CMP417 Authentication Assessment

Jack Gates
1500763
1500763@uad.ac.uk

***Abstract*— With the growing population of seniors struggling with newer technologies, more focus should be placed on keeping this group secure. This age-group presents new challenges when it comes to designing and implementing an authentication mechanism that caters to their needs. For example, many seniors are affected by age-related infirmities. This paper presents a design for an ATM authentication mechanism that will allow the group to securely handle their money. The paper also demonstrates ways in which the mechanism can be evaluated, as well as how machine learning can be incorporated to secure the design from fraud.**

Keywords—design, authentication, seniors, ATM, security

I. Introduction

The older population of the UK is growing significantly. By 2040, projectably nearly one in seven people are to be aged over 75 [1]. With the population aging, more consideration should be given to older people as they struggle with many things that younger people take for granted. One of the things they struggle with in particular is the use of newer technologies. Among these technologies is authentication mechanisms, which are vital in keeping this group secure. It is not uncommon for seniors to be victims of fraud, or to have their credentials stolen due to a lack of implementation of authentication designs which are appropriate for them.

This focus of this report is to select and design an appropriate authentication mechanism for an ATM in a senior citizens home. This is because the traditional ways are arguably not the most suitable for this age group. The seniors are all over 70 years old, many of which have hearing impairments. Besides this, none have disabilities beyond the usual age-related limitations that seniors possess. The report will first go into the background of authentication mechanisms, reviewing authentication mechanisms for other groups that struggle with the traditional ways, such as children or those with disabilities. Literature regarding the challenges faced by seniors that make passwords and pins problematic will also be sought. Although most of these groups struggle for similar reasons and there is a lot of cross over between those with disabilities and seniors, such as reduced memory, mobility etc. After the literature is reviewed and the challenges faced by this group highlighted, a design that accommodates these challenges will be illustrated. An outline of how this system could be tested will be presented, as well as ways in which machine learning could be used in order to detect intrusions and help secure the residents. Finally, the challenges of producing an authentication mechanism for this user group, and the challenges involved in engendering adoption will be outlined.

II. Background

A. Literature

The default authentication mechanism on the web these days are passwords. This is because passwords are a suitable method of authentication for most people. However, the use of passwords may not be the best authentication mechanism for all kinds of user groups. For example, a study by Read and Cassidy was performed in order to understand how children created text-based passwords [2]. One of the findings were that 50% of the children had difficulty recalling the passwords after only 75 minutes. This shows that children have poor recall when it comes to text-based passwords. A popular alternative to textual-based passwords is graphical passwords. Assal, Imran and Chiasson studied the usability of three different graphical password schemes among children and adults [3]. A 6x8 grid of squares were used for each authentication mechanism, and the user has to select an un-ordered combination of these squares in order to authenticate. The three different schemes were, a mechanism that makes use of recalling certain object images; certain words on each tile; and a single image divided into squares. It was found that children and adults were most successful at recalling the objects. The paper also highlights that both adults and children preferred graphical passwords to their existing schemes. However, it was found that the login success rates were too poor for real world deployment, which the paper suggests is possibly to do with the nature of the study and would be less of an issue in the real world. It does suggest recommendations to make this scheme more effective for children, such as increasing memorability through training, and tailoring the interface to better fit the children's age-group. Overall, this study shows a promising alternative to text-based passwords that can be used as an authentication mechanism for children. However, other groups besides children need to be thought about as methods which use visible aids, are not suitable for persons with visual impairments.

When it comes to the authentication of people with disabilities more issues arise when using text-based passwords. A paper by Helkala focusses on the difficulties faced by certain disabilities in authenticating on certain methods such as pin codes, textual passwords and one-time codes [4]. The disabilities studied in this investigation are Parkinson's, dyslexia, vision impairment, and upper extremity disabilities. Overall, the paper highlights that having one of these disabilities typically results in the user being more vulnerable to attacks, taking longer to authenticate, failing to correctly authenticate, and having a lower password/pin entropy. Some of the specific challenges faced by users with Parkinson are difficulties in using the mouse and keyboard due to issues with balance and coordination. Memory problems and slowed motor skills also increase the difficulty in memorising and submitting text-based password. The paper also mentions that Dyslexia may cause a user difficulty in spelling longer words or entering random sequences of characters. It could therefore

