**Author:** **Lor, Chong Z.**

**Title:** ***Password Memorization Alternative***

The accompanying research report is submitted to the **University of Wisconsin-Stout**, **Graduate School** in partial completion of the requirements for the

**Graduate Degree/ Major: Information and Communication Technology**

**Research Advisor: Dr. Steven Schlough, Professor & Department Chair, Apparel and Communication Technologies Department**

**Submission Term/Year: Spring/2015**

**Number of Pages: 36**

**Style Manual Used: American Psychological Association, 6th edition**

☐ **I have adhered to the Graduate School Research Guide and have proofread my work.**

☐ **I understand that this research report must be officially approved by the Graduate School. Additionally, by signing and submitting this form, I (the author(s) or copyright owner) grant the University of Wisconsin-Stout the non-exclusive right to reproduce, translate, and/or distribute this submission (including abstract) worldwide in print and electronic format and in any medium, including but not limited to audio or video. If my research includes proprietary information, an agreement has been made between myself, the company, and the University to submit a thesis that meets course-specific learning outcomes and CAN be published. There will be no exceptions to this permission.**

☐ **I attest that the research report is my original work (that any copyrightable materials have been used with the permission of the original authors), and as such, it is automatically protected by the laws, rules, and regulations of the U.S. Copyright Office.**

☐ **My research advisor has approved the content and quality of this paper.**

**STUDENT**:

**NAME: Chong Lor** **DATE:**

**ADVISOR:** (Committee Chair if MS Plan A or EdS Thesis or Field Project/Problem):

**NAME: Dr. Steven Schlough** **DATE:**

---

**This section for MS Plan A Thesis or EdS Thesis/Field Project papers only**

**Committee members (other than your advisor who is listed in the section above)**

1. **CMTE MEMBER'S NAME:** **DATE:**
2. **CMTE MEMBER'S NAME:** **DATE:**
3. **CMTE MEMBER'S NAME:** **DATE:**

---

**This section to be completed by the Graduate School**

This final research report has been approved by the Graduate School.

Director, Office of Graduate Studies: **DATE:**

**Abstract**

With the increase in the number of passwords users have to memorize, it is apparent that many users have become careless about their passwords; thus, the user and the institution are vulnerable to compromise. The study of this paper is to evaluate alternatives to the burden of user memorizing complex passwords. Some of these alternatives include software, service, hardware, and hybrid solution.

## Acknowledgments

## Table of Contents

## Chapter I: Introduction

The computer password was developed over 50 years ago at the Massachusetts Institute of Technology for use with compatible time-sharing system (CTSS) (Hiscott, 2013). The idea behind CTSS was to allow multiple users to login to the system from different points of entry. However, researchers were able to trick the system and submit an offline printout of the passwords. At that time, there was no sophisticated hacking network and password cracking software. However, as the average machine got powerful enough to sophisticated brute force attacks, passwords need to be stronger to minimize security risks.

With the rise of ecommerce, portable devices, and social networks, the number of passwords users have to remember has increased dramatically. Based on a 2007 study of web users by Microsoft Research, "each user has about 25 accounts that require passwords, and types an average of 8 passwords per day" (Florencio & Herley, 2007, para. 7). Despite everything about a user's digital life being protected by passwords, users often choose passwords that are weak, guessable, and reused. Reused passwords that are weak across multiple accounts compounded the problem further. If when an account is compromised, the rest of the accounts are vulnerable to the same attack. For some complex passwords, users often resort to writing down their passwords to a sticky note and putting it underneath their keyboards, mouse pads, or easily found locations. It does not matter how strong one's front door is, if a thief is able to get the key underneath a rug or rock near one's front door then that door is useless. These practices post a serious threat to an organization's security. A Robertson's research (Ian Robertson, professor of psychology at the Institute of Neuroscience and School of Psychology at Trinity College in Dublin, Ireland) showed that nearly 60 percent of users studied felt like they just cannot remember the alphanumeric passwords (Wailgum, 2008). The most commonly used

password of 2014 was “123456”. “More likely, you were lazy and wanted something easy to remember, like 123456” (Kelly, 2014)(Kelly, 2014, para. 2).

There are various methods that organizations have tried to minimize this vulnerability. Some have policies that enforce from the server side to require every user to have a password that has a certain amount of complexity, is not repeated, and is changed frequently. Other methods include “limiting the number of logon attempts or requiring that additional imaged data be keyed” (Campbell, Ma, & Kleeman, 2011, p. 1). However, offline hash file attacks, password discovery, and social engineering are still a possibility. Companies like Google, Apple, and Facebook etc. have implemented two-factor authentication but most people either do not know about it or simply do not have it turned on. Microsoft just announced that its Windows 10 would support the FIDO (Fast Identity Online) technology that allows the “use of fingerprint or eye scan – possibly integrated with a key fob for two-factor authentication” (Paul, 2015, para. 1). However, this is still relying on a third party to build upon the feature.

There are several methods that users can use to help memorize complex passwords. The first method is using a sentence like, “I pay $250.99 a month for my electricity bill” for a password. This method requires using upper and lower cases, numbers, and special characters. The second method is to pick the first and third character of each word in the sentence. Here is an example of this method, Ipy$5anfrmeebl, from the sentence “I pay $250.99 a month for my electricity bill”. The third method would be to mix and match special characters with the alphabet. Something like “myStraingeBook” would turn into “m1$tr@in93800k”. The fourth method involves using a common root word by changing only a prefix or suffix is the easiest way to remember. For example, “superM@n” is the common root word. Therefore, a Facebook password can be something like “facesuperM@n” or “superM@nBook”. However, the user

would still have to remember all of these passwords. In the United States each user carry an average of three portable devices (Eddy, 2013) and that does not include all the accounts in social network, bank, ecommerce, forums, blogs, PIN etc.

