safe clicking on links in email messages from people I know	1	1	3	22	6
I never click on links in email messages	5	19	7	2	0

Table B.1: General Security Questions