Gamifying Authentication

Christien Kroeze*, Martin S Olivier†
Information and Computer Security
Architectures Research Group
Department of Computer Science
University of Pretoria
South Africa
*christien.kroeze@gmail.com †molivier@cs.up.ac.za

***Abstract*—The fields of security and usability often conflict with each other. Security focuses on making systems difficult for attackers to compromise. However, doing this also increases difficulty for the user. Users in security are often seen as an obstacle - they are the weakest point of the system, willing to circumvent security policies in order to access their work faster. A large part of security is authentication: knowing who a user of a system is and denying access to unauthenticated users. Authentication is very often the starting point of user interaction with security systems. Unfortunately, authentication is still most commonly achieved using text-based passwords. This is often the easiest and cheapest system to implement. Most websites and services advise users to select unique, complex and lengthy passwords. These passwords are difficult for users to remember and often lead to irresponsible behaviour such as writing down or reusing passwords. Serious games are games that are designed for a different primary purpose than pure entertainment. This field includes gamification, where non-gaming contexts are enhanced by using principles from gaming. Examples include experience points, achievements, progress indicators and leader boards. Gamification uses these tools to persuade users to change their behaviour. If gamification can be applied to security, it may aid in convincing users to act more securely. This paper discusses the possibilities of applying gamification to authentication as a new approach to usability and security.**

***Index Terms*—Security, Authentication, Human Computer Interaction, Usability, Serious Games, Gamification, Persuasive Technology**

I. Introduction

Work has focused on merging the fields of usability and security [1], [2], [3], [4], [5], [6]. However, these fields still contradict each other. It is difficult for security experts to understand users, and for users to understand security policies. This results in users being treated as the weakest link, and inadequate technologies exist to unite the two fields. Users and security most often clash when it comes to authentication. This is the first point where users must obey security policies in order to gain access to the system.

Gamification, serious games, and persuasive technology are recent fields that apply game-like principles to other problems. They have been largely successful in other fields, encouraging users to complete profile information or do more exercise or even save a life [7]. These new fields could be applied to authentication and help to bridge the divide between usability and security.

This paper discusses the possibilities of using gamification to improve user's behaviour regarding security, by focusing on authentication and text-based passwords. Section II provides background information on usability and security, serious games and persuasive technology. Section III provides a new theoretical base for developing authentication games and suggests one such implementation. Section IV concludes the paper.

II. Background

Section II-A investigates previous work in usability and security. Sections II-B and II-C describe the fields of serious games and persuasive technologies and how they have and may be used in future to improve usability in user authentication.

A. Usable Security

Computer security protects valuable computer resources including hardware, software and data. Computer security aims to ensure that resources are only accessed or modified by authorised people and that resources are available to these people at appropriate times. Therefore, it is extremely important to the field of computer security to maintain resources, but this means more effort on the part of the users who need to identify themselves to the system. In security, authentication allows a system to identify legitimate users, protecting the system from attackers.

Users are seen as the "weakest link" by the security experts [8]. They are the point at which security policies must be followed to ensure the system's security and where human error enters the picture. The best security mechanisms are useless if a user has a weak password. Also, it is often hard for experts to understand the difficulty that average users have when using most security mechanisms. In one study, the experts could configure a system in 5 minutes, while the users took an average of 140 minutes [5]. Therefore, security experts may favour security over usability, choosing to protect the system's resources at the cost of the user's experience.

In contrast, usability is a field that focuses on ensuring that interactive systems are easy to learn, effective to use and enjoyable from the user's perspective [9]. Its design intends to make a system easy to use. It considers the *safety* of a system in terms of how easy it is for the user to make irreversible mistakes. This is a common area between security

and usability, since it ensures the integrity of the system's resources. However, the main focus of usability is still on improving the user's experience.