Users may find some password managers useful. However, password managers have their own issues such as usability, portability, and a single point of failure. Many password managers are hard to configure, manage, and update. Other desktop password managers suffer from being able to port over to mobile devices such as tablets and smart phones. If the master password is compromised, hackers have access to all the passwords. Thus, there must be some alternatives that offers portability, usability, two-factor authentication, and security. Organizations and institutions are especially vulnerable to attacks due to some of its employees using weak passwords for all their logins or to manage their password manager.

**Statement of the Problem**

Users must create and remember passwords for multiple logins. Organizations require complex passwords by enforcing a minimum number of characters and mandating a variety of special characters. Therefore, many users use weak, guessable, and repeated passwords. This leaves users and the institutions vulnerable to compromise and hacks.

**Purpose of the Study**

The purpose of the study is to evaluate alternatives to memorizing complex passwords using a quantitative method. The study will look at several security technologies in both software and hardware. In the software category, the study will evaluate some of the password managers with plugins and extensions for browsers and portable apps for mobile devices. In the hardware, the study will look at some biometric authentication devices and systems including fingerprint, face, iris, and heartwave. The study will try to review and evaluate several

technologies that are already out in the market. If the technology is still in beta or development stage, the study will try to include reviews and evaluations from other credible sources. The study will try to point out each technology's pros and cons to give a well and balance view.

**Assumptions of the Study**

**Definition of Terms**

**FIDO (fast identity online).** It is an open standard for authentication to a computer via biometric and a person's characteristics (Mendoza, 2015). A system equipped with FIDO will no longer require a user to type his/her password for login. For more information on the FIDO specification, check out the FIDO Alliance's specification web page, https://fidoalliance.org/specifications.

**BLE (Bluetooth low energy).** It is a new version of Bluetooth that used extremely low energy to operate. It is part of the official Bluetooth 4.0 specification.

**Password discovery.** It is the process of recovering lost password through various tools and methods.

**Social engineering.** It is a non-technical method of getting information from a user for the purpose of intrusion or hack. Social engineering relies heavily on human interaction and often tricking the user into breaking normal security measures.

**Limitations of the Study**

# Chapter II: Literature Review

## Introduction

Users are increasingly burdened with the task of memorizing more and more complex passwords. This leads many users to be careless about their passwords and potentially damaging to the user and their employers. The literature review will go through various technologies that will alleviate some of this burden on the users.

## Authentication Type

The three main factors of authentications are based on "what you know, what you have, and what you are" (Bartik, 2014; Gibson, 2011; Gorman, 2003). A classic example of something a person knows can be a password such as a word, phrase, or personal identification number (PIN) that is kept secret. Password authentication is one of the most widely used forms of authentication (Dole & Jadhao, 2013; SANS Institute, 2001). The second factor is "what you have" and it can be a thumb drive or smartcard that allows a user to authenticate. The third is "what you are" and that can be a person's fingerprints, iris, or heart wave.

### Password Authentication

An authenticator is a method of proving who a person says he or she is. It is a process that allows one entity to positively verify another user, device, or other identity in a computer system (Dole & Jadhao, 2013). The process of authentication can include a password, one-time passcode, security token, or biometric to aid in the process (Gorman, 2003). There are two types of authentication: human to machine and machine to machine. In the case of human to machine, a user has to interact with a device such as a computer or an ATM machine by providing a shared key secret that has been prearranged during registration or enrollment to get authenticated (Gorman, 2003). The second form of authentication is a machine verifying another machine's

identity without regard to the identity of the user (Gorman, 2003; Ma, Ren, Ren, & Yu, 2013). One example of the machine-to-machine authentication is in the single sign-on system where one system will automatically authenticate a user's initial login with multiple systems, if needed, to allow seamless login or workflow.

A password is the most widely used, but a password alone is the least secure and most vulnerable form of authentication (Dole & Jadhao, 2013; Florencio & Herley, 2007; Gorman, 2003; Ives, Walsh, & Schneider, 2004). By conventional wisdom, a user will choose the easiest password to remember, re-use passwords across multiple sites and devices, and forget their passwords (Florencio & Herley, 2007). If a person uses a weak password along with a strong encryption, his or her computer will still be vulnerable to spyware and other malicious password attacks (Flach, Kladko, & Laptyeva, 2011). Even if a person has a strong password, phishing and key logging can still cause problems (Flach et al., 2011). Thus, the vulnerabilities of password authentication have been increased greatly by the rise of phishing attacks. According to the Government Accountability Office, malicious software targeting mobile devices has increased from 14,000 to 40, 000 or about 185 percent in less than a year (Cooney, 2012). Some of these cases involved users who do not use the built-in mobile securities, and even if they did, they often picked the easiest password or PIN that can be guessed. Ten thousand passwords from Hotmail were leaked in 2009 and over 42 percent of the passwords were all lower case alpha characters containing six to nine characters only (Acunetx, 2014). About 15 to 20 percent of users regularly wrote down their passwords on a Post-it note and attached it to their computer monitor (Flach et al., 2011). Regardless of how strong the encryption is, the password is still the weakest link.

