Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

User Identification using Games

Oliver Buckley and Duncan Hodges

Centre for Cyber Security and Information Systems,
Cranfield University, Defence Academy of the United Kingdom,
Shrivenham, Swindon, SN6 8LA, UK
o.buckley@cranfield.ac.uk
d.hodges@cranfield.ac.uk

Abstract. There is a significant shift towards a digital identity and yet the most common means of user authentication, username and password pairs, is an imperfect system. In this paper we present the notion of using videogames, specifically Tetris, to supplement traditional authentication methods and provide an additional layer of identity validation. Two experiments were undertaken that required participants to play a modified version of Tetris; the first experiment with a randomly ordered set of pieces and the second with the pieces appearing in a fixed order. The results showed that even simple games like Tetris demonstrate significant complexity in the available game states and that while some users displayed repeatable strategic behaviour, others were effectively random in their behaviours exhibiting no discernible strategy or repeatable behaviour. However, some pieces and gameboard scenarios encouraged users to exhibit behaviours that are more unique than others.

1 Introduction

Society has an increasing reliance on cyberspace as progressively more of our lives transition to the digital world, whether it be interacting with friends right through to the delivery of core government services. As a result of this shift the notion of our digital identity is becoming increasingly important. Traditionally, our digital identity has been secured with the use of a username and password pair. However, this approach to identification places the cognitive load onto the individual as they are required to remember a wide-range of security credentials. In addition to this, users will rarely follow the guidelines for generating a strong passwords [1]. Security credentials are easily compromised through a wide variety of attack vectors, for example, phishing [2], hacking [3] or the credentials simply being written down and lost [4].

In this paper, we hypothesise that videogames can be used as a means of user validation, that relies on how an individual responds to scenarios within the game, rather than the security credentials that they remember. We posit that videogames provide an opportunity for a user to demonstrate a rich, multi-dimensional and unique behaviour which can be used to validate an individual is who they claim to be. In this work we specifically focus on the use of Tetris [5],

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

a popular single-screen puzzle game that presents players with an empty gameboard (a grid of 20-by-10). A sequence of 'tetrominoes' is generated and fall into the gameboard, players can rotate and move these shapes, with the aim of filling horizontal lines within the gameboard. Once a line is complete it will be removed from the gameboard and the rest of the board shuffles downwards. A player loses the game when the maximum height of the shapes exceeds the height of the gameboard.

The remainder of this paper is structured as follows: Section 2 provides a review of the related work covering alternative authentication and identification techniques. Section 3 details the methodology used to conduct the investigation. Section 4 provides an analysis of the collected data and the results of the study. Finally, in Section 5 we conclude by providing a reflection on our analysis and a discussion of further work in this area.

2 Background

Traditional approaches to user authentication, which rely on username and password pairs, are an imperfect system. The emphasis is placed on the individual to create a password that is both meaningful and memorable to them but that is also not easily guessed by a third-party. The strength of a password can be linked to the security expertise of the individual, with those with significant expertise typically choosing more secure passwords [6]. However, the choice of a password that is memorable and difficult to infer is hard to achieve, with a large percentage of passwords directly relating to personal characteristics and the reuse of passwords highly prevalent [7]. Additionally, it is becoming increasingly common for individuals to participate in risky security practices such as password sharing [8]. Once a user has successfully passed the authentication process there are typically no further challenges to their identity, which leads to the question of just how much confidence we can have that an individual is who their credentials claim them to be.

A significant amount of work has been undertaken investigating the use of graphical passwords [9] as an alternative means of authentication. Broadly speaking graphical passwords can be broken down into two broad groups: recognition based techniques and recall based techniques [10, 11]. Recognition based techniques rely on a user recognising and selecting a set of images that they selected during the enrolment phase. Recall based techniques require a user to recall something that they had created at the enrolment phase, for example, a set of points on a particular image. However, users will typically choose similar spots on an image when creating a graphical password, thus creating hotspots around points of interest [12], this increases the guessability of these schemes. An alternative to passwords, graphical or textual, is the use of biometrics, which are measurable characteristics that can be used to describe an individual. Biometrics fall into two categories, physiological and behavioural [13]. Physiological traits are related to characteristics of the body of an individual, for example, fingerprints. Behavioural biometrics relate to the innate traits displayed by in-

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

dividuals, for example, keystroke dynamics. Traditional authentication methods rely on testing something that the individual knows, whereas biometrics place the emphasis on something that the person 'is'. This shift in focus from something known to some intrinsic characteristics, displayed naturally in response to the environment makes biometrics potentially harder to spoof [14, 15].

