

March 2016

IQP Strong Authentication

Andrew Jack Mokotoff
Worcester Polytechnic Institute

Cuong Hung Nguyen
Worcester Polytechnic Institute

Nathan M. Caso
Worcester Polytechnic Institute

Romuald S. Valme
Worcester Polytechnic Institute

Follow this and additional works at: <https://digitalcommons.wpi.edu/iqp-all>

Repository Citation

Mokotoff, A. J., Nguyen, C. H., Caso, N. M., & Valme, R. S. (2016). *IQP Strong Authentication*. Retrieved from <https://digitalcommons.wpi.edu/iqp-all/2138>

This Unrestricted is brought to you for free and open access by the Interactive Qualifying Projects at Digital WPI. It has been accepted for inclusion in Interactive Qualifying Projects (All Years) by an authorized administrator of Digital WPI. For more information, please contact digitalwpi@wpi.edu.

Strong Authentication

Interactive Qualifying Project

Advisors:

PROFESSOR T. EISENBARTH
PROFESSOR A. SMITH

Written By:

NATHAN CASO
ANDREW MOKOTOFF
CUONG NGUYEN
ROMUALD VALME



WPI

A Social Study of Science and Technology
WORCESTER POLYTECHNIC INSTITUTE

A student-based undertaking submitted in the form of an
Interactive Qualifying Project at the Worcester Polytechnic
Institute.

SEPT 2015 - MARCH 2016

ABSTRACT

The threat of online personal information breaches rises as people put more critical data online, and despite ample availability, strong authentication protecting this information is not being adopted quickly enough to address the threat. To better understand this problem, the IQP team designed and conducted a study to isolate factors leading to such behavior. The team found that people had trouble surmounting the shift to stronger tools, but once past that, they readily settled into permanent use. Also, personal connection to threats was correlated to a good impression of strong authentication. The solution may be online security education that induces a personal connection to the threat, so as to create a better incentive to overcome the obstacles of transitioning and increase security.

TABLE OF CONTENTS

| | Page |
|---|-------------|
| List of Tables | v |
| List of Figures | vi |
| Executive Summary | 1 |
| 1 Introduction | 2 |
| 1.1 Introduction | 2 |
| 2 Background | 5 |
| 2.1 Overview | 5 |
| 2.2 What Is Authentication? | 5 |
| 2.3 Single Factor Authentication | 6 |
| 2.4 Dual Factor Authentication | 7 |
| 2.5 Strong Authentication Methods | 10 |
| 2.5.1 Network Based Authentication | 10 |
| 2.5.2 Authentication Without Network Connection | 11 |
| 2.6 Related Work | 13 |
| 2.7 Fido Alliance | 14 |
| 2.8 Dual Factor Authentication Failures | 15 |
| 2.9 Statistical Tests Background Information | 16 |
| 2.10 Authy | 17 |
| 2.10.1 Advantages and Disadvantages | 18 |
| 2.10.2 Capabilities | 18 |
| 2.10.3 Important Services that Authy Provides | 18 |
| 2.10.4 Privacy | 18 |
| 2.10.5 Security | 19 |
| 2.10.6 Usability | 19 |
| 3 Methodology | 20 |
| 3.1 Overview | 20 |

| | | |
|----------|---|-----------|
| 3.2 | Phase 0: Recruiting | 21 |
| 3.3 | Phase 1: Introduction | 23 |
| 3.3.1 | Participation Confirmation, Group Splitting, and Initial Survey | 23 |
| 3.3.2 | Baseline Education | 23 |
| 3.3.3 | Advanced Education | 24 |
| 3.4 | Phase 2: Data Gathering and Behavior Tracking | 26 |
| 3.4.1 | Bi-Weekly Tracking | 26 |
| 3.5 | Phase 3: Study Completion | 27 |
| 3.5.1 | Information Recall | 27 |
| 4 | Results | 29 |
| 4.1 | Overview | 29 |
| 4.2 | Basic Information | 29 |
| 4.3 | Statistical Tests | 30 |
| 4.4 | Initial Survey | 30 |
| 4.4.1 | Class Distribution | 30 |
| 4.4.2 | Prior Knowledge of Authentication | 30 |
| 4.4.3 | Acquaintance with Someone Hacked | 32 |
| 4.4.4 | Traditional Passwords | 32 |
| 4.4.5 | Value of Security | 33 |
| 4.4.6 | Private Information | 34 |
| 4.4.7 | Value of Privacy | 36 |
| 4.4.8 | Sufficiency of Single Factor Authentication | 37 |
| 4.4.9 | Willingness to Spend Additional Time Authenticating | 37 |
| 4.4.10 | Retention Rate of the Study | 38 |
| 4.4.11 | Summary of Initial Survey | 39 |
| 4.5 | Mid Study Evaluations | 39 |
| 4.5.1 | Installation Success | 39 |
| 4.5.2 | Frequency of Authentication | 40 |
| 4.5.3 | Perceptions of Usability | 40 |
| 4.5.4 | Perceptions of Security | 43 |
| 4.5.5 | Perceptions of Privacy | 48 |
| 4.5.6 | Difficulties with Authy | 50 |
| 4.5.7 | Summary of Mid-Study | 50 |
| 4.6 | Final Survey | 52 |
| 4.6.1 | Perception of Protection | 52 |
| 4.6.2 | Usability Conclusions | 53 |
| 4.6.3 | Confidence in Privacy | 53 |
| 4.6.4 | Perception Change | 54 |

TABLE OF CONTENTS

| | | |
|----------|---|-------------|
| 4.6.5 | Continued Use of Authy | 55 |
| 4.6.6 | Participants Technical Understanding of Authy | 55 |
| 4.6.7 | Knowledge Learned About Internet Security | 56 |
| 4.6.8 | Other Forms of Multi-Factor Authentication | 56 |
| 4.6.9 | Final Survey Summary | 57 |
| 5 | Conclusions and Recommendations | 58 |
| 5.1 | The Study | 58 |
| 5.2 | Key Findings | 58 |
| 5.3 | Recommendations | 59 |
| 5.3.1 | Future Research | 59 |
| 5.3.2 | Other Recommendation | 60 |
| | Appendix A: Pitch Presentation | i |
| | Appendix B: Basic Presentation | iii |
| | Appendix C: Advanced Presentation | vi |
| | Appendix D: Surveys | x |
| | Bibliography | xxii |

LIST OF TABLES

| TABLE | Page |
|---|-------------|
| 2.1 Real World Usage of Authentication Methods: A survey of 472 companies (Davis, 2014) | 8 |

LIST OF FIGURES

| FIGURE | Page |
|---|-------------|
| 2.1 Real World Usage of Authentication Methods (Davis, 2014) | 9 |
| 3.1 Diagram of Our Study | 21 |
| 4.1 Results to the first question in the initial survey: "In which class are you?". | 31 |
| 4.2 Responses to "Define computer authentication in your own words?" which was given in the initial survey. | 31 |
| 4.3 Results to "Do you know what Multi-Factor Authentication is?" which was asked in the initial survey. | 31 |
| 4.4 Results to "Have you or has a family member of yours ever experienced a computer account being hacked or compromised?" given in the initial survey. | 32 |
| 4.5 Results to "How many passwords do you use?" given in the initial survey. | 33 |
| 4.6 Results to "Do you think your passwords are secure?" given in the initial survey. | 33 |
| 4.7 Results to "How often do you reset a password for an online account?" asked in the initial survey. | 34 |
| 4.8 Results to "How much do you value internet account security?" asked in the initial survey. | 34 |
| 4.9 Responses in figure 4.8 but in respect to initial survey responses. | 35 |
| 4.10 Results to "Do you have information online that you would prefer to be kept private?" asked in the initial survey. | 35 |
| 4.11 Results to "How much do you value the privacy of your online information?" asked in the initial survey. | 35 |
| 4.12 Responses as seen in figure 4.11 but in respect to background question responses as seen in the graph. | 36 |
| 4.13 Results to "Is an account username and password enough to protect your online accounts?" asked in the initial survey. | 37 |
| 4.14 Results to "How much extra time would you spend authenticating yourself for online accounts?" asked in the initial survey. | 37 |
| 4.15 Results of the participants who dropped vs their education treatment. | 38 |
| 4.16 Results from figure 4.15 in respect to background traits as seen in the graph. | 39 |

4.17 Results of "Did your installation run smoothly?" in respect to education treatment, asked in the first mid-study survey. 40

4.18 Results of "How often did you use Authy to authenticate yourself in the last two weeks?", asked in the mid-study surveys. 41

4.19 Overview of responses to "What are your observations on the usability of the application?" through out the mid study responses. 41

4.20 Results in figure 4.19 in respect to education treatment. 42

4.21 Results in figure 4.19 in respect to prior knowledge of Multi-Factor Authentication. (figure 4.3) 43

4.22 Results in figure 4.19 in respect to knowledge of someone hacked. (figure 4.4) 44

4.23 Results in figure 4.19 in respect to prior opinion of password sufficiency. (figure 4.6) 44

4.24 Overview of responses to "What are your observations on the security Authy provides?" through out the mid study responses. 45

4.25 Results in figure 4.24 in respect to education treatment. 46

4.26 Results in figure 4.24 in respect to prior knowledge of Multi-Factor Authentication. (figure 4.3) 46

4.27 Results in figure 4.24 in respect to knowledge of someone hacked. (figure 4.4) 47

4.28 Results in figure 4.24 in respect to prior opinion of password sufficiency. (figure 4.6) 47

4.29 Overview of responses to "What are your observations on the privacy of Authy?" through out the mid study responses. 48

4.30 Results in figure 4.29 in respect to education treatment. 49

4.31 Results in figure 4.29 in respect to prior knowledge of Multi-Factor Authentication. (figure 4.3) 49

4.32 Results in figure 4.29 in respect to knowledge of someone hacked. (figure 4.4) 50

4.33 Results in figure 4.29 in respect to prior opinion of password sufficiency. (figure 4.6) 51

4.34 Responses to "Have you experienced any difficulty with Authy?" in respect to education treatment. 51

4.35 Responses to "How protected did you feel when using Two Factor Authentication?" in respect to education treatment and initial survey responses. 52

4.36 Responses to "Rate the overall usability of Authy." in respect to education treatment and initial survey responses. 53

4.37 Responses to "How confident are you that Authy keeps your data safe and private?" in respect to education treatment and initial survey responses. 54

4.38 Responses to "Did your perception of authentication change throughout this study?" in respect to education treatment. 55

4.39 Responses to "Do you think you will continue using Authy outside of this study?" in respect to education treatment. 55

LIST OF FIGURES

| | | |
|------|---|-------|
| 4.40 | Responses to "Is Two Factor Authentication, as provided by Authy, more secure than a password?" in respect to education. | 56 |
| 4.41 | Responses to "Did you learn anything about internet security throughout this study?" in respect to education. | 56 |
| 4.42 | Responses to "Did you install Authy for more than the two services we asked for?" in respect to education. | 57 |
| 4.43 | Responses to "Did you install any other methods of Strong Authentication and/or do you plan to?" in respect to education. | 57 |
| 1 | Pitch Presentation, Slides 1 - 4 | i |
| 2 | Pitch Presentation, Slides 5 - 8 | ii |
| 3 | Basic Presentation, Slides 1 - 4 | iii |
| 4 | Basic Presentation, Slides 5 - 10 | iv |
| 5 | Basic Presentation, Slide 11 | v |
| 6 | Advanced Presentation, Slides 1 - 4 | vi |
| 7 | Advanced Presentation, Slides 5 - 10 | vii |
| 8 | Advanced Presentation, Slides 11 - 16 | viii |
| 9 | Advanced Presentation, Slide 17 | ix |
| 10 | Initial Questionnaire, Page 1 | x |
| 11 | Initial Questionnaire, Page 2 | xi |
| 12 | Initial Questionnaire, Page 3 | xii |
| 13 | Mid-Study Evaluation I, Page 1 | xiii |
| 14 | Mid-Study Evaluation I, Page 2 | xiii |
| 15 | Mid-Study Evaluation I, Page 3 | xiv |
| 16 | Mid-Study Evaluation II, Page 1 | xv |
| 17 | Mid-Study Evaluation II, Page 2 | xv |
| 18 | Mid-Study Evaluation II, Page 3 | xvi |
| 19 | Mid-Study Evaluation III, Page 1 | xvii |
| 20 | Mid-Study Evaluation III, Page 2 | xvii |
| 21 | Mid-Study Evaluation III, Page 3 | xviii |
| 22 | Final Questionnaire, Page 1 | xix |
| 23 | Final Questionnaire, Page 2 | xx |
| 24 | Final Questionnaire, Page 3 | xxi |

EXECUTIVE SUMMARY

In today's technologically advancing society, the internet contains an incredible amount of sensitive information. Critical data like Social Security numbers and banking information are stored in databases accessible through the internet. Authentication for many services consists of a simple username and password. When one uses only this to protect an account, one is subject to a frighteningly high risk of online attacks that may lead to accounts being compromised. The use of strong authentication methods is highly recommended to fully protect one's accounts. Despite this, most people do not use the stronger tools available to them. The goal of this IQP is to identify solutions to the problems of spreading the use of Strong Authentication by studying how people perceive and behave while using it.

This project presents the results of a study conducted to track users' views on strong authentication. The study consisted of gathering a group of individuals willing to try out a two factor authentication, educating a portion of the subjects on the current threats and methods to mitigate them, and requiring them to use the service for ten weeks. During this time, the subjects filled out bi-weekly surveys to track behavior and perception. At the end of the study, all subjects completed an exit survey to assess the experience. The data collected gave insights into how to solve the problem of the missing widespread use of strong authentication.

The team found that individuals frequently stated that they desired increased security, but they were unwilling or unaware of how to improve. The team also found that background factors generally had no relation to perception of the strong security method used throughout the study, with the notable exception of prior knowledge of Multi-Factor Authentication. Subjects were typically happy with the security, privacy, and usability of the two factor authentication application after the burden of installation and linking of services was complete.

This study helps explain the overall experience of using strong authentication. Improving overall experience is pivotal to spreading the adoption of secure practices. The IQP team recommends that strong authentication awareness education be given in a way that invokes a strong personal connection to the threat, so as to help people surmount the difficulties of transitioning to strong authentication methods.

For future related work, the team suggests more in-depth education be supplied to future participants of a similar study. Having a larger and more diverse pool of subjects may also aid in obtaining widespread and valuable data. One final recommendation is hosting regular meetings with participants to further illicit reflection on perceptions.

INTRODUCTION

1.1 Introduction

In the summer of 2014, J.P. Morgan Chase (JPMC), the largest bank in the United States, experienced the worst ever cyber-attack to date. Accounts of seventy-six million households and seven million small businesses were compromised in the attack. The hackers, who operated overseas, were able to generate a list of applications used on the local machines at the offices of JPMC by gaining access to an employee's account password. Using that list, they were able to figure out which applications were vulnerable and used them as a backdoor into JPMC's system (Silver-Greenberg, 2014). Despite spending \$250 million each year for cyber security, JPMC's security team neglected to upgrade one of their network servers to use **Multi-Factor Authentication**¹ (MFA). This left the entire bank vulnerable to a cyber-attack (Goldstein, 2014).

Earlier in 2014, hackers compromised Jennifer Lawrence's iCloud account, resulting in nude pictures and videos being exposed to the internet. The attackers gained access to her account because they were able to bypass the MFA on iCloud. Many other celebrities were also hacked, including Victoria Justice, Teresa Palmer, Kate Upton, and Lea Michele.

Ashley Madison, an adult dating website that assists married people engage in extramarital affairs, was compromised in July of 2015. Hackers gained access to the database that contained user account information, and they figured out how to decrypt all of the data. Ashley Madison lost control of users' names, addresses, and personal photographs. As a result, Ashley Madison's CEO, Noel Biderman, resigned after the third leak. The increasing frequency of stories about corporations and individuals being hacked demonstrates a bit of the larger trend of online security: it is not relatively strong enough to shrug off the storm of malicious attacks anymore.

¹**Multi-Factor Authentication:** A form of strong authentication requiring the use of more than one verification step, adding critical layers of security to user sign-ins and transactions

However, there is still hope. One of the relevant protagonists in the battle for online security is strong **Authentication**²

Insecure authentication is widespread and gives hackers an easy route to successfully attack a computer system. The current standard of authentication (username and password) is not sufficient for modern day usage. Computers are powerful enough to try every combination of characters in a password until they break in, a method known as **Brute Force**³. Using brute force, modern computers can crack any possible six character password almost instantaneously (in 0.0024 seconds) (Kevin Forgy, 2012). If stronger authentication were more commonly used, J.P. Morgan Chase, Jennifer Lawrence, and countless other entities would have been far more likely to prevent their data being breached. MFA drastically reduces online identity theft and other forms of fraud, because even if a password is stolen, it is not enough to give an attacker access to the system (Rouse, 2015).

There are few previously completed studies pertaining to why people do not use strong authentication. One such study focused mainly on privacy and usability as motivation criteria, drawing specific but inconsistent conclusions: (Weir, 2009) found that people were motivated to use a particular method by usability and convenience rather than added security, whereas (Christofaro, 2014) found that perception of privacy is not negatively correlated with usability, and that perception of usability is dependent only on user background factors rather than the specifics of an application. This discrepancy illustrates that there is still much to learn. Designing smarter strong authentication techniques that build off of people's motivation requires further investigation of their incentives.

The ultimate goal of the following report is to analyze the influence on motivation to use strong authentication of several targeted factors: awareness education, user background, and perceptions of usability, privacy, and security. In order to address these goals, the IQP team designed a study that recruited participants with a cash incentive and split them into two groups with different levels of awareness education treatment: baseline and advanced education. The two groups attended separate educational meetings where they received their differing education and completed an initial survey, which was used to assess the participants' background information before education.

The IQP team required all subjects to complete five surveys sent to them on a bi-weekly basis while they incorporated a third party **Two-Factor Authentication**⁴ (2FA) application, Authy, into several of their online services. The aforementioned surveys were used to assess any change in perception throughout the study and identify trends relative to background traits, study treatments, and time. The surveys determined student's thoughts on the usability, privacy, and security of Authy. After the mid-study period passed, the subjects were asked to attend a

²**Authentication:** The process by which a computer system verifies that the claimed identity login attempt is genuine. A common example is a username and password combination.

³**Brute Force:** A trial and error method used by hackers to decode encrypted data such as passwords relying on exhaustive effort rather than employing intellectual strategies

⁴**Two-Factor Authentication:** Multi-Factor Authentication using exactly two verification steps

final meeting, during which they completed an exit (Final) survey and received compensation for their participation. The final survey data was used to generate an overall view of the study from an individual's perspective and to collect participants' final perceptions on strong authentication.

The analysis of the results from each of the surveys suggested that education may play a role in perception of 2FA, but not so much in user behavior. The team found that background personal factors, such as if a subject knew someone who was hacked, or whether or not a subject had prior knowledge of Strong Authentication, were far more likely to predict a positive behavior or perception. Additionally, participants do not seem to accurately report their true values of the aforementioned criteria and often think they are better off than they actually are. Many subjects had difficulties or concerns when installing and linking their services to Authy. By the end of the study, participants generally favored the use of 2FA, similar to how they blindly favored the use of single factor authentication passwords at the beginning of the study.

The IQP team recommends that strong authentication methods such as 2FA should receive more attention in the media to increase overall usage until it becomes the norm. Entities using strong authentication may benefit by having clear, foolproof installation guides. If the barrier to entry is too high, few will put in the work to secure themselves. Supporting more services and/or standardizing strong authentication across platforms may also go a long way in expanding overall usage. Additionally, the team recommends that more research be done with varying study conditions such as having a larger number of participants, diversifying the participants, or using a different strong authentication method like Google Authenticator. Society can benefit from changes like these to strengthen online security.

BACKGROUND

2.1 Overview

The following background section contains in-depth information regarding the definitions of authentication, single and dual factor methods with examples, related work, and several other topics including the FIDO Alliance's work and weaknesses of two factor authentication. One must understand these to understand the goals of this research and the methods taken in the design of the user study.

2.2 What Is Authentication?

Authentication is the process by which a system verifies the identity of a user who wishes to access it. The recent growth of internet technology and its associated security requirements demand for strong authentication. Authentication can be classified three ways:

1. Verifying proof of identity by confirming a credible person's claim who had first-hand evidence that the identity is genuine.
2. Contrasting the attributes of the object to common knowledge about objects of that origin.
3. The last definition relies on documentation or other outside claims. For example, in computer science, a user can gain access to a secure system based on provided credentials that imply authenticity.

In computer science, verification is conducted by proving the truth of an attribute of a particular datum (a "factor" of authentication). These factors can be split up into three categories that cover a plethora of elements. Any number or combination of the following may be used to

verify an individual's identity before granting access, approving a transaction, signing a document, granting authority to another person, or establishing a chain of power. These factors are:

1. *Knowledge factors*: Something a person knows, for example: passwords, person identification number (PIN), challenge question response, and pass phrases.
2. *Ownership factors*: Something a person has, for example: security token, cell phone, software token, ID card, wrist band, and etc.
3. *Inherence factors*: Something a user is or does, for example: biometrics including fingerprints, retinal patterns and etc, signatures, face, voice, and biometric identifiers.

2.3 Single Factor Authentication

Single Factor Authentication (SFA) is authentication that uses one of the three factors to identify a user. For example, a key and lock system is a single factor authentication method because it uses a possession factor to identify a user and give him/her access. Similarly, a fingerprint or retinal scanner relies on the uniqueness of one's physical body, an inherence factor. But perhaps the most common example is the computer password, which relies on the user's knowledge of a correct password, a knowledge factor.

Single factor authentication has the advantage of simplicity over its stronger multiple factor counterparts. SFA methods are quicker, easier, cheaper, and better known. Therefore, they were the most economic choice for internet security for many years. SFA still remains the most economic choice for home invasion security; one rarely needs to secure a household beyond a simple lock and key. However, just as one can use a strong pair of pliers to cut through a padlock, one can use a brute force attack on an internet security system. The difference nowadays is that the tools and strength necessary to break a single factor authentication system on a computer are far more commonplace and reward yielding than those required to break a padlock. SFA is universally less secure than multi-factor methods by the nature complexity itself, but the focus of this project is the economic disadvantages of the most relatively important SFA system: the standard password. The significant disadvantage thereof is the lack of security.

Password authentication is becoming susceptible to breaches by brute force attacks now that more powerful computers are more common and less expensive. To illustrate the scale of this, in 2014, a group of Russian criminals compiled a list of 1.2 billion internet username and password combinations, including those from 500 million e-mail accounts. According to a Radicati study, 4.35 billion e-mail accounts are in existence. That means roughly 11.5% of all e-mail addresses have been hacked mainly due to brute force attacks. This is compounded by the phenomenon of people using the same password for multiple accounts. According to a study that BitDefender conducted in 2010, 75% of people use the same account names and passwords on their social networking sites as they do on their email accounts. On top of all of this, the security of password

SFA relies on the user create a unique knowledge factor; knowledge factors tend to be less unique than inherence and possession factors inherently, and there is little need to justify the claim that people tend to use simple, non-unique passwords. The combination of the disadvantages mentioned above justifies the relative risk of standard internet SFA as high, and, therefore, uneconomic.

