Behavioural Authentication Using Computer Games

Ahmed Al-Khazzar, Nick Savage
Electronic and Computer Engineering Dept.,
University of Portsmouth
Portsmouth, UK
ahmed.al-khazzar@port.ac.uk, nick.savage@port.ac.uk

Abstract—Biometric mechanisms of authentication are becoming a popular approach to securing computer systems, networks and other critical resources. This paper proposes a behavioural authentication system based on user interaction with computer games. Literature about current physical and behavioural biometric methods is reviewed and game based authentication design and implementation issues are discussed. Some common biometric data analysis measures are introduced and reviewed.

Keywords- Behavioural Authentication; Biometric Authentication; Identification; Access Control.

I. INTRODUCTION

A reliable authentication system is a critical component for many applications that require access control. Biometric mechanisms of authentication are becoming a popular approach to securing computer systems, networks and other critical resources. While there has been a significant surge in the use of biometric systems for user authentication in recent years, they have not been a perfect solution and there are a large number of known attacks against these systems. A few security attacks have been reported in [1-5]. Reference [5] identifies a number of different types of spoofing attacks to biometric systems:

- Coercive Impersonation- in this type of attack the attacker physically forces a genuine user to identify himself to the authentication system or removes the biometric trait (for example finger) to gain access to the resources.
- Replay Attack- is based on re-presentation of a previously recorded biometric trait, such as recording someone voice or taking a picture of a person and presenting it to a face recognition biometric system.
- Impersonation Attack- is based on a change in attacker’s appearance to match a genuine user, for example using makeup to copy somebody’s face.

Although there are a number of counterattacks against spoofing by using liveness detection methods as described in [6] or using a multi-model biometric system [7], these methods add to the complexity and cost of the biometric system and they are not always successful. For example a multi-model voice and face recognition system can be attacked by concurrent presentation of recorded voice together with a picture of user’s face.

Studying possible attacks against current biometric systems reveals a common characteristic of such systems that makes the spoofing attack possible. This common characteristic is the trait physical accessibility. This is where behavioural biometrics takes advantage over physiological biometrics. The behavioural traits of a user are not physically accessible. Examples of behavioural biometrics are keystroke dynamics [8,9], pointing device interaction [10] and game based authentication [5,11,12].

In this paper we propose a behavioural authentication system based on computer games similar to the one that has been created in [11]. Reference [11] performed a feasibility study for an authentication system that authenticates based on user interaction with a three dimensional maze. The results of this study showed that the system had an average accuracy of 88.33% in identifying different users from each other. This paper is an extension to the work that is done in [11] and describes design and implementation of three different games that can be used for authentication purposes. A number of users have been asked to play each game for a specified amount of time. During this period the system collects and audits statistics about the users’ behaviour. This process is to be repeated a few times in a one month period. At the end of the data collection, statistical methods will be used to distinguish between different user behaviours.

II. BACKGROUND

A. Recent Advances in Biometric Authentication

Biometrics refers to the recognition of a legitimate user by using physical or behavioural traits associated with that individual. Any physical or behavioural trait can be used for biometric recognition as long as it has the following characteristics [13]:

- Universality: any human should possess the trait.
- Distinctiveness: all humans should be sufficiently distinctive in terms of the measured trait.
- Permanence: the trait should remain constant throughout a period of time.
- Collectability: the trait should be measurable quantitatively.

A practical biometric authentication system should also have a satisfactory accuracy and speed, good acceptability among users and high security against attacks. Reference [13] reported that biometric systems based on fingerprints [14], face [15] and iris [16] have received the most attention in recent years. Reference [13] also reported the state of the art error rates of four popular biometric traits (TABLE I). Due to
intrinsic variability of biometric traits, it is a challenging task to maintain the performance of the biometric system while ensuring the security demands of an authentication system. Whilst the development of a comprehensive biometric mechanism is crucial as biometric systems grow rapidly into access control systems, developing such a mechanism with guaranteed security demands and recognition performance has remained an unreached objective.

### B. Behavioural Authentication, an Overview

Behavioural authentication is a subset of biometric authentication which uses measurable properties of a person’s actions to identify the person. All behavioural biometric systems work in a similar manner: by analysing the current user actions create a model of individual user behaviour and then use this model to predict the future user behaviour.

Although behavioural biometrics generally introduces less accuracy levels (error rates) than the physical biometrics, they have some advantages over physical methods:

- As discussed in the introduction, behavioural methods are more resistive against spoofing attacks.
- Data gathering process is often unnoticeable by the user.
- They are often less expensive and require no specialized hardware.

Most of the current research in behavioural biometrics concentrates on very low level user behaviour such as keystroke dynamics and mouse movements. Although these traits are accurate, they reveal user behaviour directly related to physical abilities of the human and ignore higher level intentional behaviours, which may describe identity of the person more successfully [17].