**Token-based Authentication**

Using passwords posed many threats; therefore, token-based authentication using a smart card with a security chip is a more secure alternative. A token-based authentication consists of "something that you know" and "something that you have" (Smart Card Alliance, 2003). It is a two-factor authentication system that is much more secure than just a password alone (SearchSecuritycom, 2008). The Smart Card uses a password with a dynamic ID or PIN number that uses a one-way hash function (Das, Gulati, & Saxena, 2004; Hwang & Li, 2000; Li & Hwang, 2010). The process allows the user to register the Smart Card or dynamic ID once and thereafter, there is no need to reregister or enter a password to authenticate. In some schemes, a timestamp is used to synchronize clocks on the user and system side to prevent replay attacks. The smart-card is a temper-resistant device and the information is only accessible if the user passes the verification. The card only has limited computational capability; therefore, if it is lost or stolen, there is not much an identity thief can retrieve. Hwang (2010) proposed a scheme where a user inputs his biometric information into the device and the system is able to compute a secret information with a password that corresponds to the user and store that information in an undisclosed location for the user's future authentication. Therefore, even if the Smart Card is lost or stolen, an identify thief would have a hard time trying to authenticate because the PIN or ID's secret information changes dynamically.

A Smart Card with a security chip can be used to access multiple physical and logical resources. The Smart Card is also capable of storing information about the user, paying a fee or a fair, certifying transactions, and tracking ID holder activities for audit purposes (Smart Card Alliance, 2003). Smart Card comes in a variety of forms and capability. A multipurpose Smart Card technology is able to support legacy access authentication as well as including a contact or contactless security chip. A contactless Smart Card does not require the card to physically make

contact with the card reader. The security chip implements a data security standard using triple Data Encryption Standard (DES) or Advance Encryption Standard (AES), all operation modes specified in the standard, and the flexibility to use the chip for banking and other related activities (De Man, Hoornaert, Vandewalle, & Verbauwhede, 1987; Englender, Solihin, Rogers, Prvulovic, & Yan, 2006). A Smart Card with both read/write and data storage is able to store privileges, authorizations, and attendance records (Smart Card Alliance, 2003). PIN and biometric information can be stored in the chip offering two or three-factor authentication capabilities for better security.

**Biometric Based Authentication**

The biometric authentication is a more reliable indicator of identity than legacy systems such as password and PINs. The biometric falls in the "who you are" classification and can be subdivided into physiological and behavioral approaches (Weaver, 2006). The biometric authentication is an automatic, real-time, and non-forensic form of the broader human identification methodology (Wayman, 2001). Biometric authentication is a more attractive alternative to password or tokens because it cannot be forgotten or stolen (Akkermans et al., 2005). The biometric authentication process involves scanning the sample, storing the sample as a template in the system, and verifying the user provided biometric identification against the stored template to authenticate.

The physiological approach includes fingerprint; iris and retina scans; hand, finger, face, and ear geometry; hand vein and nail bed recognition; DNA; and palm prints (Weaver, 2006). However, fingerprint and iris scanning are the most widely used form of biometric authentication. Fingerprint usage has been found in clay seals attached to business documents since the days of the ancient Babylon to secure commercial transactions (Weaver, 2006).

Fingerprints contains the unique characteristics of ridge endings and bifurcation known as minutiae points (Bolle, Hong, Jain, & Pankanti, 1997; Wayman, 2001; Weaver, 2006). Fingerprint scanners can be attached to a device via a USB device or embedded such as some of the later version of smart phones, tablets, and laptops.

Iris scanning as an authentication alternative is even more accurate than fingerprint because the iris has about 260 degrees of freedom with regard to its vein patterns (Kumar & Ryu, 2008; Wayman, 2001; Weaver, 2006). The iris pattern are isolated from external environments and remain unchanged through the life of the person. The randomness of the iris pattern are unique even for identical twins (Kumar & Ryu, 2008; Weaver, 2006) which makes it a very attractive method of authentication. A person's right eye iris patterns are different from his/her left so enrolling the right eye and trying to authenticate with the left eye will fail. Even if a person is wearing glasses or contacts, it will not affect the authentication.

Voice authentication is the process of identifying a person by his or her voice. According to Liu and Silverman (2001), voice authentication is based on voice-to-print authentication by transforming voice to texts. In a text dependent authentication system, the recognition system must have prior information about the text to be spoken by the user and it is expecting the user to speak this exact text back to the recognition system (Bigun, Gonzalez-Rodriguez, Reynolds, & Ortega-Garcia, 2005). These prior texts or commands must have already been established for the recognition system to work. On the other hand, a text-independent is more flexibility. For example, it allows the speaker to be verified while he or she is conducting other speech interactions. There is no need to speak only pre-recorded set of texts. The acoustics of a person's voice contains both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style) (Kumar & Ryu, 2008). Since most

computers and smart devices already have microphone and audio card, voice authentication is desirable because all it needs are just software updates (Lawton, 1998). There is no new hardware requirement and can be delivered by landline or mobile phone (Akram, Kaman, Swetha, & Varaprasad, 2013).

Face authentication or recognition is the analysis of facial characteristics. Facial recognition is one of the most acceptable form of authentication because human face is always bare and is often use for visual interactions (Ando, Kurihara, & Zhan, 2006). Facial recognition involves the challenging area of artificial intelligence, computer vision, pattern recognition and image sensing (Ando et al., 2006). The method usually involves capturing a facial image (Liu & Silverman, 2001) and digitizing that image as template for future authentication. In the past two decades most capture facial image captured are in 2D (Pan, Wu, & Wu, 2003) but recently there are technologies in capturing 3D facial real-time imaging system based on correlation image sensor (CIS) that could provide a rich set of depth and surface information (Ando et al., 2006). The use of CIS result in a depth map that has the advantages in a) robustness to the variation of the illumination condition, (b) robustness to the variation of the pose, and (c) capability of rejecting impostor with highly reliability (Ando et al., 2006).