2.4 Dual Factor Authentication

Two Factor Authentication allows for increased security by requiring a combination of two factors. These components can be something that a user has (a possession factor), something that a user knows (a knowledge factor), or something that the user is (an inherence factor). An example of one such method is a transaction at a cash register. One must swipe his/her card and also enter a pin number to allow a debit transaction. Both the physical card and knowledge of the pin number are required, thus satisfying the two factor requirement.

Two factor authentication primarily has the advantage of increased security over single factor methods. A brute force attack will not work because at least one of the factors is not an entity that can even be "guessed". Two factor authentication is even more secure when used locally and not connected to a server; the chances of Man in the Middle Attacks are greatly reduced (A Man in the Middle Attack occurs when a hacker uses a counterfeit "service" to deceive his/her victim into entering personal account information). 2FA's security is furthered by its high number of implementation techniques. Its forms range from a password plus and inherence factor as with a biometric scanner to a username and password plus a one-time passwords (OTP's) sent via SMS to a cell phone. Two factor authentication is also frequently and advantageously free on the user end, as seen in SMS OTP and mobile application systems.

Although two factor authentication has many advantages, it comes with drawbacks. 2FA practices using a to a server connection to distribute one of the factors are susceptible to Man in the Middle attacks, and all 2FA is vulnerable Trojan attacks. Even so, any hacker must overcome two factors instead of one. 2FA may also be inconvenient; separate physical devices are sometimes used to distribute OTPs, necessitating the device's presence when authenticating and maintenance associated with such hardware. Additional physical devices may also be costly.

Table 2.1 shows data that approximates usage of the aforementioned authentication methods. Figure 2.1 contains a histogram of the same data:

| Company Genre | SMS | Phone call | Email | Hardware Token | Software Implementation | Totals |
|----------------------|------------|-------------------|--------------|-----------------------|--------------------------------|---------------|
| Backup & Sync | 9 | 2 | 3 | 2 | 13 | 29 |
| Banking | 11 | 7 | 5 | 11 | 7 | 41 |
| Cloud Computing | 5 | 2 | 0 | 2 | 14 | 23 |
| Communication | 7 | 1 | 1 | 2 | 8 | 19 |
| Cryptocurrency | 9 | 1 | 1 | 6 | 26 | 43 |
| Developer Software | 11 | 3 | 0 | 3 | 16 | 33 |
| Domains | 10 | 2 | 0 | 8 | 24 | 44 |
| Education | 1 | 0 | 0 | 1 | 2 | 4 |
| Email | 6 | 1 | 2 | 4 | 9 | 22 |
| Entertainment | 1 | 0 | 0 | 0 | 0 | 1 |
| Finance | 3 | 1 | 1 | 0 | 2 | 7 |
| Gaming | 4 | 0 | 6 | 3 | 17 | 30 |
| Health | 2 | 0 | 1 | 0 | 3 | 6 |
| Hosting/VPS | 6 | 0 | 0 | 5 | 18 | 29 |
| Identity Management | 5 | 1 | 1 | 6 | 11 | 24 |
| Investing | 3 | 2 | 1 | 4 | 3 | 13 |
| Payment | 7 | 1 | 1 | 3 | 6 | 18 |
| Remote Access | 0 | 0 | 2 | 1 | 5 | 8 |
| Retail | 2 | 0 | 0 | 1 | 2 | 5 |
| Social | 11 | 1 | 0 | 1 | 9 | 22 |
| Security | 3 | 1 | 1 | 3 | 8 | 16 |
| Utilities | 0 | 0 | 0 | 0 | 0 | 0 |
| Other | 11 | 2 | 1 | 1 | 15 | 30 |
| Totals | 127 | 28 | 27 | 67 | 218 | 467 |

Table 2.1: Real World Usage of Authentication Methods: A survey of 472 companies (Davis, 2014)

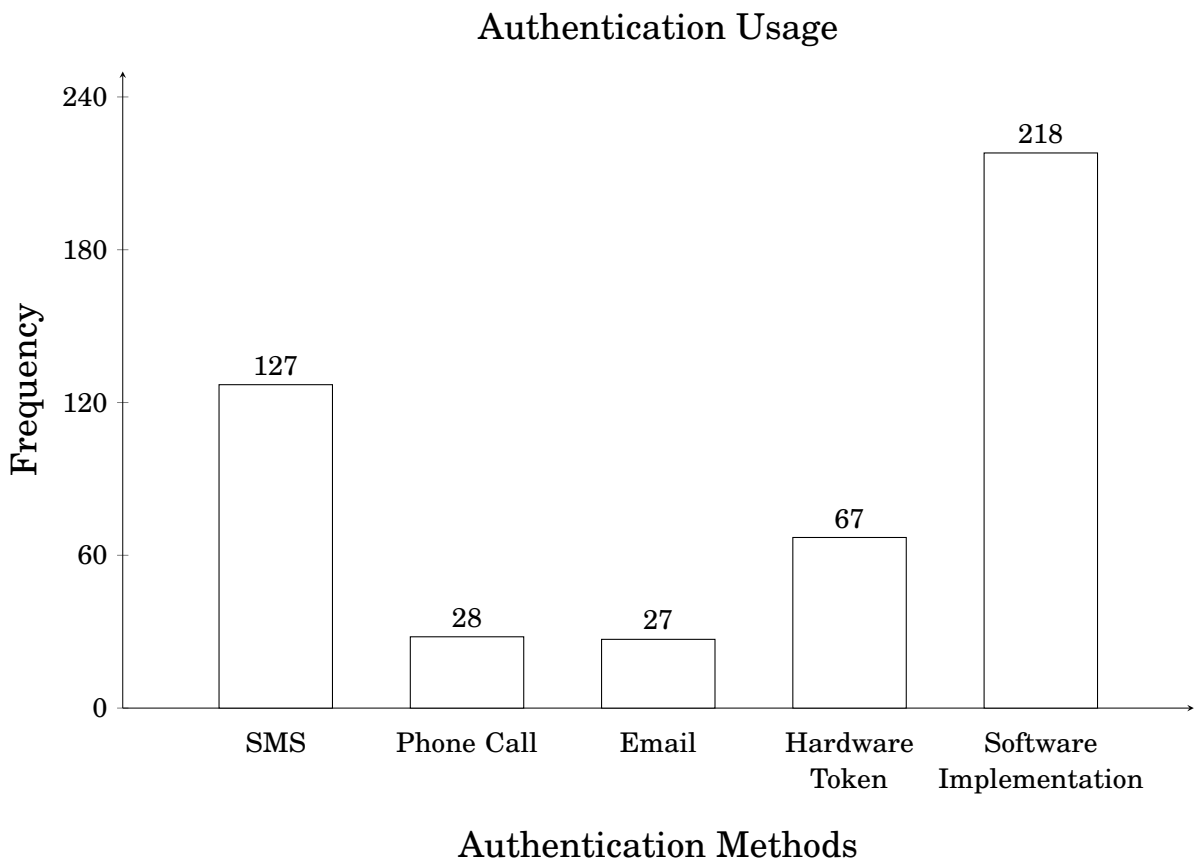


Figure 2.1: *Real World Usage of Authentication Methods (Davis, 2014)*

2.5 Strong Authentication Methods

2.5.1 Network Based Authentication

SMS

SMS verification is a common network-based authentication system. This technology requires a user with a phone signal to get access to an account by entering a one-time password (OTP) sent to their phone via SMS after entering a username and password. The two factors in this case are knowledge (username and password) and ownership (cell phone).

An example of this method is Facebook using a login approval authentication system that requires one to enter a code that Facebook sends to his/her mobile phone via SMS message when logging in from a new IP address in addition to the standard username and password. Once successful, the user can mark the device as approved so that he/she need not use both factors for every future usage. Dropbox also has a similar SMS two-step verification in which a user may elect to use to add a knowledge factor of authentication to their logins. Once a user opts in, he/she must enter a onetime password for each login session.

SMS verification adds a second step to authentication that makes hacking into an account significantly more difficult; if a hacker obtains or bypasses only the username and password fields, they will still be unable to log in as they lack the Onetime Password (OTP). Furthermore, SMS verification systems are inexpensive on the user's side; SMS messages are typically free with today's standard cell phone carrier plans.

One potential problem with this method is the dependency upon one's cellphone. The method is ineffective when one is out of network range or if one's phone is lost or stolen. Additionally, this method is considered relatively insecure; SMS text messages can be intercepted or forwarded to another phone number, which may provide a hacker with an authentication code and therefore account access.

Email

Email verification is another common 2FA method that requires one to enter a OTP sent to him/her by e-mail after entering a username and password. Again, this method uses two authentication factors: knowledge (username and password) and ownership (email).

Valve, a videogame company and the creator of the online videogame/software catalog Steam, uses "Steam Guard", a setting where each time one logs into one's account on an unknown device, one must enter an OTP sent via email. Origin, another videogame manufacturer, uses another exemplary login verification setting: Whenever one's account is logged into on a remote device, a verification code will be sent to his/her contact email address and required to complete the authentication process. E-mail verification is completely free for users and simple to implement for developers, and thus advantageous.

However, email verification has its disadvantages. First is the typical usability complaint a

longer login process with possible complications such as a spam filter marking and deleting the email containing the code. Second, this method can be considered as merely an extension of a knowledge factor rather than an ownership factor; to access one's email, one only needs to enter another username and password, so one can argue that using an e-mail as an authentication step is just a longer password.

2.5.2 Authentication Without Network Connection

Embedded Devices

Another type of two-factor authentication is the embedded system random code generator. This comes in the form of a physical device that randomly generates output codes that are required in addition to a username and password. This satisfies the knowledge and ownership conditions of two-factor authentication. One should note that the device is not connected to a server; it uses a parallel algorithm to the so that the codes match.

One such embedded hardware security token is the RSA SecurID. This and similar devices operate by having their internal clocks synced with their central servers' clocks. Each token with a unique seed generates a random number. The server and embedded device run matching algorithms based on the same seeds, which results in the same value on both ends. Therefore, the device does not communicate with the server. Rohos uses a login USB key which must be plugged in to authenticate a user. The method further removes the complexity of learning how to log in the system because after a single login, the software on the individual device remembers the USB and authenticates automatically when plugged in (Cooperband, 2015).

Embedded devices typically are the most common highly secure two-factor authentication methods. Using OTPs is extremely effective in both corporate and local logins. Because OTP generators are offline, there is no vulnerability to an attack on a network channel such as those that SMS and email methods use. Hardware devices are considered secure enough to use in banking such as with Bank of America, National Bank of Abu Dhabi, the Bank of Queensland and many more (Aloul, 2009).

Hardware token devices do have several disadvantages. Buying, supplying, maintaining, and replacing physical devices for customers can be costly. If an individual uses several banks, he/she might inconveniently need to purchase several expensive tokens. Additionally, learning to use such devices may be inconvenient for those who are not technically inclined (Aloul, 2009).

Mobile Application

Companies such as Google and Twilio showcase yet another method of two-factor authentication: the smart-device app. This method uses a smart device (i.e. cell phone or tablet) application with a time-based one-time password algorithm (TOTP) to generate a passcode necessary for authentication in addition to a regular account password. Thus, this method uses a knowledge

factor (the password) and a possession factor (one must physically have their smart device to open the application) to ensure secure access.

To illustrate exactly how this works, one can use this method for verifying one's Microsoft account. Every time one signs in, one is required to enter a six digit 60-second iterative password that is generated by only Google's Authenticator app on his/her cell phone and is unique to one's Google/Microsoft account. This system has several advantages: First, it is versatile and can be utilized by a variety of third-party applications. For example, Microsoft accounts can be linked to Google's Authenticator App or Twilio's Authy's application, which will be described in more depth later. Phone applications are more secure than SMS verification or e-mail OTP systems because they are time-based and disconnected from server connections. The disadvantages of this system stem from the relative complexity and lack of broad usage. Google's Authenticator and Twilio's Authy are the two widely used examples of the method, but many account services still do not support either of them or 2FA in general.

Common Access Card

The common access card is a standard identification tool for active-duty military personnel and other government employees. The common access card (CAC) is used as an authentication factor for military and government computers and additionally for physical access to buildings, and controlled spaces. Each CAC is encrypted using 2048-bit encryption. In some cases, the card is used in conjunction with a personal password and others a simple pin number is required. The card qualifies as an ownership factor (the physical CAC), and the password/pin is a knowledge factor. Most CAC cards have an integrated circuit chip on them containing either 64 or 144 kilobytes of personal data including the password/pin for the chip. Also, CACs are also used to encrypt emails and sign documents. Many workplaces use local networks that require a CAC card to gain access. If a user fails to enter the password/pin a certain number of times, the CAC's access permissions are removed.

Some of the government employees that use the CAC include active-duty armed forces, reservists, National Guard members, the National Oceanic and Atmospheric Administration, the United States Public Health Service, Emergency-essential employees, contingency contractor employees, contracted ROTC cadets, deployed overseas civilians, non-combatant personnel, DoD/uniformed service civilians residing on military installations in CONUS, Hawaii, Alaska, Puerto Rico, and Guam, DoD/uniformed service civilians or contracted civilians living in a foreign country for more than 365 days, Presidential appointees approved by the United States Senate, DoD civilian employees, United States military veterans with a Veterans Affairs Disability rating of 100%, Eligible Contractor Employees, and non-DoD/other government and state employees of the National Guard.

The CAC's usage is not limited to enter protected systems. It can also be used as an all-in-one card. The chip technology may also be used as identification or as a credit or debit card: integrated circuit chips are more secure than traditional magnetic strips. However, embedded integrated

circuit chips are fragile and known to malfunction with minor wear. Even if the contacts on the chip are dirty, a reader may not recognize it. If the CAC is locked due to failed password attempts, the owner cannot use the card until they visit a RAPIDS facility. Finally, in order to authenticate for the first time, one must have access to the computer's parent active directory. A soldier in the field would not be able to gain access to a new computer not prepared with his/her CAC unless there were some means of direct access to the active directory.

Biometrics

Biometric methods for authentication have been introduced over the past few years and are starting to gain attention for their ability to use unique factors. Some of these methods include measuring hand-writing variables (pressures, writing speeds, etc.), analyzing typing patterns, scanning irises (which turn out to be incredibly unique and unlikely to return false positives), fingerprints, examining hand/palm geometry, vocal features, and facial features. Fingerprint verification is the most widely used biometric authentication system due to its simplicity and accuracy. Several of these methods are used as 1FA, but recently, mobile applications have started to require a pin number additionally for real two-factor authentication wherein the biometric is considered an inherence factor and the pin number is a knowledge factor.

Recently, startup companies have begun to use biometrics to make ensure security in their products. The Nymi Band, made by Bionym, is a heartbeat tracking bracelet that verifies identity by the characteristics of one's heartbeat. Myris, made by Eyecorp, scans the human iris to authenticate users. Fingerprint scanning hardware on recent smartphone models has made biometric identification possible for mobile applications such as Venmo and Discover.

Inherence factors inherently cannot be lost, stolen, hacked, duplicated, or shared. A user cannot "forget" an inherence factor, thus bypassing any potentially vulnerable password recovery procedure. On the other hand, biometric systems can never be 100% accurate. One must provide the device with a sample which may take a long time and require expensive equipment to analyze, and record inaccurate information depending on the device. Often, these devices are sophisticated, fragile, and expensive.

2.6 Related Work

There is not a large amount of extensive research on two-factor and strong authentication, and several cases have opposing results. Weir et al. (2009) explores the usability of several two-factor banking authentication token devices. They compare the use of push button and card-activated tokens and the chip/pin method. According to their findings, the push button token was the simplest to use while still maintaining security, but the card-activated token was also found to be usable and secure when in default mode. The PIN entry method was the least popular due to subjects failing to see the security payoff of the work required to receive the additional passcode. Users were motivated to use a particular method by usability and convenience rather than added

security, although a small population was willing to sacrifice usability for added security: nine people (18% of the study) chose the other methods as their preference (Weir et al., 2009).

Similarly, Cristofaro et al. (2014) present a study that surveyed 219 Mechanical Turks to analyze experiences with popular 2FA technologies such as OTP generating tokens, email and SMS PINs, and smartphone apps. They also measure how perceived usability impacts motivation. Their research concludes that user perception of 2FA usability is positive and dependent on personal background and not the specific the system. Furthermore, the study claims that perception of privacy is not negatively correlated with usability in contrast to expectations and previous research (Cristofaro et al., 2014).

Another study by Krol et al. (2015) investigates UK banks' use of 2FA. They conducted interviews, collected entries from study subject logs over 11 days, and analyzed the data both qualitatively and quantitatively. Their findings are in line with the research Weir et al. conducted: 2FA is not difficult to use in the short term, but user effort, more specifically the need to remember credentials or carry addition devices, presented issues. Their subjects found biometrics to be ideal, as they do not require memorization or possession of physical tokens (Krol et al., 2015).

Strouble et al. (2009) present a focused conclusion on impressions of the U.S. Military's Common Access Card (CAC). They produced an extensive survey throughout the U.S. Air Force and attempted to understand their experiences during the transition from SFA to the CAC system. Their analysis concludes that the change negatively affected users' productivity and the overall network usability. During the transition, 66% of the users lost their CAC cards, and the Air Force lost over 260 person-years of productivity as well as \$10.4 million (Strouble et al., 2009).

Clarke and Furnell emphasize problems with PIN-based authentication in their study (2005). They argue that the growth of cell phone functionality and accessible services demand stronger authentication. In their study, one third of their participants refused to use PIN authentication, and problems were reported for those that did. Subjects much preferred to use biometric authentication (Clarke et al., 2005).

2.7 Fido Alliance

The FIDO Alliance is an organization whose mission is to strengthen the current state of online authentication and assist in the adoption of strong authentication across services. Their goals thereby are to foster a decline in the reliance on simple password authentication and foment the creation of regulations to raise security standards. FIDO also aims to address the lack of interoperability in strong authentication devices. FIDO has published two proposed protocols: the UAF, which sets the standard for inherence factors that are used in replacement of passwords for an acceptable level of strong authentication, and U2F, which sets a standard for two factor methods by requiring authentication via a dongle/USB plugged into a computer in addition to a password (Fido Alliance, 2015).

The Universal Authentication Framework (UAF) protocol allows for FIDO's vision of a password-less experience in which a user must register his/her account to an online service through a local biometric authentication mechanism. UAF argues that a single inherence factor provides enough security to remove the need for a password altogether. FIDO's second protocol, Universal Two Factor (U2F), contains Fido's vision of an ideal dual factor authentication system through a readily accessible possession factor (Fido Alliance, 2015).

Both of FIDO's protocols require public key cryptography technology. Public and private key pairs are created upon registration to with an online service such that FIDO holds the private key and registers the public key with the account service. A client is only given access after authenticating locally, upon which FIDO's challenge is signed, verifying the customer's identity (Specifications Overview, n.d.).

FIDO strives toward three goals for their standards: ease of use, privacy, security. They hope that by standardizing protocol, clients will better be able to adopt strong authentication to the internet a safer place (Fido Alliance, 2015).

2.8 Dual Factor Authentication Failures

Though Dual Factor Authentication is generally more secure than Single Factor Authentication, it is still subject to attacks. One such attack is described in *When Organized Crime Applies Academic Results*, published by researchers at the École Normale Supérieure university (Greenberg, 2015). A widely used 2FA application is the credit card chip and pin combination. In this system, one inserts his/her credit card into a card reader. They enter their PIN number into the card reader's interface, and the reader queries the card to see if the PIN is correct. The card sends back the corresponding positive or negative response based on the inputted attempt (Ferrardi, 2015).

The system, however, is vulnerable to a "man in the middle attack": one can use a separate device or chip installed into the card to preempt the query response sent back to the card reader with a message sent from the hacking chip, which can force a "yes" message regardless of the PIN number queried to the card. All the chip needs to do is listen for messages sent to the card. Cambridge University Researchers detailed this vulnerability in 2010 and created a proof of concept example of this system using an FPGA. In 2011, a group of French citizens implemented this system and managed to steal and use about \$680,000. The criminals used stolen credit cards on which they installed chips with the desired functionality. Unfortunately, this method of spoofing is difficult to detect because a legitimate or fraudulent transaction will appear the same to the card reader at any teller, and the individual using the card does not identify him/herself. A notable point is that this attack overcomes only the knowledge factor. The thieves had to physically steal a credit card. Therefore, an attack may be nulled by an individual canceling his/her credit account after his/her card disappears. The card will be internally wiped, and card readers will not recognize it.

A potential fix for this attack is to have the card reader require signature verification to ensure the query response message is coming from the correct chip. Another solution proposed by many banks is to have the card reader send a preliminary query with a default response of "not accepted" immediately upon establishing a connection. The expected response is "not accepted" because the pin number would not have been sent yet. If "accepted" is the answer, the card must have been tampered with, and the reader may cancel the transaction. However, this implementation is still subject to further exploitation if the attacker is clever enough.

Another 2FA system known to have been successfully compromised by attackers is Mobile Transaction Authentication Number (mTAN) technology, a variation of TAN technology often used by banks. TAN technology is used when a bank allocates and distributes a specific number of single-use TANs to a user. The user then utilizes a TAN as an authentication factor for a bank transaction. mTAN technology is a more specific TAN method that distributes the TAN to a mobile device by means of an SMS message.

The vulnerabilities in this system are showcased mainly with online banking systems and have led to a series of frauds with several companies. An attack can be conducted by gaining account information through keyloggers or phishing software to impersonate a victim and obtaining a SIM card to their phone from a mobile network operator (Betrüger knacken Online-Konten, 2015). The SIM card is used to receive mTANs that the victim requests from that point onwards. The victim may recognize that they are not receiving an mTAN from their cellular provider and get the issue resolved, but until then, the attacker can use mTANs they received to make fraudulent transactions. One can prevent this from happening by using anti-spyware software, and cellular networks could avoid repercussions by implementing a more rigorous system for replacing SIM cards.

2.9 Statistical Tests Background Information

The analysis portion of this study uses three types of statistical tests: T-Tests, one-way ANOVA, and two-way ANOVA Tests.

The type of T-Test that the team used was a Two Sample T-Test assuming unequal variances between populations. Also known as an Aspin-Welch Test or the Satterthwaite method, this theorem works under the assumption that the distributions of the populations are normal and allows one to test the difference between sample means where the population variances are not known and may not be equal. As a result, there are fewer degrees of freedom in this test than in a test when one assumes the variances are equal. The team used these tests to check for significance with responses between 2 categories or treatments only when the responses were on a scale. The equation for this test is (Hintze, 2005):

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}}}$$

Where t is significant error ($\frac{t}{t_{crit}} = P$), n_i is the size of sample i , and S is the standard deviation. The equation for degrees of freedom is:

$$d.f. = \frac{\left(\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}\right)^2}{\frac{\left(\frac{s_1^2}{n_1}\right)^2}{n_1-1} + \frac{\left(\frac{s_2^2}{n_2}\right)^2}{n_2-1}}$$

A one-way analysis of variance (ANOVA) test, or factorial analysis, tests for significance between the means of independent groups. This is useful for data where the sample populations are divided and given two or more unrelated "treatments", or in other cases where a numerical mean cannot represent the average of qualitative ideas. The two-way ANOVA tests builds off of the one-way by adding another independent variable. It tests for significance between two factors and then interaction between the two factors, and is again useful for testing between treatments over survey number. Here is a summary of relevant formulae (Explorable.com, 2009):

$$FactorA : SS_a = \sum_i (\bar{x}_i - \bar{x})^2$$

$$FactorB : SS_b = \sum_j (\bar{x}_j - \bar{x})^2$$

$$Interaction : SS_{ab} = \sum_i \sum_j (\bar{x}_{ij} - \bar{x}_i - \bar{x}_j + \bar{x})^2$$

$$d.f._a = (rows - 1), d.f._b = (columns - 1), \text{ and } d.f._{ab} = (r - 1)(c - 1)$$

Finally,

$$MS_a = \frac{SS_a}{df_a}, MS_b = \frac{SS_b}{df_b}, \text{ and } MS_{ab} = \frac{SS_{ab}}{df_{ab}}$$

where SS_i is the sum of squares, a and b are the two factors, \bar{x}_i is the mean of sample i , and MS_i is a measure of significance that is compared to a critical value to calculate the P value of the test.