### C. Related Work

#### 1) Pointer device authentication

Reference [10] proposed a behavioural biometric technique based on human computer interaction. Their developed system captures data via a pointing device, and uses this data to authenticate an individual. The acquisition module of the system is a web based memory game. An equal error rate of 0.02 was reported.

#### 2) User verification via web interaction

Reference [18] proposed the use of a biometric trait based on behaviour extracted from interaction with a web page. It is proposed to integrate this trait into a conventional login web page to enhance the security of the system. The proposed system is a multi-model authentication system that uses both biometrics and memorable traits. This work suggested that the users are more cooperative in data collection if it is done in game environment than a non game environment. The results of testing the system on a population of 50 users were equal error rates of 6.2%–12.5%.

#### 3) Strategy-based behavioral biometrics

Reference [12] showed that a behavioural biometric signature can be generated based on the strategy used by an individual to play a game. They implemented a software to extract behavioural profiles for each player in the game of poker. The generated behavioural signature is continuously compared with players’ current actions and significant changes in behaviour are reported as security breaches. Yampolskiy reported equal error rates of as low as 7% for the behavioural profiles enhanced with temporal and spatial information [19].

### D. Three Dimensional Authentication

Reference [11] proposed using a three dimensional behavioural authentication system. The project involved implementing a three dimensional maze game that records user interactions as users navigate through the game. The project included testing of the proposed system on a small group of users and analyzing the collected signatures by means of statistical analysis methods. The results of conducting the tests showed an average true rejection rate of 88.33% with an average false acceptance rate of 11.67%. Reference [11] suggested that the developed system has the potential to be introduced as a powerful authentication system for very high security demands. However the authentication system was only tested on 5 users enabling multiple analysis techniques to be assessed. For this reason only a small amount of data were collected to test the method proposed. Another drawback of the work was the unattractiveness of the game and that it occasionally caused headache and dizziness for some users.

In the current paper it is proposed to extend the game authentication method developed by [11]. Three different games has been designed and implemented. Then an average of 50 users have been asked to play the games for four periods of 4 minutes during a one month period. This paper focuses on the design of the games and presents some user feedback about the games.

### III. METHODOLOGY

#### A. Games

Two parameters are considered in games design. First was that the games intended to be easy to play and graphically interesting for users. Failing to meet this requirement may decrease the acceptability of the system among users. To meet this requirement Blender 3D game engine is used to implement the games. Some open games are chosen as a base for two of the games aiming to provide a state of the art game experience to the users.

Second parameter was that the games should provide users with easy decisions in the course of the game. This is against a

<table>
<thead>
<tr>
<th>Biometric Trait</th>
<th>False Rejection Rate</th>
<th>False Acceptance Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>0.1%–2.2%</td>
<td>1%–2.2%</td>
</tr>
<tr>
<td>Face</td>
<td>0.8%–1.6%</td>
<td>0.1%</td>
</tr>
<tr>
<td>Voice</td>
<td>5%–10%</td>
<td>2%–5%</td>
</tr>
<tr>
<td>Iris</td>
<td>1.1%–1.4%</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

---

TABLE I. FALSE REJECT AND ACCEPT RATES WITH STATE-OF-THE-ART FINGERPRINT, FACE, VOICE AND IRIS VERIFICATION SYSTEMS [13]
strategy based game which needs complicated decisions to be made inside the game. The difference is between two approaches: pointless game and target based game. In a target based game the users should follow a logical method to finish the game and win or loss based on the quality of their decisions. Examples are chess, poker and other strategy based games. In this type of games since the decisions are logical, behaviour of the user can be predicted based on the current situation in the game. However the degree of predictability differs among different strategy based games. For example a chess game behaviour is more predictable than a poker game. Reference [17] stated this difference and created a behavioural biometric using a poker game [12]. However he reported that a spoofing attack is possible against his developed system by secretly and automatically monitor the target user during the play in an online casino.

In this paper the idea is brought further and the games designed to be pointless. The authors believe that the pointless nature of the game can reveal more accurately the behavioural difference of a human and increase the resistance of the system against spoofing attacks.

1) Maze game

The maze game consists of a large series of corridors that connected together and created repeated random shapes. The user will not have any idea during the game of the start and the end point of the maze. The user controls the movement of the game character; a squirrel (Fig. 1(a)). The character has the abilities to walk forward and backward, turn right and left, jump, double jump, rotate its tale and run. The user has complete control over the mentioned activates.

2) Car game

The car game uses the same map as the maze game, but this time instead of corridors the map is used to create roads. Again the game environment is large enough for the user to navigate through. A third person camera view is used from the back of the car. The user can drive the car through the provided controls (accelerate, brake, steer left, steer right) (Fig. 1(b)).

3) Subracer game

The subracer game is a submarine game that can be played in an underwater environment. The submarine can be driven in different directions as well as up and down in a large circular path. This game provides more controlling options to the users than the first two games (Fig. 1(c)). Subracer is slightly breaking the rule of pointless game as there are some collectable boxes around the game environment. However the users are not aware of existence of the boxes until they play the game. These objects are included in to the game to compare with two first games which are completely aimless. The environment also includes some rocks, mines, plants and other different objects.

