Aug 10th, 12:00 AM

Reconceptualizing Knowledge Based Authentication for Augmented and Virtual Reality Contexts

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

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

Reconceptualizing Knowledge Based Authentication for Augmented and Virtual Reality Contexts

Emergent Research Forum (ERF)

Christopher Kreider
Dakota State University
chris.kreider@trojans.dsu.edu

Omar El-Gayar
Dakota State University
omar.El-Gayar@dsu.edu

Abstract

Augmented and Virtual Reality (AR/VR) technology has advanced significantly in recent years, with recent applications in military, medicine, and education. Currently, most security artifacts utilized in AR/VR contexts are drawn from existing computing. These artifacts, however, were developed during the early ages of computing, to satisfy a completely different set of assumptions. In the context of AR/VR these assumptions have changed significantly. This research seeks to develop a general model of knowledge-based authentication (KBA). The model will be evaluated in the AR/VR context. This research will draw attention to the importance of considering security artifacts in the context for which they are being used, not for which they were originally developed. This work is expected to guide development of knowledge-based authentication in AR/VR, as well as provide guidance as future computing technologies are developed.

Keywords

Authentication, Augmented Reality, Virtual Reality, Cybersecurity, Design Science

Introduction

Virtual Reality (VR) and Augmented Reality (AR) are two technologies with potential to change the way we experience the world around us. While VR provides fully immersive experiences AR augments the world around us with context sensitive experiences (Billinghurst and Starner 1999). These devices classified as "wearable" devices, no longer utilize a traditional physical keyboard as the primary method of entry, and instead, have adapted the physical keyboard into virtual spaces. This simple transference of the structure of a physical keyboard into the AR/VR space provides a familiar interface for authentication but has been responsible for vulnerabilities that were otherwise not expected, such as shoulder surfing attacks. As VR and AR continue to increase in adoption their ability to provide mobility and context sensitivity also provides extensive capabilities to present entirely new artifacts. These digital artifacts can be either totally immersive (VR), or privately augment existing views (AR). Despite these capabilities, most existing solutions for solving vulnerabilities such as shoulder surfing rely on the concept of a making manipulations to virtual traditional keyboard such as randomizing keys (Maiti et al. 2017) or warping the keyboard (Kreider 2019). However, by decoupling authentication from the physical keyboard, significant room exists to develop alternative authentication mechanisms that provide security and usability.

Using a design science approach, we deconstruct the most common authentication system into a series of underlying constructs. This series of constructs is then used to build a generic model of authentication. Using this model, a new search space can be utilized in the development and verification of novel methods and implementations of authentication systems in AR and VR. The rest of this paper will be structured as follows. First, we will discuss relevant literature related to VR and AR, authentication and the Design Science methodology. We will then propose a generic model of authentication systems and discuss several implications of our proposed constructs when applied to VR and AR space. Finally, we will draw conclusions from the work, and discuss future work and limitations.

Literature Review

The most common form of authentication has remained the traditional password for greater than 5 decades (Furnell 2005). This form of authentication requires a user to enter a secret value during the verification process and comparing it with a value that was entered during enrollment. Despite the lengthy tenure of passwords as the most common form of authentication, they are frequently criticized for their role in lapses in security and increased organizational costs. Passwords may be compromised if they are weak (Shay et al. 2010), predictable (Bonneau et al. 2015), reused (Ives et al. 2004), or otherwise treated insecurely such as writing them down (Porter 1982).

Multiple novel alternatives to password based authentication have been proposed such as pass-algorithms (Haskett 1984), musical passwords and graphical passwords (Wiedenbeck et al. 2005). Additionally, criteria for assessing and evaluating authentication systems have been developed (Way and Yuan 2009). These criteria include: accuracy, robustness, acceptance, accessibility, feasibility, applicability, responsiveness, non-reputability and maintainability. The development of new authentication artifacts should be considered in the context of these criteria through the search process.

One primary mechanism of maintaining confidentiality in AR and VR devices is through using authentication. Despite significant advances in computing, and the ability to present 3D information in both totally immersive, and augmented environments, the concept of the traditional keyboard has been transferred to both VR and AR environments. Both environments, expected to provide private experiences, were expected to provide additional security to attacks such as shoulder surfing as the keyboard is no longer viewable by an attacker (Roesner et al. 2014). However, subsequent research identified successful shoulder surfing attacks that took advantage of the structure of the traditional keyboard, and users head and hand motions to determine the characters that were selected (Kreider 2018). This study adopted a shoulder surfing attack strategy applied to mobile devices that utilized drawmetric authentication, an authentication scheme based on the connecting of dots in a structured layout as opposed to selection of characters (De Luca et al. 2014). Specifically, the authors video recorded user's during password entry on a Microsoft Hololens AR device, and then manually transposed the head and hand motions into visualizations that could then be overlaid on a traditional keyboard. Using this attack method, they discovered the password entered with very high accuracy.