2.10 Authy

The mobile application Authy provides strong authentication through several methods. Authy consolidates the storage of authentication tokens for multiple services, and makes them available for a phone app, desktop app, or laptop. With the goal of making it easy for anyone to use two factor authentication, Authy's verification process conforms easily with everyday activities. Authy

is also capable of working across apps that function with Google Authenticator. Authy was an ideal 2FA system to use in this IQP's user study because of its straightforwardness and broad compatibility across services. The IQP team has even elected to personally use Authy, and they believe it provides adequate security without being much of a hassle.

2.10.1 Advantages and Disadvantages

Authy has many advantages such as: supporting 2FA compatible sites like Facebook, Google, Dropbox, etc., allowing the application on multiple devices such as PC, tablet, and smartphones. It may also help a user retrieve a lost account; Authy backs up every 2FA token ID in its cloud. Authy also has some disadvantages, including a complicated user interface compared to SFA methods, and user privacy concerns such as sharing users' private information under subpoena. However, most companies do this so it is not uncommon or a particularly large concern.

2.10.2 Capabilities

Authy offers several variations of its 2FA app: Authy Onetouch sends a push notification to one's cell phone/device upon request of login or transaction. The user then can simply approve it with their cell phone without the need to enter a code. Authy Softtoken uses a 20-second iterative one time password generated on the Authy app on a smartphone/device that one is required when requesting to login/transact with a website. Lastly, Authy Onecode sends a one-time password via SMS to one's cell phone/device that is required gain access to a sponsored site. Authy is currently supported by 19 large services, including Facebook, Google, Dropbox, Amazon, and Microsoft.

2.10.3 Important Services that Authy Provides

An important service that Authy brings to the user is inherited trust. Under this model an already "trusted" device can extend this "trust" to another device, meanin that a user can authorize any other device to access his accounts from an authorized device - the new device can also further extend trust to other devices. When a device is lost, one can simply use another device to access one's accounts. Furthermore, if one purchases a new device, he/she can simply use the old device to authorize the new one instantly.

2.10.4 Privacy

Authy prides itself on being a private service that records as little data as possible about the user. Authy uses a one-time passcode algorithm which can either be a Hash Based Message Authentication Code - One Time Pass Code (HOTP) or a Time Based One Time Pass Code (TOTP). Both algorithms are similar in that they both require a seed and a counter to create the next passcode. HOTP will increment a counter when the user uses a passcode or requests one, whereas TOTP will increment a counter regarding a time variable. When a user enters Authy and submits

a PIN to the server, the server will search for the user's seed and calculate the value based on the timestamp of the request and then generate a passcode. If the passcode entered on the user end matches the server's version, then access is granted. The algorithm is almost impossible to break because the seed data is unknown. However, if the server were breached, and a hacker gained entry into the database, they could gain access to previous PINs and generate the proper formula to gain entry into an account.

2.10.5 Security

In Authy, security is ensured through a two factor authentication process. In this process, one's username and password serve as the knowledge factor, and one's cell phone with the application serve as a possession factor. Authy generates a one time passcode, and the user is required to enter this passcode into the service to gain access. The user has thirty seconds to enter the token before a new OTP is generated.

This one time passcode is created by a seed that is generated on registration of the service onto Authy. This seed is based on unique aspects of one's individual device. Authy also has a database that stores this seed and generates the same token in time with the token generated on one's device. This process allows the app to be disconnected from any network, allowing for more secure authentication.

2.10.6 Usability

Authy not only provides powerful two factor authentication security, but it also supports users as much as possible. Authy supports most platforms from iPhone and Android to IOS and Windows. It is easy to migrate tokens from one device to another. Because Authy uses the cloud to store tokens, users need not panic if the authentication device is lost. Additionally, internet connection is not necessary; Authy generates its OTP's offline without a network connection.

METHODOLOGY

3.1 Overview

To address the goal of finding out what influences people's decisions to use strong authentication, the IQP team designed a study that collects data from users to determine how user behavior and impressions of two-factor authentication are affected by four criteria: usability, security, privacy, and prior informational exposure to strong authentication and its benefits of mitigating online threats.

To gather data discerning user perceptions for the criteria as mentioned earlier, the team distributed surveys to the subjects throughout the study, either by e-mail or during a physical meeting. To determine how prior exposure to two-factor authentication affects users' perceptions and behavior, the IQP team randomly assigned participants into two groups, both of which received a baseline informative briefing about the definition of two-factor authentication and several examples. One of these groups, however, was exposed to a higher level of information about cyber security threats and how strong authentication mitigates security-associated risks. The team's expectation was that participants' reactions to the different conditions between the two study groups would be reflected in the results of the surveys.

The study was designed around four phases: recruitment, introduction, bi-weekly usage tracking, and a final outgoing perception survey coupled with the monetary payment. All of the information gathered was used to give insight into participants' decision-making processes and motivations to use strong authentication.

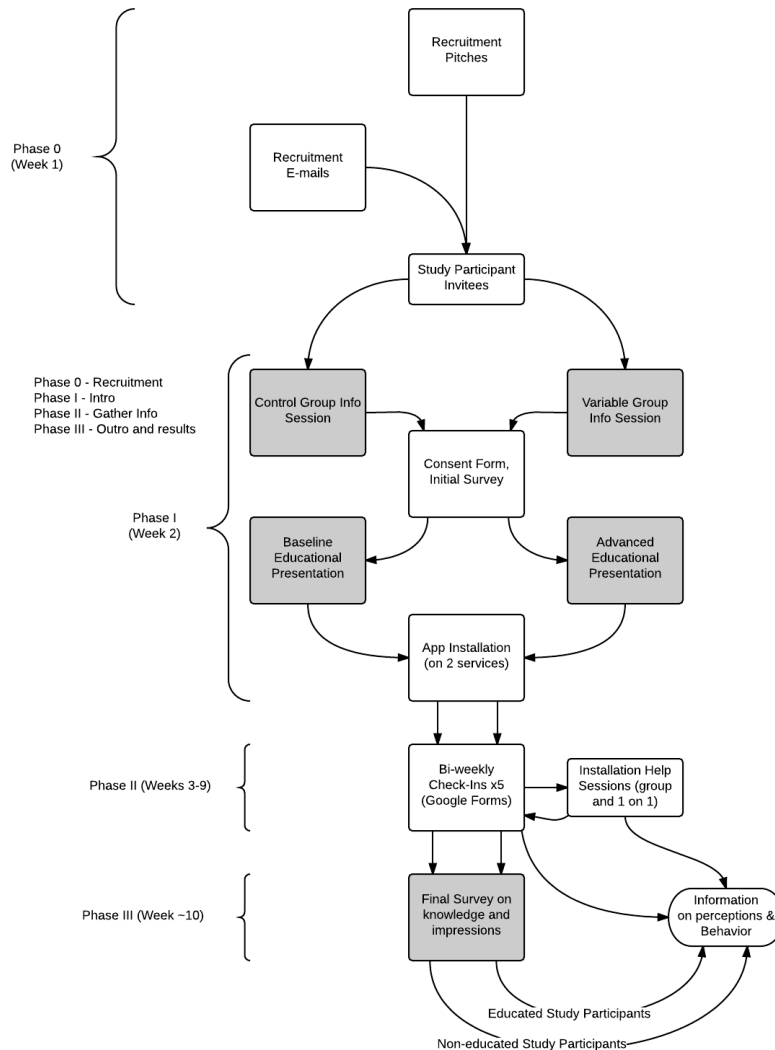


Figure 3.1: Diagram of Our Study

3.2 Phase 0: Recruiting

The first step within the user study was obtaining participants. This happened during the first two weeks of WPI's B-term. Subjects were incentivized with a cash payment of \$40 to be distributed at the end of the study. Advertisements for the study were networked through two channels, as modeled by Figure 3.1 and explained in depth below.

The study could have involved up to 3 audiences: WPI Students, WPI faculty, and students

enrolled in Worcester Consortium schools. The team decided that the most feasible of these was WPI Students. The scope of audiences was limited by ethical inspection procedures and the unfeasibility of consistent communication with people outside of the student body. Even though this was a thin slice of the general population, the team could still learn about the motivations of this generation and how to incentivize them to use stronger methods.

The first recruitment channel was two introductory economics classes. The IQP team presented a short pitch of the user study which consisted of a slide show (found in Appendix A) during the classes. The team advertised \$40 in cash and a better understanding of stronger security practices as the incentives for participation and explained the goals of the study to ensure that participation was understood to be a mutually beneficial exchange. The team briefly introduced the potential participants to Authy to give them a quick example of a secure authentication method and additionally preview the application used throughout the study. Students were told the requirements to receive compensation at the end of the study to give them a clear picture of what was expected from them. Lastly, the IQP team showed a timeline of the requirements to give a time-based reference regarding the duration of the project. A sign up sheet with fields for name and e-mail address was passed around the classes to gather contact information for interested students.

The second recruitment channel was a pre-planned chain of e-mail aliases chosen for their reach to a broad variety of the student population. A pitch similar to those given in the classes and an invitation coupled with the link to the sign up spreadsheet to the information sessions was included in an advertisement e-mail to the following on-campus group aliases:

- nsbenews@wpi.edu - National Society of Black Engineers
- news4shpe@wpi.edu - Society of Hispanic Professional Engineers
- hcsa@wpi.edu - Hispanic and Caribbean Student Association
- wpibsu@wpi.edu - Black Student Union
- brasa@wpi.edu - Brazilian Student Association
- sase@wpi.edu - Society of Asian Scientists and Engineers
- connectionsprogram@wpi.edu - Connections Program
- insight16@wpi.edu - New Student Orientation insight team
- riley1st@wpi.edu - Riley Hall First Floor Freshmen Residents

Study participation was granted by the IQP team on a first come-first serve basis to those who expressed interest and signed up to register for an info session. The team confirmed participation with a signed consent form that stated the participants' requirements to qualify for receipt of the monetary compensation.

3.3 Phase 1: Introduction

3.3.1 Participation Confirmation, Group Splitting, and Initial Survey

The potential participants who signed up for an info session were randomly assigned to either the “control” (baseline education) or the “treatment” (advanced education) group and invited to that group’s corresponding series of info sessions. To participate in the study, subjects had to choose among one of three dates that the team made available from 6:00 - 7:00 p.m. The IQP team conducted each group’s meetings simultaneously, but in different locations, on the three separate nights. The information sessions had three purposes: To confirm participation in the study using the aforementioned signed consent form, to conduct an initial survey to determine prior knowledge about authentication practices, and to subject each group to an educational presentation as described below. The IQP team referenced back to the initial information once the study was completed for comparisons before/after exposure to the educational material.

The initial survey (Found in Appendix D) contains questions with varying purpose: Questions 1-2 Ask for student demographic information to assess the correlation of other results with academic major and class year. Question 3 asks for an e-mail address for identification, and to which the bi-weekly surveys were sent. Questions 5-6 assess participant’s prior knowledge of both standard and strong authentication methods so as to create a reference point to compare with the final survey’s questions. Questions 7 and 9 assesses single factor authentication behavioral tendencies, while 8, 10, and 11 ask directly about single factor authentication impressions and the importance of security to the user. If a user expresses a high value for internet account security and does not think that a mere password is safe, then it would follow that they would favor the stronger authentication methods in their behavior, such as using application/account specific passwords. Questions 12 and 13 assess user’s values and tendencies towards internet privacy, the second criteria of determination in the study. Question 14, again, determines the users’ impression of the security of single factor authentication. The last question, 15, asks the user how much time they would be willing to spend on different types of accounts (banking vs. social media vs. email, etc.) to gain more reinforcement on the user’s overall value of security and privacy in online accounts.

3.3.2 Baseline Education

The baseline presentation (Found in Appendix B) exposed the control study group to some basic concepts about authentication and a description of the study. The IQP team first introduced the definition of authentication and the three factors to provide a basic educational understanding and went into further detail in explaining knowledge, ownership, and inherence factors and gave examples about each factor to reinforce the concepts as mentioned earlier (slides 1-3). The team then defined single factor authentication and provided the anecdote of computer passwords to allow for a practical connection to the theoretical definitions (slide 4).

Afterward, the team defined two-factor authentication, followed by more examples including Google Authenticator, and fingerprint scanning on iPhones (slides 5-6). The team then introduced Authy, explained how it works (inclusive of all 3 Authy applications), and listed the compatible internet account services to provide a basic understanding of the use (slides 7-8). The team further explained the goal of the user study so as to be transparent about our incentives, and then ended the informational session with a detailed description of the participants' requirements in the study so as to explain the qualifications for receipt of monetary compensation (slides 9-10).

3.3.3 Advanced Education

The variable group of participants received a more advanced educational briefing that contained not only the information presented in the baseline education presentations but also further information on the field of cyber security. They were briefed on the importance of increased internet security, exposed to several examples of security failures, and saw examples of how two-factor authentication is being used in larger organizations to mitigate security risks. Additionally, they saw Authy's privacy policy and the amount of data Authy collects through the application. The purpose of the advanced education was to provide a sophisticated understanding of the risks that two-factor authentication mitigates corresponding to the question "why use strong authentication?", and to provide a comparative perspective on users' perceptions when exposed to greater information than the control group.

The treatment group of participants received a more advanced educational briefing that contained not only the information presented in the baseline education presentations but also further information on the field of cyber security. They were briefed on the importance of increased internet security, exposed to several examples of security failures, and saw examples of how two-factor authentication is being used in larger organizations to mitigate security risks. Additionally, they saw Authy's privacy policy and the amount of data Authy collects through the application. The purpose of the advanced education was to provide a sophisticated understanding of the risks that two-factor authentication mitigates corresponding to the question "why use strong authentication?", and to provide a comparative perspective on users' perceptions when exposed to greater information than the control group.

In the advanced education presentation, the IQP team introduced the cyber-security field and some of the real world issues that pertain to it. We presented statistics about what most computer hacking victims have in common regarding authentication and showed how vulnerable information can be on the cloud. This allowed the participants to gain more of an understanding as to why strong authentication exists. The team then introduced the concept of authentication in software and the differences between single and dual factor authentication and proceeded to show real world examples of dual factor authentication. We mentioned some of the user bases and then we introduced the intent of the project. The team explained what Authy is, how it works, and the application's privacy policy for the test subjects. Finally, we explained to the subjects the

remaining tasks for the project.

The team started the presentation by showing the test subjects information about their likelihood to be targeted by cyber attacks and how even a small amount of effort can keep them safer, the purpose being to ensure the treatment group subjects were exposed to the current security risk of having simple account authentication and why companies such as Authy are taking measures for stronger authentication (slide 2). The team then introduced five real-world hacking incidents that happened between 2007 and 2015 to gain the concern of the treatment group subjects. Educational material was reiterated to portray that security is imperative for safety. The team educated the users on the definition and explanation of authentication (slide 4). The team realized that this is a simple concept, but it is something that the ordinary person does not usually think about, so the presentation showed the three factors and explained how most people merely use one factor. The statement that single factor authentication is no longer all that secure was said, reinforcing the educational message that strong authentication is more secure than single factor. The team introduced the concept of going further and using two factors for authentication (slide 5). The team used a diagram to present this and vocally explained how two same-factor prompts for information such as the combination of a password and a security question is not dual factor authentication because the factors must be unique. A medium for dual factor authentication was then shown (slide 6). The team presented the example of how government employees use the Common Access Card in conjunction with their usual password for authentication. This anecdote serves to expand the treatment group's practical understanding of the educational content. The team introduced the concept of biometric authentication techniques and provided the example of the iPhone 6's fingerprint reader (slide 7). Then the most familiar form of 2FA was introduced: the team explained how the ownership and knowledge factors associated with a hardware token qualify the method as dual factor. The team made it clear that the token has no internet connection to the actual authentication system (slide 8) (so that if someone were to hack a user using this, they would need to know the password and steal the actual physical token).

The IQP team showed participants two more common forms of two-factor authentication: email and SMS verification (slide 9). The team used the familiar example of a service that ensures your identity by requiring that you have access to an e-mail account or that you own your mobile phone. These examples served as further educational reinforcement tools to ensure understanding. Study members showed contemporary 2FA usage examples among universities, the government, and organizations in the private sector (slide 10). The purpose of these anecdotes was to give credibility to the claim that two-factor authentication works; if another school uses it, it has as much merit as that school has. Then exactly why the IQP team was conducting the study and our intent was explained. The team summarized what it was trying to learn and what the subjects will learn. This gives a positive feeling and further motivation for completion of the study and explains the IQP team's incentives. Then Authy was introduced Authy for the first

time: the team showed a picture of Authy, explained its limitations and how Authy is used, and showed how it is compatible with many common services and is easy to adopt into accounts (slide 12). This slide's purpose was to familiarize participants with the application they would be using for the next ten weeks. Author's privacy policy was explained, and the participants were told what they are potentially becoming involved (slide 13). The team explained how Authy follows the standard regulations and how, just like most companies, it cannot guarantee one's privacy for some situations. The purpose of this information was to provide an educational background on the study criterion of Privacy and how it relates to Authy. The team then described all the data that Authy collects and explains how Authy records browser information and cookies to help the company (slide 14). The idea was that the treatment group subjects would be aware and better informed on the study criterion of privacy. The team then listed exactly what Authy does with any data it collects (slide 15); the team explained to the subjects that if there is a subpoena to Authy, they will disclose any necessary information. This further reinforces the educational background of privacy given to the treatment group. The team went into further depth about the legal requirements and circumstances that would allow Authy to disclose information, once again furthering educational content about privacy (slide 16). Finally, the team ended the presentation by describing the overall plan for the test subjects. Everything participants must do to qualify for obtaining compensation was then clearly defined to participants. The team asked the subjects for questions and concluded the informational session.

3.4 Phase 2: Data Gathering and Behavior Tracking

3.4.1 Bi-Weekly Tracking

Once the two groups' education phases were completed, all participants were asked to install Authy for two services out of the services that Authy supports. Throughout the rest of B-term, winter break, and the first week of C-term (ending at Martin Luther King Jr. Day), all participants were required to complete a Google survey sent out by e-mail every other weekend. They had from Friday morning until Sunday evening to complete the questionnaire. If a participant failed to fill out the survey, the next step was to discontinue them from the study (at the IQP team's discretion). The surveys tracked user behavior in the realm of usage and problems as well as observations on privacy, security, and usability. The first two of these surveys emphasize proper installation on all of the services the IQP team asks participants to install Authy. The third and all following identical surveys focus on continued usage and observation.

The online surveys (Found in Appendix D) had several types of questions: some geared towards user behavior and others geared towards user observation; all of which were based on the study's criteria. For the Mid-Study Evaluation I, Question 1 identifies the user via participation number. Question 2 asks the participant which two services they installed Authy for to assess how the installations went to determine behavior tendencies, the idea being that if a participant

did not install Authy on two services as we asked, they must have either had problems or did not want to continue. Question 3 asks whether or not the installations ran smoothly and redirects to these two questions if not: 4 asks that services presented problems, and 5 asks for a description of the problem. This series of three questions assesses the usability of Authy using catching the people who had trouble installing it on their own. Question 6 is another behavior tracking question to determine relative levels of motivation towards Authy and installation success, which we assume correlates with the criteria of usability. Questions 7 - 9 directly ask the participant for any observations on their perceptions of security, usability, and privacy to directly assess those criteria. Question 10 is an open-ended paragraph where any user may ask any question or make the IQP team aware of any concern. The responses to the online surveys were linked to a Google spreadsheet for analysis.

The Mid-Study Evaluation 2 survey is similar to the first online questionnaire, with a few changes: It asks for current usage of Authy to determine user behavior later on in the study, it asks for relative usage of Authy within the services to possibly find correlations with the specific accounts for which Authy was installed, and it gives the same opportunities to report problems and observations that the first online survey included. The Mid-Study Evaluations III-V surveys change only the wording in several of the questions and no longer assesses current Authy account usage (However, they do still ask about usage frequency). The IQP team members made themselves accessible via e-mail for questions and any help with an installation that was needed. The number and names of people who failed to install Authy were also recorded for later analysis.

3.5 Phase 3: Study Completion

3.5.1 Information Recall

During the first week of C-term, all study participants reconvened in a classroom for a debriefing session with the IQP team. They were given the final survey and asked to complete it. The IQP team also asked for general impressions about the study itself, and how well it collected and tracked perceptions and behavior. Upon completion of this debriefing session, all participants were dismissed from the survey and immediately received their monetary compensation of \$40.

The Final Survey's questions (found in Appendix D) differ slightly from those of the initial survey, their purpose being to discover if the study groups answered perception and behavior questions differently. Question 1 is an identification question by participant number to track study groups and find correlations. Question 2 asks for the overall security of two-factor authentication about an internet password 1FA method. Question 3 assesses participant's perceptions of security as provided by Authy about a strong password to find correlations between the study's security criterion. Question 4 likewise evaluates usability, and 5 assesses confidence in privacy. Question 6 is an open-ended question to determine how knowledge of 2FA, particularly among the treatment

group, changes perceptions of authentication. Question 7 asks for users to explain if and why they stopped using Authy for any reason to potentially connect their lack of usage to one of the four study's criteria. Questions 8, 12, and 13 assess user behavior that is expected to occur when the user has positive impressions of two-factor authentication. Question 10 is a direct attempt to evaluate the user's most basic perceptions of 2FA, which could be a result of any combination of the four study criteria and their relative importance to the user. Questions 9 and 11 assess the final level of knowledge of strong authentication methods; 9 by a quiz-like question about how Authy protects users, and 11 by asking the user if they think they learned anything new.

4.1 Overview

In order to understand how people interact with Strong Authentication, the team analyzed the factors that affect these by conducting a 10 week long study, as described in detail by the Methodology. Subjects attended meetings where they completed the initial survey, took part in one of two prescribed educational sessions, and installed Authy. For the next 10 weeks, the subjects used the app in their daily lives and filled out 5 biweekly surveys sent by the team. Lastly, the remaining participants attended a final meeting, received the advertised compensation for their time, and completed the final survey.

This section presents the results of the study in the order that the data was received, and discusses its potential interpretations.

4.2 Basic Information

At the beginning of WPI's B-term, the IQP team held three info sessions: Wednesday, November 4th, 2015, Thursday, November 5th, 2015 and Monday, November 8th, 2015. The participants arrived in two separate classrooms and thus were split into a baseline and advanced education group. These groups were to complete the initial survey and receive education. After the three info sessions, sixty-one participants had joined the study; thirty-four in the advanced group and twenty-seven in the baseline group. Next, the team sent out the mid-study surveys every other week. The dates for these are as follows: Mid-Study Evaluation 1 was due on Sunday, November 22, 2015, Mid-Study Evaluation 2 on Sunday, December 6, Mid Study Evaluation 3 on Sunday, December 20, Mid-Study Evaluation 4 on Sunday, January 3, 2016, and Mid-Study Evaluation 5 on January 17. In the first week of WPI's C-term, the team held 2 closing sessions, held on

Tuesday, January 19, 2016 and Wednesday, January 20. At the time of the final survey, forty-one participants had completed all of the surveys; twenty-three were from the advanced group, and eighteen were from the baseline group.