In this work we present the use of videogames, specifically Tetris, as a behavioural biometric. We propose that individuals will display identifiable behaviours based on the state of the game. This approach will not rely on the individual remembering security credentials but will instead analyse their response to the context provided by the game they are playing.

3 Method

In this paper we focus on the use of Tetris to identify individuals based on the way in which they interact with the game. Tetris was chosen as it is a game that is both simple and intuitive for someone who does not have experience with videogames. However, Tetris also provides a consistent challenge that allows players to continually develop and refine their skills and strategies. Despite the depth of complexity of the demonstrable behaviours, the game board itself has a finite and manageable set of states and there is a limited set of pieces available to the player, as shown in Figure 1.

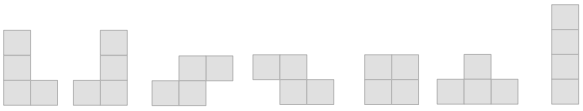


Fig. 1: The pieces available (from left to right: 'L', 'J', 'S', 'Z', 'O', 'T', 'I')

To conduct this study a website was developed and deployed to play a modified version of Tetris, the modifications are required to allow data collection; the aim of the game and way the game is played remain entirely unchanged. During the study there were four key data dimensions that were collected:

- Current board state
- Current piece
- Next piece
- Keystrokes for the current piece

The study comprised of two experiments, the first required participants to simply play a game of Tetris with a random selection of pieces (i.e. there was no predetermined ordering to the shapes). Participants were required to play the game until they 'lost' the game, by the height of the pieces exceeding the height of board, or until they had played for three minutes. The second experiment

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

again required participants to play the game for three minutes, or until they 'lost' the game but in this instance all participants were using a fixed set of pieces. That is to say, all of the participants would have exactly the same set of pieces, appearing in the same order, where the order was: 'S', 'S', 'T', 'Z', 'O', 'J', 'J', 'L', 'S', 'T', 'Z', 'Z', 'O', 'J', 'O', 'I', 'L', 'I', 'I'. This sequence of shapes was randomly generated prior to the start of the second experiment and remained constant throughout, with the sequence beginning again once the player had reached the end.

Recruitment for the survey was carried out using social-media networks as well as making use of the student population at Cranfield University. In total there were 50 unique participants who played 73 games during the first experiments and 75 unique participants who played 117 games during the second experiment.

4 Analysis and results

It was hypothesised that there were two top-level approaches to playing Tetris: one approach only considers solving shorter-term problems whilst the other is based on longer-term problems. In the short-term approach the user only considers the current piece and the profile of the top of the current board state, however in the longer-term approach the user also considers the next piece in addition to any 'holes' that are trapped in the current board state. In the research presented in this paper the focus is on the short-term approach, in essence, the state of the game (i.e. the stimulus to the user) is entirely characterised by the board state and the current piece.

Initially the board state is characterised as the gradient of the profile of the pieces in the board, an example is shown in Figure 2 along with the array defining this board state.