Alternative authentication schemes have been proposed to counter shoulder surfing attacks in AR. One such scheme obfuscated the character selection process through the usage of an electromyography (EMG) wristband. This solution, while removing one of the vectors of attack for successful shoulder surfing attacks, failed several of the criteria for authentication systems, with only an 86% accuracy rate, and requiring additional hardware that may not be feasible to acquire and utilize across widely adopted devices (Zhang et al. 2017). Another proposed solution implemented various forms of randomization, overlaying them on a traditional keyboard with three randomization schemes: inter key randomization (IKR), column shifting (CS) and row shifting (RS). While this solution was not tested for resistance to shoulder surfing attacks, other concerns were raised in terms of criteria for authentication systems including *user acceptance, responsiveness* and *feasibility* (Maiti et al. 2017). Another proposed solution suggests making systematic transformations to the traditional keyboard such as warping or bisecting the keyboard to provide randomization that does not alter the traditional arrangement of characters such as keyboard bisection and keyboard warping (Kreider 2019; Reed et al. 2020). While each of these solutions provides novel advances to the authentication artifact, none of them demonstrate the ability to adequately solve the security problem while also exhibiting appropriate levels of usability. We argue that, while the advancements are novel, they are novel within the constraints of a traditional physical keyboard, applied to a virtual space resulting in the weaknesses in the designed artifacts.

Methodology

This research will utilize a design science approach (Hevner et al. 2004; Peffers et al. 2007) to propose a novel artifact for authentication in AR/VR that is capable of meeting several requirements. First, that the construct generated should be generic enough that it can describe existing authentication systems, while also providing guidance for the development of new and novel systems. Additionally, the implementation of artifacts should be capable of considering both usability and security, and satisfy existing criteria for evaluating authentication systems. Specifically, we propose an authentication mechanism that abstracts the

elements of the traditional KBA into an underlying artifact. These constructs will be developed through a deconstructive process, that will systematically identify the assumptions that are inherent in the traditional physical keyboard, and abstract them into underlying constructs such as the physical locations of keys and visual stimuli used to identify each key. The proposed series of constructs will utilize mathematical and set notation to provide an abstract model of the user input of authentication processes related to enrollment and verification. This set of constructs and model will then discuss several implications that make the model novel, and capable of developing novel methods and implementations as well. Specifically, the goal of these constructs will be to enable design as a search process across a generic model of authentication. This generic model of authentication will then be capable of developing novel authentication artifacts that can be utilized not only in VR and AR, but other unique technologies of the future as well.

A general model for Knowledge Based Authentication (KBA)

The process of enrolling, and authenticating via Knowledge Based Authentication can be conceptualized as a set of potentially selectable spatially identified regions: ***R***. Each member of this set, denoted ***r*** then represents an individual potential selection from the set of all ***R*** capable of constructing a Knowledge Based Authenticator (KBAr).

Each ***r*** in ***R*** can be identified via a set of addressing schemes. Addressing schemes can be spatial, or sensory. *Spatial addressing* refers to the coordinate system via which elements in ***R*** can be described in terms of relative positions across the traditional physical dimensions. *Sensory addressing* refers to an observable attribute assigned to ***r***, capable of being observable when presented. These can be represented as the sets R_{spat} and R_{sens}. This model for conceptualizing the components of a KBAr can be used to generate a subset of **R** that can be used for the two key phases of KBA: *enrollment* and *verification*, both requiring the presentation of ***R*** or a subset of ***R***. The set of **R** presented at enrollment can be denoted as $\mathbf{R_{enroll}} \subseteq \mathbf{R}$. The set of **R** presented at verification can be denoted as $\mathbf{R_{verify}} \subseteq \mathbf{R_{enroll}} \subseteq \mathbf{R}$. Once the set **R** for enrollment or verification has been presented, a subset from **R** needs to be selected. The set of selections from **R** at enrollment and verification can be denoted as the ordered sets $\mathbf{r_{enroll}}$ and $\mathbf{r_{verify}}$. These constructs can then be combined to develop a generic model of authentication.

Given the above specifications, a KBA system can be specified in terms of the following generic model, presented in figure 2 below.

