Usability Case Study: Reduce an Organization’s Usage of Text-based Passwords by Using Built-in Device Hardware for User Authentication

James Sicuranza
Seidenberg School of CSIS, Pace University, White Plains, New York

Abstract—Despite advances in biometrics and other device authentication technologies, password base authentication remain the most commonly used means of authentication in computer systems. Today’s hardware opens avenues for new authentication techniques that go beyond text passwords. In the common workplace biometrics (facial recognition) can be utilized as the primary authentication method for laptops and tablets considering the built-in camera. Another already in place technology is the smartphone that can double as a wireless key using Bluetooth to access the workstation without the need to type in the password. This study is to investigate the usability and feasibility in using alternative technologies to replace text based passwords at the workplace. We will examine the acceptance of these password alternatives to minimize the use of text base passwords, a hybrid approach, and determine whether the user community will accept these already in place technologies.

1. INTRODUCTION

Research has demonstrated that passwords are plagued by security problems and openly hated by users [1]. To help with progress the user community should have knowledge regarding both passwords and their alternatives [2]. However, among other challenges, unbiased evaluation of password replacement schemes is complicated by the diverse interests of various communities. In my experience, security experts focus more on security but less on usability and practical issues related to deployment; biometrics experts focus on analysis of false negatives and naturally-occurring false positives rather than on attacks by an intelligent, adaptive adversary; usability experts tend to be optimistic about security; and originators of a scheme, whatever their background, downplay or ignore benefits that their scheme doesn’t attempt to provide, thus overlooking dimensions on which it fares poorly. The password management problem is aggravated by users need to maintain multiple accounts from diverse websites and multiple devices that require passwords.

With the growing popularity of mobile computing applications and using them to accessing corporate data, such as email, file share portals, and other transactional applications, protecting user credentials on mobile devices is becoming increasingly important. Most mobile devices today make use of traditional text-based password schemes to authenticate a user. The use of mobile devices expands the use of the corporate user account to access corporate data therefore passwords are used even more so today than before. At the workplace a typical user is assigned a laptop or desktop computer, a smartphone device, and a tablet. This means a typical user will have three different devices to access corporate data with text base passwords versus a traditional one office PC. These multiple platforms that storing passwords can cause problems when it comes to simple password resets.

2. PROBLEM STATEMENT

At NBCUniversal, a media company, the employee user account depend solely on text base password to access their device or workstation. Majority of users will carry a laptop device, own two small devices (smartphone and tablet), and have a home base Workstation device. The workplace application will be installed on all of these devices with their text base password. Company policy will reset the password every 60 days. The user must check every device to ensure the password is change correctly. If the user misses a device, that device can potentially lock out the user account by auto sending the expired password. Secondly, on these devices there are multiple business application that require authentication, these credentials can be saved in credential manager on the operating systems or nested inside the application. When the password cycle hits, the user must remember which application to reset the password. Again, if the user misses to reset a password for a particular application, the device or application in question could continuously send the expired password in which will lock out the user.

NBCUniversal has approximately 40,000 users, and on daily basis there are substantial number of users need to do the password reset cycle. The pain point is to ensure every device an application is correctly reset. The Help Desk is busy to assist users with their reset since they can’t find which device is locking them out. There are ways to track the device that is locking the account, but as devices are more mobile it’s more
challenging to track the culprit as they can be on or off the corporate network throughout the day.

The problem is amplified in finding why the user’s account is locked from the system after they just change their cycled password. Here is a list of different passwords that are stored for a typical user:

1. IPhone – email application
2. IPad – email application
3. Laptop – general access
4. Remote Desktop - remote usage
5. Wi-Fi access – secure access
6. Drive mappings
7. Key chain applications
8. Drop Box – cloud service for file sharing

The 60 day policy is a security measure to strengthen the password policy, but it is not designed for today’s multiple entry points (8 entry points listed above), as this bring out a great deal of pain to ensure all access points passwords are synced. This study will investigate ways to minimize the use of text passwords, to avoid 60 day password resets on various devices, and at the same time improve the security access at the workstation.

3. KEY IDEA

Biometrics can be used as a technique to provide authentication. This technique is based on a unique characteristic of a person that provides an improvement on the current authentication. Biometrics is identification and verification of individual based on human characteristics. Biometric approaches are typically subdivided into two categories: physiological and behavioral biometrics. Physiological biometric is based on bodily characteristics, such as fingerprint, facial recognition, and iris scanning. Behavioral biometric is based on the way people do things, such as keystroke dynamics, mouse movement, and speech recognition. We can use one of these types of biometrics as a strong authenticating method for general login to access the workplace applications.