Some of the major problems in uniting usability and security were described in [3]. For instance, security is seen as a secondary goal. Users want to do their job, and are willing to circumvent security measures in order to accomplish their primary goals faster. Other problems involve lack of feedback - users only see the result of their actions in terms of their own work and how they are personally affected by security policies. They may not be aware of what is happening behind the scenes and what weaknesses they may expose to an attacker. Moreover, users lack an accurate mental model of security. In one study, an employee suggested using his wife's maiden name as his password, believing it unlikely that an attacker could obtain his personal information and deduce his wife's maiden name [6]. Security often operates on a "need-to-know" basis, assuming that if users know more about a security mechanism it will be more vulnerable [10]. This kind of thinking leads to uninformed users. Users are ignorant of the possible tactics and resources employed by malicious attackers. Furthermore, users do not understand the significance of their own data if placed in the wrong hands. They do not believe that an attacker could do much harm should their account be compromised [11].

Text-based passwords are used most often as an authentication mechanism, since they are easy and cheap to implement. Users authenticate to numerous systems leading to a large amount of different text passwords that they need to remember. While these passwords were traditionally limited to use in the workplace, now more than ever users are generating passwords for personal use, without the guidance of an expert [2]. Guidelines given to users on password creation often confuse the matter more. They suggest that passwords should be memorable, but not easy to guess; they should be as long as possible, but should never be reused; they should contain as many special characters as possible, but still be meaningful to the user. Randomly generated passwords that are assigned to users are the most secure, but also the hardest to remember [4]. Users are frustrated by the endless array of passwords that they need to generate and remember. This leads to security vulnerabilities and the need for more user-friendly password authentication.

B. Serious Games

According to [12] the total spend on the digital games industry in 2010 was $25.1 billion. The industry today is also diverse, indicating that most people enjoy playing games regularly. This industry is not only focused on a select group of "hardcore" gamers. In 2011 72% of American households reported playing computer and/or video games. The average gamer age was 37; 29% of gamers were over the age of 50; and 42% were female. Furthermore, 70% of high-level executives reported taking daily casual gaming breaks in order to decrease stress and improve productivity in a recent survey [13]. Most people play some sort of game as part of their daily lives.

Beyond the measurable growth of the digital games industry, games and their effects have been studied closely. The psychological benefits of games include better motivation and less stress. Gaming is less stressful than real work since it is usually assured that the goals of a well designed game are achievable - they have been designed to be - and that even losing is still safe to the player. Games make us feel more productive, even when we are avoiding real work [13].

Games offer better incentives than the real world [14] and are designed to provide feedback to players, motivating them to keep playing. It is therefore much easier for people to know that they are making progress and achieving something in games than it is in reality. Experience points, achievements and cinematic cut-scenes are just some of the ways that players are rewarded for playing a good game. Games give players the feeling of blissful productivity - being deeply immersed in work that produces immediate, obvious results. Players of the online role playing game World of Warcraft (Wow) will complete numerous "raids", at the risk of complete failure (which happens 50% of the time [15]) and an uneven distribution of rewards in the form of treasure. These raids are also repetitive and perhaps even tedious. But players pay subscription to be able to do this repetitive work, because the feedback is instant, making players feel productive [15]. This is an example of an *intrinsic* motivation. Instrinsic motivations drive people by interesting them in the experience of the task at hand, rather than counting on an extrinsic rewards such as more money or a better office. The feeling of doing productive hard work and gaining life experiences (intrinsic rewards) turns out to be much more rewarding to humans than money, fame or being attractive (extrinsic rewards) [16]. Players experience several other emotions when they are immersed in a game including bliss, relief, naches (feeling proud of a student), surprise, fiero (feeling triumph over adversity), curiosity, excitement, wonderment, contentment and amusement. The three emotions that are experienced least in games are: sadness, guilt and embarrassment [17].

The field of serious gaming applies these benefits of game playing to other problems. Serious games are games used for purposes other than entertainment [18], [19]. One of the most popular examples of this is edutainment, or learning games. These are usually games designed to teach math and literacy skills to young children. For example, the Khan Academy evolved from Salman Khan's desire to help his cousins learn math. It is a collection of instructional videos that Khan placed online. The videos correspond to disciplines that students learn. Khan academy uses knowledge maps where different skills flow into other skills. If a student has mastered basic algebra, for instance, he may move onto introduction to calculus [20]. This kind of skill tree is a concept that is present in Role Playing Games (RPGs) such as the Diablo series to guide skill selection when characters level up. Quest to Learn is another example of serious gaming in education. Quest to Learn is a school that applies gaming principles to the 6th to 12th grade level [21]. Other non-education examples of serious games include Chore Wars, an online game that hands out

experience points for doing housework [22]. Another example is Fold-it, a game that crowdsources human skills to solve a medical question. It is the player's goal to find the most stable configuration of a folded protein, guided by the game's scoring system and interface. This is work that is easier for humans to do than computers. With the data from the game, researchers hope to gain more knowledge about how proteins naturally tend to fold, which may help us understand HIV/Aids and cancer better [23].