Fig. 1. Snapshot of the games: (a) maze game. (b) car game. (c) subracer game.
B. Data Acquisition

A unique data acquisition module is written for all three games. This module collects user behaviour throughout the game. This behaviour includes the keys pressed, exact time of key press and the location of game character (animal, car or submarine) at the time of key press.

50 users (engineering students) have been asked to play all the games one time a week for a period of one month. Each time the games allow the user to play for a period of 4 minutes. At the end of data collection period it is expected to have a minimum of 200 samples of data for each game.

C. Users’ Feedback

Some users stated that their emotions in different situations may change their behaviour. This could affect the false rejection rates adversely. However this could also make the system more secure against Coercive Impersonation attack. When an attacker try to force a genuine user to authenticate, the change in user’s emotions may affect his behaviour significantly and he may not be able to log in to the system. For other situations when the user is naturally in a different emotional mood, a longer registration period can help to improve false rejection rates.

Many users complained about the time consuming process of the authentication. They argued that this could be a very tedious and boring process. Some suggested that defining goals in the games could improve them. This was the case for a few who found subracer game more interesting for not being totally pointless.

Some users liked the non-requirement for memorable or physical tokens, and other users found the environments user friendly. A few users noted the privacy concerns of such systems. They argued that these systems would not be acceptable until the attitude of the society as a whole towards privacy changes.

IV. DATA ANALYSIS

When a new biometric data sample is presented to an authentication system, the system should be able to measure how similar the new sample is to template data, gathered at registration stage [19]. A similarity measure should consider the statistical characteristics of the data distribution assuming that enough data is available to determine these properties [20]. A number of similarity measures have been used in behavioural biometrics. Some are introduced in this section.

A. Maximum and Minimum Similarity Measure

Reference [11] used a simple algorithm to measure the similarity of a given vector \( x = (x_1, x_2, x_3, ..., x_N) \) to a group of vectors with the maximum vector \( M = (M_1, M_2, M_3, ..., M_N) \) and the minimum vector \( m = (m_1, m_2, m_3, ..., m_N) \). The similarity score of vector \( x \) to the group of vectors is:

\[
S = \sum_{i=1}^{N} 1, \quad m_i < x_i < M_i.
\]

The similarity score \( S \) has a maximum value of \( N \). Hence the distance of the vector \( x \) to the group of vectors can be calculated as:

\[
D = N - S.
\]

B. Distance of Two Samples Using Degree of Disorder of an Array Method

Reference [8] used the concept of degree of disorder of an array to calculate the distance between two samples. Given an array \( V \) of \( N \) elements, the degree of disorder of \( V \) with respect to a second array \( V' \) can be calculated as the sum of the distances between the position of each element in \( V \), with the same element in \( V' \) [8]. The arrays elements should be identical, and they should differ only in position of the elements. As an example, assume that array \( A = \{R, T, Y, U, I\} \) and \( B = \{I, R, T, U, Y\} \). The degree of disorder of \( A \) and \( B \) is: \( (1 + 1 + 2 + 0 + 4) = 6 \) (Fig. 2).

C. Euclidean Distance

Euclidean distance is one of the most popular distance functions. Euclidean distance can be calculated as the sum of the squared distances between the elements of the \( n \)-dimensional vectors \((x, y)\) [12]:

\[
d_E = \sqrt{\sum_{i=1}^{N} (x_i - y_i)^2}
\]

D. Mahalanobis Distance

The Mahalanobis distance of a multivariate vector \( x = (x_1, x_2, x_3, ..., x_N) \) from a group of values with mean \( \mu = (\mu_1, \mu_2, \mu_3, ..., \mu_N) \) and covariance matrix \( S \) is defined as [12]:

\[
D_M(x) = \sqrt{(x - \mu)^T S^{-1} (x - \mu)}
\]

Mahalanobis distance is widely used in classification techniques and is closely related to Hotelling’s T-square distribution used for multivariate statistical testing and other analysis methods [21].

E. Manhattan Distance

The Manhattan distance between two points is defined in a Euclidean space with fixed Cartesian coordinate system, and is the sum of lengths of the projections of the line segment between the points on to the coordinate axes. It can be considered as the absolute differences of the elements of two vectors [12].

\[
D = |x_1 - y_1| + |x_2 - y_2| + ... + |x_N - y_N|
\]
V. CONCLUSION

In this paper current physical and behavioural authentication methods were reviewed. Advantages of behavioural methods in comparison to physical methods were argued. A game based behavioural authentication system was proposed. Pointless and target base types of games were discussed and it has been shown that pointless games have more capacity to collect behavioural traits of users and can be more secure than strategy based games. Finally some common similarity measures that can be used in a behavioural authentication system have been reviewed.

REFERENCES