Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2018 Proceedings | Midwest (MWAIS)

5-2018

How Wearable Technology Will Replace Verbal Authentication or Passwords for Universal Secure Authentication for Healthcare

Chad R. Fenner
Dakota State University, Chad.Fenner@dsu.edu

Cherie Noteboom
Dakota State University, cherie.noteboom@dsu.edu

How Wearable Technology Will Replace Verbal Authentication or Passwords for Universal Secure Authentication for Healthcare

Chad R. Fenner
Dakota State University
Chad.Fenner@dsu.edu

Cherie Noteboom, PhD
Dakota State University
Cherie.Noteboom@dsu.edu

ABSTRACT

Technology use is increasing in healthcare services, creating a concern for privacy, security, accessibility, and sharing of personal information. The issue increases for persons with disabilities. Cognitive, physical, or multiple disabilities make identification of individuals difficult or impossible, thus increasing the need for a caregiver or family member to verify the individual's identity. The paper will present a conceptual model of knowledge contribution in patient authentication without verbal information exchange through the following factors: authentication with wearable technology, central location for personal information, and an authentication context model direction.

Keywords

Authentication, wearable technology, disabilities, universal design, health services, security.

INTRODUCTION

The creation of a wearable technology artifact for the user authentication without the need for verbal or physical interaction may increase security, privacy, and simplification of authentication process. Current authentication techniques are non-inclusive for individuals with disabilities. Technological advancements in architecture, hardware, applications, networks, and systems create the potential for a superior universal solution.

This paper will discuss a design research concept for authentication using wearable technology: A multi-layer authentication model that uses interactions between the wearable device and a service provider's peripheral hardware. Initial personal identifiable record creation will be a key component in the design. The peripheral device will need to allow for multiple forms of biometric authentication. There will also be restrictions on the information sharing based on provider role and data necessary to perform duties.

BACKGROUND RESEARCH REVIEW

An increasing issue with the use of technology platforms for services, social interaction, education, and other areas of individual's daily lives is discriminating user authentication techniques. "The need for inclusive design authentication is going to be a legal issue instead of a technical inconvenience. The legal implications are necessary, but the proper construction of information systems is a business requirement (Fuglerud and Dale, 2011)."

CURRENT AUTHENTICATION MODELS

The current methods of authentication focus on individuals with full physical and cognitive abilities while assuming certain economic status. Individual exclusion cannot be the method of development for future authentication standards. The ability to access social, economic, legal, health, government, commercial, and educational interaction is necessary for all individuals.

People with disabilities may not have the capacity to remember a password or understand why it is necessary. For example, some individuals do not have the physical ability to interact with a biometric authentication system, due to a physical abnormality, accident, or birth-related issue (Fuglerud and Dale, 2011).

Biometric authentication is one area of exploration for authentication for older adults and persons with disabilities. The barriers are cost concerns of implementation for providers, inconsistent results due to outside factors, and ease of use by individuals (Kowtko, 2014). The difficulties of using keyboards effectively and issues recalling complex passwords create an additional burden for mature adults. The individuals understand the need for passwords but lack the comprehension of necessity for strong security (Ahmed et al., 2017). The type of disability can increase the scope of consideration for design solutions. Part of the group of individuals with disabilities would include addressing Parkinson's disease, dyslexia, vision impairment, and upper extremity disabilities. The final evaluations should examine "…usability vs. disability vs. security (Helkala, 2012)."

GAPS AND LIMITATIONS

The ability to authenticate without interaction will allow the implementation of this technique at multiple locations and for medical home care. Current issues with remote authentication designs do not allow for a person with a disability to authenticate without assistance for eHealthcare. The current architecture requires authentication to the telehealth network which is not possible for persons with disabilities in a care from home scenario.

The creation of a multi-factor solution increases the challenges for users but is beneficial in the security verification process. The authentication types most widely in use are something you know, something you have, something you are, or something you do (Anani and Ouda, 2017). Remote authentication increases the need to address confirmation that an individual is indeed the person requesting access to the environment. The authentication technique will to be unique and confirm the individual is alive. This issue further enhances the need for an inexpensive multi-layer form of authentication (Ijbaoun et al., 2016).

The cloud allows access to education, socialization, and personalization items for individuals able to use the resource. Security and accessibility are integral parts of using a cloud platform and present the greatest challenge to all user groups (Chourasia et al., 2014).

SOLUTION PROPOSAL

Future authentication artifacts should conform to an individual, not to a system. The system should adapt to the user (Chourasia et al., 2014). Focusing on the changing research necessary in authentication artifacts will allow an individual from a different culture, who speaks a different language or comes from a difficult social environment, to participate in the use of information systems. A proposed group for this study will include at least six minority groups for consideration youth, mature adults, refugees, ethnic minorities, women, people with disabilities, and people with mental health issues (Briggs and Thomas, 2015).

The wearable technology device in conjunction with remote personal file sharing system will reduce the amount of personal information accessed for verification purposes. This artifact model will begin with a chip in a wearable device that will store a private single-use verification code. The use of RFID, a password, and biometric measure with a microcontroller that increases speed and reliability for verifying identity. The final peripheral device will combine the functionality of a keypad, multi-biometric scanner, and RFID chip reader for authentication (Medhi, 2015).