People today carry smart phones essentially everywhere they go. According ComScore Report April 2014 US Market Subscriber Share, 167.9 million people in the U.S. owned smartphones (69.6 percent mobile market penetration) during the three months ending in April 2014, up 5 percent since January. Apple ranked as the top OEM with 41.4 percent of U.S. smartphone subscribers. Samsung ranked second with 27.7 percent market share (up 1 percentage point from January), followed by LG with 6.5 percent, Motorola with 6.3 percent and HTC with 5.3 percent. [3] The commonality of smartphone ownership can be used at the workplace as a means of an authentication device.

We can use these current cost effective technologies as a mechanism to minimize the use of password, not eliminate of passwords altogether, but to minimize their usage. Laptops and tablets come with cameras for video chatting, microphones, and built-in Bluetooth transmitters to attach wireless devices. These three pieces of hardware can be taken advantage as a means in accessing your station. The camera can be used for facial recognition as an individual biometric. The mobile device is something you have with you at all-time this can be used as a wireless key to access the station, an off device authentication through Bluetooth.

The key idea is to execute these already built-in hardware technologies as means of authenticity in a real work environment. To do a case study at the workplace environment on the user acceptance that these technologies in fact can minimize the use of typing in text base passwords at their workstation. If we can minimize the use of passwords then password alternatives could be adaptive in the today’s workplace.

3.1 Technology

We will use three software technologies listed below to load on the user’s PC or MAC laptop:

A. Facial Recognition

The facial recognition software will use the built-in camera on the lid of the laptop. The live camera will verify the user’s face to permit access.

B. Proximity Software

This software is loaded on the user on the laptop and will require a mobile phone with Bluetooth technology to act as the secure key to access the PC or MAC Laptop. When the phone is within 1-5 feet proximity, the user will gain access.

C. Voice Recognition

The Voice recognition software will use the built-in speaker on the laptop. The live speaker will verify the user’s voice to permit access.

4. HYPOTHESIS

1. In a corporae work environment, users will accept password alternatives if they are simple enough to integrate with their daily access of their workstation.
2. User will accept password alternatives even with a moderate failure rate if they can simply fall back on text base passwords.
3. We can reduce the use of typing the text base passwords in accessing their workstation by 5%.
4. Many (most) users will prefer password alternatives.

5. METHODOLOGY

The nature of the research is to focus on a concentrated group of users that are somewhat context free. The purpose of this research is to confirm and validate that these technologies are easy to use as means to minimize the use of passwords. We will use a Qualitative approach with questionnaires and ratings of the data. The data will be statistically analyzed with deductive
reasoning. The data will be communicated through statistics, aggregated style, and explained in a formal voice.

5.1 Study Settings – User Population

We will assign 20 participants for 20 business days to use each of the three technologies. At NBCUniversal, 24% of the org structure makes up of leadership positions, meaning this position will have at least one direct report. The other 75% are non-leadership roles. We will breakdown the 20 participants in the same format:

- 15 of the 20 participants will be non-leadership role
- 5 of the 20 participants will be in a leadership role

We will have an engineer setup the software for the user and show them how to use it on daily bases. We will instruct the user not to remove the software as it must be used throughout the study. We will ask a set of pre-study interview questions of the participants in finding out how many times a day they type in their password.

5.2 Data Capture

We will use the System Usability Scale (SUS) [4], a usability evaluation metric developed at Digital Equipment Corp., to rate the usability of the three technologies by asking participants to respond to ten statements on a Likert scale (Figure 1). We included these statements as part of the survey we administered to participants.

![SUS Score](image)

*Figure 1. An adjective oriented interpretation of SUS scores*

In addition, we will run two more SUS evaluations on generic password usage, one before the participants use the three new technologies and one after, to see if the new technologies influence the participant’s evaluation in using text-based passwords.

5.3 Software Logs

We will collect the data logs from the software to list how many times the participant authenticated and how fast it takes to authenticate.

5.4 Post Case Study Interviews

We will interview the participants to determine how many times they went back to text base password, and ask to identify which password alternatives they would accept overall.

5.5 Data Analysis

- We will compare the three SUS scores between the technologies. We will also compare the SUS score for generic password usage.
- We will list the results of the Software logs to determine how much a reduction of usage of text base passwords.
- We will identify the participant’s preference of choice through the post interviews.
- We will identify any patterns in the user acceptance.
- We will address the Hypothesis questions.

6. Conclusion

This paper is an expanded Idea paper with a plan of execution in doing a Usability Study. The goal is to identify if the current laptop built-in hardware using the alternative text-based password software are acceptable and adaptable at the workplace. When this study is complete we will interpret the results to complement this paper.

References
