Fall 9-11-2020

A Framework for Describing Alternative Keyboard Structures in Augmented Reality

Eric Reed
Christopher Newport University, Eric.reed.14@cnu.edu

Christopher Kreider
Christopher Newport University, chris.kreider@cnu.edu

Mohammad Almalag
Christopher Newport University, mohammad.almalag@cnu.edu

Keith Perkins
Christopher Newport University, Keith.perkins@cnu.edu

A FRAMEWORK FOR DESCRIBING ALTERNATIVE KEYBOARD STRUCTURES IN AUGMENTED REALITY

Eric Reed
Christopher Newport University
Eric.reed.14@cnu.edu

Christopher Kreider
Christopher Newport University
Chris.kreider@cnu.edu

Mohammad Almalag
Christopher Newport University
Mohammad.almalag@cnu.edu

Keith Perkins
Christopher Newport University
Keith.perkins@cnu.edu

ABSTRACT

As adoption of Augmented Reality (AR) devices, such as the Microsoft Hololens, has been increasing in fields such as military and medicine, security should be considered. One type of attack that has been demonstrated is the shoulder surfing attack, whereby an observer can discover a password that was entered by the user through observation of their actions without ever seeing the characters they select. One proposed countermeasure to this is altering the structure of the keyboard without altering the relative arrangement of the keys. This paper proposes a framework for specifying a base keyboard in AR devices, as well describe alterations to this structure. The resultant framework should be ideal for developing randomization schemes that can be assessed for usability and implemented in AR devices.

KEYWORDS

Augmented Reality, Password Security, Keyboard Structure

INTRODUCTION

Augmented Reality (AR) devices have potential to change the world as they become more mainstream. AR can display valuable information to a soldier on the battlefield in a more intuitive manner than other means (Livingston et al., 2002), and help medical professionals perform surgery (Shuhaiber, 2004). Billinghurst and Starner (1999) assign three qualities to these wearable devices. They must be mobile in order to be properly functional; they must enhance reality as opposed to overwriting it; and finally they must be able to provide context-sensitive data. These properties introduce unique security considerations that may differ from traditional computing devices.

One way that an AR device can be compromised is through shoulder surfing attacks, where an attacker attempts to discover a secret value that is entered, such as a password or a pin, through external observation (Maiti, Jadliwala, & Weber, 2017). Traditional countermeasures to shoulder surfing attacks include inspecting the area for observers, and obfuscating the password entry process, such as covering one's hand (Kreider, 2018). As mobility and context sensitivity are important properties of AR devices, these traditional countermeasures interfere with the usability of the device. For example, to obfuscate the actions of a user entering their password

on an AR device, they may need to change their location to obfuscate their actions, thus changing their context and reducing their mobility during the password entry process. Due to the personal nature of AR experiences, it was expected that shoulder surfing attacks should not be possible, as the keyboard is expected to be only viewable by the user wearing the device. However, recent research has demonstrated the ability to perform a shoulder surfing attack on a person using AR (Kreider, 2018). In this attack, an observer video records a user entering their password while wearing an Microsoft Hololens AR headset. Once the recording is complete, shared knowledge of the keyboard structure enables the attacker to reverse the head and hand motions, and overlay them onto a keyboard with the same structure, discovering the password that was entered.

Three countermeasures to this attack have been proposed: specialized hardware, alternative keyboard layouts and alternative keyboard structures. Each of these solutions has various levels of usability, which is important in security, as software is only as secure as its users are comfortable using it (Whitten & Tygar, 1999). The specialized hardware proposed by Zhang et al. (2017) was expensive, and prone to errors in the entry process, significantly decreasing the feasibility and usability. Keyboard layout randomization proposed by (Maiti et al., 2017) resulted in longer entry times decreasing usability of the solution. Finally, Kreider (2019) proposes alternative keyboard structures, where the relative key layout remains the same, with manipulations to the structure of the keyboard, such as keyboard warping, as shown in figure 1 below.