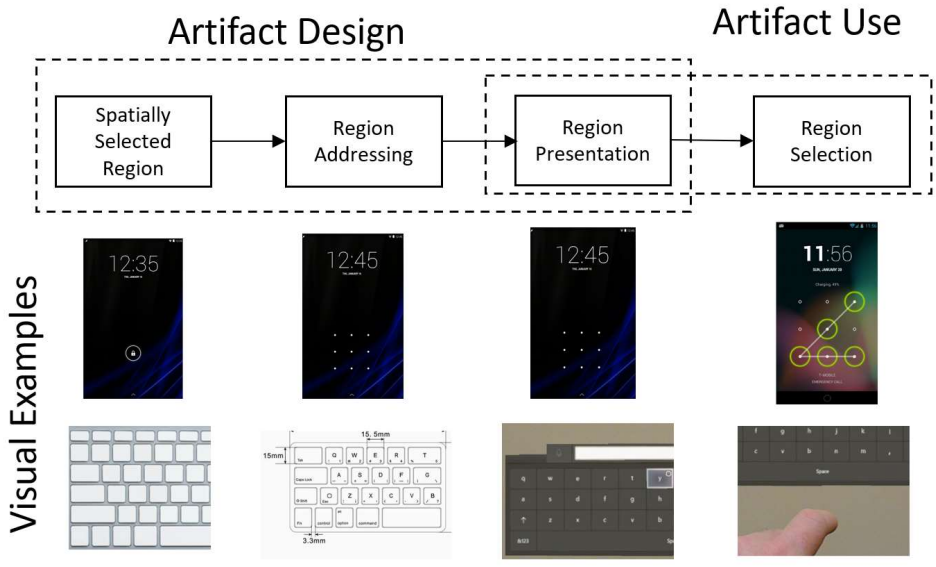

Figure 2: A General Model for KBA and Visual Examples

This model represents the four key areas of design in an authentication system: spatial arrangement of the elements used for authentication; determining what information will identify these selected regions; presenting the regions in such a way that they can be selected; and the selection of the regions as part of the enrollment or verification processes. Using a traditional physical keyboard as inspiration, a developer in

AR or VR would create a series of spatially arranged keys on a keyboard. Assuming such a keyboard was intended to hold only the characters of the English, the |R| would be 26. The next phase would be to assign identifiers to each selectable key, using a known arrangement; the physical representation of a set of options, of which an authenticator with knowledge of the options, is capable of selecting a subset of those options during verification, that match that was provided during enrollment. As the number of characters entries to provide appropriate *accuracy* and *non-repudiation* properties increase, the ability of human users to remember and select sequences is expected to diminish. This addresses the importance of the second element of an authentication system, *region addressing*. most spatial locations in authentication systems are visually addressed, such as the numbers on a pin entry at an ATM, and the characters on the keyboard.

Once a relationship between a set of selectable locations and how they are addressed is established, the input selection needs to be presented to the authenticator. Traditionally, a physical keyboard is displayed perpetually, not being removed when not relevant. This, however this is no longer the case in AR and VR spaces. When prompted with a scenario needing authentication, regions need to be presented for selection. Finally, at the point of authentication, the developed authentication artifact needs to be capable of accepting and encoding input consistently, in such a way that input at time of enrollment, can be repeated when verification is performed at a future time. This model can be operationalized using viual examples of the artifacts, also shown in figure 2 using a traditional QWERTY keyboard, and android based drawmetric authentication.

This provides a graphical representation of the authentication process using this model. From the artifact designers perspective, the goal is to develop a predefined system, that can be presented during authentication processes. This is just one part of the process, with the use of the artifact being the second phase. In this phase, a user will select the regions in a manner appropriate for enrollment or verification processes.

Evaluation

The constructs and general model of authentication will be evaluated based on evidence of their external and internal reliability. Externally, the resultant artifacts should be capable of modeling current authentication systems, as well as novel authentication systems. We intend to provide evidence for this by applying the general model to traditional QWERTY keyboard based, ATM Pin Pads, and Android drawmetric authentication schemes. Additionally, internal reliability will be assessed experimentally by calculating entropy and estimated brute force cracking times, then performing the attacks showing congruence between the values. Finally, the resultant artifacts will be in terms of criteria for evaluating authentication systems including accuracy, robustness, acceptance, accessibility, feasibility, applicability, responsiveness, non-reputability and maintainability. Using these measures, the implemented authentication artifact can then be developed using an iterative process (Way and Yuan 2009).