potentially affect the strength of a user's text-based password due to them wanting a password easier to authenticate with. Although visually impaired individuals may be able to authenticate with passwords and pins in around the same amount of time as the average person due to braille keyboards, inconsistent layouts can potentially cause them to take longer in entering passwords. Another significant problem is the use of one-time codes that are sent over another device. These codes could be delayed, or the user may miss the prompt that triggers the event due to their poor vision. It is common for the visually impaired to get help from another person regarding this, which makes them more vulnerable if the person has malicious intent. As discussed in the paper this is also a difficulty faced by those with upper extremity disorders. For these extremity disorders, although there are many devices to make navigating the web easier for these individuals, factors such as the inability to perform multiple key combinations affect the strength of the password. It also is likely to cause them considerably more time to enter passwords or pins. The paper does a very good job of covering all of the difficulties faced by users with these specific disabilities and even presents some alternative methods that could potentially be used.

A musical password system can work as an alternative authentication method. A paper by Gibson, Renaud, Conrad, and Maple illustrates a method of authentication through listening to audio clips [5]. When setting up this authentication method the user selects their password from a range of audio clips. When authenticating, the audio clips are played by waving the mouse over them and the correct one is selected through a click of the mouse. The system was compared with traditional passwords for overall memorability after a period of disuse and it was found that the musical system offered a 48% increase in performance. A system such as this may be effective for those with memory issues, such as Parkinson's, or those with difficulty in spelling complex passwords, such as dyslexia. Although this method may be affective for dealing with some disabilities, it can exclude others. For example, those with hearing impairments may struggle or find it impossible to authenticate. It is also a much longer authentication process than textual passwords. The authors themselves mentioned that this form of authentication is probably better suited for low security systems.

Another method of authentication which would be useful for those with disabilities would be biometrics. Well known biometric authentication includes fingerprint scans, and iris scans, although a lesser known example of a design using biometrics is written about in a paper by Lugovaya, where an investigation into using a person's electrocardiogram as a form of authentication is performed [6]. The study argues that this is a valid method due to the fact that the electrical currents generated by the human heart is a unique characteristic. These currents were recorded, processed to remove noise, and classified using linear discriminant analysis which resulted in 96% correct identifications on a group of 90 individuals. One of the greatest benefits of this method is that it is suitable for all people, as everyone has a heart-beat. The main findings of this investigation are that ECG is a valid method of authentication, although ECG is not unique enough to be used for a large population. It is better suited to small predetermined groups.

More focus should be given to the technological difficulties faced by the aging population. These difficulties can be attributed to several different factors, one of which is a poor adoption of new technologies. A paper by Rebola and Jones states that traditional design methods may not be sufficient to develop adoptable design products for older adults [7]. The paper mentions that the older generation find newer technologies complicated and confusing, as well as costly. The paper argues that design plays a significant role in making technologies more approachable for an ageing population, and presents the "sympathetic design" framework as a valid approach for designing technologies with seniors in mind. This framework has 6 different parameters which are used to ensure a successful design. An example of one of these is product functionality, the framework recommends that the functionality of a product should be simple, and address basic needs. Another focus of this framework is the product interface, which should be physically tangible for the user and should be arranged in a way that makes sense. The paper does a good job of describing why a framework such as this is necessary for the older generation and also demonstrates current designs which implement it. Older adults will likely experience some difficulties and limitations in vision, dexterity, physical function, hearing, and cognition as they age. They are also more susceptible to the illnesses and disabilities previously mentioned, such as dementia and Parkinson's. Due to these limitations as well as traditional methods not meeting their design needs, text-based passwords may not be suitable as an authentication mechanism. Designing alternatives is difficult, as it is impractical to design/develop interfaces with all of these limitations and disabilities in mind [8]. However, some of the systems discussed above are promising.