Heartwave is a relatively new biometric authentication technology by capturing the person's heartbeat in the form of electrocardiogram recording (ECG). The ECG of a person's heartbeat is unique due to the change in size, position, and anatomy of the heart, chest configuration, and various other factors (Hegde et al., 2011). Heartwave or ECG can be used as an authentication alternative because a heartbeat signal is unique to each person and stable over long periods of time. Every living person must have a heart and the heartbeat can be captured from the hand, liveness is an inherent property of this modality, and it is difficulty to steal or

mimic a heartbeat (Md Saiful Islam, 2014). Other biometric authentications such as password, PIN, and Smart Card can be stolen, lost, replayed attacks, and man-in-the-middle attacks. By using heartbeat as an authentication mechanism, it resist many of these weaknesses.

## Password Alternatives

There are several ways that password alternative can be achieved. These includes password managers and services, hardware, and a combination of both software and hardware. Some password managers provide plugins or extensions that work across different devices and platform. In the hardware alternative, some work wirelessly via Bluetooth, Bluetooth Low Energy, and Wi-Fi. While in the hybrid scenario, it requires software to be installed and updated on the computer or device.

### Software and Services

Among the top password managers, LastPass and Dashlane ranked in the top three with 1Password as number one (Ferrill, 2014; Parker, 2014; Rubenking, 2015) and Keepass is not far behind others. Password managers such as these has the capability to auto populate forms and web logins (Ferrill, 2014). With 20, 30 or sometimes 100+ different kinds of logins, these password managers come in very handy. Not only is it good for auto populate forms and logins, it is "cross-platform and cross-browser synchronization, mobile device support, secure sharing of credentials, and support for multifactor authentication" (Ferrill, 2014, para. 5). KeePass and 1Password can synchronize to online storage services such as DropBox. One of the greatest features of many password manager is the capability auto generate random passwords with 256-bit AES encryption (Parker, 2014). LastPass also have a few tricks up its sleeve such as the LastPass for Application (Rubenking, 2015) and being to store various secure notes. The LastPass for Application uses a plugin that sits in the system tray and the user can train the

software to autofill an application's login screen with a password. Dashlane and LastPass also support Google Authenticate and the ability to work with Apple's Touch ID authentication (Rubenking, 2015). Okta is a single sign on and access management service for the enterprise that uses cloud services and web applications on a daily basis (Sturdevant, 2012). Once logged into Okta, users are presented with app like icons to be clicked to launch. Okta also provide IT administrators the capability to manage user accessibility and monitor software as service (SaaS) resources (Sturdevant, 2012). If when Okta is integrated with Windows Active Directory, all the user has to remember is their daily login user name and password they would be able to access both third party services as well as hosted services (Gohring, 2011). Since Okta has over 1,200 cloud and Web app services, this makes it desirable and easier for organizations to adopt and allows IT administrators to look at what resources are being used the most for better negotiation (Dignan, 2011).

**Hardware**

When it comes to an alternative to password memorization, hardware authentication may be the best option. These includes three types of technologies; USB, Bluetooth, and blue tooth low energy (BLE). Many may know or have used a USB device before but the difference between Bluetooth and BLE is that while BLE is still within the Bluetooth 4.0 umbrella; however, it uses a totally new technology (Nilsson & Saltzstein, 2012). The main feature of a BLE is its ultralow energy usage. A CR2032 battery is able to power a small device for five to ten years (Nilsson & Saltzstein, 2012).

Two of the hardware password managers includes Sesame 2 and EveryKey. The Sesame 2 is small enough to fit in a user's keychain or slips into his or her pocket. The Sesame 2 key fob can be paired to a Mac over Bluetooth (Logan, 2016). The Sesame 2 has two settings, near and

far, for customizing the proximity of triggering the lock and unlock screen when the user walks away from the computer (Cole & Monday, 2013). The EveryKey works similar to the Sesame 2 except it is a wristband wearable. If the EveryKey were ever stolen or lost, the user can easily disabled it from the Internet (NDTV Correspondent, 2014). The EveryKey stores the password on the Everykey server instead of on the device itself for security (Lomas, 2014).

The Nymi and Arkami myIDKey are among other hardware authentications. The main difference between the myIDKey is that the device works over Wi-Fi or connect to the computer via USB (Fahmiday Y. Rashid, 2014) instead of Bluetooth like other devices. The passwords are actually stored in the myIDKey 16GB USB device with a AES256 encryption (Gloria, 2013; Kooser, 2013). The Nymi on the other hand uses Bluetooth low energy (BLE) for communication and heartbeat or ECG for biometric authentication. The device is a wearable wristband that authenticates that has six axis sensors that can be used to unlock car if the user wants to (Lomas, 2013; Pierce, 2013). Not only is Nymi use for password authentication, it can also be used as a remote control for a user's Netflix account (Santus, 2014). Nymi seems to be the ultimate device for password memorization alternative.