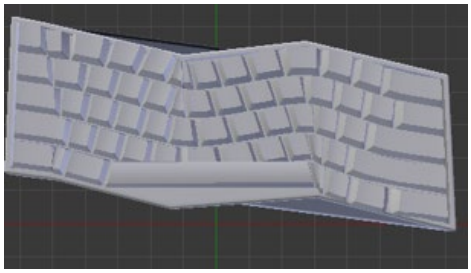

Figure 1. An example of a slightly warped keyboard

In keyboard warping, the goal is to find a balance between usability and security by changing the special relation of keys to each other, without changing their general arrangement, such as the traditional QWERTY key layout. Keyboard warping is just one example of how a keyboard structure can modified without changing the character arrangement, with several other possible approaches to performing this modification.

This study will specifically explore these possible approaches to specifying alternative keyboard structures and developing a framework to describe them. The purpose of this framework will be to develop a common way to define alternative keyboard structures with the goal of enabling randomization of the parameters. Within these parameters, future studies can then explore the usability properties of various alternative keyboard structures. For this study, we chose to use the on-screen keyboard from the first generation Microsoft Hololens as the base keyboard due to this AR devices current uses in the fields of medicine, military and even space flight.

The rest of this paper will be structured as follows. We will first explore the existing research in augmented reality security and the importance of usability in security. We will then introduce

our framework for alternative keyboard structures and briefly explore several alternative structures. We will then discuss our framework and draw conclusions from our work.

LITERATURE REVIEW

Augmented Reality and Security

Roesner, Kohno, and Molnar (2014) explore security concerns with Augmented Reality (AR) focusing on two main questions: What are the security and privacy problems with AR? One security concern with augmented reality devices is shoulder surfing attacks (Kreider, 2018). In this attack, a drawmetric profile (De Luca et al., 2014) is generated from either a known password, or a recording of a user entering an unknown password, shown in Figure 2. These drawmetric profiles can then be used to infer information about the unknown password that was entered, resulting in a 100% match rate when using passwords from a list of commonly used passwords.

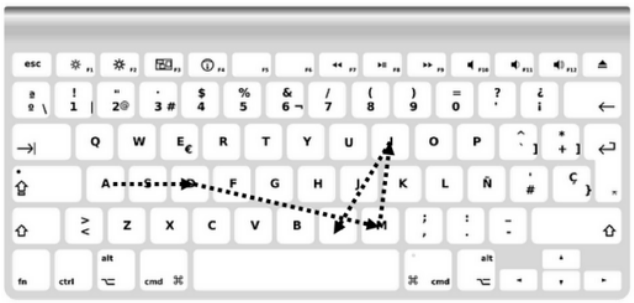

Figure 2: A drawmetric profile of the word "admin" overlaying a standard QWERTY keyboard.

Alternative password entry mechanisms have been explored in the context of augmented reality. Zhang et al. (2017) propose a solution to shoulder surfing attacks in Augmented Reality. Zhang et al's solution uses the Microsoft Hololens to provide a private keyboard that only the user can see, a Myo gesture control wristband to receive input data that is obscured from any observers, and a classifier to interpret that data. This approach was subject to errors in the detection process and required additional hardware. As security is not a user's first priority (Whitten & Tygar, 1999), many users may not even purchase this input method, or find the error rate to be within an acceptable tolerance. Maiti et al. (2017) proposed an approach in which they superimpose a scrambled keyboard in augmented reality for the user, so that the attacker doesn't know what the "true" keyboard configuration is. In this scenario, the keyboard is randomized according to one of three proposed algorithms: individual key randomization (IKR), row shifting (RS) and column shifting (CS). IKR created a new keyboard where each keys location was randomly selected. RS created a keyboard layout where the key rows were circularly shifted left or right by a random number. Column shifting is similar to Row shifting except that letters are circularly shifted by column instead of row. Column and row shifting appear to be more usable than IKR. Maiti et al evaluated usability of this solution by both entry time and accuracy. For measuring entry time, 13 participants were asked to use an unaugmented qwerty keyboard as a baseline. The results of typing random letters, familiar words, and passwords were 2.03 seconds, 1.80 seconds, and 2.37 seconds respectively. When IKR was turned on, the average time increased to 3.13, 3.15, and 3.36 seconds. With column and row shifting, the entry time was in the middle at 2.58, 2.93, and 3.20 seconds for column shifting, and 2.94, 284, and 3.19 seconds for row