B. *Summary of the challenges*

Since seniors can find newer technologies quite complicated, the design will be as simple as possible. Actions at each stage of enrolment and authentication will also be clearly defined and will use graphical pictures. Although none of the residents are visually impaired, it is common for older residents to have reduced eyesight, so large paragraphs of text will be avoided, and any text on the screen should be large and clear to read. A portion of the residents have hearing impairments, so no hearing should be required in order to operate the ATM. In case of residents with any sort of mobility issues with their upper extremity, such as arthritis, which can be quite common in older people, limited key use should be sought after in the design. Physical buttons will be used instead of touch screen because as mentioned earlier, older adults prefer a tangible interface. It is common for seniors to have reduced memory, or memory related illnesses like dementia and Parkinson's, so no pin will be required to use the ATM, instead the machine could use an authentication method which is easier to remember, such as a graphical one, or a method that requires no memory, such as biometrics.

III. RECOMMENDATIONS

A. *Features*

Facial recognition will be used to authenticate along with a chip. Facial recognition was chosen as it is fairly secure, and also quick and easy. An iris scan will also be done during the enrolment phase, and this scan will be used in

order to allow the user to re-register a face scan for authenticating, in case authentication with this method no longer works. An iris scan was chosen as a back-up authentication method as although it may be more time consuming, it is also more secure than face-scans as everyone's iris is completely unique and never changes. The chip is linked to the senior's bank account and is stored in a wristband that the senior can wear around their wrist. The RFID reader on the machine communicates with the wristband when it is in close contact with the wristband. Using a contactless wristband instead of a card that needs to be entered into the machine is arguably better, as it takes less dexterity to operate and is less likely to be lost or stolen if it is around the senior's wrist.

The text of the interface is large, and makes good use of spacing, so that those with poor eyesight will not struggle. Actions at each stage of enrolment and authentication are also clearly defined and make use of graphics to help illustrate what is happening. The buttons on the side are tangible and not touch screen and also spaced out as this complies with the sympathetic design framework. There is also limited key use necessary for those with mobility issues in their upper extremities. No hearing is required for this system.

There are many security benefits of a biometric system. In general, there is an added degree of security in relying on an extremity or pattern that only you possess and carry at all times. It also leaves less pressure on the user for securing themselves. As an example, it doesn't give them the option to enter weak credentials. Another added benefit is the fact that authentication can't be stolen through observation, or guessed. A security benefit of having a contactless wristband is that the user has the ability to carry it around at all times, and not leave it in an exposed place.

B. Design

The senior will have their contactless wristband and will enrol on the system upon scanning it for the first time. In panel 3 the user will perform an iris scan, if an error occurs then the enrolment process will terminate and the user will be presented with panel 4. Pressing any button will return to panel 1. If the iris scan is successful then the user will perform a face scan. If unsuccessful the system will terminate enrolment the same way as before. This step is repeated for confirmation. If successful then the user will be successfully enrolled in the system and their biometric scans will be saved and required for authentication.

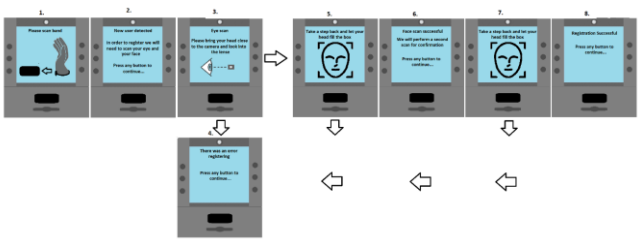

Figure 1 - Enrolment Interface

To authenticate the user will scan their wristband, the system will then automatically scan their face. If unsuccessful then they will face panel 3, that will either let the user reregister (see figure 3), try again or cancel. Cancelling at any stage will return the user to panel 1. If successfully authenticated, the user can then either check their balance or withdraw money.

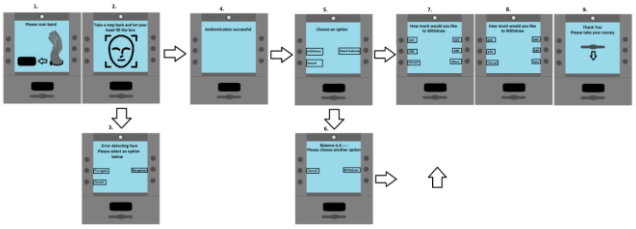

Figure 2 - Authentication Interface

The interface for the reregistering process is very similar to the enrolment process, except, when performing the iris scan the system is checking that it matches the previously stored scan. If there was an error or it does not match the stored scan during enrolment, then the user returns to panel 1. Otherwise they will be able to reregister their face scan and use it as authentication.