Within the broader field of serious games lies gamification. Gamification uses game mechanics to enhance other systems. For instance, the website Fitocracy [24] awards players experience points for doing exercise, and suggests quests for players to perform. These include quests such as "Go for a jog... Run 1 mile (1.61 km) in under 12 minutes". Some fitness milestones are recognised by achievements. Adding gamification to a fitness logging website increases the player's determination and rewards their achievements, thereby increasing the persuasive power of the fitness tool.

Bogost [25] discusses the persuasive power that video games have, because they form a procedural rhetoric. Rhetoric is the art of convincing an audience of a point. Verbal rhetoric convinces using speech, for example a story or a debate, and visual rhetoric convinces using images, for example an article on hunger in Africa in National Geographic containing many photos. Procedural rhetoric uses procedures to convince. Procedural rhetoric lets the audience experience the steps of an argument in real time by following a *procedure*, allowing them to come to their own conclusions, hopefully the same as those intended by the author. If a picture is more vivid than a story, and a movie is even more vivid than an image [26], then following a well thought out narrative in the form of a procedure (a game) will be even more vivid and more convincing. Videogames and their built in procedural rhetoric are much more convincing than any other format. The players of a game not only see a convincing image, or read a persuasive article - they live through the experience and gain deep insight into what the game represents. This suggests that a game could be used as a way to persuade users to change their behaviour, even how they choose their passwords.

C. Persuasive Technology

Fogg [27] describes Persuasive Technology as using technology to influence and motivate people. He describes methods for making technology more effective by using seven tools. These tools may be used together or stand alone, but they generally increase the persuasive power of a technology. These seven tools have been applied to authentication, for example in [11], [28], [29], [30]. The tools are:

- *Reduction*: Simplify a complex task in order to convince users to perform it. If a person believes performing the task will be beneficial to them, and there is little work associated with it, there is a better chance of them completing it.
- *Tunnelling*: Put the user on a pre-determined course that guides their actions step-by-step. Tunnelling also keeps users from becoming distracted, and creates a captive audience - they will not easily cancel the process or lose interest.
- *Tailoring*: Providing information that is most relevant to the user will ease the computational load of finding the information themselves.
- *Suggestion*: Offering suggestions at the right moment increases their effectiveness. People may forget about a suggestion if it is not relevant to them at that point. The key to success is creating a decision point at the time when it's appropriate to act.
- *Self-monitoring*: Allow people to monitor themselves in order to change their attitudes and behaviour according to good feedback. Self-monitoring directs people to take action when they are slipping from their intended goal.
- *Surveillance*: When people are being watched, they behave differently than they would have alone. Having someone monitored can increase desired behaviours as long as the surveillance is overt. Covert surveillance focuses on punishment while overt surveillance changes attitudes merely because of the fact that the person is being monitored.
- *Conditioning*: Rewarding good behaviours persuades people to continue performing them.

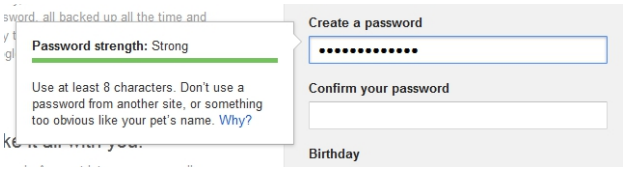

Fig. 1: Google's password creation tool

Usability in security has previously been improved by employing persuasive technology. For instance, some password creation tools show a strength rating next to your chosen password, for instance the Google account creation page as is shown in Figure 1. This uses the *self-monitoring* and *tailoring* persuasive tools. Chiasson [29] used persuasive technology to improve the selection of graphical passwords by encouraging users to avoid frequently chosen areas in the image. Forget et. al. [28] suggested a Persuasive Authentication Framework to guide users in selecting and remembering their passwords. Weirich and Sasse [11] investigate the reasons why users may act insecurely. They suggest that policies are not set up in line with what would persuade users to act securely, and that force will not get users to change their behaviour.