shifting. The second usability aspect was accuracy. Average accuracy for random words, familiar words, and passwords on a qwerty keyboard was 94.37%, 93.78%, and 99% for a baseline measurement. With an IKR keyboard, accuracy dropped to 93.19%, 93.19%, 98.53%. Accuracy for column and row shifting were similar to the qwerty keyboard at 92.89%, 94.08%, 98.53% for column shifting, and 93.78%, 94.37%, 97.76% for row shifting. This solution has some serious limitations including a low camera resolution on the augmented reality device which made letter recognition difficult as well as a noticeable lag when the user moved their head. These limitations significantly impact the usability of such a solution. Finally, Kreider (2019) suggests keyboard warping as a possible solution. In this solution, the relative position of the keys to each other remains the same, with the shape of the keyboard changing shape.

Usability, Adoption and Security

Usability is important when developing new technology, as research has shown that Perceived Ease of Use and Perceived Usefulness are predictors of behavioral intention to adopt (Davis, 1989). Perceived ease of Use is simply defined as "The degree to which a person believes that using a particular system would be free of effort". Perceived Usefulness is defined as "The degree to which a person believes that using a particular system would enhance his or her job performance". As AR devices are a relatively nascent technology, adoption is a particularly important issue that may play a role in its future success.

Additionally, usability plays an important role in security. Whitten and Tygar (1999) define several principals of usable security. Among these include preventing users from making dangerous errors, and ensuring users are sufficiently comfortable with an interface to continue using it. These two concepts further illustrate that users of security software must be comfortable with security software to gain use from it. To become comfortable, they must be able to understand it.

FRAMEWORK

When exploring alternative mechanisms for users to enter passwords in augmented reality (AR), the goal is to balance usability and security, objectives which are often in conflict with each other (Whitten & Tygar, 1999). The objective of the alternative keyboard structure framework described below is to enable a common way to discuss alternative keyboard arrangements so as to be better capable of striking this balance. This framework identifies two key components to a keyboard used for character entry, the *keyboard layout* and the *keyboard structure*. *Keyboard layout* describes the relationship of the character a key on the keyboard represents, relative to other keys on the keyboard. For example, the traditional QWERTY keyboard as a keyboard character arrangement where Q is adjacent to W, which is to the right, and A, which is below. Alternatively, *Keyboard Structure* describes the shape/arrangement of these keys with respect to each other, without altering the keyboard character layout. Examples of this may include the size, shape and spacing between keys. Altering these properties of the keys alters the final structure of the keyboard. Additionally, the structure can be altered across the keyboard as a whole, for example, taking a traditional rectangle keyboard and warping it. This keyboard warping will result in the structure of the keys being changed. Below we will discuss a variety of measures necessary to describe alternative keyboard structures. This framework assumes a standard or *base keyboard* that will serve as the starting point for modification. Additionally, the purpose of this framework is not to enable a faithful replication of a keyboard based on the description, however, to identify important parameters which may be candidates for randomization.

Base Keyboard Measures

The base keyboard serves as the foundation for the keyboard that will be modified. An example of the base keyboard used in the Microsoft Hololens is shown below in figure 3.

Figure 3. Base Keyboard for a Microsoft Hololens

The important measures for this keyboard include the mean, mode, minimum and maximum key sizes, as well as the key count (horizontal) and key count (vertical). Using the above keyboard as an example, assuming each key is .5 in x .5 in, the mean key dimension is .61 in x .5 in with a mode key dimension of .5 x .5. It is expected that the mode will be a more useful measures of standard key structure as a majority of keys on many keyboards are the same size, with a few commonly known keys existing well outside that size, such as the spacebar and return keys. The minimum key width is .5 in, with a maximum key width of 4.5 in. The key count (horizontal) is 13, as there are 13 separate keys at the widest point of the keyboard. The key count (vertical) is 4. Of particular interest is the modal key size. This value is expected to serve as a relative benchmark, and enable keyboard structures to be described in relative terms. For example, when presented with a small keyboard such as may be seen on the screen of a mobile device, and a full screen keyboard, these keys will have very different physical dimensions. To specify that spacing should be increased to .5 inches would result in the keyboard on the mobile device being much larger than the screen it is displayed on, with potentially little implications for a keyboard on a full-size screen. By specifying manipulations to the keyboard structure relative to the modal key size, the change can be made relative to the dimensions of the base keyboard.