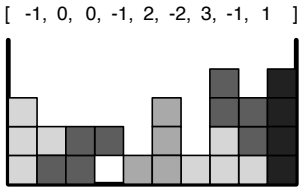
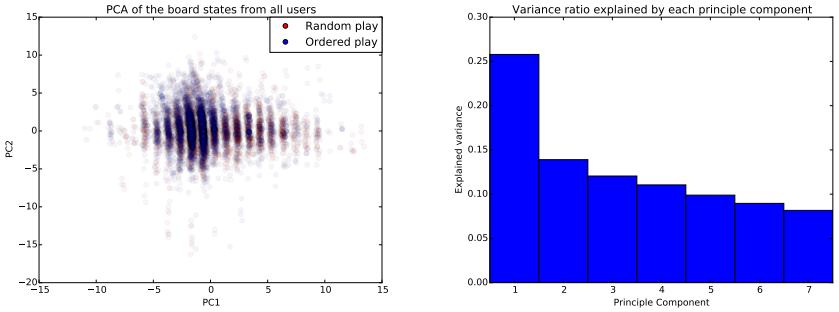


Fig. 2: An example of the codification of the board state

An initial analysis explores the dimensionality associated with these profiles. Principle Components Analysis (PCA) was used to explore the set of board states that appeared in every game, that was played as part of both the experiments involving random and ordered play. The plot of the first two components is shown in Figure 3a.

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1



(a) The PCA of the board states for the two experiments

(b) The variances of the various principle components

Fig. 3: A principle components analysis of the board states in Tetris.

As can be seen there is some discrete structure in the first component, which can be expected given the discrete nature of the elements of the state vector. As expected the states associated with random play demonstrate a greater spread of states, the unconstrained nature of the piece order enabling a broader set of profiles.

The variance described by each of the first 7 components is shown in Figure 3b. As is consistent with Figure 3a the first component describes around 25% of the variance, however there is also significant variance contained in the other components. This implies that dimensionality reduction techniques will loose a significant amount of information within the state vector and the board state should be used as complete vector as the information content of the higher dimensions is significant.

The previous analysis considered each 'turn' in the game as an individual discrete state, given that a game is a time-ordered flow of these game states it is intuitive to plot the users 'journey' through these states as the game is played. Intuitively this can be represented as a directed graph, with the board states represented by the nodes and the type of the current piece representing the edges.

One game from each of the participants was randomly selected and the directed graph of the board states associated with the experiment with ordered play is shown in Figure 4. In this graph the width of the transitions is proportional to the number of times an edge is used in play, with all edges that are used by one or more different users coloured red.

As can be seen the graph in Figure 4 there are a number of common approaches to the early game phase — this is not surprising given the ordered nature of the pieces and the initial empty board state. There are two main approaches most users took for the first three or four pieces at which point the graph begins to diverge quickly. Once the graph has begun to diverge there are only three times a users' game reaches the same board state as that of another