Persuasive technology tools have also been employed in games. Many games use these tools to increase the usability of a game. Tutorial levels employ *simplification*. They guide the player in figuring out the controls and main dynamics of the game. Games also use *tunnelling* tools, by placing the player on a path that is predetermined by the story. *Tailored* and well timed *suggestions* are offered to the player along the way. For instance, if a player keeps missing the target in a first person shooter, the game may suggest "Use the

right mouse button to aim your weapon". Players can *monitor* themselves and take appropriate action to direct their progress. They can check their experience points to see how far they have progressed towards a level-up; mini maps to see their opponent's location; or health points to indicate when they might need to take a health potion. Behaviour in-game may be controlled by *surveillance*. In multiplayer games, players are often watched to ensure that they don't behave improperly by, for instance, quitting before the game ends to improve their score, or flaming other players. *Conditioning* is very often the main motivator in games. Players are rewarded with scores, experience points, achievements and treasure. Serious games and persuasive technologies have the potential to improve authentication, making it more usable for the average user.

III. Designing an Authentication Game

This section discusses theory toward designing games for authentication. An authentication game should satisfy the requirements for effective authentication and usability by applying gaming principles to these fields. Section III-A discusses the limitations of applying gamification to authentication and how it may improve usability, while maintaining the features of all three fields. Section III-B suggests a game for improving the memorability of text-based passwords using visual cues, and finally Section III-C evaluates this based on the theoretical basis that precedes it.

A. Framework for an Authentication Game

In this section, the qualities of a game, authentication and usability are taken into account to form a guiding framework to determine how an authentication game should be structured to lead to a usable authentication mechanism. This process may be aided by persuasive technology tools as discussed in section II-C. Figure 2 is a summary of the relationship between authentication, games and usability, which is discussed further below.

Game Elements: Salen and Zimmerman develop a definition of games as a composite of other definitions [31]. They define a game as "a system in which players engage in artificial conflict, defined by rules, that results in a quantifiable outcome". Other common features of games in other definitions include [31]:

- *Voluntarism* [32], [33], [34]: Games should not be obligatory.
- *Inefficiency* [34]: Games are about following the rules, not about achieving the goals as efficiently as possible.
- *Boundaries* [35], [33]: Games take place in a bounded time and space.
- *Safety* [36]: Games are a safe way to experience reality without endangering yourself.
- *Interaction and contest* [32], [36]: Players interact with each other or with obstacles.
- *Unbalanced outcome* [37], [38], [34], [39], [32]: A player can win or lose.
- *Unprofitable* [35], [33]: A game should not result in any physical profit such as monetary gain.

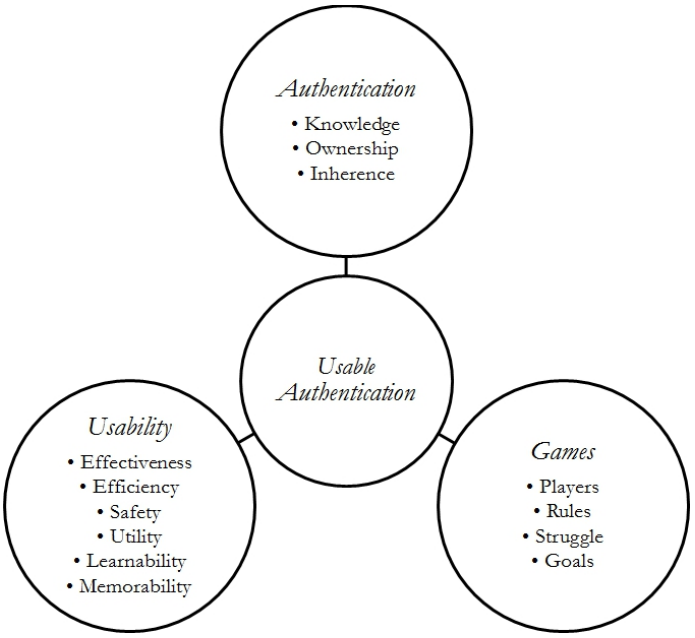

Fig. 2: Summary of the elements of an authentication game

For the purposes of this paper, we will use the Salen and Zimmerman's definition. Therefore in this paper, a game must have:

- *Rules*
- *Players*
- *Struggle* (artificial conflict)
- *Goals* (quantifiable outcomes)

Authentication Qualities: Users are authenticated by any of three qualities [40]:

- *Knowledge*: Something they know. For instance, a text based or graphical password.
- *Ownership*: Something they have. For instance, a security token or bank card.
- *Inherence*: Something they are. For instance, iris or fingerprint scanning.