Expected Results and Contribution

This research proposes an abstract set of constructs that represents human-computer knowledge-based authentication (KBA) schemes. These constructs are then arranged to form a model of authentication systems; conceptualized from a series of selectable regions, through to the process of those being selected for enrollment or verification. This enables elements of the underlying constructs to be explored in the context of the model, providing a search space from which an alternative authentication design can be identified. Several potential implications that can be considered for future implementations are discussed. First, Elements of R do not need to be spatially organized like a traditional keyboard. This will enable the presentation of selectable locations across multiple spatial locations in 3 Dimensions. Second, Elements of R can be identified by sensory observation other than English characters, such as objects, images or shapes. Finally, Either *spatial* or *sensory addresses*, can be transformed as long as $\mathbf{R}_{\mathbf{verify}} \subseteq \mathbf{R}_{\mathbf{enroll}} \subseteq \mathbf{R}$ remains true. This could be operationalized by ensuring that the selectable regions are presented at random *spatial addresses* (e.g. randomly moving the regions to be selected). Additionally, this could result in the *sensory presentation* of a region can be modified or changed between selections.

Conclusion

This research in progress challenges the assumptions of traditional knowledge-based authentication schemes which rely on passwords entered on a fixed structure physical keyboard. As VR and AR gain in adoption, authentication is necessary to maintain confidentiality in these devices. This research deconstructs the authentication process into an underlying set of constructs, which are then used to develop a generic authentication model. The elements of the basic constructs, and how they are applied to the model are then discussed. Using the set of underlying constructs in the applied model provides an implementation activity that conceptualizes the design as a search process through the optimization of the parameters in the underlying construct. Using this series of artifacts should provide a framework for future work in authentication when applied in novel contexts, not just AR and VR.

REFERENCES

Billinghurst, M., and Starner, T. 1999. "Wearable Devices: New Ways to Manage Information," *Computer* (32:1), pp. 57-64.

Bonneau, J., Herley, C., Van Oorschot, P. C., and Stajano, F. 2015. "Passwords and the Evolution of Imperfect Authentication," *Communications of the ACM* (58:7), pp. 78-87.

De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M.-E., Slawik, B. E., Hussmann, H., and Smith, M. 2014. "Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*: ACM, pp. 2937-2946.

Furnell, S. 2005. "Authenticating Ourselves: Will We Ever Escape the Password?," *Network Security* (2005:3), pp. 8-13.

Haskett, J. A. 1984. "Pass-Algorithms: A User Validation Scheme Based on Knowledge of Secret Algorithms," *Communications of the ACM* (27:8), pp. 777-781.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp. 75-105.

Ives, B., Walsh, K. R., and Schneider, H. 2004. "The Domino Effect of Password Reuse," *Commun. ACM* (47:4), pp. 75-78.

Kreider, C. 2018. "The Discoverability of Password Entry Using Virtual Keyboards in an Augmented Reality Wearable: An Initial Proof of Concept," *Southern Association for Information Systems*, Atlanta, GA.

Kreider, C. 2019. "An Exploration of Countermeasures for Augmented Reality Shoulder Surfing Attacks," in: *Southern Association for Information Systems*. St. Simons Island.

Maiti, A., Jadliwala, M., and Weber, C. 2017. "Preventing Shoulder Surfing Using Randomized Augmented Reality Keyboards," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*: IEEE, pp. 630-635.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. 2007. "A Design Science Research Methodology for Information Systems Research," *Journal of management information systems* (24:3), pp. 45-77.

Porter, S. N. 1982. "A Password Extension for Improved Human Factors," *Computers & Security* (1:1), pp. 54-56.

Reed, E., Kreider, C., Almalag, M., and Perkins, K. 2020. "A Framework for Describing Alternative Keyboard Structures in Augmented Reality," in: *23rd Annual Conference of the Southern Association for Information Systems*.

Roesner, F., Kohno, T., and Molnar, D. 2014. "Security and Privacy for Augmented Reality Systems," *Communications of the ACM* (57:4), pp. 88-96.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., and Cranor, L. F. 2010. "Encountering Stronger Password Requirements: User Attitudes and Behaviors," *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pp. 1-20.

Way, S. C., and Yuan, Y. 2009. "Criteria for Evaluating Authentication Systems," *Proceedings of the 15th Annual Americas Conference on Information Systems (AMCIS)*, San Francisco, California.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., and Memon, N. 2005. "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," in: *Proceedings of the 2005 symposium on Usable privacy and security*. Pittsburgh, Pennsylvania: ACM.

Zhang, R., Zhang, N., Du, C., Lou, W., Hou, Y. T., and Kawamoto, Y. 2017. "Augauth: Shoulder-Surfing Resistant Authentication for Augmented Reality," *Communications (ICC), 2017 IEEE International Conference on*: IEEE, pp. 1-6.