PROPOSED METHODOLOGY

The paper will discuss a design science theory that produces a universal design authentication solution for the largest population of individuals. The theory begins with a multi-layer security authentication scheme. The artifact will begin with a physical device that is a form of wearable technology that is with the individual at all times. This device will act as the first layer and most essential piece of the model. The device can be something as simple as an RFID chip that contains a one-time code that updates after each use.

A peripheral device interacts with the wearable device. This will allow reading of a code that checks against the electronic records to retrieve identification information. Achieving verification of different types (photo, biometrics, pattern or image recognition, and two-way verification) with the device will allow for a simple, effective approach for credibility and security.

Design Science Research Method	
Guideline	Description
1. Design Science as an Artifact	Wearable technology artifact and method for user authentication process
2. Problem Relevance	User authentication for individuals with disabilities
3. Design Evaluation	Ease of use and effectiveness of authentication process
4. Research Contributions	A universal design that will allow wearable technology artifact to be used for authentication with no need for user interaction.

5. Research Rigor	Quantitative and qualitative analysis of the artifact and individual ease of use.
6. Design as a Search Process	RFID chips, peripheral device readers, and cloud-based record keeping
7. Communication of Research	Results will show the effectiveness of the artifact, qualitative survey ease of use by individuals with and without disabilities, and quantitative results for use and security

Table 1. Design Science Research Method Guidelines and Descriptions (Hevner, 2004)

STRUCTURAL MODEL

The creation of a wearable device in conjunction with eFiles will allow personal authentication that will enable access to private authentication records. The device stores an encrypted identification code verifying the individual with the service system to allow the retrieval of authentication records from a cloud system. The data released will be determined by the professional service person's role.

The initial creation of the record will allow the individual control over their personal data. Determination of viewable data will be distinguished by the provider's role. Health, financial, personal, legal, travel, and other areas to be part of the individual data record as chosen by the individual and role assignments to allow access to certain areas of data records.

The design of the wearable device can be as simple as a pendant, bracelet, glasses, ring, or key fob device. There is also the ability to create flexible devices that are part of the individual's clothing such as a scarf, hat, belt, or shoe. A wireless signal sent from the system to the device will cause a blinking light and audible sound which will confirm the device is authentic, in possession of the individual, and working properly. After this verification, there will be a new code assignment to the device for the next authentication process.

The information system design will consist of a provider system that connects to a larger database of consumer information. The system will first retrieve the data record for verification through the consumer identification code. The reader will use the consumer code to retrieve a record for verification of the consumer's identity. Additional information release will be according to the role of the provider.

PROPOSED STUDY

The measurement of effectiveness is the successful verification of the individual by the system. Additional testing of the device will include groups of individuals with and without disabilities. An inclusion of qualitative research method from previous research papers for guidance with comparisons between previous design models will be used. The scenario specifies security levels for the application and data, user population, physical environment, software, hardware, system, acceptance levels, rules, regulations, and final cost estimate (Helkala and Snekkenes, 2009).

A final quantitative measuring metric involving security and usability will be used to determine a quality value for the implementation. The parameters are secrecy, abundance, revelation, privacy, and breakability. Other influences include a value for authentication recall of criteria and a value for mental effort (Mihajlov et al., 2011).

CONCLUSION

The ability to create an inclusive form of authentication is necessary for improving privacy, security, and the inclusion of larger portions of the population. The creation of models built for a specific group of users is a prejudice and requires a resolution. This paper lays the groundwork from earlier security architecture and creates a more inclusive model theory. The model addresses security with a service environment but should expand to a personal model. Continuing studies can examine the different methods of authentication that will simplify or enhance the verification process possibly biometric or other authentication. Architectural design modifications will also improve efficiency through peripheral devices, network speeds, cloud solutions, and encryption techniques.

REFERENCES

Ahmed, E., DeLuca, B., Hirowski, E., Magee, C., Tang, I., & Coppola, J. F. (2017). *Biometrics: Password replacement for elderly?* Paper presented at the Systems, Applications and Technology Conference (LISAT), 2017 IEEE Long Island.

Anani, W., & Ouda, A. (2017). *The importance of human dynamics in the future user authentication.* Paper presented at the Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering.

Briggs, P., & Thomas, L. (2015). An Inclusive, Value Sensitive Design Perspective on Future Identity Technologies. *ACM Transactions on Computer-Human Interaction (TOCHI), 22*(5), 1-28. doi:10.1145/2778972

Chourasia, A. (2014). State of the science on the Cloud, accessibility, and the future. *Universal Access in the Information Society, 13*(4), 483-496. doi:10.1007/s10209-013-0345-9

Fuglerud, K., & Dale, O. (2011). Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client. *Security & Privacy, IEEE, 9*(2), 27-34. doi:10.1109/MSP.2010.204

Helkala, K. (2012). *Disabilities and authentication methods: Usability and security.* Paper presented at the Availability, Reliability and Security (ARES), 2012 Seventh International Conference on Availability, Reliability and Security.

Hevner, A. R. (2004). DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH. *MIS Quarterly, 28*(1), 75-106.

Kowtko, M. A. (2014). *Biometric authentication for older adults.* Paper presented at the Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island.

MEDHI, P. (2015). *AN EFFICIENT MULTISTAGE SECURITY SYSTEM FOR USER AUTHENTICATION.* Paper presented at the Proceedings of 29th IRF International Conference, 21st June.

Mihajlov, M., Jerman-Blazič, B., & Josimovski, S. (2011). *A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives.* Paper presented at the Network and System Security (NSS), 2011 5th International Conference on Network and System Security.