Usability Goals: An authentication game should not increase the difficulty of authenticating to a system and should strive to reach the usability goals defined in [9]:

- *Effectiveness*: Can users do what they wanted to do with the system?
- *Efficiency*: Can users sustain a high level of productivity while using the system?
- *Safety*: What is the range of errors that are possible using the system and can users recover from them?
- *Utility*: Does the system provide the correct functions?
- *Learnability*: Is it easy to learn how to use the system?
- *Memorability*: Is it easy to remember how to use the system once it has been learnt?

If authentication is done by knowledge, ownership or inherence, how could elements of a digital game be used to test these qualities?

Since games consist of players who are competing to achieve some quantifiable outcome, according to a system of rules, some qualities of a user have to be conveyed in the game in order to authenticate the user. Therefore, some secret should be shared between the player and other elements of the game. In short, an authentication game should test one or more qualities of the user by utilising one or more game elements. Examples of game elements that may be shared include: other players, rules, storylines, goals, outcomes, obstacles, items, graphics, controllers or input devices, control mappings to keys, tactics commonly used and style of play or reactions to events. This is list is not exhaustive - any element in a digital game may be used for authentication.

Perhaps the player shares a secret with the game (something the player knows). For instance, only the correct player may know what the rules of the game are. If only legitimate users know the rules of the game, and if these rules are different for each player, only the correct player will be able to complete the game. Another possibility is if some physical object can be the key to a puzzle in the game (something the user has). Only the correct player owns the object, and therefore only that player can solve the puzzle and therefore be authenticated. Alternatively, a physical object can be an input device used to play the game. A Rubik's cube could be arranged in some pattern that the user understands - a two-factor authentication using the cube (ownership) and the configuration (knowledge), similar to a bank card and pin code. A game could also reveal some pattern of player behaviour (something the player is). For example, the game could detect certain tendencies in the way the game is played. Minesweeper is a good example. Some players will be more cautious than others when flagging mines, some players may tend to start the game in the corners, and some players may tend to move between discovered clusters, while others will tend to stay in one cluster.

However, only some game elements may be combined with some authentication qualities. For instance, it would be difficult to use the game's narrative to test ownership since a story does not exist in physical space. Similarly, a game's control devices are not inherent to a certain person - it is not unique to every player and can not be used to test inherence. However, some game elements could be used to test various authentication qualities. Players could have a unique narrative, that reveals patterns of behaviour when they are choosing storyline options, or they could be the only person who knows their character's history in the game. Therefore, the story's narrative may test inherence, or knowledge, or both. Figure 3 shows how these game elements and authentication qualities are related.