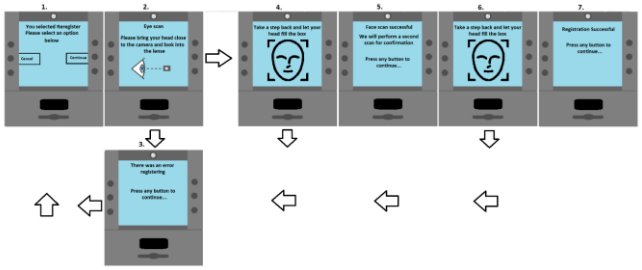

Figure 3 - Reregistration Interface

C. Design limitations

A slight limitation to this system is the use of text. Although there are no visually impaired residents on the premise, reduced eyesight is still an issue affecting the older population, and some residents may find the text difficult to read. One of the greatest limitations of this authentication method is possibly the contactless authentication wristbands. One of the reasons being the costs involved in giving contactless wristbands to all the residents. Although it gives users with issues involving their dexterity greater ease of authentication, and it also provides added security by allowing the elders to wear it, it is also possible that the residents find the wristbands uncomfortable or annoying. This may result in them deciding to take it off and leave it in an unsecure location, which ultimately negates the added security that it provides.

Biometrics also have certain limitations, such as requiring additional hardware which may also be costly. Another limitation of biometrics is that if biometric data is compromised, it is unable to be changed in the same way a password is changed, as a user's face cannot be easily changed, nor can the iris of their eye. It is also possible that residents may be uncomfortable giving away their biometric data as a means of authentication. This could be for various reasons personal reasons, or because they don't want to risk their biometric data being stolen. Having biometric data

stolen has greater consequences than having other types of credentials stolen, as they do not vary between other systems where a person might use them to authenticate. They can also potentially be used to falsify legal documents, passports, or criminal records.

IV. Experiment outline

A. Usability

One of the ATM's can be beta tested on the premises. A select group of the elders, ranging in different abilities, will have their account set up with the wristband. They will then perform the following steps:

1.) Enrol on the ATM.

2.) After enrolment, they will attempt to authenticate.

3.) The resident will then attempt to authenticate while hiding their face from the camera.

4.) After failing, they will go through the reregistration process.

5.) Participants will continue to use this system to withdraw money for the next week.

These steps will provide comprehensive testing of the systems enrolling and authentication. The first 4 steps are for ensuring the system functions correctly, the final step is to test the usability of the system. Another group of elders will be selected, also ranging in different abilities, and will be monitored using the traditional chip and pin method of authentication. At the end of the experiment, in order to measure performance, the number of successful authentications, and unsuccessful authentications will be recorded, as well as the time taken per authentication. This will be done for both groups. The results obtained will then be compared with each other. This will give good insight into the usability and the effectiveness of the proposed system.

B. Preference

Another way to measure the performance is to find out the preferences of the first group of participants. For this they will be asked the following four questions:

1.) Do you prefer this authentication mechanism to traditional chip and pin? (yes or no)

2.) Do you feel safer using this authentication mechanism when compared to the previous mechanism in place? (yes or no)

3.) On a scale of 1 to 5, how easily did you understand this system? (1 being not at all, 5 being clearly).

4.) Do you have any disabilities or impairments? If so, did the system cater to your needs? (yes or no)

These questions will give good insight into the opinions of the targeted group on the implemented system.

C. Encouraging adoption and recruiting evaluators

As explained in the previous sections, elders are slow to adopt to new technologies due to finding them overcomplicated and due to them being reluctant to change. A good way to encourage adoption of this technology is to fully explain each step. Full explanations of each stage have already been implemented into the design itself, although further demonstrations of the machine could be shown to the residents. Another good way to encourage adoption is to explain the benefits of the new system, the most important of which being security. It is also important to address the physical limitations that this system makes less of an issue for the residents*. When it comes to recruiting the seniors for evaluating the system a good way to do this would be to hand out flyers in the places they frequent, for example a bingo hall, or coffee shops. To encourage participation, the flyers will highlight that their contributions could potentially help secure many senior citizens.