ALTERNATIVE KEYBOARD STRUCTURE MEASURES

Measures for altering the keyboard structure are broken down into micro, or *key based* and macro or *keyboard based*. Key based alternative structures describe how the keys will be changed from the base keyboard to the alternative keyboard. Keyboard based alternative structures describe how the shape of the keyboard will be changed from the base keyboard to the alternative keyboard.

Key Based

Key based alternative structures describe how the keys of the keyboard will be manipulated. The benefit of this approach is it enables a single description to be applied to all of the keys of the keyboard with minimal description of the change. Key Level measures include key size, key spacing, and key shape, summarized in Table 1 below. An example of an alternative keyboard structure specified at the key level may modify the key spacing, such as Spacing:Base Mode * 2. This would result in an exploded keyboard where all of the keys were further apart, by a factor 2 times the modal key size.

Measure	Description
Size	The most common key size in terms of length and width
Shape	The geometric shape (e.g. square, rectangle, circle)
Spacing	The distance between the keys

Table 1: Key Based Measures for Altering Keyboard Structures

Keyboard Based

Keyboard based alternative structures describe how the keyboard will be manipulate. The benefit of this approach is a macro level decision can be made, which can then be applied to the keyboard as a whole. The results will inevitably manipulate the key structure the keyboard is comprised of, without specifying the actual manipulation necessary for each key. These include measures of warping and bisection.

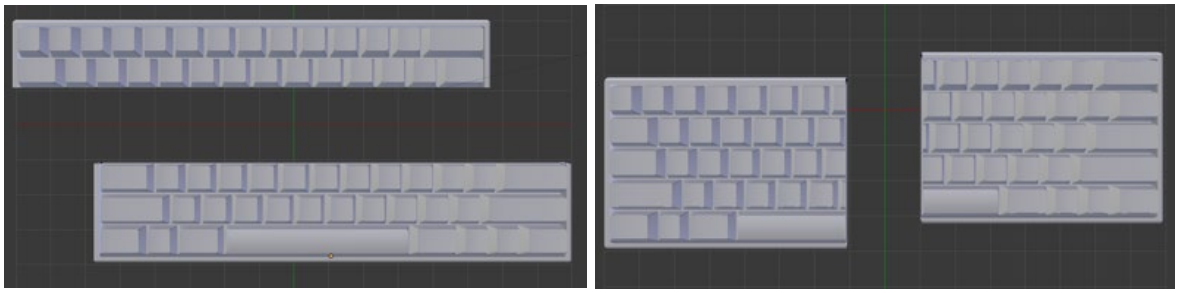

Figure 4. Vertical and Horizontal Bisected Keyboards

Warping based measures identify the amplitude and frequency of the warping to be applied to the base keyboard. Bisection measures indicate the number of times, and direction of which keyboard separation could occur, including horizontal and vertical bisection, shown in figure 4 above.

Strategy	Measure	Description
Warp	Amplitude	The difference between the lowest key and the highest key along an edge of the keyboard
Warp	Frequency	The number of times the keyboard moves between the lowest and highest points in the specified warping
Bisection	Vertical Count	The number of times they keys are separated on the vertical axis a distance greater than the base spacing
Bisection	Horizontal Count	The number of times the keys are separated on the horizontal access at a distance greater than the base spacing
Bisection	Distance	The distance between the separated portions of the keyboard
Bisection	Offset	The distance the leading edge of the subsequent bisected portions of the keyboard is offset from the initial edge

Table 2: Keyboard Based Measures for Altering Keyboard Structures

DISCUSSION

The above framework specifies several key elements that are capable of representing the transformation from a base keyboard to an alternatively structured keyboard. This framework is designed to encourage a common way to discuss and implement alternative keyboard structures in AR. Elements of the framework may be mixed and matched to develop unique keyboard structures that maintain general key arrangement, avoiding full keyboard randomization, such as a warped/bisected keyboard, shown in figure 5 below.