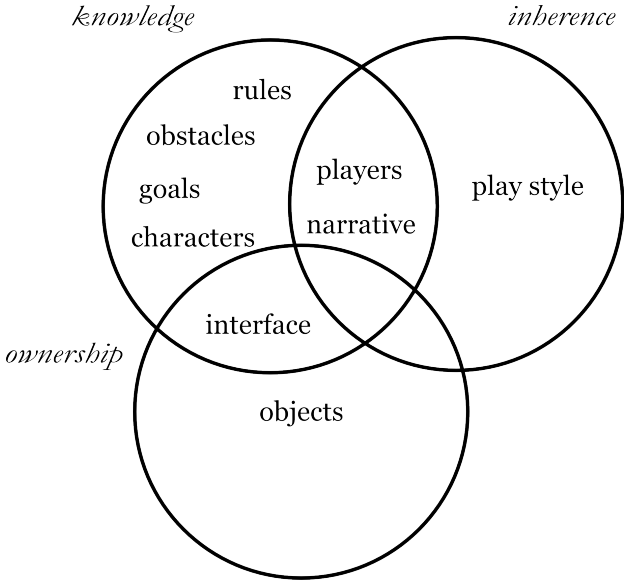

Fig. 3: The relationship between games and authentication

B. A Proposed Solution: Memorability Game

Graphical password schemes have been suggested to improve the memorability of passwords as opposed to text-based username and password combinations [41], [42], [29]. Psychological studies have suggested that humans can remember graphical passwords more easily than text-based passwords [43]. This characteristic of images can be used to encourage users to remember complex passwords. Furthermore, Forget suggests Password Rehearsal Games to help users remember their passwords by rehearsing them a few times before they are used [44]. For instance, *Mix-up* shows users a jumbled version of their password, and the object of the game is to reorganise the letters to form their chosen password. An authentication game can use this kind of memory aid to encourage players to remember their passwords and also create more complex passwords.

In the game *Pokemon*, players catch and train creatures called by the same name[1]. They battle these in order to gain points. With enough points the *Pokemon* evolve into better versions of the original. For instance, the *Pokemon* called *Charmander* evolves into *Charmeleon* and then finally into *Charizard* as seen in Figure 4. The incentive for the player to keep playing is to evolve all their *Pokemon* and catch as many as possible. The game's catchphrase is "Gotta catch 'em all!". There are currently 646 different *Pokemon* in the *Pokedex*, a list of all the *Pokemon* in the *Pokemon* universe[2]. These include strange names such as Marowak, Kangaskhan and Snorlax. However, players can remember all these names and their matching Pokemon image.

Considering the massive amount of names that most *Pokemon* players will learn during the course of the game, an authentication game that is derived from it could help users remember similar semi-random names. In this game, the player chooses a password mascot from a collection of creatures. This mascot is a small animal that will be given a name. That name is the password. The password will be an eight character long computer generated name. This algorithm would be similar to programs such as *pwgen*[3] which generate pronounceable

[1] http://www.pokemon.com/us/pokemon-video-games/
[2] http://www.pokemon.com/us/pokedex/
[3] http://pwgen.sourceforge.net/

(a) Level 1: Charmander (b) Level 2: Charmeleon (c) Level 3: Charizard

Fig. 4: Example of *Pokemon* evolution using *Charmeleon*

random passwords. These passwords are extremely robust against dictionary attacks. Examples of generated passwords from *pwgen* include words such as noobaida, yieheehe and oomongai. Words like these can be slightly altered to make them sound like names for the mascots. After a certain amount of successful login attempts, the mascot evolves. When the mascot evolves, it receives a new, longer name as a password and a new appearance. The player's reward for consistently using and remembering the mascot's name is an upgrade to their mascot. The mascot's appearance can be published online to the user's peers on a social networking site, or a workplace could have leaderboards for the "most evolved" password. This solution can be combined with other existing solutions, including password managers such as LastPass[4] in order to reduce the number of passwords that need to be remembered.

C. Evaluation

The suggested solution is a *knowledge* based authentication mechanism, meant to improve the quality and memorability of text passwords. It uses all the game elements.

- The *players* choose mascots and enter passwords to progress in the game.
- The *rules* of the game are that the player's mascot must have a generated name and may only be evolved once a password has been correctly entered multiple times.
- The *goal* of the game is to have a highly developed mascot and to increase its level.
- The artificial *struggle* engaged in exists between different players. A leaderboard provides encouragement to players to improve their scores and creates conflict to achieve the top score. On a higher level, the struggle is to consistently enter the correct password. The struggle should increase in difficulty as the game continues to keep players interested. The increasingly difficult password could provide this kind of engagement.

The proposed game also reaches the usability goals.

- *Effectiveness*: Users can authenticate by entering a password, and it does not add additional difficulty to the process.
- *Efficiency*: The system adds efficiency since users do not need to think up complex passwords of their own.
- *Safety*: Users are not able to choose weak passwords.
- *Utility*: The system provides the ability to authenticate and improve passwords.
- *Learnability*: The system guides the user in choosing passwords and mascots.
- *Memorability*: The system reminds users to enter the mascot's name, and prompts them to level up their passwords.