V. Machine learning

Machine learning could potentially be used in order to improve the security of the system and detect whether any staff member is defrauding the residents. A machine learning approach for detecting deviations is available in a system presented in a paper by Chekina, Mimran, Rokach, Elovici, and Shapira [9]. The presented system measures the deviations of network behaviours in Android applications. This system used a cross-feature analysis approach on a series of aggregated network related features. Cross-feature analysis assumes that strong correlations between normal behaviour patterns are useful for detecting malicious abnormalities using a machine learning model. This system evaluated several different learning models, testing them on the network's patterns, and the best was found to be a decision tree classifier named REPTree [10]. An anomaly detection module is then used to determine if the deviations from the expected network behaviour are enough to be considered malicious using a predefined 'acceptance rate'. A similar system could be implemented on the ATM, except the features extracted will be related to the way in which an individual interacts with the machine.

This would be a challenge as biometrics doesn't exactly allow for many features of the authentication process to be extracted for accurate learning of typical benign behaviour. However, it is still possible to construct some sort of aggregation of features based on how the seniors may use the machine, and identify any behaviours that lie outside of behaviours considered by the system to be normal. Features that could potentially be extracted are:

- The number of successful authentications
- The number of failed authentications
- The time of day the senior uses the machine
- The amount typically withdrawn

After receiving sufficient data of a resident over a given period of time, the features extracted would be used to represent the personal behaviour pattern for each individual and used to train a classification model in a similar way to the previously mentioned system. Each resident will have their own model trained after them. This classification model should then be able to measure different levels of deviations of what is considered normal behaviour for that resident. Due to there being a somewhat limited number of features that could be extracted, a higher acceptance rate of deviations should be given to this system. Any transaction with a high deviation from normal behaviour, for example withdrawing an unusually large amount of money late at night (a period in

which the resident would never typically withdraw money), could result in the account being temporary locked for further investigation. This threat detection system could also be effective for working outside of the home, by taking other features into consideration when training the model on a resident's data. For example, the location of any transactions can be taken into account. If a transaction is made a distance away from the care home and other aggregated features about the transaction seem suspicious, then the transaction could be declined, or the card holder notified. One limitation to this approach is the time it takes to train the model to be effective at detecting deviations.

Due to the system proposed in this paper utilising a similar method to the aforementioned system, the machine learning algorithm that worked best in that system may also work best in this system. Reduced error pruning (REP) Tree is a type of decision tree classifier – which is a graph that uses a branching method to illustrate all of the possible outcomes of a decision. The REPTree algorithm in this case will produce a regression tree using information gain and variance with minimised error. Regression is needed over classification as the features that will be used in the algorithm will be numeric values. The tree will then be pruned to reduce its size using a reduced-error pruning with backfitting. There are several advantages of using decision tree regression, such as it requiring little data preparation for the features, as no data normalisation is needed. The REPTree algorithm is fast learner and can handle large amounts of data. Often decision-tree classifiers suffer from overfitting, but REPTree's effective use of pruning makes this less of a problem. One of the limitations of using a decision tree classifier is that they are not very robust against changes in the training data, so introducing new variables in future iterations of the model may cause instability [11].

There are also other ways in which machine learning could be used to detect when staff may be defrauding residents. An example of this is in an article discussing the detection of dead iris' [12]. Fake irises could potentially be crafted, modelled after a real eye to fool an iris scanner, and authenticate. This paper demonstrates a way in which machine learning could be used to detect whether an eye is real or not.

VI. LIMITATIONS AND CHALLENGES

To conclude, there are many challenges faced when producing authentication mechanisms for senior citizens. One of the major challenges that need to be addressed are the age-related infirmities that are common in this user group. It is common for seniors to have reduced memory, or memory related illnesses, so this alone rules out the most traditional methods such as passwords or pins. Decreased dexterity in this age group also means that having an interface littered with fine buttons, or anything requiring a steady hand like inserting a card into a slot should be avoided. This specific group of seniors also have hearing deficiencies, so the system should not require the user to hear. This means that authentication solutions requiring sound to function, such as Musipass which was presented in the literature review, would be inappropriate for this user group.