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

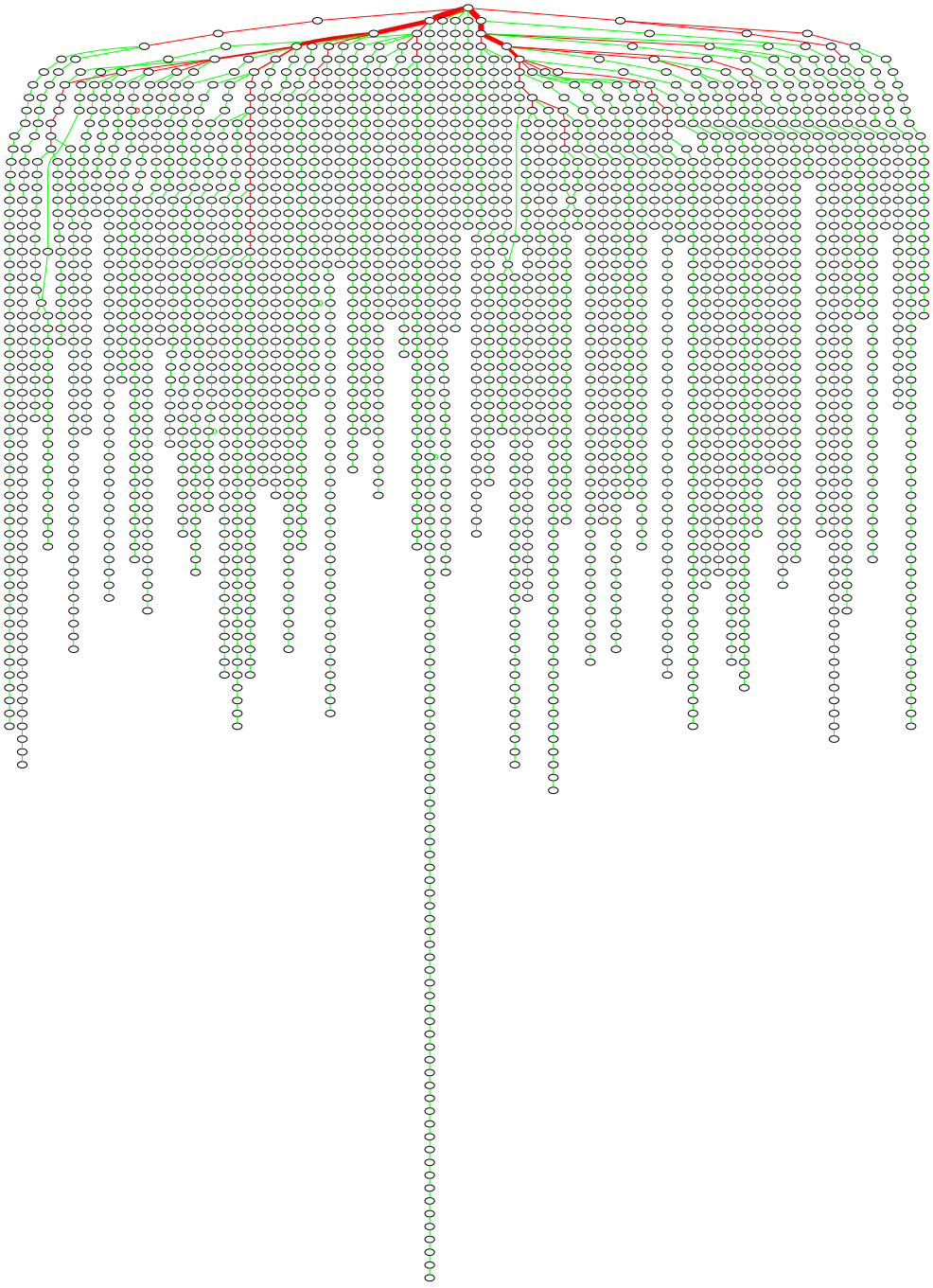


Fig. 4: The directed graph of the board states for one random game per user from the experiment in ordered play

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

user, at which point the games immediately diverge again (i.e. the indegree of the node is greater than 1 and the indegree and outdegree are identical). Two examples of this are shown in Figure 5 which shows a cropped and zoomed area of Figure 4.

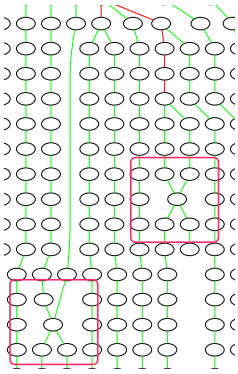


Fig. 5: Two examples of different users transitioning through the same game state.

This implies that even in the ordered play experiment within a few pieces the games become relatively unique, the same graph analysis is shown in Figure 6 for the random play experiment. Due to the more unconstrained nature of the game it is clearer that the board state diverges quicker than the ordered play, also of note is that the number of times board states are revisited is also small.

In addition to the uniqueness between users it is also important to assess the repeatability of users' play. In order to examine the repeatability of users behaviour the graphs associated with users who played multiple games were extracted from the ordered play experiment.

The first interesting characteristic is that it is apparent that a number of users exhibit little repeatable behaviour, with every game effectively taking a unique path, examples are shown in Figure 7a and Figure 7b. The games are also relatively short with few pieces placed during the three minute length of the game. This can be contrasted with other users such as those in Figure 7c, Figure 7d and Figure 7e which demonstrate significantly more repeatable strategy for much longer. It is also notable the number of pieces placed in the same time-frame is significantly higher.