This game also uses several persuasive technologies discussed in Section II-C. It uses *reduction* by eliminating the process where users need to choose their own, strong passwords. It *tunnels* users by putting them on a course towards increasing their password strength. It *suggests* better passwords to users only once they have mastered their current password. It allows users to *monitor* themselves by associating mascots with levels that indicates their progress and allowing them to compare against other users on the leaderboard. Users are *conditioned* to keep improving their password strength, because they will be rewarded with an evolved mascot and better score.

The generated passwords should be robust against brute force attacks and should not form predictable patterns in their construction. Should a leaderboard be used, it would be important not to reveal those users who have the weakest passwords in case an attacker uses this information to target their usernames for a brute force attack. It should also not reveal enough information to enable an attacker to derive a list of the worst passwords from a list of users and a list of the best username and password combinations. The altered algorithm to produce name-like passwords should also not weaken the randomness of the password generator. Therefore, any additions to the password should be minimally predictable and should not shorten the password.

While this is still a text-based password system, it illustrates the possibilities of using gamification in authentication and how it may be achieved.

IV. Conclusion

Gamification and persuasive technology tactics have a place in improving user behaviour with regards to authenticating. If users can be encouraged to act more securely a culture of security conscious users can be created, improving users' mental model of what constitutes secure behaviours in computer systems. Further work will focus on developing a game that does not rely on text-based passwords as a basis. The suggested game is closer to a memory aid than an authentication game.

Acknowledgement

The support of SAP Research Pretoria towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are solely those of the authors and cannot necessarily be attributed to SAP Research.

References

[1] L. F. Cranor and S. Garfinkel, "Guest Editors' Introduction: Secure or Usable?" *IEEE Security and Privacy*, vol. 2, pp. 16–18, 2004.

[4] http://www.lastpass.com/

[2] D. K. Smetters and R. E. Grinter, "Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications," in *Proceedings of the 2002 Workshop on New Security Paradigms*, ser. NSPW '02. New York, NY, USA: ACM, 2002, pp. 82–89.

[3] A. Whitten and J. Tygar, "Why Johnny Cant Encrypt : A Usability Evaluation of PGP 5.0 University of California," in *8th USENIX Computer Security Composium*, Washington, 1999.

[4] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password Memorability and Security: Empirical Results," *Security Privacy, IEEE*, vol. 2, no. 5, pp. 25–31, 2004.

[5] D. Balfanz, G. Durfee, D. K. Smetters, and R. E. Grinter, "In Search of Usable Security: Five Lessons from the Field," *IEEE Security and Privacy*, vol. 2, no. 5, pp. 19–24, Sep. 2004.

[6] A. Adams and M. A. Sasse, "Users Are Not the Enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[7] S. Deterding, M. Sicart, L. Nacke, K. O'Hara, and D. Dixon, "Gamification: Using Game-Design Elements in Non-Gaming Contexts," *Proceedings of the 2011 Annual Conference Extended Abstracts on Human Factors in Computing Systems*, vol. 66, pp. 2425–2428, 2011.

[8] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the Weakest Link - A Human/Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001.

[9] H. Sharp, Y. Rogers, and J. Preece, *Interaction design: beyond human-computer interaction*. Wiley, 2007.

[10] D. Parker, "Restating the Foundation of Information Security," in *National Computer Security Conference*, vol. 14, 1991, pp. 480–493.

[11] D. Weirich and M. A. Sasse, "Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World," in *Proceedings of the 2001 workshop on New security paradigms*, ser. NSPW '01. New York, NY, USA: ACM, 2001, pp. 137–143.

[12] Entertainment Software Association, "Essential Facts About the Computer and Video Game Industry," Tech. Rep., 2011. [Online]. Available: http://www.theesa.com/facts/pdfs/ESA_EF_2011.pdf

[13] L. Reinecke, "Games at Work: The Recreational Use of Computer Games During Working Hours," *Cyberpsychology and Behavior*, vol. 12, no. 4, pp. 461–465, 2009.

[14] J. McGonigal, *Reality Is Broken: Why Games Make Us Better and How They Can Change the World*. Penguin Press HC, The, 2011, vol. 22.

[15] S. Bardzell, J. Bardzell, T. Pace, and K. Reed, "Blissfully Productive: Grouping and Cooperation in World of Warcraft Instance Runs," in *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*, ser. CSCW '08. New York, NY, USA: ACM, 2008, pp. 357–360.