**Hybrid**

The combination of hardware and software makes it attractive solution password authentications. Hybrid solutions for authentications include devices like Knock, Nok Nok, MyLok, SplashID Key Safe, and Yubikey. Knock is a software that works on Apple's operating system. The software is installed on the Mac machine and the iOS app is running on the iPhone, iPod, or iPad device. When in proximity, the user will knock on their iOS device and that will unlock the Mac computer thus avoiding entering a password. The software and hardware hybrid solution works from within 20 feet away from the Mac computer and uses BLE so it would not

drain the battery off of the iDevices (Warren, 2013). The Nok Nok authentication software uses a protocol developed by the Fast IDentity Online Alliance (FIDO) (Counter, 2014; Messmer, 2013). The Nok Nok Labs developed and uses the Online Security Transaction Protocol (OSTP) to go beyond simple user passwords and logins with a much stronger multi-factor identity verification before allowing web access or online transaction to occur. Nok Nok is not only convenient but secure. It works by sharing the secret between the back-end server and the device to authenticate a user (Messmer, 2013). MyLok manages and stores the user's credentials in the 8GB USB typed device that has a 36KB of EEPROM onboard cryptographic processor chip for security (Rubenking, 2011). The SlashID Key Safe is a software and an optional USB stick for password manager (Rubenking, 2010). SplashID Key Safe also utilized Apple's Touch ID for authentication to its password manager app for secure access. Yubikey is a USB keychain type of password manager that sends a static password after the user touched the sensor end of the stick and dynamically-generate a one-time password to any application that is listening for its input (Rubenking, 2009). This prevents any key logger software from capturing the password because the password will be discarded after the session is over.

**Caveat**

These solutions are not without faults or caveats. Software password manager post certain burdens on the user's ability to install, update, and manage. Even though the problem was fixed in LastPass and four other web-based password managers, researchers found critical defects in all of them. The serious defect allows remote user to siphon the password from plaintext passcode from a user's wallet with no of anything going wrong (Goodin, 2014). Another possible vulnerability is when a user enters his or her credentials on a compromised website, an attacker can easily grabbed the information.

Hardware solutions also have their share of frustrations and issues. Since biometric measures a unique characteristic of the user, it faces accuracy issues due to noise to signal ratios (Kumar & Ryu, 2008). Regardless of fingerprint, voice, iris, facial, or heartbeat, there is always a chance of introducing noise during the capturing of the signal or image. Other issues involve a person's finger being cut, burned, stained etc. and the readers would not be able to read (Duncan, 2013). Voice and iris recognition also faces the same challenge, not to mention the cost of the scanner or reader and once it is compromised, it is permanent (Duncan, 2013) .

Hybrid solutions that include both hardware and software face similar fate. On the hardware side, the device can be stolen, lost, or compromised. Since many of these hardware devices use Bluetooth that means both devices must already have Bluetooth chip embedded or connected externally (Lomas, 2014). Many software hardware hybrid do not work across different platforms, brand, versions, and operating systems (Lomas, 2014; Rubenking, 2009). Hybrid solution requires the software to be installed either one or both machines, it is not very practical when accessing a computer that does not belong to the user such as at public places or a friend's computer (Seltzer, 2013).

## Chapter III: Methodology

As more mobile devices such as wearables, smart phones, phablets, tablets, and Internet of Things (IoT) are getting more into the hands of consumers, to the complexity in authenticating one's identity to access the devices and its functionalities has increased. As discussed in the previous chapter, there are several alternatives to securing these devices via passwords. This chapter will discuss the methodology in evaluating some of the alternatives.

**Subject Selection and Description**

After the approval of Institute Review Board (IRB) from UW-Stout, recruiting students, faculty, and staff will start. The target sample size is at least 30 participants who meet the criteria. The criteria for participation requires that the participants must have an iPhone or Android smartphone with finger print authentication and use at least three different user names and passwords per day. On the survey, the participant will require to list his or her department, major, and status (whether he/she is student, and faculty/staff), gender, and age.

**Instrumentation**

As of this this study, some of the devices are not available for consumers. They are still in beta testing or too expensive to purchase for evaluations; therefore, this study will not be evaluating Nymi, Nok Nok, MyLock, myIDKey, Everykey, and Sesame 2. The study will use LastPass, Dashlane, KeePass, Okta, Knock, and TouchID. The LastPass, Dashlane, KeePass, and Okta will represent the software category. Since many of the hardware authentication devices are not available for testing, Apple TouchID, Android, or Windows fingerprint authentication will represent the biometric category. SplashID Pro and Knock will represent the hybrid category. Participants will use the finger print authentication capability on their smart phone in combination with some of the applications listed above. See Appendix A for the survey.

**Data Collection Procedures**

To collect the data an email will be sent to all students, faculty, and staff regarding the study with the requirements stated above. Participants who are interested will receive the informed consent form in the email, instructions on the six different technology alternatives, and links to download the apps.

The participants will evaluate the various technology alternatives for two weeks. They will involve in registering the device and/or software, installing, and upgrading if necessary. The participants' task is to use the six technology alternatives to manage their passwords and authenticate web and computer logins. Each of the participants must have 10 or more logins to manage. After the two weeks, an email will be sent to each participant to take the survey via UW-Stout's Qualtrics. The survey will try to determine three key categories: usability, accuracy, and maintenance. The survey is listed in Appendix A below. The data gathered from this survey will be tallied and use in the data analysis. Any identifiable information about a particular participant will be stripped out for the final result.

**Data Analysis**

The data analysis will involve ranking which alternative technologies are most preferred and among which group of participants. The study will look if there is any correlation between the preferred alternative technology and the participant's gender, major, department, and status (student, faculty, and staff). The study will add all the ratings and find out which technology rank the highest in the three categories: usability, accuracy, and maintenance.