This difference in overall strategy is maybe not surprising as, although Tetris is a popular and common game, there will be differing degrees of experience with the game. This implies the users whose games are shown in Figure 7a and 7b have not yet had enough experience in order to develop strategies for play. This also implies that an individual's strategies will evolve over time — in the same way that over time other behavioural biometrics (such as keystroke dynamics) will evolve, although the rate of this change is likely to decrease as the user becomes

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

Fig. 6: The directed graph of the board states for one random game per user from the experiment in random play

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

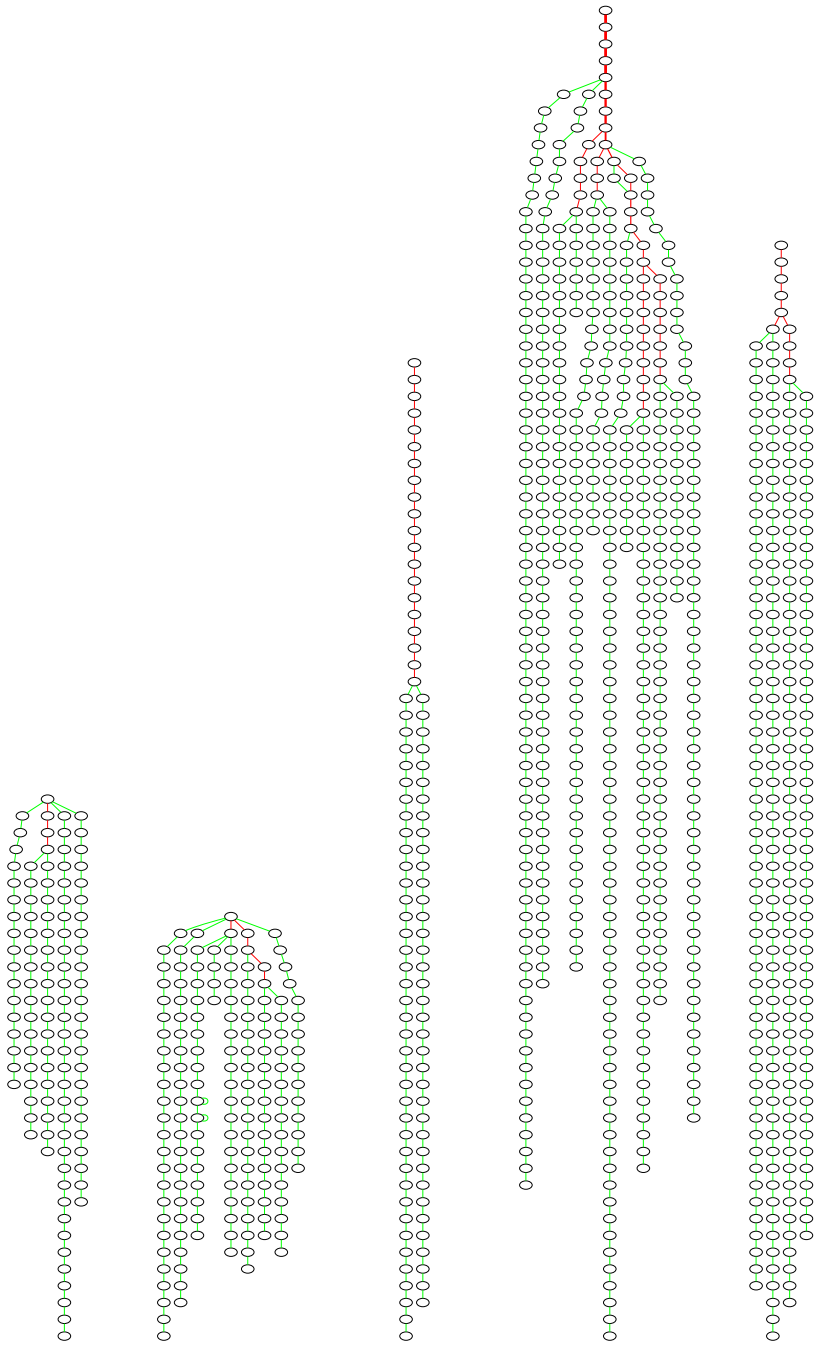


Fig. 7: Examples of individual users games.