4.3 Statistical Tests

The following analysis uses three types of statistical tests: T-Tests, single factor ANOVA, and two factor ANOVA Tests. These tests corresponded to three types of data: data on a scale with two samples/sample groups, data with responses that are not on a scale in two sample groups, and data with responses not on a scale and in three categories. The term “on a scale” refers to data categorized on a scale where the number rank is a direct representation of a subject’s opinion, or data that has only two possible values (e.g. 1 vs. 0, or perhaps “Subject favors usability” vs. “Subject does not favor usability). The team routinely numerically categorized responses for analysis, after testing the accuracy of each team-mates’ quantification on a small sample.

The team used a two-sample T-Test assuming unequal variance (using the two-tailed P value) to test for significance within responses between two categories or treatments only when the responses were on a scale. When responses are not on a scale and average, the comparison of the averages is irrelevant. For these situations and comparing two factors, the team used a single factor ANOVA test, also known as a factorial analysis test. When comparing three factors (for example Time, Education level, and Perception of Security), the team used a two factor ANOVA test (assuming overlap between samples) to determine statistical significance.

4.4 Initial Survey

4.4.1 Class Distribution

In the Initial Survey, subjects answered questions designed to identify participants and gather demographic and study-related information. The first relevant question asked the students to identify their academic major, for the purpose of demographic information. Similarly, students were asked for their class year. Figure 4.1 is a graph presenting class year information of the participant pool. Figure 4.1 shows that the majority of the participants are sophomores and juniors. There are a fair amount of seniors and a small amount of freshmen.

4.4.2 Prior Knowledge of Authentication

In order to gauge subjects’ initial knowledge of authentication for comparison to later results, the initial survey asked them to define computer account information in their own words.

The team quantitatively classified the data into three categories depending on the accuracy of the response. A majority of the participants already had an understanding of authentication. Some of the participants understood something about the concept but failed to adequately explain

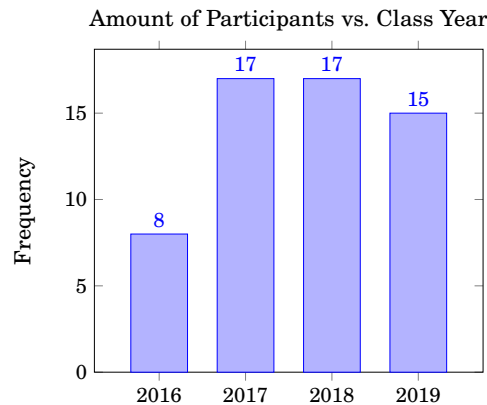


Figure 4.1: Results to the first question in the initial survey: "In which class are you?".

it. Finally, a handful had absolutely no idea what authentication was. The overall result had a higher proportion of prior knowledge than expected, likely because the participants are generally well educated and technically inclined as students of an engineering university.

The team assessed each subjects' prior experience or knowledge with multi-factor authentication under the hypothesis that if one knows about strong authentication, one may be more likely to be stronger in other behavioral factors.

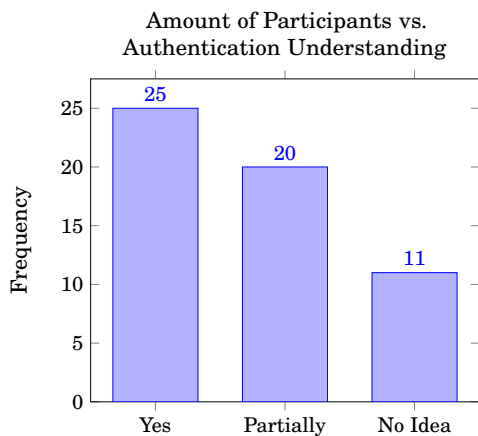


Figure 4.2: Responses to "Define computer authentication in your own words?" which was given in the initial survey.

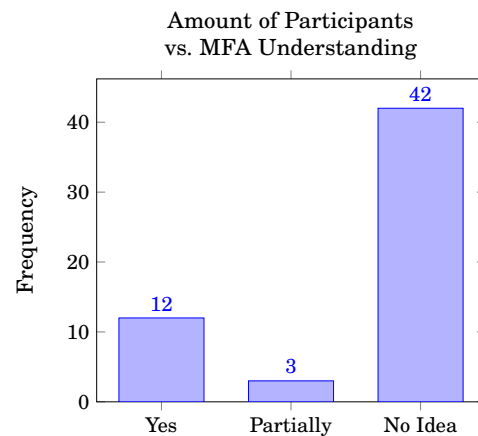


Figure 4.3: Results to "Do you know what Multi-Factor Authentication is?" which was asked in the initial survey.

In figure 4.3, one can see that the majority of participants had no knowledge about multi-factor authentication. Individuals without this knowledge come into the study knowing little about the field of authentication and resultingly may have radically different perceptions of how it should work, the different factors, and topics in the field.

4.4.3 Acquaintance with Someone Hacked

An individual having an encounter with a security attack could greatly impact their security practices. If hacked, a user could strengthen the security of the different services that they have. This experience with hacking can cause a person to be aware of the important information that they might have stored in some service. This occurrence makes it worthwhile to ask if an individual has or knows someone close to them who has experienced a computer account being hacked or compromised.

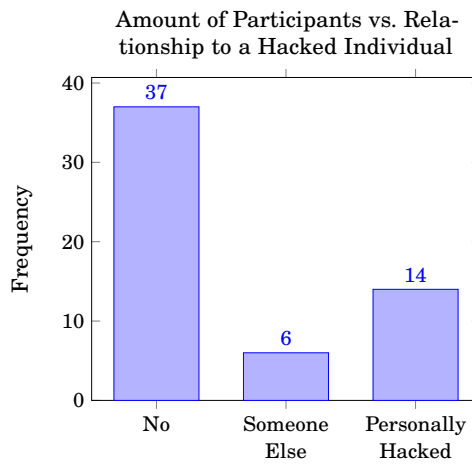


Figure 4.4: Results to "Have you or has a family member of yours ever experienced a computer account being hacked or compromised?" given in the initial survey.

Figure 4.4 shows the number of participants with negative hacking experience by category. The team hypothesized that this experience, more than most other factors, may positively influence perception and behaviors on different security and authentication topics. Those who have been involved or have knowledge of others who have been involved in security attacks may also more than others may have researched stronger forms of authentication in order to become more secure online.

4.4.4 Traditional Passwords

Another hypothesized indicator of a person's view of security is the number of passwords they use.. According to Ofcom the UK communication watchdog, 55% of individuals use the same password for most if not all websites despite that being a weak security practice. The initial survey asked participants how many passwords they use as a gauge of their tendencies of online security.

Figure 4.5 shows that the majority of participants claimed to use one or two unique passwords for each of their accounts. This shows how insecure most individual's accounts are. Using only

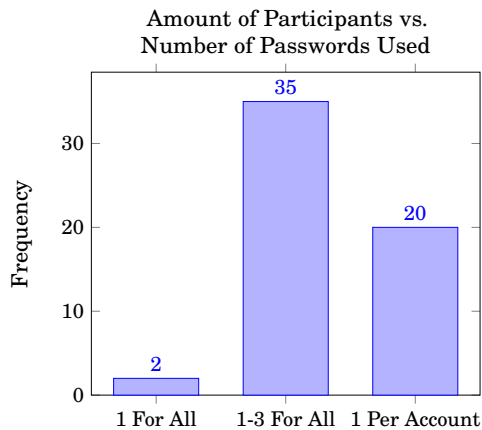


Figure 4.5: Results to "How many passwords do you use?" given in the initial survey.

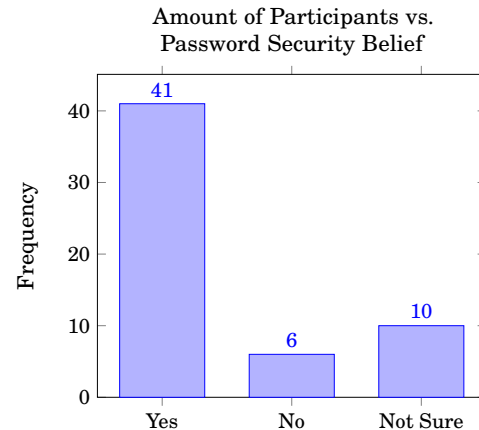


Figure 4.6: Results to "Do you think your passwords are secure?" given in the initial survey.

one or two passwords for one's accounts is extremely dangerous because as soon as an attacker knows one password they have access to an individual's entire online identity.

The following graph shows the number of individuals who believe their passwords are secure. Though these individuals may believe their passwords are secure, they very well may not be. This data can only be reflective of confidence in security and single factor authentication.

The results in figure 4.6 were surprising, and suggest general overconfidence in password protection. Only six participants out of fifty-one believed their passwords to be insecure. The team hypothesized that these beliefs may change with Education later in the study.

The frequency at which one resets their password may be a symptom of education in stronger authentication practices; one who understands the threats of single factor authentication may tend towards stronger security. The question below gauges how often participants changed their passwords:

As one can see, subjects' habits are less than stellar. Almost all of the participants hardly change their password, increasing the likelihood of a security breach. The team hypothesized that this may have to do with usability; more specifically that users are not willing to put in extra time for authentication.

4.4.5 Value of Security

The team hypothesized (and truly hopes) that belief in strong security translates to action involving stronger security practices, such as frequency of password resetting. Subjects rated their value of internet safety.

Figure 4.8 shows that the majority of the participants at least view security to be somewhat significant. This result is interesting in that that the other responses, such as those in figure 4.7,

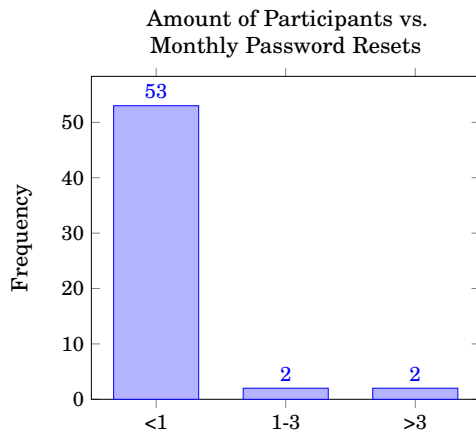


Figure 4.7: Results to "How often do you reset a password for an online account?" asked in the initial survey.

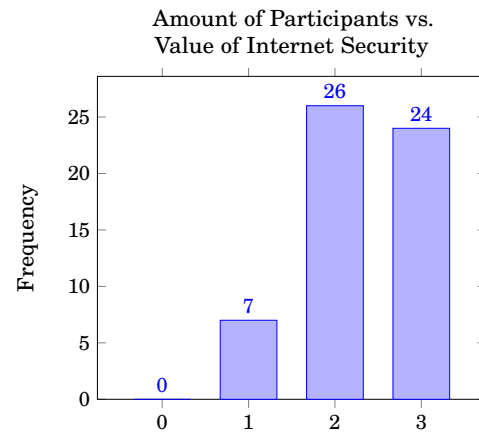


Figure 4.8: Results to "How much do you value internet account security?" asked in the initial survey.

seem to contradict this. Participants claimed to value internet security, yet did not have great security practices and knowledge.

One of the objectives of the study is to better define the discrepancy between people saying they value account security and actually acting on their value accordingly. The team addressed this by looking for significant positive correlations between subjects' reported value of internet security and other factors, such as prior knowledge of 2FA, the belief that one's passwords are not secure, and first-hand experience with hacking. The following graph shows these comparisons:

Figure 4.9¹ examines the data from figure 4.8 with several other sets of data. The team found that acquaintance with someone who was hacked had no significant effect on perception of security (T-Test, $P = 0.977$). The team also found that belief in the sufficiency or insufficiency of a password had no significant correlation with value of security (T-Test, $P = 0.869$), and that prior knowledge of MFA almost had a statistically significant effect on reported value of security (T-Test, $P = 0.164$).

4.4.6 Private Information

Many individuals have critical banking and social security information online that could cause significant harm if stolen. Having vital information online may impact one's value of security, so as to keep information safe. Figure 4.10 shows what participants reported regarding privacy.

Figure 4.10 shows that majority of participants have private information online. The team hypothesized that the participants who have private information online to should be more cautious and value security more.

¹Figure 4.9 Note that the graphs showing background information are highly broken down and may contain small groups of participants.

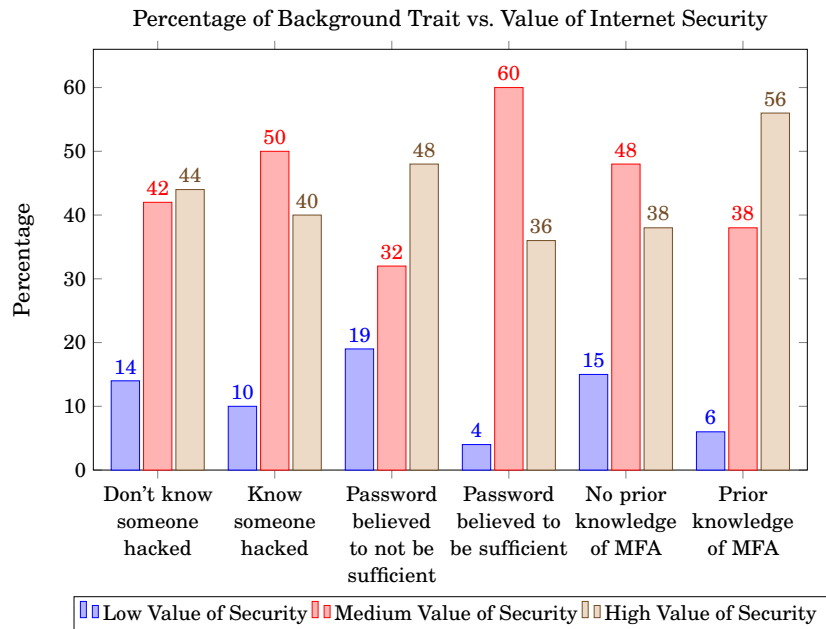


Figure 4.9: Responses in figure 4.8 but in respect to initial survey responses.

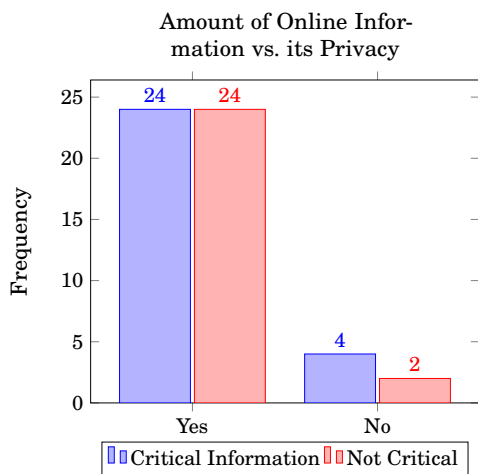


Figure 4.10: Results to "Do you have information online that you would prefer to be kept private?" asked in the initial survey.

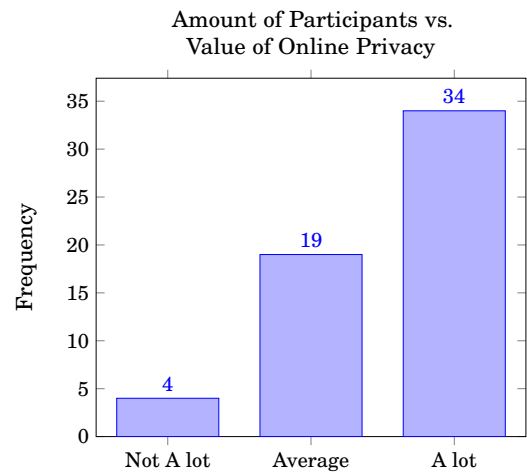


Figure 4.11: Results to "How much do you value the privacy of your online information?" asked in the initial survey.

4.4.7 Value of Privacy

Often-times, corporations may share or sell information that users provide for advertising. Such practices may violate one’s online privacy and can result in unwanted outcomes. The team expects that those who value the privacy of their online information would also value internet account security. The figure below shows participants’ reported value of their online privacy.

Figure 4.11 shows how the participants valued online privacy before they entered the study. The majority of the participants reported that they valued it a lot, and the team believes that participants who value it the most will also be the ones who value internet account security. This comparison illustrates this. Even though the team earlier discovered that there is no correlation between reported value of security, these factors may say more about value of security than what subjects reported.

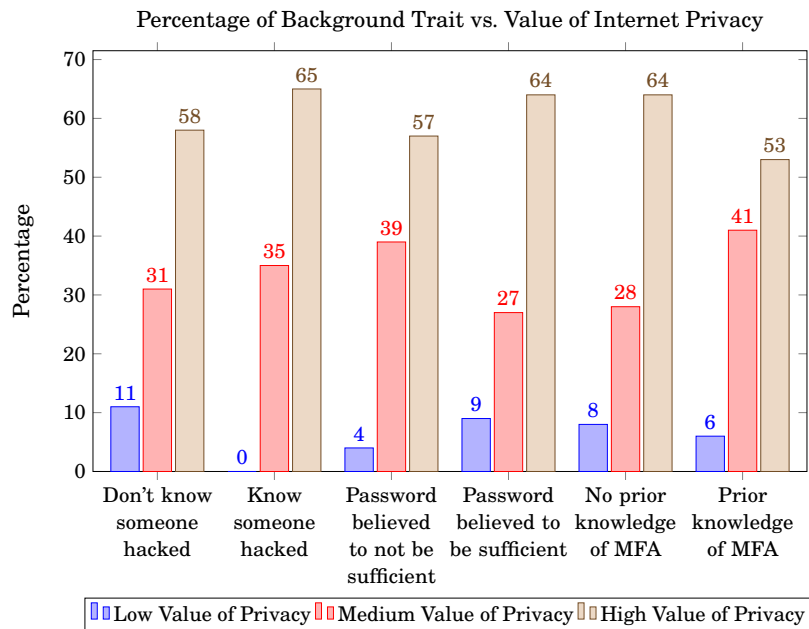


Figure 4.12: Responses as seen in figure 4.11 but in respect to background question responses as seen in the graph.

The results in the above graph show that most individuals (around 60%) from each subset stated that they highly value the privacy of their online information. Most others stated that the value they put on privacy is moderate. Despite varying differences of up to 9% of the sample size, the team found that acquaintance with someone who had been hacked (T-Test, $P = 0.270$), belief that a password is/is not enough (T-Test, $P = 0.889$), and prior knowledge of MFA (T-Test, $P = 0.613$) had no significant correlation with value of privacy. This means that there is not a significant difference in the subsets in the positive versus negative responses, suggesting that a high value of privacy is not correlated with any of the three subset factors.

4.4.8 Sufficiency of Single Factor Authentication

Ever since the online revolution started, service providers have used usernames and passwords as authentication for online accounts. The security issues with these accounts have increased in more recent years. The team gauged subjects' perception of the security of single factor authentication with the the following question under the hypothesis that education into the dangers may play a positive role in this belief. Students were allowed to explain whether they knew of any issues or problems that can come with these accounts.

Figure 4.13 shows that the majority of participants believed that a username and password are not sufficient for online information. The team acknowledges that this question may have encouraged participants to choose no simply due to the nature of the study. An interesting finding is that of the eleven people who believed an account username and password is enough to protect one's online account, nine of them did not have any acquaintance with a person whose account was hacked or compromised. Their responses may be a product of this lack of experience with the truth of SFA security.

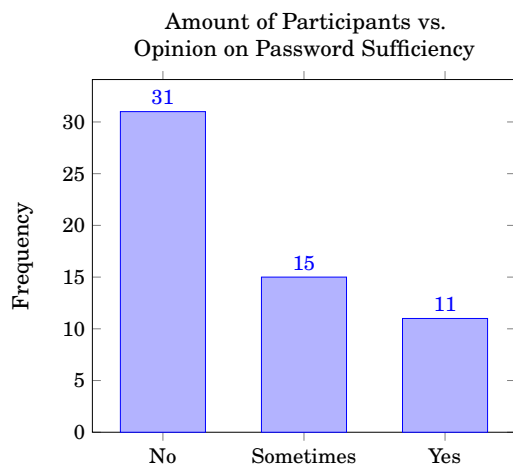


Figure 4.13: Results to "Is an account username and password enough to protect your online accounts?" asked in the initial survey.

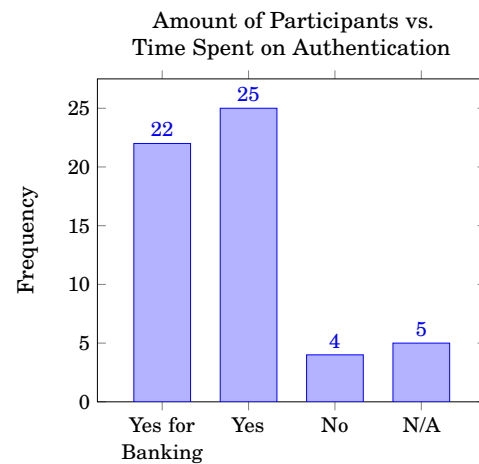


Figure 4.14: Results to "How much extra time would you spend authenticating yourself for online accounts?" asked in the initial survey.

4.4.9 Willingness to Spend Additional Time Authenticating

There are multiple ways to improve account security for common services. However, these methods have a cost. For example, they may increase the time of authentication. This extra time may be acceptable in circumstances where stronger authentication is necessary, such as banking applications, but less so in others. The following chart assesses participants' willingness to spend more time authenticating.

Figure 4.14 shows that many subjects were willing to claim that they would spend more time on authentication. This again may not be a significant result; subjects may by default say they are willing to spend more time. Additionally, the amounts of time subjects reported they would be willing to spend (in some cases upwards of ten minutes) were unrealistic and suggest that the subject did not understand the question.

4.4.10 Retention Rate of the Study

The education treatments occurred prior to the mid study evaluations. Roughly fifteen people dropped the study after this point and never made it through the first mid-study evaluations. The team hypothesized that education level may be a factor in retention rate. The following graphs show the distribution of dropouts by education level and several other factors:

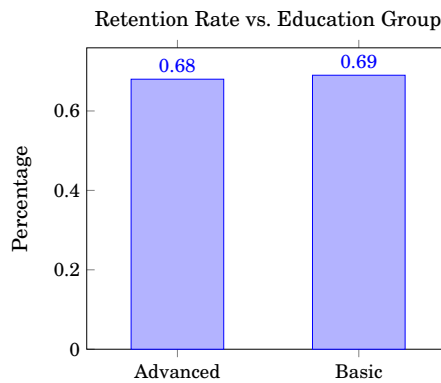


Figure 4.15: Results of the participants who dropped vs their education treatment.

Figure 4.15 shows that the distribution of dropouts was nearly identical between the advanced and baseline group. It is safe to assume that education was not a significant factor to the dropout rate.

Figure 4.16 shows that individuals who knew someone that has been hacked or have been hacked themselves stayed in the survey much more than those who did not know anyone who has been hacked so much so that the team found a strong positive statistical correlation (T-Test, $P = 0.0374$). The most logical incentive for individuals with acquaintance with someone who was hacked to stay in the study is an increased motivation to use and learn about strong authentication.