**Limitations**

The limitation of this study may not apply to the general public since all the participants are from UW-Stout only. Although the study does try to get a wide range of participants, the participants may be influence by the level of their experience, education, and preference or methods of using the technology. The distance between each interval ranking may be uneven. There is no guarantee that between Excellent and Good equals Fair and Good.

## References

Acunetx. (2014). Weak password vulnerability: More common than you think, 1–5. Retrieved from http://www.acunetix.com/blog/articles/weak-password-vulnerability-common-think/

Akkermans, A., Bazen, A., Kevenaar, T., Schrijen, G.-J., Tuyls, P., & Veldhuis, R. (2005). Practical biometric authentication with template protection. *Audio- and Video-Based Biometric Person Authentication*, 436–446. http://doi.org/10.1007/11527923_45

Akram, S., Kaman, S., Swetha, K., & Varaprasad, G. (2013). Remote user authentication using a voice authentication system. *Information Security Journal: A Global Perspective*, *22*(3), 117–125. http://doi.org/10.1080/19393555.2013.801539

Ando, S., Kurihara, T., & Zhan, S. (2006). Facial authentication system based on real-time 3D facial imaging by using correlation image sensor. *Sixth International Conference on Intelligent Systems Design and Applications*, *2*, 396–400. http://doi.org/10.1109/ISDA.2006.253869

Bartik, C. (2014, January 10). 3 different types of user authentication. Retrieved from http://www.cloudentr.com/latest-resources/industry-news/2014/1/10/3-different-types-of-user-authentication

Bigun, J., Gonzalez-Rodriguez, J., Reynolds, D., & Ortega-Garcia, J. (2005). Authentication gets personal with biometrics, *21*(2), 75–80. http://doi.org/http://dx.doi.org/10.1109/MSP.2004.1276113

Bolle, R., Hong, L., Jain, A., & Pankanti, S. (1997). Identity authentication using fingerprints. ... *Biometric Person Authentication*. Retrieved from http://link.springer.com/chapter/10.1007/BFb0015985

Campbell, J., Kleeman, D., & Ma, W. (2011). Impact of restrictive composition policy on user password choices. *Behaviour & Information Technology*, *30*(3), 379–388. http://doi.org/10.1080/0144929X.2010.492876

Cole, S., & Monday, C. (2013, November 4). New bluetooth accessory ' Sesame ' automatically locks your Mac when you step away. Retrieved from http://appleinsider.com/articles/13/11/04/new-bluetooth-accessory-sesame-automatically-locks-your-mac-when-you-step-away

Cooney, M. (2012). 10 common mobile security problems to attack, 1. Retrieved from http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

Counter, P. (2014, April 22). Nok Nok Labs selected to power Galaxy S5 mommerce. Retrieved from http://mobileidworld.com/nok-nok-labs-selected-to-power-galaxy-s5-mcommerce/

Das, M. L., Gulati, V. P., & Saxena, A. (2004). A dynamic id-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*, *50*(2), 629–631. http://doi.org/10.1109/TCE.2004.1309441

De Man, H. J., Hoornaert, F., Vandewalle, J., & Verbauwhede, I. (1987). Security and performance optimization of a new DES data encryption chip. *IEEE Journal of Solid-State Circuits*, *23*(3), 647–656. http://doi.org/10.1109/4.302

Dignan, L. (2011, December 15). Okta launches self-service cloud single sign-on provisioning. Retrieved from http://www.zdnet.com/article/okta-launches-self-service-cloud-single-sign-on-provisioning/

Dole, L., & Jadhao, P. (2013). Survey on authentication password techniques, (2), 67–68. Retrieved from http://www.ijsce.org/attachments/File/v3i2/B1430053213.pdf

Duncan, G. (2013). Why haven't biometrics replaced passwords yet? *March 9*. Retrieved from http://www.digitaltrends.com/computing/can-biometrics-secure-our-digital-lives/#!E61ae

Eddy, M. (2013, March 14). Infographic: Everyone is carrying too many mobile devices. Retrieved February 18, 2015, from http://securitywatch.pcmag.com/none/309173-infographic-everyone-is-carrying-too-many-mobile-devices

Englender, D., Solihin, Y., Rogers, B., Prvulovic, M., & Yan, C. (2006). Improving cost, performance, and security of memory encryption and authentication. *Proceedings - International Symposium on Computer Architecture*, *2006*, 179–190. http://doi.org/10.1109/ISCA.2006.22

Fahmiday Y. Rashid, N. J. R. (2014, May 23). Arkami myIDKey. Retrieved from http://www.pcmag.com/article2/0,2817,2458385,00.asp

Ferrill, T. (2014, June 18). Review: The best password managers for PCs, Macs, and mobile devices. Retrieved from http://www.infoworld.com/article/2607798/security/review--the-best-password-managers-for-pcs--macs--and-mobile-devices.html

Flach, S., Kladko, K., & Laptyeva, T. V. (2011). The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs, *50007*, 5. http://doi.org/10.1209/0295-5075/95/50007

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web - WWW '07*, 657. http://doi.org/10.1145/1242572.1242661

Gibson, D. (2011, June 6). Understanding the three factors of authentication. Retrieved from http://www.pearsonitcertification.com/articles/article.aspx?p=1718488

Gloria, B. (2013, June 29). MyIDkey fingerprint-protected, voice-searchable USB drive available for pre-order. Retrieved from http://www.digitaltrends.com/computing/myidkey/

Gohring, N. (2011, January 27). Okta' s service offers single sign-on for all cloud apps. Retrieved from http://www.pcworld.com/article/217927/article.html