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

more experienced and their strategies stabilise. In solo games these strategies are likely to be more stable than in adversarial games where a users' strategy will evolve with respect to an opponent's.

Moving to a 'piece-centric' view it is possible to explore whether certain pieces result in more unique behaviours. In order to explore this question the board state at a given time is less important, what is more important is the change in the board state caused by a given piece. In this study the board state transition caused by a given piece is simply the change in the height of the board, as demonstrated in the two examples shown in Figure 8.

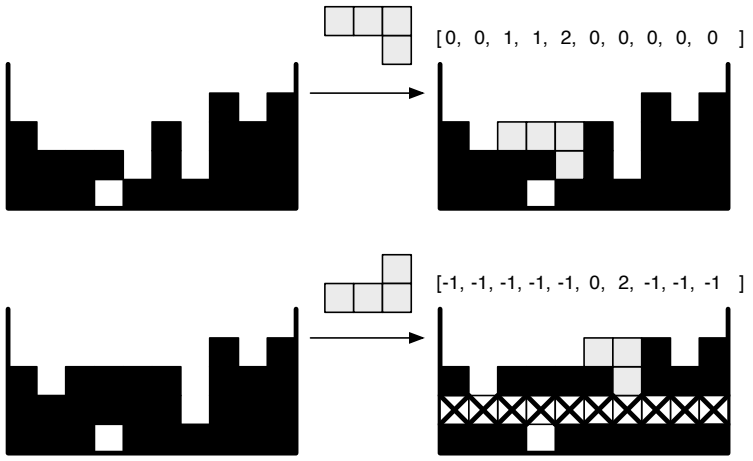


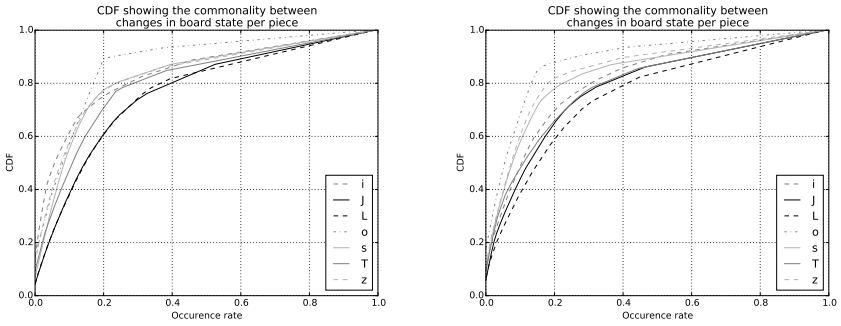
Fig. 8: An example of the codification of the board state changes

These board state changes were assessed for all participants and for all pieces, before calculating the number of times each board state change was seen for each piece. This highlighted very common board state changes which were seen per piece, the Cumulative Distribution Function (CDF) of these counts are shown in Figure 9. As can be seen in both the graphs in Figure 9, the commonality between the board state changes associated with the 'O' piece[1] is much higher — this indicates that the 'O' piece is less useful for discriminating between users. In this case the piece commonality will also be affected by rotational symmetry being greater than the other pieces.

Also of note in Figure 9a is the similarity between the curves associated with pieces that are mirror images of each other (e.g. 'J'/'L' and 'S'/'Z'). The 'J'/'L' pair also represent pieces that have a wider diversity of use than other pieces, this implies that using these pieces to discriminate between users will potentially provide more discriminatory power than other pieces.

[1] The 2×2 square piece

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1



(a) Random play (b) Ordered play

Fig. 9: The commonality of board changes associated with different shapes.

Considering the ordered play, where the order of pieces is predetermined and all players receive the same pieces in the same order, the same analysis results in the plot shown in Figure 9b. This plot shares several characteristics with that from random play, most notably that the 'O' piece has the greatest commonality in use. However, a number of the profiles for pieces differ from that of random play.

This indicates that by controlling the order of pieces it is possible to control the discriminatory power of individual pieces, in this example the 'J' piece has become less discriminatory whilst the 'Z' piece has become more discriminatory. The ability to control the discriminatory power of individual pieces by changing the order in which they appear is key to creating a system that can leverage gaming to aid user identification.