There was not much a difference between those who believed single passwords are sufficient and those who believe passwords are insufficient. The team found that belief that a password is sufficient/insufficient had no significant correlation with retention rate (T-Test, $P = 0.852$). The team also found that prior knowledge of MFA had no significant effect on retention rate (T-Test, $P = 0.604$).

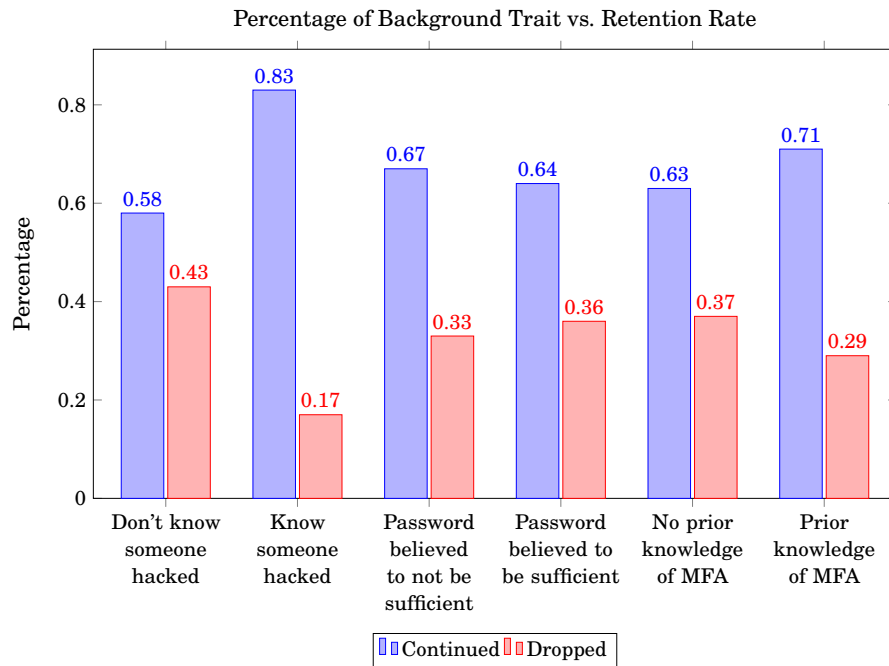


Figure 4.16: Results from figure 4.15 in respect to background traits as seen in the graph.

4.4.11 Summary of Initial Survey

The initial survey shows that a majority of individuals lack a knowledge of strong authentication. Individuals perceive themselves to value security and privacy, but seem unaware and do not practice basic security measures such as frequently resetting passwords or using application-specific passwords. Many of them believe they are already secure.

4.5 Mid Study Evaluations

4.5.1 Installation Success

People use many services throughout the course of their day. Participants were asked to secure at least two of their accounts with Authy. The team hypothesized that the initial impression of Authy may affect perception of usability later on in the study, and that educational level may indirectly affect the success of installations, and so the mid-study evaluations asked participants to report how the installation went.

As illustrated in the graph above, there is a discrepancy between the responses of the advanced and baseline groups. The team found that education level almost had a positive statistically significant effect on the success of installation (T-Test, $P = 0.163$). While not assuming that a correlation is definite, a possible explanation of this is that upon hearing more motivational material for MFA, the advanced group put more time and effort into their installations and

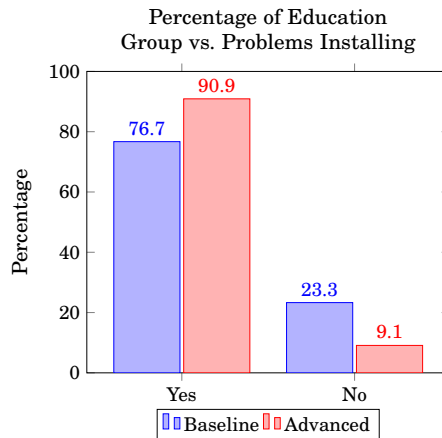


Figure 4.17: Results of “Did your installation run smoothly?” in respect to education treatment, asked in the first mid-study survey.

therefore encountered fewer problems.

4.5.2 Frequency of Authentication

Authy requires one to authenticate oneself using a software token given by the Authy application on one’s phone or other device. The team hypothesized that the frequency of use may affect perception of security or usability. Following is a graph detailing how participants reported frequency of authentication over throughout the study.

The results above may be skewed by participants failing to correctly estimate their usage of Authy, but there are several noticeable trends. The percentage of participants who reported fewer than five uses of Authy starts off high but decreasing, comes around and increases, and falls off in the last survey. This may be explained by subjects using more services in weeks two and three than earlier, then authenticating less because of Authy’s feature that remembers devices. But perhaps the most reliable set is the percentage of subjects who did not use Authy in the previous two weeks; it is easier to remember not using something than remembering an exact count. This percentage can be explained the same way as earlier. One interesting occurrence is the drop in individuals authenticating and more individuals authenticating in the 1 - 4 range during week four. This may have been due to the winter break and some individuals not having access to the various services they use regularly due to being off of the WPI campus.

4.5.3 Perceptions of Usability

Under the hypothesis that usability may be related to education, background, and value of privacy and security, the team categorized participant’s observations of usability. The following graph depicts these responses.

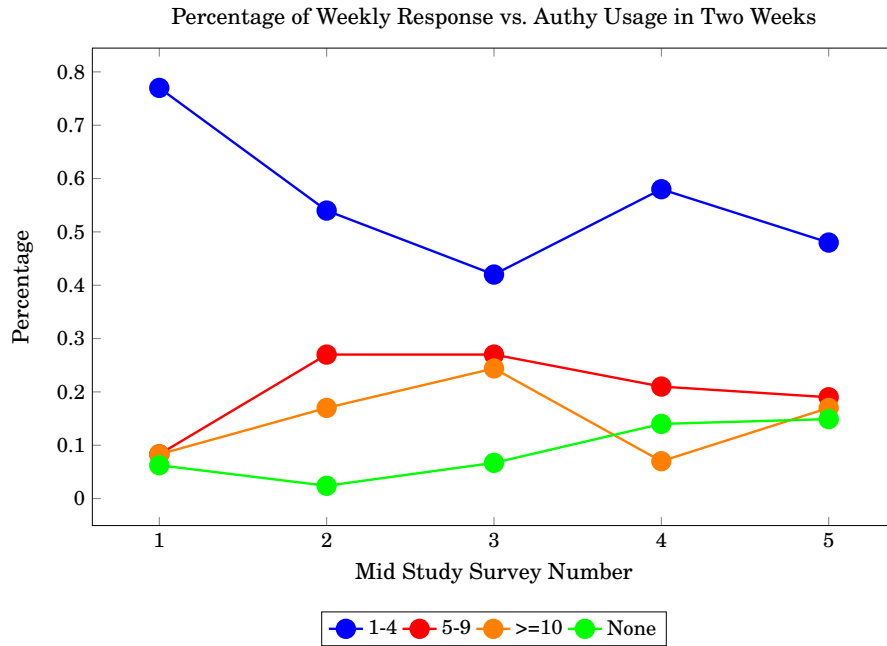


Figure 4.18: Results of "How often did you use Authy to authenticate yourself in the last two weeks?", asked in the mid-study surveys.

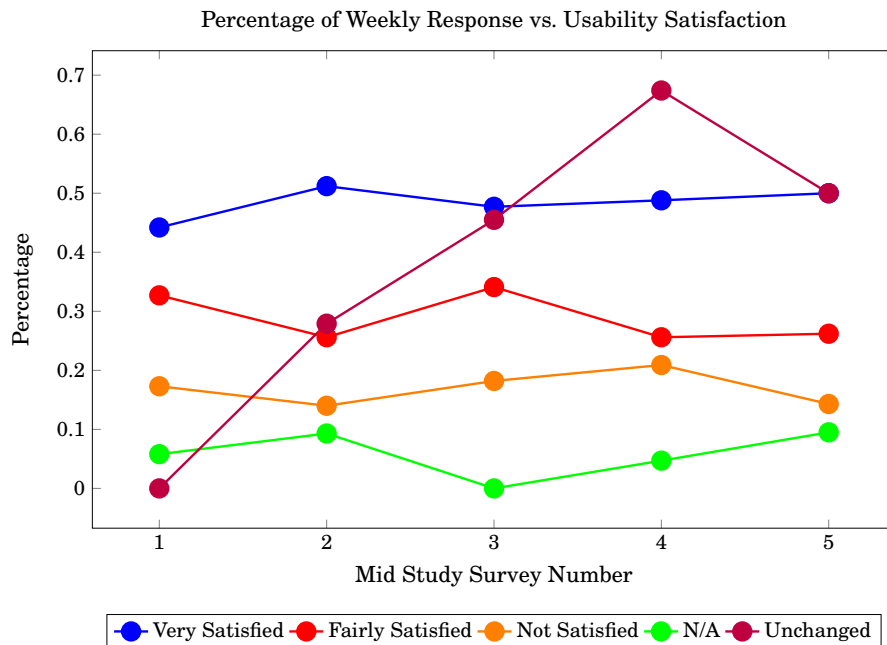


Figure 4.19: Overview of responses to "What are your observations on the usability of the application?" through out the mid study responses.

The figure above shows the change in general perception of usability throughout the study. These levels stay relatively constant. Although there is no obvious trend, there may be key issues with the usability of Authy as one participant stated that they had a problem when their phone died, leaving them unable to access their Google Drive account. Another user stated that since they had an older version of iOS software they were unable to install Authy on their phone.

Following is more in depth analysis of the perceptions of Authy’s usability. Since there is no obvious trend to this data, the team graphed relative responses of other questions and compared it to perception of usability to see if this would yield significant results.

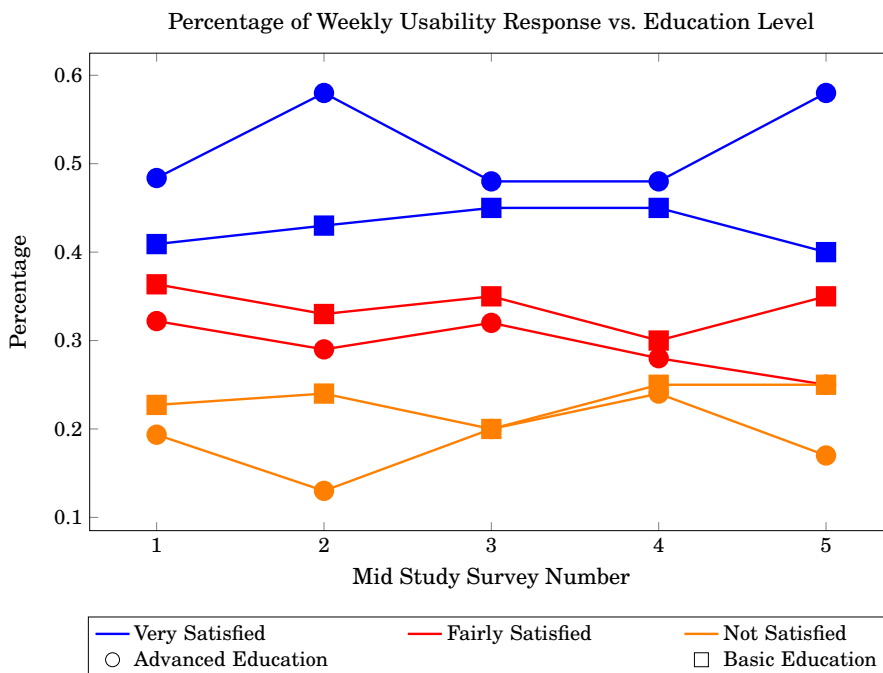


Figure 4.20: Results in figure 4.19 in respect to education treatment.

Testing statistical significance between survey number and education level, the IQP team found that there was no significant effect of survey number on perception of usability (ANOVA, $P = 0.981$), and not quite enough evidence to support a claim of significant difference within the education study groups (ANOVA, $P = 0.207$). Upon even further exploration, the team still found no significant difference between the study groups upon direct comparison between the first and last surveys (T-Test, $P = 0.647$). Therefore, perception of usability was generally not related to level of prescribed education.

The IQP team found that there was a nearly statistically significant relationship between perception of usability and prior knowledge of Multi-Factor Authentication (ANOVA, $P = 0.160$), and no significant relationship between survey number and perception of usability (ANOVA, $P = 0.963$). Therefore, there may be enough evidence to support the claim that prior knowledge of MFA affects perception of usability. A possible explanation for this is that those with prior

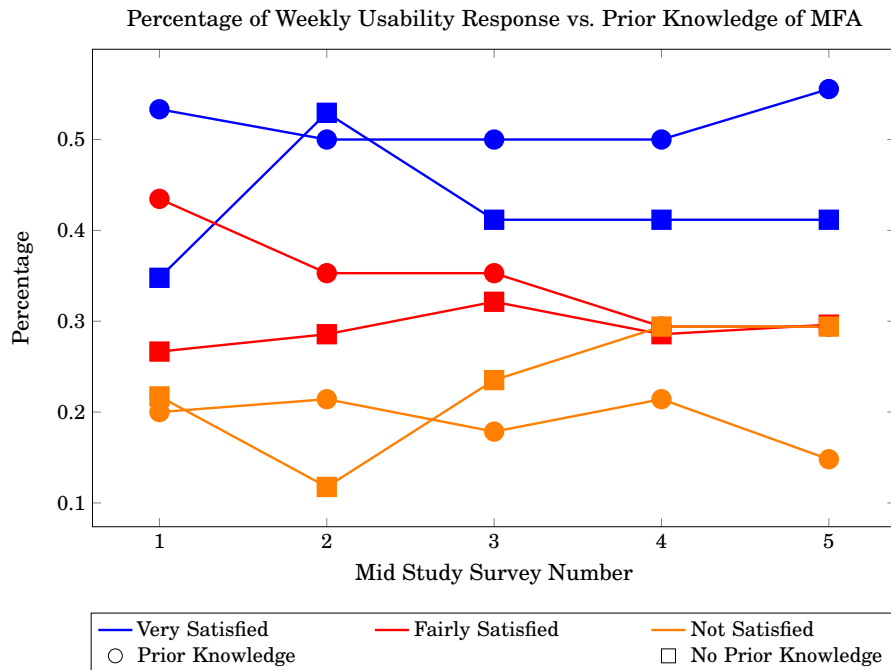


Figure 4.21: Results in figure 4.19 in respect to prior knowledge of Multi-Factor Authentication. (figure 4.3)

knowledge of MFA already knew how the 2FA Authy System worked and what to expect, and thus reported better usability.

Using a similar analysis, the team found that there was no significant correlation between acquaintance with someone who was hacked, and usability. However, the result was, again, close to being statistically significant (ANOVA, $P = 0.139$). Therefore, acquaintance with somebody who was hacked may have an impact on perception of usability. A possible explanation of this may be that those who were acquainted with someone previously hacked had more motivation to find Authy easy to use, and therefore reported better usability.

The team found that there was not a statistically significant difference in the data to support the claim that perception of usability is correlated with either initial view on the adequacy of a password (ANOVA, $P = 0.823$) or survey number (ANOVA, $P = 0.956$).

4.5.4 Perceptions of Security

A service that promises to provide certain functionality must properly execute on that initiative if it is to be successful. Authy promises to secure online accounts for participants. The following graphs show the observations on the security of Authy compared to survey number and several background factors.

This graph shows that the overall trend of perception of security slightly increases over time. This may have been caused by increased familiarity as time progressed. The following analysis

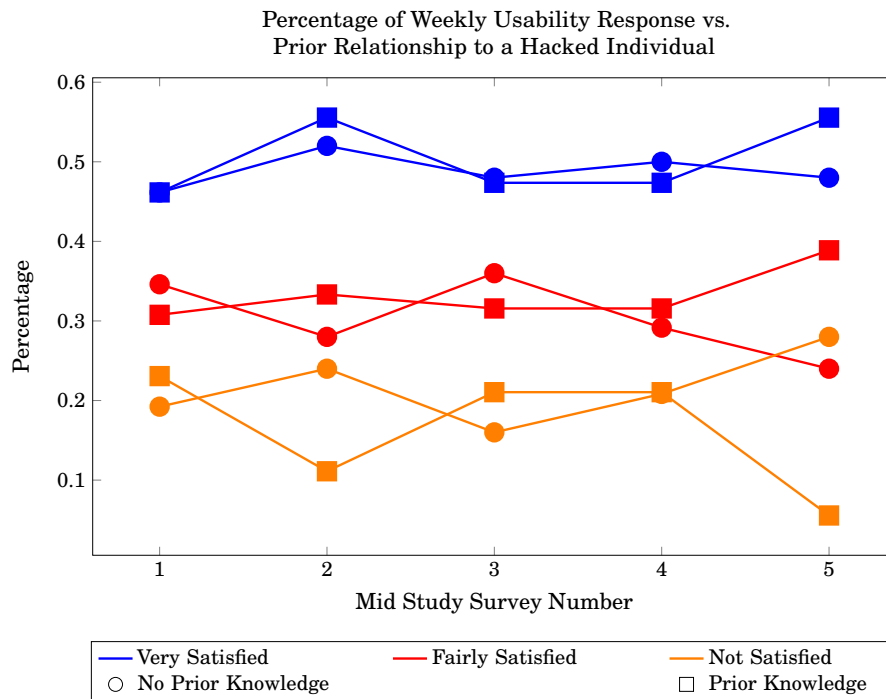


Figure 4.22: Results in figure 4.19 in respect to knowledge of someone hacked. (figure 4.4)

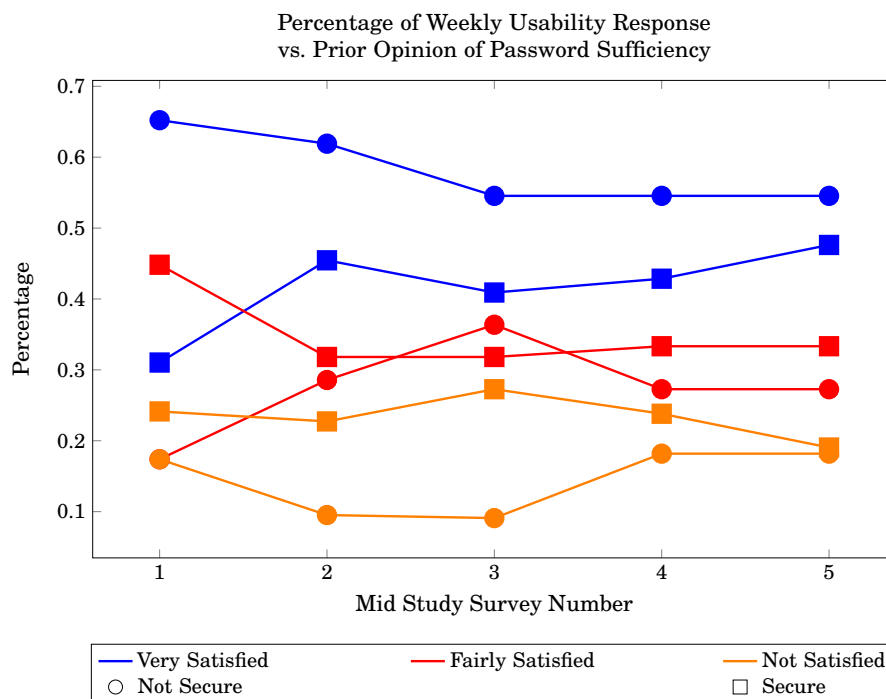


Figure 4.23: Results in figure 4.19 in respect to prior opinion of password sufficiency. (figure 4.6)

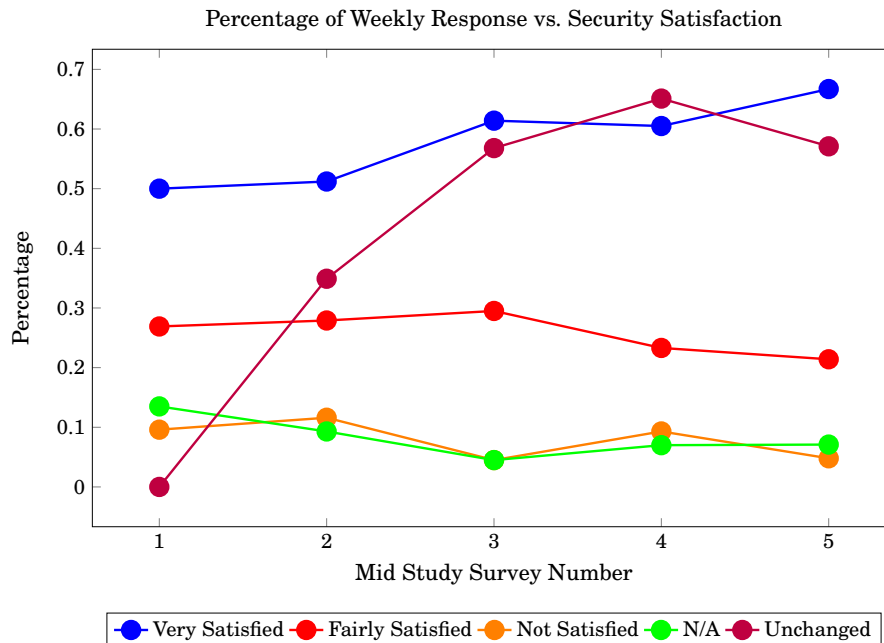


Figure 4.24: Overview of responses to "What are your observations on the security Authy provides?" through out the mid study responses.

test this observation and several others relative to the study criteria.

The IQP team analyzed the significance of the difference in study group percentage and percentage over survey number, and determined that there is not sufficient evidence to claim that difference in study group (ANOVA, $P = 0.592$) has a correlation to security observation. It was noted that between the first and last week there is an increase in favored security, but there is still not quite enough statistical evidence (T-Test, $P = 0.199$) to support a claim that survey number is a significant enough factor to explain the difference. Therefore, neither survey number nor education level have a significant correlation to perception of security.

Upon statistical analysis, there are no statistically significant correlations between prior knowledge and perception of security (ANOVA, $P = 0.166$) or survey number and perception of security (ANOVA, $P = 0.987$). It should be noted that prior knowledge of MFA is close to being statistically significant, and therefore may have an effect on perception of security. An explanation for this is that subjects with first or second hand experience with being hacked may directly see the threat of weak authentication and therefore report higher security with a strong authentication outlet.

The team found no statistically significant correlation between either survey number and perception of security (ANOVA, $P = 0.991$), or acquaintance with somebody hacked and perception of security (ANOVA, $P = 0.480$). Acquaintance to somebody hacked and survey number are not significant factors in predicting perception of security.