Another challenge to take into consideration when creating an authentication mechanism for this user group is the fact that they are often easy to take advantage of and are targeted by malicious people. In residential homes such as these, it is sometimes the case that staff may be defrauding residents. When designing an authentication mechanism, security should be of the utmost importance. This also means security against any trusted member of staff attempting to take advantage of any residents on the premises. An intrusion detection system should be implemented to make this less likely. As previously mentioned, machine learning could be used to detect any deviations in a senior's interactions with the ATM. Depending on the level that the interaction deviates from what is considered normal, it could be classed as an intrusion. It can however be quite challenging creating an intrusion detection system such as this, as it requires training of machine learning algorithms which takes time. It also requires meaningful features for training and classification, of which there are a limited number of in this system.

Making the design appealing would help when it comes to engendering adoption for this user group. However, it is especially challenging to engender adoption for this user group due to elders being so reluctant to try new technologies. The challenge of producing an authentication mechanism for this group arises from the fact that special considerations need to be considered into making the design appealing. As previously mentioned, design plays a significant role in making technologies more approachable. This is because older generation find newer technologies complicated and confusing. The "sympathetic design" framework should be followed to make the design friendly for this group of seniors. This framework involves design decisions such as: the functionality of the design being simple; a physically tangible interface; and the layout being easy to understand.

REFERENCES

[1] Future of an ageing population. (2016). [ebook] GOV.UK, p.6. Available at: https://www.ageing.ox.ac.uk/files/Future_of_Ageing_Report.pdf [Accessed 10 Mar. 2019].

[2] Read, J. and Cassidy, B. (2012). Designing textual password systems for children. In: IDC '12 Proceedings of the 11th International Conference on Interaction Design and Children. New York, NY: ACM, pp. 200-203.

[3] Assal, H., Imran, A. and Chiasson, S. (2016). An Exploration of Graphical Password Authentication for Children. In: International Journal of Child-Computer Interaction.

[4] Helkala, K. (2012). Disabilities and Authentication Methods: Usability and Security. In: Seventh International Conference on Availability, Reliability and Security. IEEE.

[5] Gibson, M., Renaud, K., Conrad, M. and Maple, C. (2009). Musipass: authenticating me softly with "my" song. In: NSPW '09 Proceedings of the 2009 workshop on New security paradigms workshop. ACM, pp.85-100.

[6] Lugovaya, T. (2005). Biometric Human Identification based on ECG. [online] Physionet.org. Available at: https://physionet.org/physiobank/database/ecgiddb/biometric.shtml [Accessed 10 Mar. 2019].

[7] Rebola, C. and Jones, B. (2013). Sympathetic devices: designing technologies for older adults. In: SIGDOC '13 Proceedings of the 31st ACM international conference on Design of communication. ACM, pp.151-156.

[8] Older Computer User. (n.d.). [online] semanticscholar. Available at: https://pdfs.semanticscholar.org/6a80/685fcd202fce96766c79f0d343b76cbaab37.pdf [Accessed 10 Mar. 2019].

[9] Chekina, L., Mimran, D., Rokach, L., Elovici, Y. and Shapira, B. (2012). Detection of Deviations in Mobile Applications Network Behavior. In: Annual Computer Security Applications Conference. arXiv.

[10] Weka.sourceforge.net. (2019). REPTree. [online] Available at: http://weka.sourceforge.net/doc.dev/weka/classifiers/trees/REPTree.html [Accessed 1 Apr. 2019].

[11] Gareth, James; Witten, Daniela; Hastie, Trevor; Tibshirani, Robert (2015). An Introduction to Statistical Learning. New York: Springer. p. 315. ISBN 978-1-4614-7137-0.

[12] Papadopoulos, L., Miley, J., Barnett, T., Barnett, T. and Loeffler, J. (2019). AI Scanner Can Differentiate Between Live Irises and Dead Ones. [online] Interestingengineering.com. Available at: https://interestingengineering.com/new-ai-scanner-can-differentiate-between-live-irises-and-dead-ones [Accessed 10 Apr. 2019].