[16] C. P. Niemiec, R. M. Ryan, and E. L. Deci, "The Path Taken: Consequences of Attaining Intrinsic and Extrinsic Aspirations in Post-College Life," *Journal of Research in Personality*, vol. 43, no. 3, pp. 291–306, 2009.

[17] C. Bateman, "Top Ten Video Game Emotions," 2008. [Online]. Available: http://onlyagame.typepad.com/only_a_game/2008/04/top-ten-videoga.html

[18] T. Susi, M. Johannesson, and P. Backlund, "Serious Games: An Overview," Web at GamesLearningSociety, GLS University of Wisconsin-Madison, Tech. Rep., Feb. 2007.

[19] D. R. Michael and S. Chen, *Serious Games: Games That Educate, Train and Inform*. Thomson Course Technology, 2006.

[20] Khan Academy, "Khan Academy: About," 2012. [Online]. Available: http://www.khanacademy.org/about

[21] Quest to Learn, "Learning Model." [Online]. Available: http://q2l.org/node/13

[22] K. Davis, "Chore Wars," 2007. [Online]. Available: http://www.chorewars.com

[23] University of Washington, "The Science Behind Foldit," 2008. [Online]. Available: http://fold.it/portal/info/science

[24] R. Talens and B. Wang, "Fitocracy," 2012. [Online]. Available: http://www.fitocracy.com/home/

[25] I. Bogost, *Persuasive Games: The Expressive Power of Videogames*. MIT Press, 2007.

[26] C. A. Hill and M. H. Helmers, *The Psychology of Rhetorical Images*. Lawrence Erlbaum, 2004.

[27] B. J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do*, 1st ed. Morgan Kaufmann, Dec. 2002.

[28] A. Forget, S. Chiasson, and R. Biddle, "Persuasion as Education for Computer Security," in *Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2007*, T. Bastiaens and S. Carliner, Eds. Quebec City, Canada: AACE, Oct. 2007, pp. 822–829.

[29] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing Users Towards Better Passwords: Persuasive Cued Click-Points," in *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1*, ser. BCS-HCI '08. Swinton, UK, UK: British Computer Society, 2008, pp. 121–130.

[30] A. Forget, S. Chiasson, and R. Biddle, "Lessons from Brain Age on Persuasion for Computer Security," in *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '09. New York, NY, USA: ACM, 2009, pp. 4435–4440.

[31] K. Salen and E. Zimmerman, *Rules of Play: Game Design Fundamentals*. Cambridge, Massachusetts: The MIT Press, 2004.

[32] E. M. Avedon and B. Sutton-Smith, *The Study of Games*. J. Wiley, 1971.

[33] R. Caillois and M. Barash, *Man, Play, and Games*. University of Illinois Press, 2001.

[34] B. Suits and T. Hurka, *The Grasshopper: Games, Life and Utopia*. Broadview Press, 2005.

[35] J. Huizinga, *Homo Ludens: A Study of the Play-Element in Culture*. London: Routledge and Kegan Paul, 1949.

[36] C. Crawford, *The Art of Computer Game Design: Reflections of a Master Game Designer*. McGraw-Hill Osborne Media, 1984.

[37] D. S. Parlett, *The Oxford Guide to Card Games*. Oxford University Press, 1990.

[38] C. C. Abt, *Serious Games*. University Press of America, 1987.

[39] G. Costikyan, "I Have No Words & I Must Design : Toward a Critical Vocabulary for Games," in *Computer*, F. Mäyrä, Ed., vol. 4, no. 1, Texas State Techincal College. Tampere University Press, 2002, pp. 9–33.

[40] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*. Prentice Hall PTR, 2003.

[41] L. D. Paulson, "Taking a Graphical Approach to the Password," *Computer*, vol. 35, no. 7, p. 19, Jul. 2002.

[42] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceesdings of the 8th USENIX Security Symposium*, Washington, 1999.

[43] R. N. Shepard, "Recognition Memory for Words, Sentences, and Pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, no. 1, pp. 156–163, 1967.

[44] A. Forget, "Helping Users Create and Remember More Secure Text Passwords," in *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 2*, ser. BCS-HCI '08. Swinton, UK, UK: British Computer Society, 2008, pp. 247–248.