The team found that there was not a statistically significant difference to support the claim

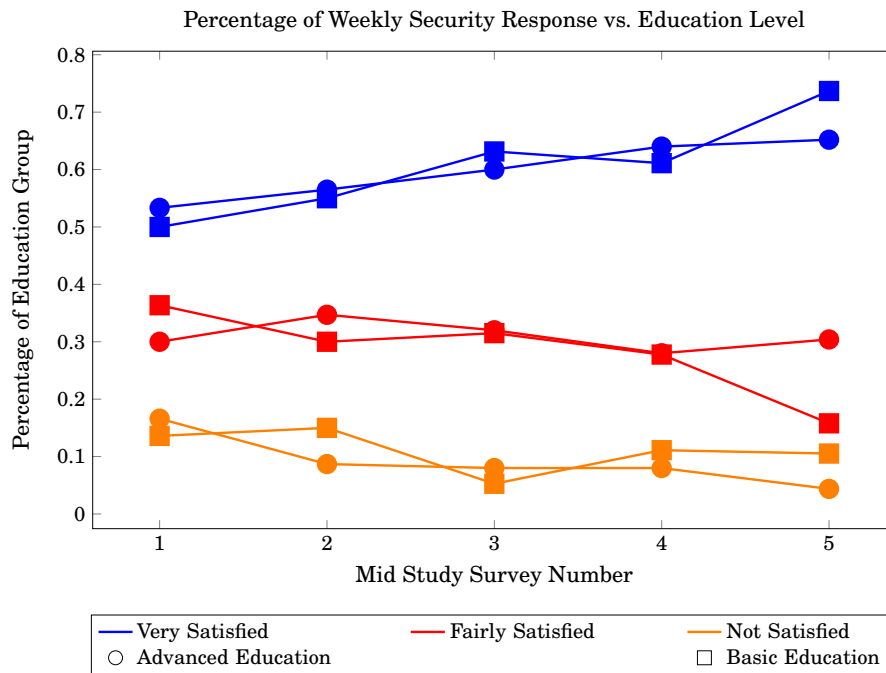


Figure 4.25: Results in figure 4.24 in respect to education treatment.

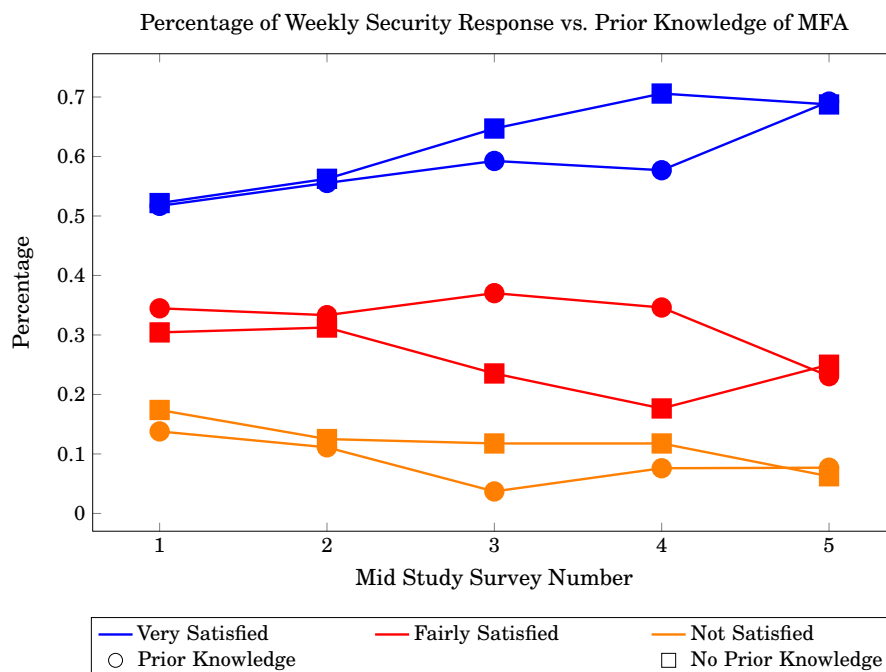


Figure 4.26: Results in figure 4.24 in respect to prior knowledge of Multi-Factor Authentication. (figure 4.3)

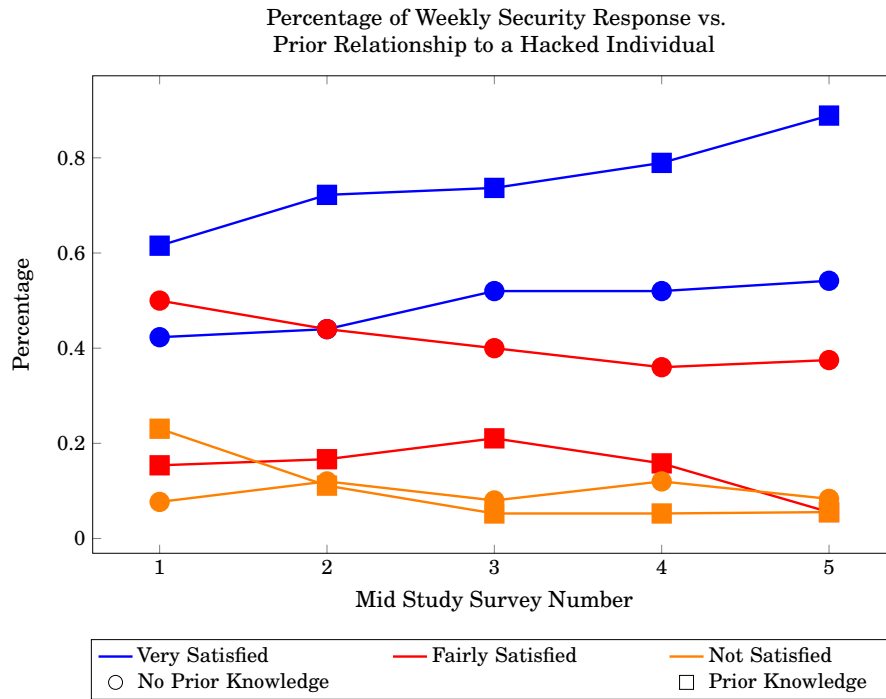


Figure 4.27: Results in figure 4.24 in respect to knowledge of someone hacked. (figure 4.4)

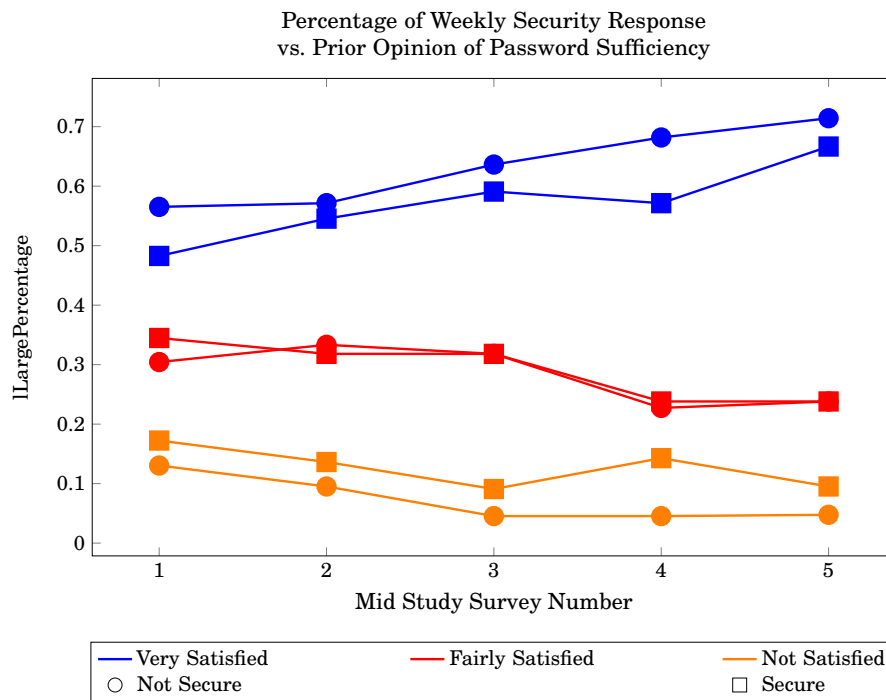


Figure 4.28: Results in figure 4.24 in respect to prior opinion of password sufficiency. (figure 4.6)

that perception of security is impacted by either initial view on the adequacy of a password (ANOVA, $P = 0.874$) or survey number (ANOVA, $P = 0.984$).

4.5.5 Perceptions of Privacy

An application that desires to be trustworthy and maintain a good relationship with their users will not share private data. Following are the observations that participants reported about privacy compared with survey number and several background factors.

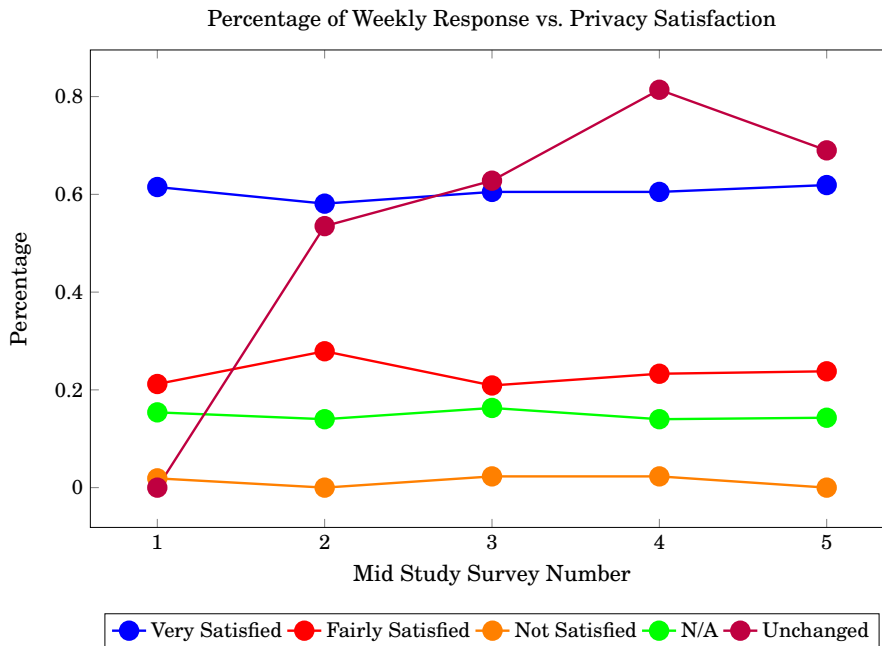


Figure 4.29: Overview of responses to “What are your observations on the privacy of Authy?” through out the mid study responses.

The general trend for overall perception of privacy relative to Authy is a static highly favorable percentage over the entire survey. Subjects had an unchanging view that Authy kept their information private.

The team analyzed the results above and found no statistically significant evidence to support a claim that survey number (ANOVA, $P = 0.999$) or education level (ANOVA, $P = 0.653$) plays a role in explaining differences in privacy observations. Neither education level nor survey number had an impact on perception of privacy.

The team found that there is no statistically significant correlation between either survey number and perception of privacy (ANOVA, $P = 0.997$) or prior knowledge of MFA and perception of security (ANOVA, $P = 0.321$). Neither prior knowledge of MFA nor survey number had a significant impact on perception of privacy.

The team found no statistical evidence to suggest that perception of privacy is impacted by either survey number (ANOVA, $P = 0.996$) or acquaintance with someone who was hacked

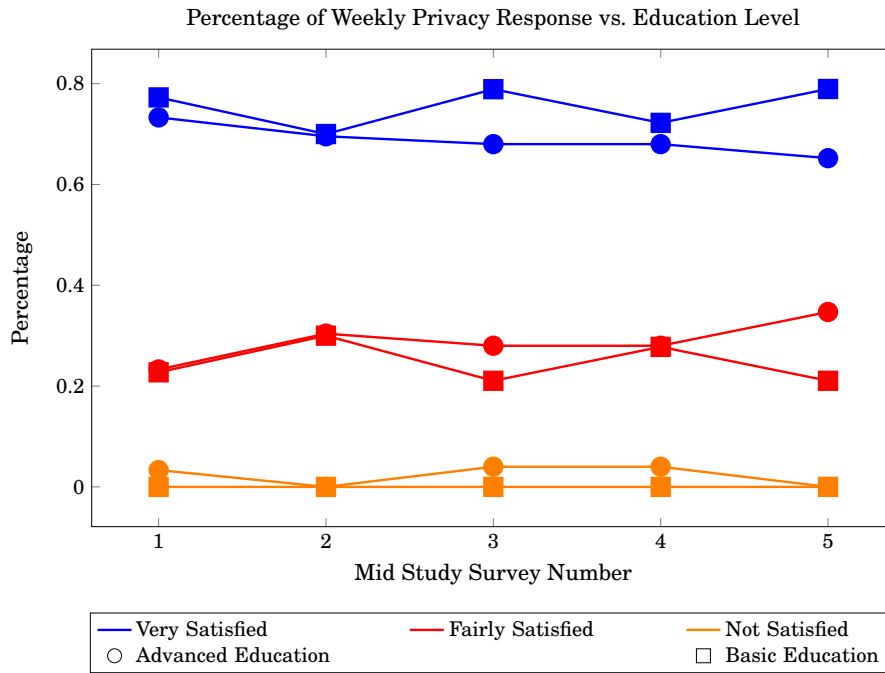


Figure 4.30: Results in figure 4.29 in respect to education treatment.

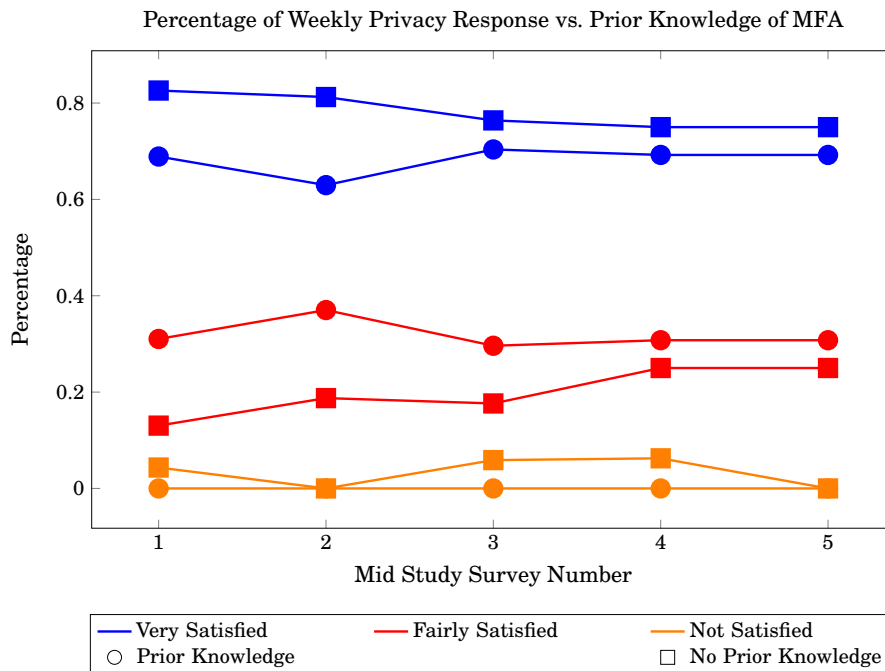


Figure 4.31: Results in figure 4.29 in respect to prior knowledge of Multi-Factor Authentication. (figure 4.3)

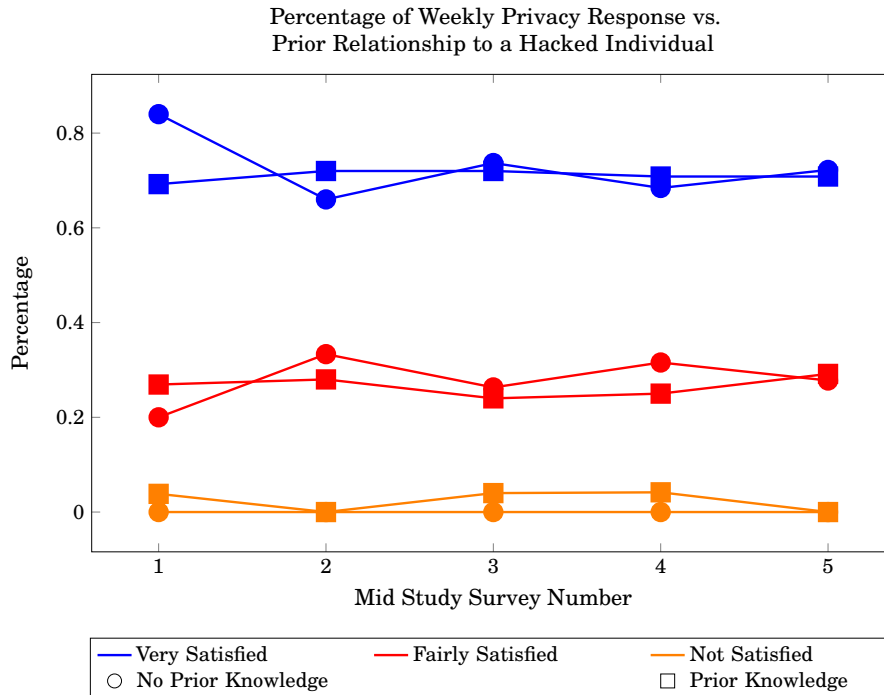


Figure 4.32: Results in figure 4.29 in respect to knowledge of someone hacked. (figure 4.4)

(ANOVA, $P = 0.596$).

The team found that there was not a statistically significant difference to support the claim that perception of usability is impacted by either initial view on the adequacy of a password (ANOVA, $P = 0.857$) or survey number (ANOVA, $P = 0.994$).

4.5.6 Difficulties with Authy

The team hypothesized that education level may be a factor in predicting whether subjects had difficulties or not. Throughout the course of the study if an individual experienced difficulties they were asked to note it describe the problem. The following graph shows the percentages of individuals that have had issues with Authy over the course of the study by education level.

The preceding graph shows the trend of difficulties as time went on in the study. As survey number increased, the number of difficulties participants encountered decreased. Intuitively it makes sense that most of the issues occurred at the beginning of the survey, while very few if none occurred at the end. However, the differences in percentage between the educational groups is minimal, and it can be assumed that education does not play a role in difficulties with Authy.

4.5.7 Summary of Mid-Study

The team measured subjects' perceptions of security, usability, and privacy throughout the mid-study phase. Upon comparison of these perceptions with education level and other background

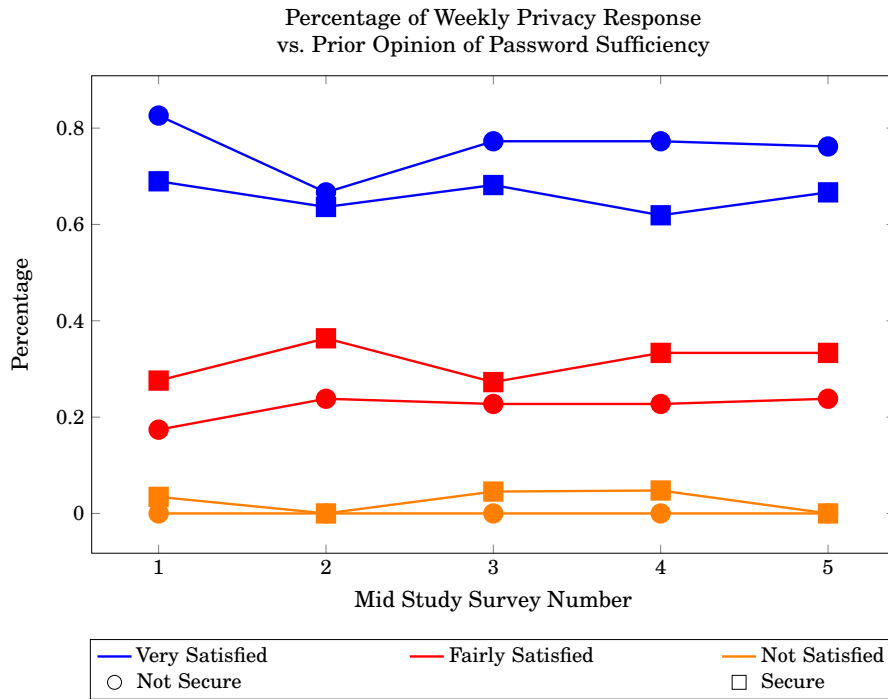


Figure 4.33: Results in figure 4.29 in respect to prior opinion of password sufficiency. (figure 4.6)

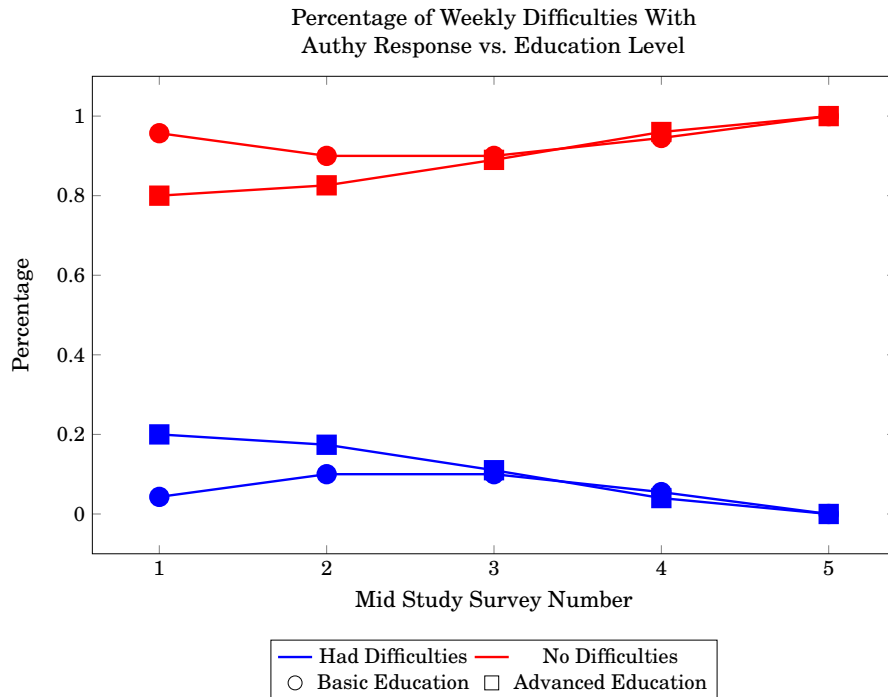


Figure 4.34: Responses to "Have you experienced any difficulty with Authy?" in respect to education treatment.

indicators, the team found little significant correlation. The only significant background factor was prior knowledge of MFA, which proved to be a positive indicator of usability perception. This evidence leads the team to conclude that either a more in-depth education or a larger number of participants may have had a larger impact. However, the fact is that the education that the IQP team gave, prior experience with MFA, password preferences, and a past with security attacks do not have a significant effect on the subjects' perception of Strong Authentication.

4.6 Final Survey

4.6.1 Perception of Protection

Two factor authentication promises stronger security than single factor password authentication. Under the hypothesis that perception of protection may be related to education and other background factors, the team assessed the former in the Final survey:

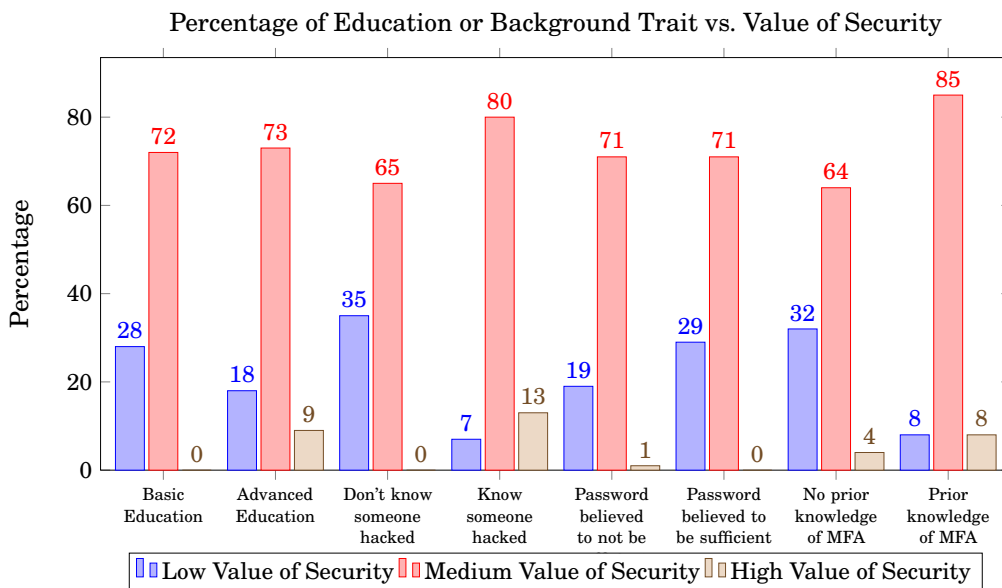


Figure 4.35: Responses to "How protected did you feel when using Two Factor Authentication?" in respect to education treatment and initial survey responses.