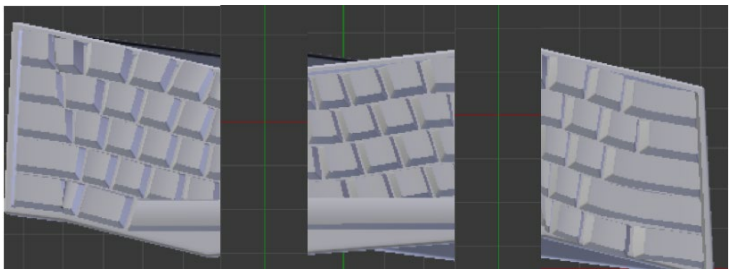

Figure 5. Warped and Bisected Keyboards

Each of the measures identified in the framework have both practical as well as usability bounds. Practical bounds for these values are device specific, for example, specifying that the key size of the alternative keyboard should be 100 times the base key size would result in problems with the target display being incapable of displaying the entire keyboard. Usability bounds are more closely related to the base keyboard structure as well as usability from the user's perspective. To specify a horizontal bisection count greater than the base keyboards key count (vertical) would inevitably result in keys being split in unusual and inconsistent manners, which would need to be addressed at the time of implementation. Similarly, to specify a warping strategy with a frequency greater than the base keyboards key count (horizontal) would result in extreme warping of all keys on the keyboard, significantly impacting readability and hindering usability. Successful implementation of this framework should take into account both the practical and usability bounds when identifying elements of the framework to incorporate into an alternatively structured keyboard. These bounds should be explored from both theoretical and empirical perspectives that seek to strike the balance between usability and security.

CONCLUSIONS

This paper develops a framework to quantify several ways in which a base keyboard in an AR device can be manipulated into an alternative keyboard structure. The purpose of this keyboard manipulation is to develop mechanisms to counter shoulder surfing attacks in AR devices. Such countermeasures should address security concerns that exist with the base keyboard, as well as exhibit usability properties so as not to interfere with a user's ability to perform a security task, or the general adoption of a nascent technology. This paper has several limitations. The first is that this framework is not empirically tested for usability. As the purpose of this paper is to develop a framework for alternative keyboard structures, it is our hope that future research will utilize this framework to identify alternative keyboard structures which are both usable and secure. The second is that there is no expectation that the elements of this framework are comprehensive. Specifically, there may be additional modifications to a keyboards structure that are not captured in this framework. The elements of this framework were chosen to represent some of the most common keyboard structures drawn from physical keyboard variants. Future research should explore the upper and lower bounds for the parameters of this framework as they pertain to usability. Once such bounds are established, randomization schemes may then be implemented to further strengthen the security of the alternative keyboard structure countermeasure.

REFERENCES

1. Billinghurst, M., & Starner, T. (1999). Wearable devices: new ways to manage information. Computer, 32(1), 57-64.
2. Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340. Retrieved from http://www.jstor.org/stable/249008
3. De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M.-E., Slawik, B. E., Hussmann, H., & Smith, M. (2014). Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
4. Kreider, C. (2018). The Discoverability of Password Entry Using Virtual Keyboards in an Augmented Reality Wearable: An Initial Proof Of Concept. Paper presented at the Southern Association for Information Systems, Atlanta, GA.
5. Kreider, C. (2019). An Exploration of Countermeasures for Augmented Reality Shoulder Surfing Attacks. Paper presented at the Southern Association for Information Systems, St. Simons Island.
6. Livingston, M. A., Rosenblum, L. J., Julier, S. J., Brown, D., Baillot, Y., Swan, I., . . . Hix, D. (2002). An augmented reality system for military operations in urban terrain. Retrieved from
7. Maiti, A., Jadliwala, M., & Weber, C. (2017). Preventing shoulder surfing using randomized augmented reality keyboards. Paper presented at the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).
8. Roesner, F., Kohno, T., & Molnar, D. (2014). Security and privacy for augmented reality systems. Communications of the ACM, 57(4), 88-96.
9. Shuhaiber, J. H. (2004). Augmented reality in surgery. Archives of surgery, 139(2), 170-174.

10. Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Paper presented at the USENIX Security Symposium.
11. Zhang, R., Zhang, N., Du, C., Lou, W., Hou, Y. T., & Kawamoto, Y. (2017). AugAuth: Shoulder-surfing resistant authentication for augmented reality. Paper presented at the Communications (ICC), 2017 IEEE International Conference on.