5 Conclusion and Future Work

In this paper we have investigated the use of videogames, specifically Tetris, and the associated strategies as a means of user validation. The findings have shown that some individuals exhibit repeatable strategies, although conversely there are those who appear to exhibit no notable, repeatable strategies. We posit that the degree of strategy that a player displays is linked to their experience with Tetris and is something that will be investigated in future work.

The other key finding from this work is that within Tetris there are certain states of the game board that are more divisive than others when trying to validate the identity of individuals. Similarly, some of the pieces are more useful when trying to discriminate between users, for example, it was discovered that the 'O' piece (as seen in Figure 1) is less useful for determining individuals. This suggests that it will be possible to manufacture scenarios that allows users to exhibit more unique behaviours. Further experimentation will allow this idea to explored in more depth, and will help to determine those board states and pieces that are better suited to discriminating between individuals.

Buckley O., Hodges D. (2016) User Identification Using Games.
In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016.
Lecture Notes in Computer Science, vol 9750. Springer, Cham
DOI: 10.1007/978-3-319-39381-0_1

References

1. Edward F Gehringer. Choosing passwords: Security and human factors. In *Technology and Society, 2002.(ISTAS'02). 2002 International Symposium on*, pages 369–373. IEEE, 2002.
2. TechRadar. Hackers using advanced phishing attack to steal Google passwords. http://www.techradar.com/news/internet/web/hackers-using-advanced-phishing-attack-to-steal-google-passwords-1248188, 2014. [Online; accessed 21-January-2016].
3. Welivesecurity. Secure password: CyberVor hoard of 1.2 billion details 'used in attack'. http://www.welivesecurity.com/2014/09/02/secure-password/, 2014. [Online; accessed 21-January-2016].
4. Naked Security. Prince William photos accidentially reveal RAF password. https://nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password/, 2012. [Online; accessed 21-January-2016].
5. Tetris. Tetris. http://tetris.com/about-tetris/, 2016. [Online; accessed 02-February-2016].
6. James Dodson, Duncan Hodges, Monica Witty, and Sadie Creese. Does personality and security expertise predict password strength? *Selected Papers of Internet Research*, 4, 2014.
7. Alan S Brown, Elisabeth Bracken, Sandy Zoccoli, and Douglas King. Generating and remembering passwords. *Applied Cognitive Psychology*, 18:641–651, September 2004.
8. Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges. Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, 18(1):3–7, 2015.
9. Ian Jermyn, Alain J Mayer, Fabian Monrose, Michael K Reiter, Aviel D Rubin, et al. The design and analysis of graphical passwords. In *USENIX Security*, 1999.
10. Xiaoyuan Suo, Ying Zhu, and G Scott Owen. Graphical passwords: A survey. In *Computer security applications conference, 21st annual*, pages 10–pp. IEEE, 2005.
11. Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4):19, 2012.
12. Matthieu Devlin, Jason RC Nurse, Duncan Hodges, Michael Goldsmith, and Sadie Creese. Predicting graphical passwords. In *Human Aspects of Information Security, Privacy, and Trust*, pages 23–35. Springer International Publishing, 2015.
13. K. Delac and M. Grgic. A survey of biometric recognition methods. In *Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium*, pages 184–193. IEEE, 2004.
14. Andrew P. Rebera, Matteo E. Bonfanti, and Silvia Venier. Societal and ethical implications of anti-spoofing technologies in biometrics. *Science and Engineering Ethics*, 20(1):155–169, 2013.
15. Ricardo N. Rodrigues, Lee L. Ling, and Venu Govindaraju. Robustness of multimodal biometric fusion methods against spoof attacks. *Journal of Visual Languages and Computing*, 20:169–179, 2009.

User identification using games

Buckley, Oliver

2016-06-21

Buckley O, Hodges D. (2016) User Identification Using Games. In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2016. Lecture Notes in Computer Science, Volume 9750, Springer, Cham

http://doi.org/10.1007/978-3-319-39381-0_1