Goodin, D. (2014, July 14). " Severe " password manager attacks steal digital keys and data en masse. Retrieved from http://arstechnica.com/security/2014/07/severe-password-manager-attacks-steal-digital-keys-and-data-en-masse/

Gorman, L. (2003). Comparingpasswords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), 2020–2021. http://doi.org/10.1109/JPROC.2003.819611

Hegde, C., Patnaik, L. M., Prabhu, H. R., Sagar, D. S., Shenoy, P. D., & Venugopal, K. R. (2011). Heartbeat biometrics for human authentication. *Signal, Image and Video Processing*, *5*(4), 485–493. http://doi.org/10.1007/s11760-011-0252-6

Hwang, M.-S. H. M.-S., & Li, L.-H. L. L.-H. (2000). A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, *46*(1), 46–52. http://doi.org/10.1109/30.826377

Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75–78. http://doi.org/10.1145/975817.975820

Kelly, H. (2014). "123456" tops list of worst passwords. *Cnn*, 2. Retrieved from http://www.cnn.com/2014/01/22/tech/web/most-common-passwords/

Kooser, A. (2013, February 20). Biometric USB password key worthy of ’ Mission: Impossible '. Retrieved from http://www.cnet.com/news/biometric-usb-password-key-worthy-of-mission-impossible/

Kumar, D., & Ryu, Y. (2008). A brief introduction of biometrics and fingerprint payment technology. *Proceedings of the 2008 2nd International Conference on Future Generation Communication and Networking, FGCN 2008*, *3*, 185–192. http://doi.org/10.1109/FGCNS.2008.11

Lawton, G. (1998). Biometric: A new era in security. *Computer*, 16–18. http://doi.org/10.1109/MC.1998.707612

Li, C.-T., & Hwang, M.-S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, *33*(1), 1–5. http://doi.org/10.1016/j.jnca.2009.08.001

Liu, S., & Silverman, M. (2001). Practical guide to biometric security technology. *IT Professional*, *3*(1), 27–32. http://doi.org/10.1109/6294.899930

Logan, M. (2016, February 16). A wireless sensor that locks your Mac when you walk away. Retrieved from http://www.wired.com/2015/02/atama-sesame-2/

Lomas, N. (2013, September 3). Nymi is a heartwave-sensing wristband that wants to replace all your passwords & Keys.

Lomas, N. (2014, November 8). Everykey wants to put your passwords on your wrist. Retrieved from http://techcrunch.com/2014/11/08/everykey/

Ma, L., Ren, W., Ren, Y., & Yu, L. (2013). How to authenticate a device? Formal authentication models for M2M communications defending against ghost compromising attack.

*International Journal of Distributed Sensor Networks*, *2013*. http://doi.org/10.1155/2013/679450

Md Saiful Islam. (2014). Heartbeat biometrics for remote authentication using sensor embedded computing devices, (i). Retrieved from http://www.hindawi.com/journals/ijdsn/aa/549134/

Mendoza, M. (2015, February 19). Windows 10 aims to kill the password with biometric authentication support. Retrieved February 20, 2015, from http://www.techtimes.com/articles/33624/20150219/windows-10-aims-to-kill-the-password-with-biometric-authentication-support.htm

Messmer, E. (2013, February 12). Startup Nok Nok Labs pitches strong new authentication process. Retrieved from http://www.networkworld.com/article/2163448/security/startup-nok-nok-labs-pitches-strong-new-authentication-process.html

NDTV Correspondent. (2014, November 6). The Everykey is a wristband that wants you to stop remembering passwords. Retrieved from http://gadgets.ndtv.com/wearables/news/the-everykey-is-a-wristband-that-wants-you-to-stop-remembering-passwords-617005

Nilsson, R., & Saltzstein, B. (2012, June 8). Bluetooth low energy vs. classic bluetooth: Choose the best wireless technology for your application. Retrieved from http://www.medicalelectronicsdesign.com/article/bluetooth-low-energy-vs-classic-bluetooth-choose-best-wireless-technology-your-application

Pan, G., Wu, Y., & Wu, Z. (2003). *Face authentication based on multiple profiles extracted from range data*. *Springer-Verlag Berlin Heidelberg*. Zhejiang University, Hangzhou. Retrieved from http://dl.acm.org/citation.cfm?id=1762222.1762291

Parker, J. (2014, April 18). Take control of password chaos with these six password managers. Retrieved from http://www.cnet.com/news/best-password-managers/

Paul, I. (2015, February 15). Windows 10 embraces password-killing biometric authentication. Retrieved February 18, 2015, from http://www.pcworld.com/article/2884886/windows-10-embraces-password-killing-biometric-authentication.html

Pierce, D. (2013, September 3). This bracelet could replace your passwords, your car keys, and even your fingerprints. Retrieved from http://www.theverge.com/2013/9/3/4688162/bionym-nymi-could-replace-all-your-passwords

Rubenking, N. J. (2009, April 9). What's a YubiKey? Cheap, solid security. Retrieved from http://www.pcmag.com/article2/0,2817,2345571,00.asp

Rubenking, N. J. (2010, December 14). SplashID Key Safe. Retrieved from http://www.pcmag.com/article2/0,2817,2374312,00.asp

Rubenking, N. J. (2011, September 19). MyLOK. Retrieved from http://www.pcmag.com/article2/0,2817,2393156,00.asp

Rubenking, N. J. (2015, February 18). The best password managers for 2015. Retrieved from http://www.pcmag.com/article2/0,2817,2407168,00.asp

SANS Institute. (2001). An overview of different authentication methods and protocols. Retrieved from http://www.sans.org/reading-room/whitepapers/authentication/overview-authentication-methods-protocols-118