As seen in Figure 4.53, subjects tended to feel a sense of increased protection with Authy. Upon further analysis, the team found that education level (ANOVA, $P = 0.829$), acquaintance with someone hacked (ANOVA, $P = 0.658$), initial perception on the adequacy of passwords (ANOVA, $P = 0.815$), and prior knowledge of MFA (ANOVA, $P = 0.505$) had no effect on how protected users felt with Authy.

4.6.2 Usability Conclusions

As stated prior, a device or application that provides a poor user experience or user interface has a higher chance of no longer being used or being labeled as horrible. In the final survey students were asked to rate the overall usability of Authy under the hypothesis that background factors or education may have a correlation with overall usability conclusions.

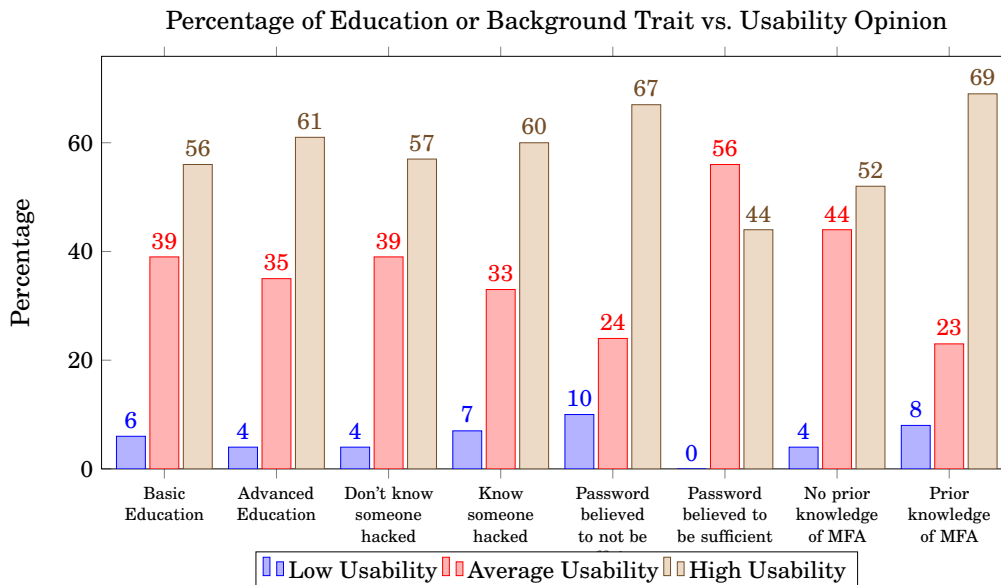


Figure 4.36: Responses to "Rate the overall usability of Authy." in respect to education treatment and initial survey responses.

As seen in the graph above, most participants stated that Authy had generally good usability. Across the board, around 60% of individuals reported good usability, with most others stating that the usability was okay. This led the team to believe that Authy's implementation of Two Factor Authentication is well and usable. However, the team found that education level (ANOVA, $P = 0.735$), acquaintance with someone who was hacked, (ANOVA, $P = 0.561$), initial belief on the adequacy of a password (ANOVA, $P = 0.843$), and prior knowledge of MFA (ANOVA, $P = 0.417$) had no significant effect on the final perception of usability. Some further usability concerns were reported in the final survey, for example, one user stated that Authy was more "cumbersome" than SMS 2FA and complained it did not support Android wear.

4.6.3 Confidence in Privacy

The team asked the participants to report how private Authy keeps their information under the hypothesis that education level and other background factors may have significant correlations with confidence in privacy.

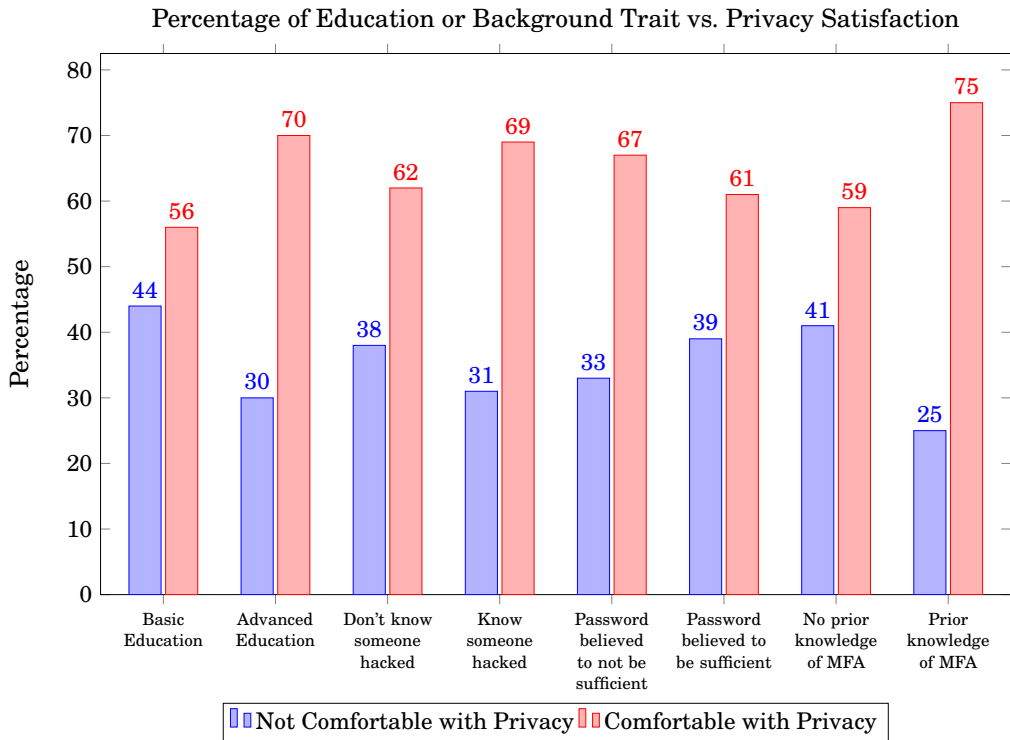


Figure 4.37: Responses to “How confident are you that Authy keeps your data safe and private?” in respect to education treatment and initial survey responses.

Figure 4.37 shows that the majority of subjects are very confident that Authy keeps their information safe and private. An average of roughly 68% of individuals across the board believe this to be true. However, the team found that acquaintance with someone who was hacked (T-Test, $P = 0.645$), initial impression on the adequacy of a password (T-Test, $P = 0.728$), prior knowledge of MFA (T-Test, $P = 0.342$), and education (T-Test, $P = 0.416$) had no significant impact on confidence in Authy privacy-wise.

4.6.4 Perception Change

Under the hypothesis that education may have an impact on how much subjects’ opinions on Strong Authentication changed, the team asked a question to detail just that:

As shown by the figure above 77.7% of individuals in the baseline group believe their perceptions of authentication changed a lot during the course of the study, while only 56.5% of the Advanced group believed their perceptions to have changed. The team found that Education level almost had a statistically significant impact on whether or not subjects’ opinions changed over the study (T-Test, $P = 0.128$). This may be a product of how the advanced group had received more education at the beginning of the study and resultingly had to figure out less about authentication on their own. This result contradicts some of the results from the mid-study evaluations;

individuals often reported no change in opinion or similar responses between surveys. Their perceptions may not have changed as much as they thought.

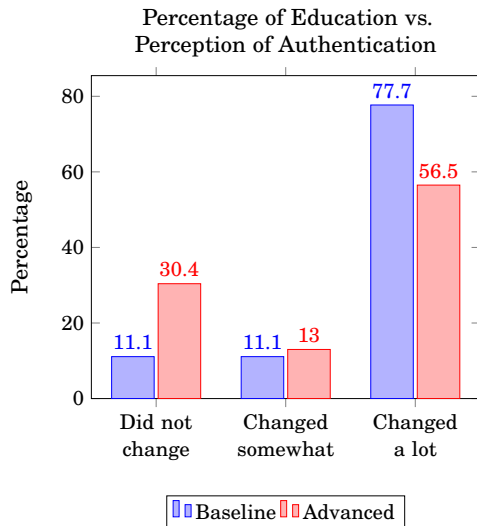


Figure 4.38: Responses to "Did your perception of authentication change throughout this study?" in respect to education treatment.

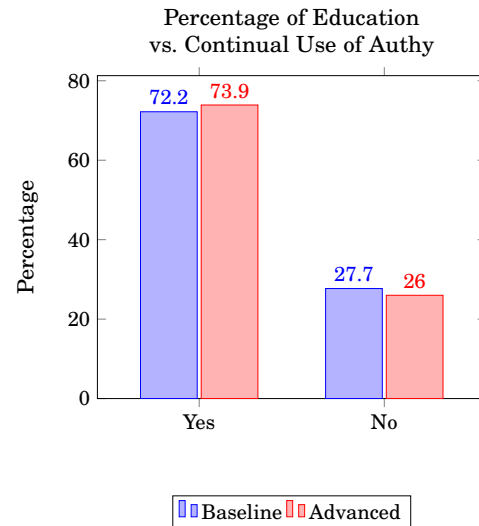


Figure 4.39: Responses to "Do you think you will continue using Authy outside of this study?" in respect to education treatment.

4.6.5 Continued Use of Authy

A good indicator of the relative importance of security to usability is continued use. The team asked subjects to state whether or not they plan to use Authy or another type of 2FA under the hypothesis that educational awareness may cause a significant effect.

According to the above graph above, most individuals in the study believed that they will continue to use Authy once this study is complete. Education level does not seem to be relevant in this case as both parties reported with nearly identical distributions. The statistical analysis supports this conclusion as well (T-Test, $P = 0.815$). Another interesting result is that subjects who think that they would not use Authy in the future had not experienced a computer account being hacked or compromised. Not having experienced with a cyber security attack may make those students think that Authy is not necessary.

4.6.6 Participants Technical Understanding of Authy

The team asked participants to explain how Authy protects them, under the hypothesis that education group and other background factors may have a significant relation to understanding of Authy's 2FA mechanism.

Based on the data above, the team found that education does not have a statistically significant impact on how well participants defined the 2FA mechanism (ANOVA, $P = 0.670$).

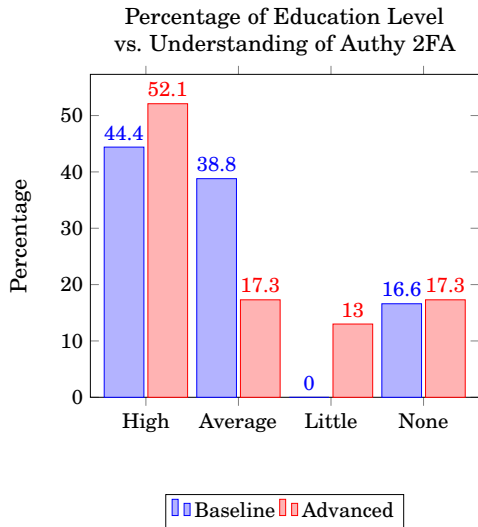


Figure 4.40: Responses to "Is Two Factor Authentication, as provided by Authy, more secure than a password?" in respect to education.

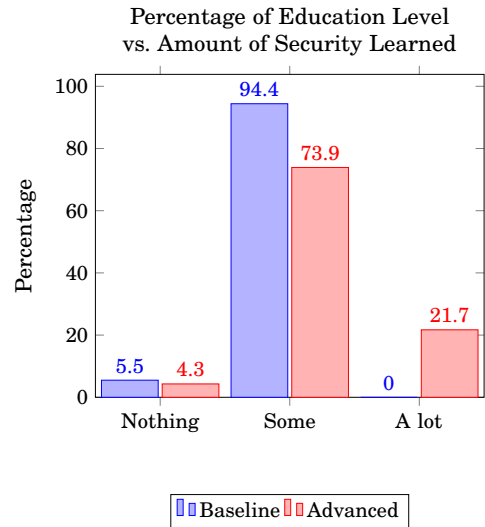


Figure 4.41: Responses to "Did you learn anything about internet security throughout this study?" in respect to education.

4.6.7 Knowledge Learned About Internet Security

Throughout the course of the study participants had much exposure to strong authentication concepts. The team gauged whether or not students felt as though they had learned anything throughout the course of the study under the pretense that education impacted the reported amount learned.

According to data above, most individuals in the study believe they learned at least a little about internet account security. However, the team found that there was no statistically significant difference between the results for each education level (ANOVA, $P = 0.831$).

One of the requirements in the study was that students install Authy for at least two services. The team hypothesized that education level may have a role, and that if subjects went beyond two, they must have a good perception of strong authentication.

The team found a highly statistically significant negative correlation between number of services and education level (i.e. you are far more likely to have three or fewer services installed if you are in the higher education group) (T-Test, $P < 0.01$). This may be caused by increased curiosity from the baseline group, or by something in the presentations themselves.

4.6.8 Other Forms of Multi-Factor Authentication

The team hypothesized that education level may be a significant factor in perception of strong authentication, so the final survey polled subjects on how they plan to proceed in the future with strong authentication. The following graph summarizes the data.

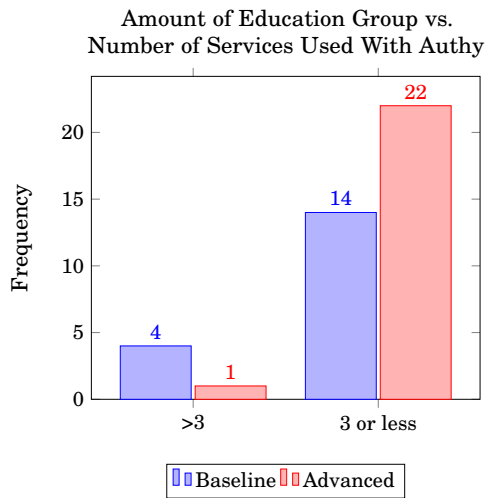


Figure 4.42: Responses to "Did you install Authy for more than the two services we asked for?" in respect to education.

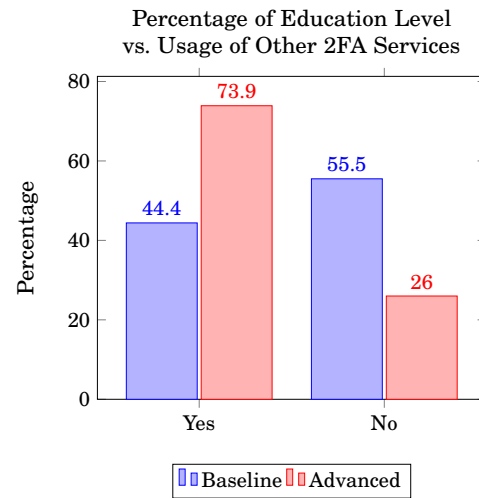


Figure 4.43: Responses to "Did you install any other methods of Strong Authentication and/or do you plan to?" in respect to education.

The team found that; education played a significant positive role in the difference between responses (T-Test, $P = 0.0619$). This result may be explained by the education level, as those in the advanced group received more education on different strong authentication methods and may be interested in trying them out.

4.6.9 Final Survey Summary

The results of the final survey show that most subjects felt as though the usability, security, and privacy of Authy was great. Users' overall perceptions are positive after using the application, and most individuals stated that they will continue using Authy after the study is over. This suggests that although the initial barriers to 2FA may be more inconvenient than those of single factor password authentication, the payoff is increased safety, and more importantly, confidence in safety and privacy generally without inconvenient usability issues. The results of the final survey also show that most individuals believe that they not only learned during the study but their perceptions of strong authentication changed greatly. However, the team discovered little significance in terms of cause and effect relationships between factors. Education was significant to perception of 2FA in two instances, but prior knowledge of MFA, opinion on the adequacy of passwords, and acquaintance with someone hacked all demonstrably had no effect.

CONCLUSIONS AND RECOMMENDATIONS

5.1 The Study

As part of the goals of this IQP, the team wanted to understand user perception of Strong Authentication, as influenced by several factors measured while using a strong authentication system. The IQP team designed a study in which participants were recruited with a cash incentive and split into two groups with different levels of educational treatment: baseline and advanced education. These groups were designed to illicit any differences in behavior and perception to discover if education affects a user's decision-making processes regarding strong authentication. The participants were required to install a third party two-factor application called Authy, connect it to at least two services, and complete five bi-weekly surveys designed to track perceptions of the application's usability, security, and privacy over time. The team later analyzed how these factors affected subjects' choices in using two-factor authentication.

5.2 Key Findings

The team discovered several trends about people's experiences with authentication, particularly in the area of individual background, education level, and experience in the study.

One overall trend was that although people claimed to value security and privacy, they did not use basic important security practices. This implies that although people may want to be secure, they are unwilling or unaware of how to take the necessary steps to achieve that security.

The team assessed the mid-study survey data, focusing on education and specific background qualities. While searching for correlations, the team found that education level and several other background had little to no significance. One of the few existing correlations, however, was between prior knowledge of MFA and perception of usability. The team found that those

who understood MFA prior to the study tended to favor the usability of Authy. This correlation strongly shows that some form of education on MFA may result in better perceptions of 2FA usability.

The initial barriers to 2FA are more inconvenient than those of a single password. The team found that after the initial difficulty (or chemistry analogy "activation energy"), students viewed the security, privacy, and usability of 2FA as implemented by Authy very positively to the extent that many subjects stated they would continue to use it after the study was completed.

5.3 Recommendations

There are a number of things that could have been done to improve the effectiveness of the study. For those who are interested in finding out more about how human motivation works when it comes to strong authentication, this section states what the team believes may be done to improve upon the work done in this study. This section also recommendations to developers and companies the team and the participants of the study believe should be put into place to improve upon the current security software for Strong Authentication.

5.3.1 Future Research

The team found that the education did not have as much impact as expected. This result was surprising, as it contradicts the correlation proven earlier that knowledge of MFA predicts higher perception of usability. It may be due to the fact that the team gave the subjects only one 30-60 minute session to learn about Strong Authentication, which may not have been enough to cover the in-depth topic. The team recommends to have a larger scope of the educational sessions, perhaps spread over several days, or even having recurring weekly or bi-weekly sessions. Education did have a small effect, and knowledge of MFA (which had to be learned somehow!) was shown to be significant in the mid study evaluations. If prior knowledge of MFA was shown to be significant to perception of Strong Authentication, then other topics may also be significant with a more extensive prescribed education. The way to test this hypothesis would be to provide more extensive education to participants during the study.

The highest number of recorded individuals at a single time was fifty-seven. This population size may not be enough to accurately detect important trends discussed throughout the analysis. For several comparison figures, the group size in one category was smaller than desired. This issue may be fixed by more participation in the study. More participants means more data, which may lead to strongly supported correlations and more unique qualitative phenomena. Either way, upscaling the participant pool may improve the credibility of the conclusions in a study such as this.

The mid study survey phase was designed to help the IQP team understand how perceptions of strong authentication changed over the course of the study. Unfortunately, the overall trends

from this data were not as defined or clear the team had hoped. Many graphs showed little to no change over the entire 10 week period. To get better data out of a mid-study evaluation period such as this, the team recommends extending the length of time to catch larger trends that 10 weeks may not spot.

With this study design, survey questions were critical to getting usable data. The responses are critical data points that are used in making analysis and acquiring results. One must make sure that any questions asked are clear and prompt the participant to be descriptive and honest about their perceptions. The team recommends that future work should be very specific about honest feedback and should design questions with the expectation that subjects will say what they think is the "correct" choice, rather than what they actually believe.

The team also recommends that further work be done using alternate authentication methods, perhaps a different software token application such as Google Authenticator, or by using a hardware token such as a yubikey. The broader the data collected, the more thorough analyses can be made.

Because of the resources available to the IQP team, all of the study participants were WPI students. WPI is known for being a technically competent community; many students are accustomed to technology and some even to security practices and techniques. The team recommends that future related work uses a more diverse participant body. People of different ages, occupations, and locations may give a more honest reflection of the truth.

A final suggestion to future researchers would be to set aside time and meet with participants face to face in focus groups. If participants discuss how they perceive authentication, they will have thought more about the topic and may resultingly be able to give better responses.

5.3.2 Other Recommendation

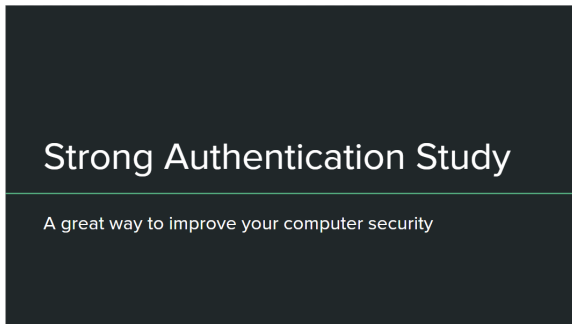
According to the aforementioned results, the so-called "activation energy" when beginning to use strong authentication may be part of the reason for its lack of widespread usage. The team recommends that online services, schools, and other organizations mandate some form of strong authentication to spread its knowledge and usage.

Many students had concerns and difficulties when installing and linking their services to third-party 2FA application used in this study. Companies may benefit by having clear, foolproof installation guides. If the barrier of entry is too high, few will put in the work to secure themselves using the application. Also supporting more services that individuals use frequently is important to making sure that all parts of an individual's online identity and activity is secured.

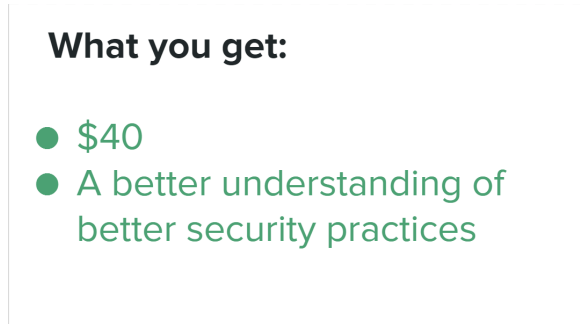
ACKNOWLEDGEMENTS

This project was made possible through the gracious financial support of the Department of Social Science and Policy Studies and the Interdisciplinary and Global Studies Division.