Santus, R. (2014, November 4). This wristband works with your heartbeat to pay for things. Retrieved from http://mashable.com/2014/11/04/wristband-heartbeat-payments/

SearchSecuritycom. (2008, November). Security token and smart card authentication. Retrieved from http://searchsecurity.techtarget.com/tip/Security-token-and-smart-card-authentication

Seltzer, L. (2013). Apple's keychain: The solution and the problem with password managers. Retrieved from http://www.zdnet.com/article/apples-keychain-the-solution-and-the-problem-with-password-managers/

Smart Card Alliance. (2003). *Using smart cards for secure physical access*. *Security*. Retrieved from https://www.library.ca.gov/crb/rfidap/docs/SCA-Physical_Access_Report.pdf

Sturdevant, C. (2012, March 19). Okta boosts single sign-on for SaaS. Retrieved from http://www.eweek.com/c/a/Cloud-Computing/Okta-Boosts-SingleSign-On-for-SaaS

Wailgum, T. (2008, September 9). Too many passwords or not enough brain power? Retrieved February 17, 2015, from http://www.pcworld.com/article/150874/password_brain_power.html

Warren, C. (2013, November 5). Tap your iPhone to pnlock your Mac with Knock. Retrieved from http://mashable.com/2013/11/05/knock-unlock-app/

Wayman, J. L. (2001). Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics*, *01*(01), 93–113. http://doi.org/10.1142/S0219467801000086

Weaver, A. C. (2006). Biometric authentication. *Computer*, *39*(2), 96–97. http://doi.org/10.1109/MC.2006.47

## Appendix A: Survey Questions

Please rate each of the following survey questions. The options are Excellent (4), Good (3), Fair (2), Poor (1), and Not Applicable (0).

1. Please rate which of the technology work faster.
    a. LastPass: Rank
    b. Dashlane: Rank
    c. KeePass: Rank
    d. Okta: Rank
    e. Knock: Rank
    f. Fingerprint (e.g. TouchID): Rank
2. Please rate which of the technology is the easiest to use.
    a. LastPass: Rank
    b. Dashlane: Rank
    c. KeePass: Rank
    d. Okta: Rank
    e. Knock: Rank
    f. Fingerprint (e.g. TouchID): Rank
3. Please rate which one has the best features?
    a. LastPass: Rank
    b. Dashlane: Rank
    c. KeePass: Rank
    d. Okta: Rank
    e. Knock: Rank

   f. Fingerprint (e.g. TouchID): Rank

4. Rate which one has the best interface?
   a. LastPass: Rank
   b. Dashlane: Rank
   c. KeePass: Rank
   d. Okta: Rank
   e. Knock: Rank
   f. Fingerprint (e.g. TouchID): Rank
5. Rate which one requires the least intervention to operate.
   a. LastPass: Rank
   b. Dashlane: Rank
   c. KeePass: Rank
   d. Okta: Rank
   e. Knock: Rank
   f. Fingerprint (e.g. TouchID): Rank
6. Rate which technology alternatives has the best authentication success.
   a. LastPass: Rank
   b. Dashlane: Rank
   c. KeePass: Rank
   d. Okta: Rank
   e. Knock: Rank
   f. Fingerprint (e.g. TouchID): Rank
7. Please rate which alternatives you feel provide the most password security.

   a. LastPass: Rank
   b. Dashlane: Rank
   c. KeePass: Rank
   d. Okta: Rank
   e. Knock: Rank
   f. Fingerprint (e.g. TouchID): Rank

8. Rate which one take the least time to authenticate.
   a. LastPass: Rank
   b. Dashlane: Rank
   c. KeePass: Rank
   d. Okta: Rank
   e. Knock: Rank
   f. Fingerprint (e.g. TouchID): Rank
9. Rate which one works best for web browser.
   a. LastPass: Rank
   b. Dashlane: Rank
   c. KeePass: Rank
   d. Okta: Rank
   e. Knock: Rank
   f. Fingerprint (e.g. TouchID): Rank
10. Rate which one has the least error.
   a. LastPass: Rank
   b. Dashlane: Rank

c. KeePass: Rank

d. Okta: Rank

e. Knock: Rank

f. Fingerprint (e.g. TouchID): Rank

11. Rate which one is the easiest to install?

a. LastPass: Rank

b. Dashlane: Rank

c. KeePass: Rank

d. Okta: Rank

e. Knock: Rank

f. Fingerprint (e.g. TouchID): Rank

12. Rate which one is the easiest to upgrade?

a. LastPass: Rank

b. Dashlane: Rank

c. KeePass: Rank

d. Okta: Rank

e. Knock: Rank

f. Fingerprint (e.g. TouchID): Rank

13. Rate which one takes the least of time to setup before you're able to use it.

a. LastPass: Rank

b. Dashlane: Rank

c. KeePass: Rank

d. Okta: Rank

e. Knock: Rank

f. Fingerprint (e.g. TouchID): Rank

14. Rate which one is the easiest to uninstall.

a. LastPass: Rank

b. Dashlane: Rank

c. KeePass: Rank

d. Okta: Rank

e. Knock: Rank

f. Fingerprint (e.g. TouchID): Rank

15. Please rate which one provides the best information such as online help, on-screen messages, and other documentation.

a. LastPass: Rank

b. Dashlane: Rank

c. KeePass: Rank

d. Okta: Rank

e. Knock: Rank

f. Fingerprint (e.g. TouchID): Rank

## Appendix B: Second Appendix