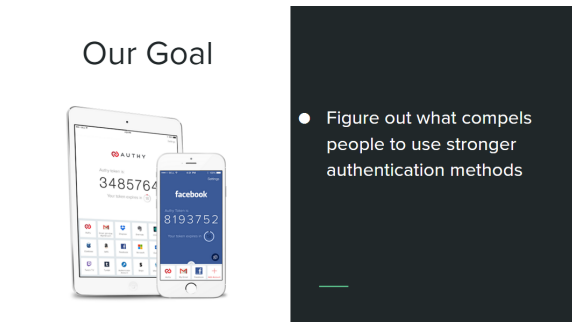
APPENDIX A: PITCH PRESENTATION



Slide 1



Slide 2



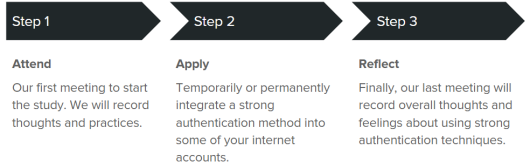
Slide 3



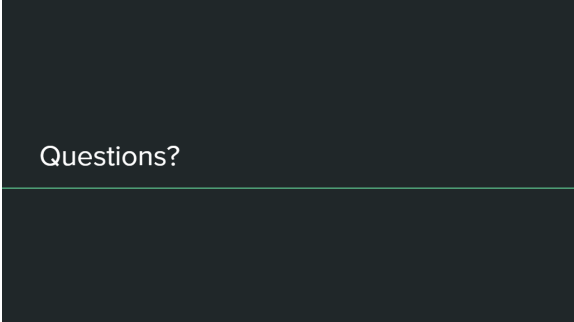
Slide 4

Pitch Presentation, Slides 1 - 4

What we need from you

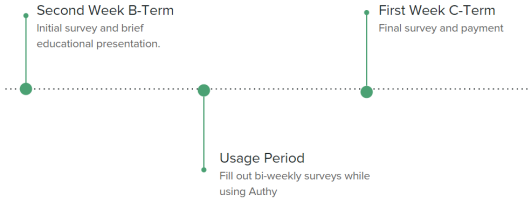


Slide 5



Slide 7

Timeline



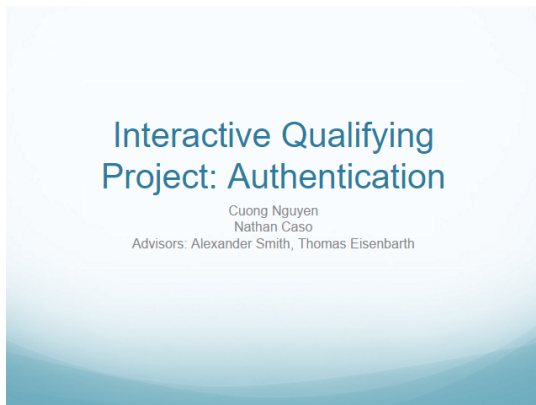
Slide 6



Slide 8

Pitch Presentation, Slides 5 - 8

APPENDIX B: BASIC PRESENTATION



Interactive Qualifying
Project: Authentication

Cuong Nguyen
Nathan Caso
Advisors: Alexander Smith, Thomas Eisenbarth

Slide 1





What is Authentication?

- The act of confirming the truth of an attribute of a single piece of data (a datum) claimed true by an entity
- Three ways to authenticate - authentication factors.

Slide 2



Authentication Factors

- **Knowledge factors:** Something the users **knows**
- **Ownership factors:** Something the users **has**
- **Inherence factors:** Something the users **is or does**

Slide 3



Single Factor Authentication

- What is single factor authentication?
 - Single factor authentication (SFA) is defined as any security authentication method that uses one factor authentication.
 - The most common type of single factor authentication is the computer password.



Slide 4

Basic Presentation, Slides 1 - 4

Two-factor Authentication

- What is two-factor authentication?
 - Two factor authentication (2FA) is defined as any security authentication method that combine two varying factors.
 - Some real world examples assuming a password: SMS verifications, Bank PIN, etc.

Slide 5

Examples of 2FA

- Google Authenticator

Whenever you sign into Google you'll enter your username and password as usual.

Next, you'll be asked for a code that will be sent to you via text, voice call, or our mobile app.

Now your account has additional protection against hijackers.

Slide 6

Examples of 2FA

- Fingerprints Authentication

Slide 7

Authy App

- Mobile application authentication tokens
- Can be used in following methods:
 - Mobile Phone Application
 - Desktop Application
 - Chrome Extension
- Compatible with:
 - Google Accounts
 - Dropbox
 - Amazon
 - Facebook

Slide 8

Authy Compatibility

| | |
|------------------------------|------------------|
| 1. Google | 1. Dreamhost |
| 2. Dropbox | 2. LastPass |
| 3. Microsoft | 3. Guildwars 2 |
| 4. Facebook | 4. Evernote |
| 5. Gmail | 5. WordPress |
| 6. Outlook | 6. Digital Ocean |
| 7. App.net | 7. Heroku |
| 8. Github | 8. Stripe |
| 9. Amazon Web Services (AWS) | 9. Tumblr |
| 10. Linode | 10. Bitcoin |

Slide 9

What is the goal of this IQP?

- We want to understand why two factor authentication is or is not used
 - Interested in usability factors
 - If people with less knowledge about cyber security can use it and install it
 - How perceptions of two factor authentication change or do not change

Slide 10

Basic Presentation, Slides 5 - 10

Tasks for participants

- Phase 1: Install Authy
 - Use with two different services for three out of this list of five.
 - Suggested to use the mobile application
 - Contact us if you have difficulties
- Phase 2: Fill out weekly check-in google forms
 - Be honest!
 - It is OK to not know something!
 - Your accuracy improves our study!
- Phase 3: Fill out final survey
 - Thoroughly and honestly explain your experience
 - It is OK to not know something
 - Your accuracy improves our study!

Basic Presentation, Slide 11

APPENDIX C: ADVANCED PRESENTATION

Authy Risk and Private Policy

...

Two Factor Authentication - Interactive Qualifying Project

Slide 1

Cyber Security is Important

- Risk of cyber attacks has dramatically risen
- We live in an era of software innovation
 - New Software = Vulnerable
 - Personal information on internet is increasing
- Many attacks require minimal effort
- Little effort on the user can dramatically decrease the probability of a successful cyber attack

WHAT DO VICTIMS HAVE IN COMMON?

| | | |
|--------------------------------------|--|---|
| 79% TARGETS OF OPPORTUNITY | 97% SIMPLY AVAILABLE | 85% TOOK WEEKS TO DISCOVER |
| 94% PROCESSED SUCCESS | 96% ATTACKS WERE NOT DIFFICULT | 92% DISCOVERED BY A THIRD PARTY |

Source: Security Report 2015

Slide 2

Cyber Attacks are a Serious Problem

- 2015: "The Impact Team" stole the user data of Ashley Madison
- 2014: White House was hacked
- 2014: \$460 million in bitcoins were stolen by hackers
- 2011: Bank of America was hacked
- 2008: Pentagon computer system was hacked

Slide 3

What is authentication?

- Confirmation of data claimed true by an entity
- Three Authentication Factors
 - Knowledge
 - Ownership
 - Inherence
- Authentication with only one factor is not secure

Slide 4

Advanced Presentation, Slides 1 - 4

Single Factor vs Dual Factor Authentication

- **Single Factor Authentication:**
 - Authentication method using only one factor of authentication
- **Dual Factor Authentication:**
 - Authentication method using at least two factors of authentication



Slide 5

Smart Cards


- Multiple options for authentication
 - Proof of physical ownership
 - Magnetic Swipe
 - Integrated Circuit Chip (ICC)
 - Wireless Verification
 - Barcode Scan
 - Proof of correct knowledge
 - Verification of encrypted PIN stored on ICC
 - Proof of being the right physical person
 - Visual Identification



Slide 6

Biometrics


- Proof of something you are
- Variety of methods available today
 - Handwriting characteristics
 - Typing patterns
 - Retina Scans
 - Fingerprint verification
 - Hand/palm geometry
 - Voice recognition
 - Facial recognition



Slide 7

Authentication Tokens

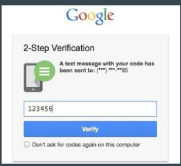
- Implemented on physical devices or mobile phone applications
- Satisfies something the user has (the device)
- Must be used in conjunction with something the user is or something the user knows
- Examples:
 - RSA SecurID
 - Google Authenticator
 - Authy



Slide 8

Email/SMS Verification

- Satisfies something the user has
 - Phone
 - Email Access
- Must be used in conjunction with something the user is or something the user knows
- Example
 - Steam
 - Google (as shown in picture)



Slide 9

Who is using Two Factor Authentication?

- **Academia Example**
 - Penn State University added Two Factor Authentication to all students and faculty
- **Public Sector Example**
 - 17 million employees of the United States Department of Defense uses the Common Access Card (CAC)
- **Private Sector Example**
 - All J.P. Morgan Chase employees use Two Factor Authentication

Slide 10

Advanced Presentation, Slides 5 - 10

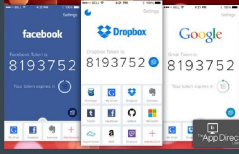
What is this project about?

- We want to understand why two factor authentication is or is not used
 - Interested in usability factors
 - If people with less knowledge about cyber security can use it and install it
 - How perspectives of two factor authentication change or do not change
- Users will:
 - Install and use authy to gauge usability
 - Fill out surveys to assess opinions and knowledge
 - Learn more about cyber security to further the study

Slide 11

What is Authy and how does it work?

- Mobile application authentication token
- Can be used in following methods:
 - Mobile Phone Application
 - Desktop Application
 - Chrome Extension
- Compatible with:
 - Google Accounts
 - Dropbox
 - Github
 - Amazon
 - Tumblr
 - Facebook
 - And more...



Slide 12

Authy's Private Policy

- Abides by US-EU and Swiss Safe Harbor Framework
 - Certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement
- Authy takes reasonable precautions such as policy based access control to protect data in our possession from loss, misuse, and unauthorized access
- Authy strives to protect data, but it cannot guarantee its security.

Slide 13

What data is collected by Authy?

- Authy Collects:
 - First & Last name
 - Organization name
 - City, State, and Zip Code
 - Email address
 - Phone number
- Records browser information including page requests and usage times
- Inspection of cookies to gauge interest

Slide 14

What does Authy do with collected data?

- Contact information only used for purpose such information was provided
- Service information only saved to conduct business with the user
- Contact users using given email/phone
- Authy complies with subpoenas and/or other legal demands for personally identifiable data

Slide 15

Authy's Data Disclosure Policy

- Will disclose personal information if
 - Proper action is performed by government services requiring it
 - Protect and defend rights of property of Authy
 - Protect the property or users of Authy site or services

Slide 16

Advanced Presentation, Slides 11 - 16

Tasks for you!

- Phase 1: Install Authy
 - Use with three accounts
 - Suggested to use the mobile application
 - Contact us if you have difficulties
- Phase 2: Fill out weekly check-in google forms
 - Be honest!
 - It is OK to not know something!
 - Your accuracy improves our study!
- Phase 3: Fill out final survey
 - Thoroughly and honestly explain your experience
 - It is OK to not know something
 - Your accuracy improves our study!

Advanced Presentation, Slide 17

APPENDIX D: SURVEYS

Initial Questionnaire

* Required

1. In which class are you? *

Mark only one oval.

- 2019
- 2018
- 2017
- 2016

2. What is your academic major? *

3. What is your e-mail address? *

4. Define computer account authentication in your own words *

Explain what you know about authentication

5. Do you know what Multi-Factor authentication is? *

Yes or no; if yes, explain what it is, and describe any examples you are familiar with

6. **Have you or has a family member of yours ever experienced a computer account being hacked or compromised? ***

If yes, explain the incident, what services were involved, and what behaviors did you change after the incident?

7. **How many passwords do you use? ***

Mark only one oval.

- I use one password for most of my accounts
 I use one or two passwords for my accounts
 I use one password per account for most of my accounts

8. **Do you think your password/s is/are secure? ***

Mark only one oval.

- Yes
 No
 Not sure

9. **How often do you reset a password for an online account? ***

Mark only one oval.

- Less than 1 time per month
 1-3 times per month
 More than 3 times per month

10. **How much do you value internet account security? ***

On a scale of 1-5

Mark only one oval.

- 1 - It's not necessary
 2 - It's helpful
 3 - It's important
 4 - It's critical

11. **Do you have information online that you would prefer to be kept private? ***

Mark only one oval.

- Yes, disclosure of my information could result in serious problems
- Yes, but there would be no severe consequences if my information was disclosed
- No, but disclosure might significantly impact my life
- No, and disclosure won't significantly impact my life
- I'm not sure

12. **Are there any web services that you refuse to use because of security/privacy concerns? ***

If so, please list them

13. **How much do you value the privacy of your online information? ***

On a scale of 1-3

Mark only one oval.

1 2 3

Not very much Very much

14. **Is an account username and password enough to protect your online accounts? ***

Please explain briefly

15. **How much extra time would you be willing to spend authenticating yourself for a banking account? email account? social networking account? ***

Think about how frequently you would use each account, and how much time the process would take on a daily basis.

Mid-Study Evaluation I

* Required

What is your participant number? *

For which services did you install Authy? *

Did your installation run smoothly? *

Did you install the app with ease on all apps?

Yes

No

Continue »

Mid-Study Evaluation I, Page 1

Mid-Study Evaluation I

* Required

Page 2

For which application(s) did you have a problem with the installation? *

Facebook

Outlook

G-mail

Please give a description of the problem *

« Back

Continue »

Mid-Study Evaluation I, Page 2

Mid-Study Evaluation I

* Required

Page 3

How often did you use Authy to authenticate yourself in the last two weeks? *

What are your observations on the security Authy provides? *

Please explain briefly

What are your observations on the usability of the application? *

Please explain briefly

What are your observations on the privacy of Authy? *

Please explain briefly

Do you have any questions, comments, or concerns?

Mid-Study Evaluation II

* Required

What is your participant number? *

Which services are you currently using Authy for? *

For which services do you use Authy the most? *

- Facebook
- Gmail
- Outlook
- I don't use any of them

How often did you use Authy to authenticate yourself in the past two weeks? *

If you have experienced any difficulties with Authy, select the second option *

- No difficulties
- I had difficulties

Continue »

Mid-Study Evaluation II, Page 1

Mid-Study Evaluation II

* Required

Page 2

Which service(s) did you experience a difficulty with? *

- Facebook
- G-mail
- Outlook

Please describe the problem *

Mid-Study Evaluation II, Page 2

Mid-Study Evaluation II

* Required

Page 3

Do you have any further observations on the usability of the application? *

Please explain briefly

Do you have any further observations on the security Authy provides? *

Please explain briefly

Do you have any further observations on the privacy Authy provides? *

Please explain briefly

Mid-Study Evaluation II, Page 3

Mid-Study Evaluation III

* Required

What is your participant number? *

Which services are you currently using Authy For? *

If you experienced any difficulty with Authy, please select the corresponding option below *

- No difficulties
 I had difficulties

Continue »

Mid-Study Evaluation III, Page 1

Mid-Study Evaluation III

* Required

Page 2

For which service(s) did you experience any difficulty? *

- Facebook
 G-mail
 Outlook

Please describe the problem *

« Back

Continue »

Mid-Study Evaluation III, Page 2

Mid-Study Evaluation III

* Required

Page 3

Roughly how many times in total have you used Authy to authenticate yourself? *

How often did you use Authy to authenticate yourself in the past two weeks? *

Do you have any further observations on the security Authy provides? *

Please explain briefly

Do you have any further observations on the usability of the application? *

Please explain briefly

Do you have any further observations on the privacy Authy provides? *

Please explain briefly

« Back

Submit

Never submit passwords through Google Forms.

Final Questionnaire

* Required

1. **What is your participant number? ***

2. **Is Two Factor Authentication, as provided by Authy, more secure than a password? ***

Mark only one oval.

Yes

No

Other: -----

3. **How protected did you feel when using Two Factor Authentication? ***

Mark only one oval.

Not as secure as a strong password

About as secure as a strong password

More secure than a strong password

4. **Rate the overall usability of Authy ***

Mark only one oval.

1. Generally bad usability

2. Generally okay usability

3. Generally good usability

5. **How confident are you that Authy keeps your data safe and private? ***

Mark only one oval.

1. I don't believe Authy will keep my data private

2. I'm not quite sure if Authy keeps my data confidential

3. I'm certain that Authy doesn't share my data

6. **Did your perception of authentication change throughout this study? ***

Explain

7. **If you stopped using Authy for any reason, please explain why**

8. **Do you think you will continue using Authy outside of this study? ***

Mark only one oval.

- Yes
- No

9. **How does Authy protect you? ***

In your own words

10. **Is two factor authentication better than single factor authentication? ***

Mark only one oval.

- Yes
- No

11. **Do you think you learned anything about internet security throughout this study? ***

Mark only one oval.

- No, nothing
- Yes, a little
- Yes, a lot

12. **Did you install Authy for more than the three services we asked for? ***

If so, please list where else you installed Authy, and why you decided to do so

13. **Did you install any other methods of Strong Authentication for any services, and do you plan to do so in the future?**

Strong Authentication methods include biometrics, alternate two factor methods, three factor methods, or anything besides a password and username

BIBLIOGRAPHY

Andrade, G. (September, 2014). *How to Use Apple's Touch ID for Two-factor Authentication*. Retrieved from <https://www.secsign.com/use-apples-touch-id-two-factor-authentication/>.

Bellefeuille, R. (2014, January). *The Benefits of Two-Factor Authentication*. Retrieved from <http://www.portalguard.com/blog/2014/01/10/benefits-two-factor-authentication-2/>.

BitDefender. (2010, August). *BitDefender Finds Exposed Social Media Credentials Often Provide Access to Email Accounts*. Retrieved from <http://www.bitdefender.com/news/bitdefender-finds-exposed-social-media-credentials-often-provide-access-to-email-accounts-1682.html>.

Cooperband, J. (2015, March). *Two-factor Authentication*. Retrieved from <https://www.linkedin.com/pulse/two-factor-authentication-jared-cooperband>.

Clarke, N.L., Furnell, S.M. (2005, October). Authentication of Users on Mobile Telephones – A Survey of Attitudes and Practices. *Computer Security*, 24(7), 519-527. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167404805001446>

Clarke, N.L., Furnell, S.M., Rodwell, P.M., Reynolds, P.L. (2002, June 1). Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices. *Computer and Security*, 21(3), 220–228. Retrieved from <http://www.sciencedirect.com/science/article/pii/S0167404802003048>

Clark, L. (April, 2012). *The Advantages & Disadvantages of Using Smart Cards*. Retrieved from <http://www.brighthub.com/computing/smb-security/articles/67274.aspx>.

Confident Technologies. (2011, May). *The Problem with Two-Factor Authentication Solutions Using SMS*. Retrieved from http://confidenttechnologies.com/news_events/problem-two-factor-authentication-solutions-using-sms/.

Cristofaro, E.D., Du, H., Freudiger, J., Norcie, G. (2014, January 31). A Com-

parative Usability Study of Two-Factor Authentication *USEC*. Retrieved from <http://arxiv.org/pdf/1309.5344.pdf>

Davis, J. (9 March 2014) "2 Factor Auth List". *Twofactorauth.org*. GitHub.com. Retrieved 15 September 2015.

Explorable.com (2009, June 6) "ANOVA" Retrieved February 22, 2016, from <https://explorable.com/anova>

Fido Alliance (2015). *Specifications Overview*. Retrieved from <https://fidoalliance.org/specifications/overview/>

FRSecure. (2013, July). *Two Factor Authentication - Pros and Cons*. Retrieved from <http://www.frsecure.com/two-factor-authentication-pros-and-cons/>.

Goldstein, M. (2014, December). *Neglected Server Provided Entry for JPMorgan Hackers*. Retrieved from http://dealbook.nytimes.com/2014/12/22/entry-point-of-jpmorgan-data-breach-is-identified/?_r=0

Hintze, L., Jerry (2005) "Two Sample T-Tests Allowing Unequal Variance" *PASS Sample Size Software* 425. Retrieved February 21, 2016, from http://www.ncss.com/wp-content/themes/ncss/pdf/Procedures/PASS/Two-Sample_T-Tests_Allowing_Unequal_Variance-Enter_Difference.pdf

Kay, R. (April, 2005). *Biometric Authentication*. Retrieved from <http://www.computerworld.com/article/2556908/security0/biometric-authentication.html>.

Khandelwal, S. (2015, July). *Bitcoin Cloud Mining Service Hacked; Database On Sale for Just 1 Bitcoin*. Retrieved from <http://thehackernews.com/2015/07/bitcoin-mining-server.html>.

Khandelwal, S. (2015, July). *Oops! Adult Dating Website Ashley Madison Hacked; 37 Million Accounts Affected*. Retrieved from <http://thehackernews.com/2015/07/adult-dating-website.html>.

Khandelwal, S. (2014, December). *Sony Pictures Hack - 5 Things You Need To Know*. Retrieved from <http://thehackernews.com/2014/12/sony-pictures-hack.html>.

BIBLIOGRAPHY

- Kozaryn, L. (October, 2000). *DoD Issues Time-saving Common Access Cards*. Retrieved from <http://usmilitary.about.com/od/theorderlyroom/l/blsmartcards.htm>.
- Krol, K., Philippou, E., Cristofaro, E.D., Sasse, M.A. (2015, January 19). *"They Brought in the Horrible Key Ring Thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking*. Retrieved from <http://arxiv.org/pdf/1501.04434v1.pdf>
- Kumar, M. (2015, January). *Taylor Swift's Twitter and Instagram Accounts Hacked*. Retrieved from <http://thehackernews.com/2015/01/taylor-swift-twitter-instagram-hacked.html>.
- Lioudvinevitch, O. (2014, April). *Benefits of Two-Factor Authentication*. Retrieved from <https://www.titanfile.com/blog/benefits-two-factor-authentication/>.
- Nali, D., Thorpe, J. (2004, May 27). *Analyzing User Choice in Graphical Passwords*. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.85.998&rep=rep1&type=pdf>
- Pelroth, N. (2014, August). *Russian Hackers Amass Over a Billion Internet Hackers*. Retrieved from http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0.
- The Radicati Group, Inc. (2015, March). *Email Statistics Report, 2015-2019*. Retrieved from <http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf>.
- Rouse, M. (2015, March). *Two-Factor Authentication (2FA)*. Retrieved from <http://searchsecurity.techtarget.com/definition/two-factor-authentication>
- Rubens, P. (August, 2012). *Biometric Authentication: How It Works*. Retrieved from <http://www.esecurityplanet.com/trends/biometric-authentication-how-it-works.html>.
- Schneier, B. (2005, April). Two-Factor Authentication: Too Little, Too Late. *Communications of the ACM*, 48(4), 27. Retrieved from http://www.itsec.gov.cn/webportal/download/2004_two-factor.pdf.
- Silver-Greenberg, J. (2014, October). *JPMorgan Chase Hacking Affects 76 Million*

Households. Retrieved from <http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/>

Strouble, D., Shechtman, G.M., Alsop, A.S. (2009, March 3). Productivity and Usability Effects of Using a Two Factor Security System. *SAIS 2009 Proceedings*. Retrieved September 15, 2015, from <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1036&context=sais2009>

U.S. Department of Defense. (2015). *Common Access Card (CAC) Security*. Retrieved from <http://www.cac.mil/common-access-card/cac-security/>.

Weir, C.S., Douglas, G., Carruthers, M., Jack, M. (2009, March). User Perceptions of Security, Convenience and Usability for Ebanking Authentication Tokens. *Computers & Security*, 28(1-2), 47-62. Retrieved from http://ac.els-cdn.com/S0167404808000941/1-s2.0-S0167404808000941-main.pdf?_tid=5ef2d0ae-5af2-11e5-a19c-00000aab0f02&acdnat=1442243452_0c9a3568cf1983bda46f2be6e6d667b7

Zah, Syed. (2009). *Two Factor Authentication Using Mobile Phones*. Retrieved from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5069395&tag=1>.